Rapportage 'hot issues' i.k.v. Validatie Normenkader door de CVT

1. Inleiding

Het College Kwaliteitstoetsing IIA-NL (CKT) heeft de Commissie Vaktechniek (CVT) verzocht om advies over het normenkader bij kwaliteitstoetsingen van Internal Audit Functies, in de vorm van een validatie van het huidige normenkader[1] of voorstellen tot wijzigingen hiervan.

Daarbij zijn 3 onderzoeksvragen gedefinieerd:

1. Is het huidige normenkader voor de kwaliteitstoetsingen voldoende concreet voor de IIA standaarden en de beroepsuitoefening in Nederland?
   Zo nee, op welke punten dient dat te worden aangepast?
2. Is het huidige gehanteerde normenkader volledig?
   (Welke branchespecifieke wet- en regelgeving en gepubliceerde best practices behoren, naast het verplichte deel van het IPPF, tot het normenkader?; Wat zijn 'must haves' resp. 'nice to haves'?).
3. Met betrekking tot welke onderwerpen ('cases'/'hot issues') kan worden geadviseerd nader onderzoek te doen naar interpretaties van regelgeving en hoe zou die interpretatie moeten luiden?

In april 2013 heeft het CVT een eerste deelrapport aan het bestuur van IIA Nederland gepresenteerd. In dat rapport is antwoord gegeven op de eerste 2 onderzoeksvragen.

Ook zijn in die rapportage in het kader van de 3e onderzoeksvraag 6 issues benoemd:

1. In hoeverre en, zo ja, onder welke voorwaarden is de combinatie van de Internal Audit Functie (IAF) met Risk Management en/of Compliance verantwoordelijkheden en/of andere 2e lijns-activiteiten acceptabel?
2. In hoeverre en, zo ja, onder welke voorwaarden, is het rapporteren van de IAF aan de CFO acceptabel?
3. Kunnen kleine IAF's afwijken van de geaccepteerde normen en wat betekent dat?
4. In welke mate is de aard van de IAF (standaard repeterende audits, veelal sterk financial audit georiënteerd versus maatwerk, meer 'managerial audits') van invloed op de invulling van het normenkader?
5. In welke mate en, zo ja, onder welke voorwaarden, is afwijking van de best practices in 'Bondgenoten in Governance' (relatie IAF en Audit Committee [AC]) v.w.b. de waarborgen voor onafhankelijkheid van de IAF t.o.v. de raad van bestuur acceptabel? (bijvoorbeeld v.w.b. de rol van het AC bij benoeming en ontslag van de Chief Audit Executive (CAE) en in goedkeuring/vaststellen auditplan)
6. Wat zijn de te stellen eisen aan de functionele aansturing van dochterorganisaties door de IAF?

Deze issues zijn in eerste instantie in twee besprekingen met vertegenwoordigers van de CVT, het CKT en het Bestuur van IIA Nederland besproken. Daarbij is afgesproken deze issues nader uit te werken op basis van literatuuronderzoek alsmede een bespreking met een brede vertegenwoordiging vanuit het vakgebied in de vorm van een Round Table.

Deze notitie geeft het resultaat weer van die uitwerking.

Daarbij geldt dat vooral het 1e punt een 'hot issue' bleek, waarover diverse en uiteenlopende meningen bestaan. Dat geldt veel minder voor de andere casuïstiek. Zodoende zijn voor de diverse issues de volgende activiteiten uitgevoerd:

[1] Het normenkader beschrijft de "de algemeen aanvaarde regels van de beroepsuitoefening in Nederland". Overigens heeft de adviesaanvraag alleen betrekking op het normenkader vanuit het IIA.

- Voor het 1e punt (ook wel 'de samenloop van functies' genaamd):
    - een uitvoerige aanvullende literatuurstudie;
    - een Round Table met organisaties waar sprake is van een dergelijke samenloop om te bezien welke overwegingen en compenserende maatregelen zij hebben (29 augustus 2013);
    - een Round Table met een brede vertegenwoordiging van het vakgebied (9 oktober 2013, met deelname van CVT, CKT, opleidingen, diverse branches, IIA en NBA).
- Voor het 3e punt (kleine IAF's) heeft de commissie PAS handvatten opgesteld die door de kleine IAF als referentie voor de minimumeisen t.a.v. de kwaliteitstoets kunnen worden gebruikt ofwel een uitwerking van de minimale voorwaarden waaraan kleine auditfuncties moeten voldoen (o.b.v. de Praktijkgids voor de kleine audit functie).
- Voor alle andere issues is een beperkt literatuuronderzoek uitgevoerd.

1. Issue 1: samengaan internal audit en second line of defense functies zoals risk management en/of compliance

In hoeverre en, zo ja, onder welke voorwaarden is de combinatie van de Internal Audit Functie (IAF) met Risk Management (RM) en/of Compliance verantwoordelijkheden en/of andere 2e lijns-activiteiten acceptabel?

