A. Molenkamp RO is zelfstandig organisatie-adviseur en verbonden aan de Amsterdam Business School

Kunnen audit, compliance en risk samengaan?

'Samengaan willen we zeker niet!,' antwoordden de geënquêteerde compliance officers, risk managers en internal audit executives op een relatiebijeenkomst onlangs eensgezind. Wel wilde men graag een klankbord voor kwesties als strategieontwikkeling, onderlinge taakverdeling en rapportagestructuur. Vraagstukken die binnen organisaties minder gemakkelijk bespreekbaar zijn en kunnen leiden tot competentiegeschillen.

Samengaan werd dus tamelijk eensgezind afgewezen. Desondanks ging men wel in op de vraag: welke zijn de favoriete combinaties?. Zoals te verwachten gooide de combinatie 'integreren van compliance en risicomanagement' hoge ogen, een minderheid koos voor 'audit en riskmanagement'.
In de financiële sector zijn het vooral toezichthouders die met behulp van regelgeving de instelling van de functies compliance en riskmanagement afdwingen. Bij aandeelhouders van Shell ontstond veel commotie over de inschatting van oliereserves. Dit leidde tot indringend herzien van riskmanagement en internal audit.
Maar nu het wel of niet samengaan. Uitgangspunten van interne controle ofwel three lines of defense bepalen of functies wel of niet kunnen samengaan. Compliance en riskmanagement staan voor de tweede lijn en internal auditing voor de derde lijn. Vanuit dat oogpunt is een samengaan van audit met andere functies niet wenselijk. Voor internal audit geldt dat een onafhankelijke positionering haar bestaansrecht is.
Dat audit met riskmanagement moet samenwerken is buiten kijf. De door audit uit te voeren onderzoeken zijn zelfs gebaseerd op de uitkomsten van het risicoanalyseproces dat heeft plaatsgevonden. Audit bepaalt dus geen risico's; audit voert slechts uit.
Eén van de audits zou zelfs kunnen gaan over het protocol voor het inventariseren en prioriteren van risico's. Slechts vanuit een onafhankelijke opstelling kan audit de top aanvullende zekerheid verschaffen.
Audit en riskmanagement gaan dus niet samen.
Wat voor risk management geldt, is ook van toepassing op compliance. Ook daar zal een onafhankelijke toets moeten plaatsvinden op het bepalen van de compliance-items, op het ontwikkelen van de compliance-structuur en op de wijze van naleving van de gestelde compliance-regels. De belangentegenstelling tussen audit en compliance is te groot voor een samenwerkingsverband van beide functies. Een voorbeeld: het voor verzekeringsinstellingen per 2012 moeten voldoen aan de Solvency II regelgeving vereist nu al een grote inzet van compliance. Uit het oogpunt van effectiviteit en