Conclusie issue 1:
Vanuit een auditperspectief is samenloop van de IAF en GRC-functies niet de meest gewenste oplossing, vanuit het oogpunt van onafhankelijkheid en het 'Three Lines of Defense' model.
Er kunnen zich echter situaties voordoen waarbij de functies worden gecombineerd en dit, met in achtneming van randvoorwaarden, mogelijk is.
Vanuit een managementperspectief kan het samenvoegen van functies zelfs de voorkeur hebben en bepalend zijn voor de inrichting van de organisatie. Dan moeten nadere waarborgen worden getroffen om voldoende onafhankelijkheid te borgen; deze randvoorwaarden worden hieronder nader toegelicht.

Overwegingen gebaseerd op theorie en afstemmingen

Kader
De CVT van het IIA NL sluit zich aan bij het standpunt in het Position Paper van IIA Inc. (2013) en ziet geen reden daarvan af te wijken of strenger in de leer te zijn. Vanuit het 'Three Lines of Defense' Model is een combinatie niet de meest gewenste organisatorische oplossing; desondanks kan de combinatie voorkomen. De combinatie van de IAF en second line of defense functies zoals risk management en/of compliance-functie(s) is in bepaalde situaties mogelijk, indien daarbij de nodige randvoorwaarden in acht worden genomen.
Het hangt dus af van de specifieke omstandigheden en randvoorwaarden die zijn getroffen bij de inrichting. Voorbeelden van specifieke omstandigheden die in de praktijk veel voorkomen:
- kleinschalige ondernemingen, waarin het afscheiden van een afzonderlijke risicofunctie niet of nauwelijks mogelijk is;
- grotere organisaties, als de ondernemingsleiding, zich bewust van de consequenties, willens en wetens het coördineren van een GRC activiteit zoals het RM-proces bij de IAF belegt.

Randvoorwaarden
De belangrijkste algemeen geldende randvoorwaarden wanneer er sprake is van samengaan van IAF en GRC-functies (IIA, 2013):

1. *Expliciet maken van gevolgen*: Indien er sprake is van samengaan van functies dan dient de IAF de gevolgen hiervan en de eventueel getroffen compenserende maatregelen te communiceren aan de raad van bestuur/senior management en het AC.
2. *Geen afbreuk effectiviteit:* De verschillende functies mogen echter nooit op een zodanige manier worden gecombineerd of gecoördineerd dat afbreuk wordt gedaan aan de effectiviteit van de IAF en de verwachting van de raad van bestuur/senior management en het AC dat onafhankelijke, objectieve zekerheid wordt gegeven over het 'in control' zijn van de business.

Nadere randvoorwaarden gebaseerd op IPPF standaarden en position papers:

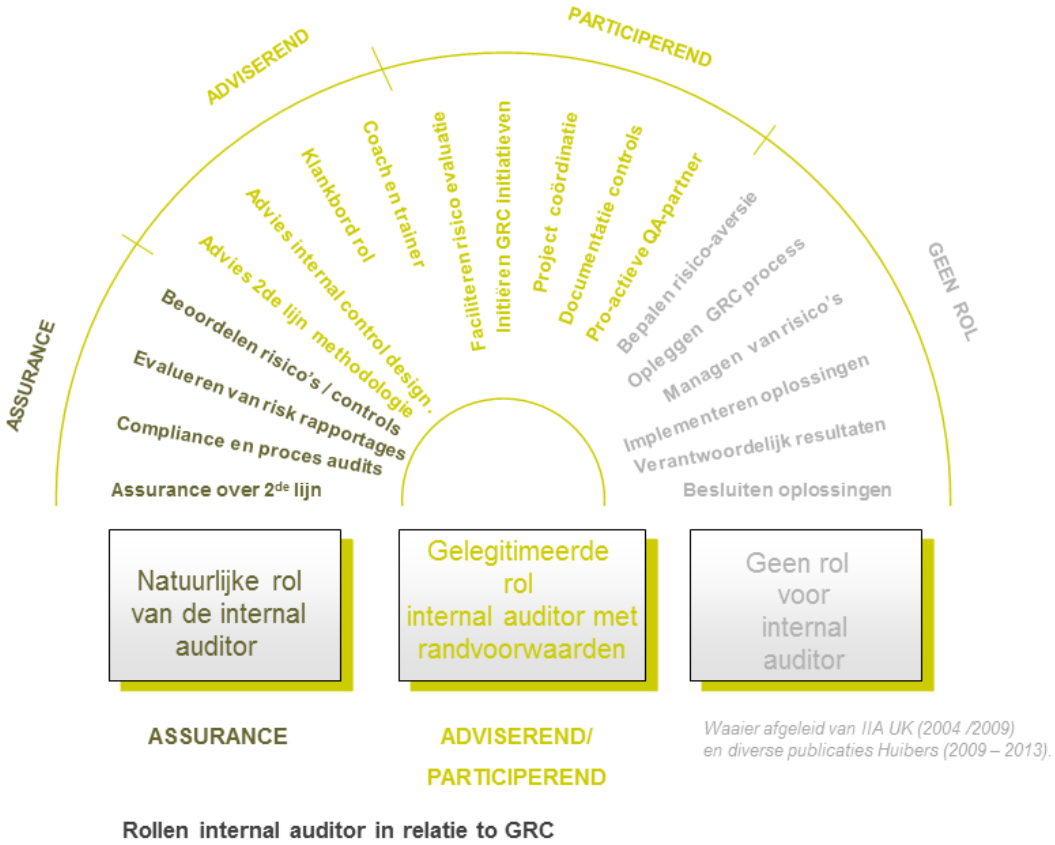
1. *Geen managementverantwoordelijkheid*
   De IAF mag geen managementbesluiten nemen; het lijnmanagement blijft primair verantwoordelijk voor het bepalen van de risicovoorkeur (position paper ERM) en het maken van keuzes over de te implementeren oplossingen.
2. *Formaliseren in het charter*
   Het is van belang om mogelijke onduidelijkheid over potentiële rollen van assurance- en adviespartijen in de organisatie te voorkomen, door deze rollen te expliciteren.
   Op organisatieniveau worden het doel, het mandaat en de aard van de activiteiten van de IAF vastgelegd in het audit charter en goedgekeurd door de raad van bestuur en het AC. Indien de IAF ook verantwoordelijk is voor second line of defense-functies dient dit expliciet in het charter te worden vermeld, alsmede welke rol en verantwoordelijkheden de IAF hierin heeft.
3. *Maturity*
   In een groeisituatie waarin de IAF een rol heeft in het design van bijvoorbeeld de risicomanagement methodologie, behoeft het plan van aanpak afstemming met het AC (standaard 2050).
4. *Uitbesteding*
   Indien de IAF een GRC functie zoals RM coördineert dan zal voor de beoordeling ervan een andere (externe) partij moeten worden ingeschakeld zodat de IAF niet haar eigen rol gaat toetsen (standaard 2010 / 2050).
   De IAF bewaakt op basis van de risicoanalyse dat de assurance over de processen voldoende is afgedekt, inclusief de processen die door derden zijn geaudit.

Functiescheiding toepassen binnen de IAF
De auditor moet mogelijke belangenverstrengelingen voorkomen om zijn onafhankelijke positie te behouden.
Ook de perceptie van de onafhankelijkheid in de organisatie is hierbij van belang. Om hier deels aan tegemoet te komen is functiescheiding binnen de IAF een vervangende maatregel. Eén van de belangrijkste uitgangspunten hierbij is de mogelijkheid tot het groeperen van verschillende activiteiten met niet-identieke of mogelijk conflicterende doelstellingen. Een scheiding in de IAF tussen adviseren/faciliteren, in dit geval met betrekking tot GRC-activiteiten, en assurance-gerelateerde activiteiten is een voorbeeld hiervan. Indien de omvang van de afdeling het toelaat, is het afscheiden van assurance-gerelateerde activiteiten in een separate *subafdeling* een extra waarborg (lees 'second best' optie)[2].
Vanuit de onafhankelijkheidsgedachte stellen de standaarden dat iemand op individueel niveau niet binnen 1 jaar kan auditen nadat hij een andere (beleidsbepalende) rol bij dat object heeft gespeeld (*Standaard 1130 A.1*). Deze lijn moet ook doorgetrokken worden voor advies- en participerende rollen zoals in de volgende paragraaf omschreven. Een auditor die een proactieve rol heeft gehad met betrekking tot een object zou op zijn minst 1 jaar geen assurance activiteiten mogen vervullen voor het betreffende object.

[2] Huibers, raamwerk randvoorwaarden onafhankelijke positie auditor, Audit Magazine 2010.

Branche-specifieke regelgeving
De aard van de onderneming waarin de GRC-processen, zoals het RM-proces, zich afspeelt, is tevens relevant. Bij organisaties waar bijvoorbeeld RM een onderdeel is van het primaire proces, zoals bij financiële instellingen, is de combinatie zeker niet verdedigbaar. Doorslaggevend is hierbij de branche-specifieke regelgeving waaraan de organisatie moet voldoen.

Rollen
Een belangrijke kanttekening is dat niet alleen functiebenaming en ophanging in de organisatie doorslaggevend is in wat wel en niet kan; de daadwerkelijke rollen en activiteiten dienen in de beschouwing te worden betrokken alsmede de hierboven genoemde randvoorwaarden. Uit de 'Round Tables' kwam expliciet aan de orde dat het niet zozeer gaat om het label dat op de functie wordt geplakt, als wel om de vraag hoe de rol daadwerkelijk wordt ingevuld en wat er inhoudelijk wel of niet aan activiteiten wordt gedaan.
In lijn met een position paper van IIA over ERM en publicaties over project auditing[3] geven we hieronder een overzicht van rollen in het kader van GRC ingedeeld in 4 categorieën:
1) *de assurance rol*: de traditionele rollen van de internal auditor;
2) *de adviserende rol*: adviesrollen zijn rollen die kunnen worden vervuld met randvoorwaarden;
3) *de participerende rol*: participerende rollen die eveneens onder voorbehoud (met randvoorwaarden) kunnen worden vervuld;
4) de rol die de auditor zeker *niet* mag vervullen.



Figuur 1: Voorbeelden rollen internal auditor met betrekking tot GRC

[3] Waaier afgeleid van Institute of Internal Auditors met betrekking tot de rol van de interne audit functie in Enterprise Risk Management (IIA UK, 2004) en diverse publicaties Huibers over de rol van de auditor door Kluwer/NBA/IIA/Norea in Nederland enTaylor & Francis in de Verenigde Staten (2009 – 2013) .

De waaier geeft een overzicht van voorbeelden van mogelijke rollen van de internal auditor, al dan niet met randvoorwaarden, gebaseerd op algemene uitgangspunten in het kader van de onafhankelijkheid van de internal auditor zoals geformuleerd door het IIA en andere beroepsorganisaties. De waaier is richtinggevend en niet bedoeld als een uitputtende opsomming van rollen.

Nadere richtlijn voor kwaliteitstoetsingen
In de rapportage van het CKT kunnen de risico's van het samengaan van internal audit en GRC-werkzaamheden worden gesignaleerd. Voordelen van afsplitsing van GRC-functies van internal audit in het kader van de onafhankelijkheid kunnen worden genoemd. Dit heeft voornamelijk als doel om een weerspiegeling van een mogelijk good practice alternatief te geven; niet zozeer om dit in de oordeelsvorming te betrekken (tenzij niet is voldaan aan de randvoorwaarden).

Voor de oordeelsvorming betekent dit concreet het volgende in het kader van standaard 1100 "Independence en Objectivity":
- Indien toereikend voldaan wordt aan randvoorwaarden: GC (Generally complies): OK.
- Beperkte aanpassing in de vervangende maatregelen nodig om aan randvoorwaarden te voldoen: PC (Partially complies): aanbevelingen.
- Niet toegestane taken met betrekking tot Risk Management / GRC, niet aan de randvoorwaarden voldaan ofwel ontoereikende vervangende maatregelen : DNC (Does not comply): aanbevelingen en negatieve invloed op het overall oordeel van de IAF.

De waaier van rollen op activiteitenniveau zoals hierboven weergegeven is richtinggevend, maar expliciet niet bedoeld als een uitputtende opsomming van rollen, als dat al mogelijk zou zijn. Het gaat om de achterliggende gedachte en de randvoorwaarden. Eén van de belangrijkste randvoorwaarden om de onafhankelijkheid van de internal auditor te waarborgen is dat hij geen managementverantwoordelijkheid neemt. De internal auditor kan advies, reflecties en ondersteuning geven aan het management met betrekking tot besluitvorming, maar is niet in een positie tot het zelf nemen van besluiten namens het management.

In de bijlagen zijn de literatuurstudie, die het perspectief van beroepsorganisaties geeft, en de overwegingen vanuit het managementperspectief opgenomen op basis van onderzoek, inventarisaties en de Round Tables.

2. Issue 2: Rapporteren aan de CFO

In hoeverre en, zo ja, onder welke voorwaarden, is het rapporteren van de IAF aan de CFO acceptabel?

Conclusie issue 2
Ophanging van de IAF onder de CFO en de directe rapportagelijn van de IAF naar de CFO is in bepaalde situaties mogelijk, afhankelijk van de omstandigheden, maar in het algemeen vanwege het risico van verminderde onafhankelijkheid niet wenselijk ('nee, tenzij …').
De standaarden geven de ruimte voor ophanging aan de CFO, maar kennen een voorkeur voor ophanging van de IAF aan de CEO.

Voorwaarden bij de ophanging onder de CFO zijn:
- Er is geen sprake van belemmeringen in de oordeelsvorming van de IAF over de GRC en de werkzaamheden die onder verantwoordelijkheid van de CFO worden uitgevoerd.
- De CAE heeft een eigen (escalatie)rapportagelijn naar de CEO en/of het AC.

- Het Auditcharter is getekend door de CEO.
- Het jaarlijks auditplan wordt goedgekeurd door de CEO (en geagendeerd in het AC),
- De auditrapporten zijn gericht aan de CEO, en via de (interne) Management Letter aan het AC.

Overwegingen gebaseerd op theorie en afstemmingen

Opgemerkt wordt dat bij een samenloop van functies (issue 1) in de praktijk vaak ook aan de CFO wordt gerapporteerd. Dit versterkt het risico van de verminderde onafhankelijkheid.

Wat in de praktijk vaak voorkomt, is dat de CFO of directeur Financiën (of soortgelijke functie) 'de goede huisvader' is; hij/zij faciliteert in de benodigde budgetten, huisvesting, doet soms ook de beoordeling van de CAE en toetst de selectie van auditors marginaal.
Voor de gewenste onafhankelijkheid is het in deze opzet belangrijk dat aan de hiervoor genoemde voorwaarden is voldaan.

Nadere richtlijn voor kwaliteitstoetsingen
Indien de IAF rechtstreeks rapporteert aan de CFO zal dat bij de toetsing weliswaar tot een "Generally complies" leiden, maar altijd vergezeld moeten gaan van "Ter overweging" in het reviewrapport om deze rapportagelijn te heroverwegen.

3. Issue 3: Kleine IAF's

Kunnen kleine IAF's afwijken van de geaccepteerde normen en wat betekent dat?

Conclusie
Ook door kleine IAF's moet aan alle standaarden worden voldaan.
Kleine IAF's kunnen in beginsel aan alle standaarden voldoen, waarbij wel sprake kan zijn van uitdagingen. De mate van uitdaging is voor de diverse standards nader beschreven in "De Praktijk gids voor de kleine audit functie" (zie hieronder).

De **Praktijk gids voor de kleine audit functie** geeft aan dat de kleine IAF kan voldoen aan de standaarden. Zij ziet de volgende mate van uitdagingen voor de kleine audit functie.

STANDAARD	OMSCHRIJVING	MATE VAN UITDAGING
1000	Doel, bevoegdheid en verantwoordelijkheid	L
1100	Onafhankelijkheid en objectiviteit	H
1200	Deskundigheid en zorgvuldigheid	M
1300	Kwaliteitsborgings- en verbeterprogramma	H
2000	Management van de internal auditfunctie	H
2100	Aard van het werk	M
2200	Planning van de opdracht	H
2300	Uitvoering van de opdracht	H
2400	Communicatie van resultaten	M
2500	Toezicht op de opvolging	M
2600	Risico acceptatie door het management	M

Indicatie van de verwachte mate van uitdaging:
***Groen** – lage mate van uitdaging, **Geel** – gemiddelde mate van uitdaging, **Rood** – hoge mate van uitdaging*

De commissie PAS is bezig met het ontwikkelen van handvatten die door de kleine IAF als referentie voor de minimumeisen t.a.v. de kwaliteitstoets kunnen worden gebruikt; dit zijn met andere woorden de minimale voorwaarden waaraan kleine audit functies moeten voldoen (o.b.v. Praktijkgids). Deze handvatten dienen nog te worden afgestemd met een brede vertegenwoordiging van de doelgroep en het vakgebied en betreft een separaat project.

Overwogen kan worden om de mogelijkheid te bieden in die beginjaren tussen het IIA en de betreffende IAF een groeipad af te spreken. Daarbij zou een (kleine) IAF in oprichting niet in haar 1^{e} en 2^{e} jaar moeten worden getoetst. Normaal gesproken kan worden verwacht dat de IAF in opbouw na 2 jaar een voldoende niveau heeft bereikt.

Voor kleine IAF's die al meerdere jaren bestaan en waarvan het duidelijk is dat zij nog niet aan de normen voldoen, kan worden overwogen de mogelijkheid te bieden een self assessment te laten uitvoeren om op basis daarvan een ontwikkelingsplan af te spreken met duidelijke tijdlijnen (bijvoorbeeld 2 jaar), waarna een definitieve toetsing plaats vindt.

4. Issue 4: Aard IAF en invulling normenkader

In welke mate is de aard van de IAF (standaard repeterende audits, veelal sterk financial audit georiënteerd versus maatwerk, meer 'managerial audits') van invloed op de invulling van het normenkader?

Conclusie issue 4:
In principe zijn alle soorten auditwerkzaamheden (maatwerk-/repeterende audits) mogelijk binnen het normenkader en geldt dus voor alle IAF's hetzelfde normenkader.
Opgemerkt wordt dat daarbij altijd sprake dient te zijn van een methodische aanpak om tot een auditplanning te komen (gebaseerd op een risicoanalyse, ook voor audits op verzoek) en om de audits uit te voeren en van voldoende competenties bij de auditors.
Dat geldt ook bij een transitie van een overwegend financial audit gerichte IAF naar een meer operational audit georiënteerde IAF.

T.a.v. de verdeling van consulting en assurance-activiteiten geldt dat er altijd sprake moet zijn van een combinatie. Beneden een bepaalde ondergrens van assurance-activiteiten kan niet meer worden gesproken over een IAF.
Die ondergrens kan overigens voor een gelimiteerde periode heel laag liggen. Zo kan een auditor in een adviesrol bijvoorbeeld een bijdrage leveren aan het opbouwen van de risicomanagement-organisatie.

Voor de bijzonderheden voor een kleine IAF danwel de IAF in oprichting wordt verwezen naar hetgeen daarover is gezegd bij issue 3.

Overwegingen gebaseerd op theorie en afstemmingen

- Voor alle audits/auditors geldt:
  - De opdrachtgever moet er verzekerd van kunnen zijn dat de titel van de door hem ingehuurde auditor staat voor een bepaalde kwaliteit van de uitgevoerde auditwerkzaamheden en van de daaruit voortvloeiende rapportage.
    Daarbij moet de auditor zich ervan bewust zijn dat hij alleen activiteiten uitvoert waarvoor hij is opgeleid en die passen binnen zijn kennis en ervaring.
  - Voorgaande heeft als logisch gevolg dat financial audits zullen worden uitgevoerd door accountants, terwijl voor managerial audits meer moet worden gedacht aan de inzet van operational auditors.
  - De auditor dient de juiste mix van auditwerkzaamheden in te zetten; ook repeterend werk mag geen blauwdruk-activiteit worden.

- Er zijn tussen repeterende en maatwerk-audits wel verschillen (in de praktijk); zo geldt bijvoorbeeld voor 'maatwerk':
  - Selectie van audits gebeurt (meer) in overleg met het (senior) management van de organisatie.
  - Invulling van de audit (scoping, bepalen normenkader) gebeurt in overleg met c.q. wordt expliciet besproken met opdrachtgever en proceseigenaar (dus niet de 'eigen verantwoordelijkheid' van de auditor en er is vaak geen 'algemeen geaccepteerd' en uitgekristalliseerd normenkader aanwezig)
  - Er kunnen afwijkende rapportagevormen zijn, bijvoorbeeld in de vorm van een sheetpresentatie.

Dergelijke verschillen leiden echter niet tot het niet kunnen voldoen aan bepaalde standards. Ook maatwerk-audits voldoen aan de (performance) standards, op het moment dat de maatwerk-audits methodologisch netjes worden geselecteerd en uitgevoerd (zoals een duidelijk, overeengekomen plan van aanpak, deugdelijke evidence (betrouwbaar en valide, met voldoende bronnen(soorten), duidelijke relatie tussen conclusies en bevindingen in dossier, …).
Wel kunnen IAF's die zich volledig richten op maatwerk-audits mogelijk een andere relatie hebben met het AC dan beschreven in de 'good practice' Bondgenoten in Governance. Dat betreft issue 5.

5. Issue 5: Relatie IAF – AC (afwijken van good practice in 'Bondgenoten in Governance')

In welke mate en, zo ja, onder welke voorwaarden, is afwijking van de best practices in 'Bondgenoten in Governance' (relatie IAF en AC) v.w.b. de waarborgen voor onafhankelijkheid van de IAF t.o.v. de raad van bestuur acceptabel?

Conclusie issue 5:
'Bondgenoten in governance' is een 'good practice' (met handvatten), maar geen harde norm. De IAF 'helpt' de raad van bestuur en het AC door assurance te geven. Dit past ook bij de rol van de IAF in de Corporate Governance Code, waar de IAF als beheersinstrument van de organisatie wordt gezien.
Geconstateerd is dat maatschappelijk gezien het belang van de relatie van de IAF met het AC toeneemt.

Overwegingen gebaseerd op theorie en afstemmingen

- Met name IAF's die zich (vooral) richten op maatwerk-audits, zonder externe werking, kiezen soms voor een duidelijke positionering als ondersteunend aan de raad van bestuur/CEO/directeur. Hun doel is additionele zekerheid te verschaffen aan de raad van bestuur en het senior management en bij te dragen aan de verbetering van de interne beheersing van de organisatie.
  Hierdoor is de raad van bestuur opdrachtgever en past het niet te streven naar onafhankelijkheid daarvan, maar wil men juist 'sparring partner' zijn.
  Dat past ook bij de rol van de IAF in de Nederlandse Corporate Governance Code, waarin de IAF ook als beheersinstrument ("tool of management") van de organisatie wordt gezien.

- In het verlengde hiervan is de relatie met het AC dan ook anders:
  - Het AC moet toezien op de kwaliteit van de 'GRC' binnen de organisatie (waarvoor de raad van bestuur eindverantwoordelijk is), dus inclusief de IAF, als onderdeel daarvan. Vanuit dat toezicht kijkt het AC ook naar de IAF, maar niet zozeer om te 'waarborgen' dat die onafhankelijk van de raad van bestuur kan functioneren, maar om te beoordelen of zij een adequate bijdrage levert aan de control/governance van de organisatie.
  - Zodoende kijkt het AC wel naar de plannen, maar keurt deze niet noodzakelijkerwijs goed (review of het auditplan past bij de verwachtingen van het AC inzake goede governance) en kijkt het AC wel naar aantrekken en ontslag van de CAE, maar niet om over te beslissen.

  Deze punten sluiten niet geheel aan bij de 'best practices' uit 'Bondgenoten in Governance', maar zijn wel consistent met de rol die de IAF speelt en consistent met de Nederlandse Corporate Goverance Code en het Modelcharter van het IIA.

Het verdient in alle gevallen aanbeveling de rol van alle betrokkenen expliciet te definiëren.

6. Issue 6: Functionele aansturing van IAF's van dochters

Wat zijn de te stellen eisen aan de functionele aansturing van dochterorganisaties door de IAF?

Conclusie issue 6:
De invulling van de relatie tussen de IAF van de moeder en de IAF van de dochter kan verschillend zijn. De belangrijkste voorwaarden voor de functionele aansturing zijn:

- de rapportagelijnen zijn duidelijk en (schriftelijk) vastgelegd, bij voorkeur in het Audit charter;
- de IAF van de dochter dient risico's en bevindingen onafhankelijk te kunnen rapporteren aan (de IAF van) de moeder, zonder beïnvloeding door het management van de dochter.
- indien op groepsniveau een oordeel wordt gegeven over de beheersing van de kernprocessen, ziet de IAF van de moeder er op toe dat de werkzaamheden die worden uitgevoerd door de IAF van de dochter toereikend zijn om dat oordeel te kunnen geven (bijv. door review op de werkzaamheden). Hiervoor dient een uitgewerkte aanpak in het Audit Manual te zijn vastgelegd.

Overwegingen gebaseerd op theorie en afstemmingen

- De standards laten de wijze van aansturing vrij. Attribute standard 1000 gaat niet verder dan dat "het doel, de bevoegdheid en de verantwoordelijkheid van de IAF formeel in een internal audit charter worden vastgelegd".
  Door een goede vastlegging van de rolverdeling in het audit charter ontstaat voor alle betrokkenen duidelijkheid over taken en bevoegdheden.

- Het belangrijkste criterium om als dochter van een IAF onafhankelijk te kunnen functioneren, is dat deze de risico's en bevindingen onafhankelijk kan rapporteren aan de IAF van de moeder.

  Een belangrijke vraag is dan hoe de onafhankelijke rapportage van risico's en bevindingen is geborgd en dus niet kan worden beïnvloed door het management van de dochter. Hiertoe dient sprake te zijn van een directe rapportagelijn met de IAF van de moeder. De rapportagelijn dient duidelijk te zijn en vastgelegd in het zogeheten assurance-model.

- Aan een effectieve functionele aansturing van de IAF van de dochter dragen de volgende punten bij:
  - Dochters hanteren dezelfde methodologie als de moeder en zijn object van de interne quality assurance activiteiten van de moeder.
  - Er is sprake van joint audits, waarbij de IAF van de moeder de activiteiten aanstuurt en coördineert. De IAF's van de dochters voeren de audits dan uit onder regie van de IAF van moeder.
  - Assurance-activiteiten van alle IAF's worden afgestemd op basis van een risicoanalyse die organisatie-breed wordt uitgevoerd en afgestemd met het senior management.
  - Medewerkers van de IAF's komen (regelmatig) met de IAF van de moeder samen voor bijeenkomsten en trainingen die worden georganiseerd door de IAF van de moeder.

Bijlage 1 hot issue 1: Auditperspectief – Literatuuronderzoek beroepsorganisaties

Hieronder geven we een korte uiteenzetting van guidance en randvoorwaarden gebaseerd op recente publicaties van beroepsorganisaties van auditors waaronder het IIA.

- Het recente *Position Paper van het IIA over het 'three lines of defense-model' (2013),* geeft aan dat risicomanagement normaal gesproken het meest optimaal werkt indien er sprake is van drie afzonderlijke ingerichte 'lines of defense'. Er kunnen zich echter situaties voordoen waarbij functies worden gecombineerd; bijvoorbeeld de IAF wordt gevraagd de risk management en compliance activiteiten op te zetten en/of te managen. Indien dit het geval is moet de IAF de gevolgen hiervan communiceren aan de raad van bestuur/senior management en het Audit Committee .De verschillende functies dienen niet op een zodanige manier te worden gecombineerd of gecoördineerd dat afbreuk wordt gedaan aan de effectiviteit van de IAF.

- Het *Position Paper van het IIA UK-Ireland over ERM (2004, 2009)* geeft nadere handvatten over de rollen van de IAF in risicomanagement. In een waaier wordt aangegeven dat in relatie tot ERM een onderscheid kan worden gemaakt in assurance-rollen en adviserende rollen die met inachtneming van randvoorwaarden door de internal auditor kunnen worden vervuld. Zo kan de IAF de activiteiten om risicomanagement op te zetten coördineren en het ERM raamwerk ontwikkelen en onderhouden. Daarbij is er, zoals hiervoor opgemerkt, wel sprake van randvoorwaarden waarbij de belangrijkste is, teneinde de onafhankelijkheid van de internal auditor te waarborgen, dat hij geen managementverantwoordelijkheid neemt. De IAF kan risk management faciliteren, maar zal nooit het eigenaarschap op zich nemen: het lijnmanagement zal altijd intensief bij het proces moeten worden betrokken en de besluiten over de risicovoorkeur en de beheersmaatregelen moeten nemen.

- In *de Practice Guide 'Coordinating Risk Management and Assurance' van IIA Inc. Global (maart 2012)* wordt aangegeven dat risk management activiteiten kunnen worden gedelegeerd aan een separate risk management functie. Daarnaast zijn er organisaties die risk management activiteiten bij de IAF beleggen, in de hoedanigheid van een consultancy activiteit. Als zodanig kan de IAF een rol spelen in het identificeren, evalueren en faciliteren van risk management methodes.

- Het discussierapport *'De internal auditor als spin in het GRC-web' (2010)* is meer een onderzoeksverslag aangevuld met good practices en kan dienen als een eerste aanzet voor nadere invulling van richtlijnen en standaarden.
  In het rapport wordt ook al aangegeven dat in termen van een 'hard normenkader' er in Nederland vrijwel geen wetgeving is over de invulling van het GRC-speelveld anders dan aanvullende wet- en regelgeving voor de financiële sector zoals de Code Banken, Basel II en Solvency II. Naast de Corporate Governance Code is eigenlijk alleen binnen de financiële sector dergelijke aanvullende wet en regelgeving voorhanden voor GRC. Een stelling in het discussierapport is dat het opsplitsen van GRC-verantwoordelijkheden over meerdere functies leidt tot betere beheersing in de organisatie.

- In een gezamenlijke publicatie van *de Risk & Insurance Management Society (RIMS) en het IIA uit 2012* staat een zo goed mogelijke samenwerking tussen de Risk Management functie en de IAF centraal. Hierin wordt aangemoedigd om meer samen te werken en in sommige gevallen zelfs resources uit te wisselen om op deze wijze op een zo effectief en efficiënt mogelijke wijze aan de verwachtingen van de stakeholders te voldoen.

IPPF standaarden

- *Standaard 2050 – Coördinatie (gecombineerd met Standaard 1130)*
  Het hoofd van de internal auditfunctie dient informatie te delen en activiteiten te coördineren met andere interne en externe auditors en adviseurs, om een adequate dekking te verzekeren en het dubbel uitvoeren van activiteiten tot een minimum te beperken.

  Indien de IAF risk management (RM) faciliteert zijn de volgende randvoorwaarden van toepassing:
  - De IAF mag geen management besluiten nemen; in het geval de IAF een rol heeft in het design van RM dan moet ze het plan van aanpak afstemmen met het AC.
  - Rollen dienen helder in charter te worden omschreven.
  - Geen assurance over RM: (intern) uitbesteden (zie ook *standaard 1130*).

- *De IPPF-standaard 1000* geeft aan dat het doel, de bevoegdheid en de verantwoordelijkheid van de IAF formeel in een internal audit charter worden vastgelegd.

Literatuur

Onderstaande literatuur is een selectie van recente publicaties van de beroepsorganisaties die ingaan op de rol van internal audit in relatie tot tweedelijnsfuncties. Dit geeft een weerspiegeling van de huidige trends en standpunten ter ondersteuning van het advies van de CVT. Het is niet de intentie een volledige literatuurlijst te geven, voor zover dit al mogelijk zou zijn.

- The Institute of Internal Auditors UK - Ireland, Position Paper *The Role of Internal Audit in Enterprise-wide Risk Management*, 2004.
- The Institute of Internal Auditors, Position Paper *The Role of Internal Audit in Enterprise-wide Risk Management*, herziene uitgave 2009.
- Het Instituut van Internal Auditors Nederland, *De Internal Auditor in Nederland, Position Paper Update 2008*, Naarden, 2008.
- The Institute of Internal Auditors, *The Professional Practices Framework*, The IIA Research Foundation, 2011.
- The Institute of Internal Auditors, IIA Position Paper: The Three Lines of Defense in Effective Risk Management and Control, 2013.
- The Institute of Internal Auditors, Inc. and the Risk and Insurance Management Society, Inc., Executive Report, *Risk Management and Internal Audit: Forging a Collaborative Alliance*, 2012.
- The Institute of Internal Auditors, Practice Guide, *Coordinating Risk Management and Assurance*, 2012
- Instituut van Internal Auditors Nederland, Naarden en Koninklijk NIVRA, Discussierapport *De internal auditor als spin in het GRC-web, Samenwerking met behoud van onafhankelijkheid*, 2010.
- S.C.J. Huibers, 'Proactiviteit en onafhankelijkheid van de auditor in projecten: contradictio in terminis?', Audit Magazine, nr. 1 maart 2010, Instituut van Internal Auditors in Nederland, VM Uitgevers, 2010
- S.C.J. Huibers,'Rol van de internal auditor in veranderingsprojecten', Finance en Control, versie 5, oktober 2009, Kluwer 2009.

Verantwoording waaier – internal audit in relatie tot GRC:
Waaier is afgeleid en aangevuld op basis van
1) position van Institute of Internal Auditors met betrekking tot de rol van de auditfunctie in Enterprise Risk Management (IIA, 2004)
2) diverse publicaties Huibers over de rol van de auditor door Kluwer/NBA/IIA/Norea in Nederland en Taylor & Francis in de Verenigde Staten (2009 – 2013) ; www.iia.nl, Download link artikel).

Bijlage 2 hot issue 1: Management perspectieven – onderzoek en ronde tafel

Uit een verkennende inventarisatie van de werkgroep en een aansluitende ronde tafel met hoofden IAF kwam duidelijk naar voren dat de inrichting van GRC en de IAF veelal per organisatie verschilt en veelal gedreven door wat het management wil.

Algemene omstandigheden die naar voren kwamen:
- Soms heeft de IAF een tijdelijke rol om mee te helpen processen in te richten.
- Momentum en maturity van organisaties is van belang; IAF kan soms helpen bij de opbouw en inrichting, tijdelijke samenloop is dan een mogelijkheid.
- Het faciliteren van management brengt (meer) toegevoegde waarde.
- Soms is de inrichting van de GRC-structuur ingegeven door sectorspecifieke regelgeving.
- Niet alleen functiebenaming is van belang, maar ook de werkelijke taak / taakafbakening moet in beschouwing genomen worden. Vaak is de rol van audit proces-georiënteerden neemt de IAF geen inhoudelijke besluiten.

Management overwegingen om de functies samen te voegen zijn hieronder samengevat op basis van resultaten van de vragenlijst.
- *Optimalisatie van de span of control*; beperken van het aantal personen die rapporteren aan Senior Management/ Board met betrekking tot assurance- en advies activiteiten.
- *Efficiency*; kostenoverweging en het efficiënter uitvoeren van activiteiten onder één paraplu.
- *Historisch*; de organisatie van activiteiten kan een voortvloeisel zijn uit het verleden; activiteiten kunnen in de loop van tijd worden uitgebreid en belegd bij één afdeling.
- *Synergie*; synergie-effect door professionals met vergelijkbare expertise / achtergrond samen te brengen onder één paraplu.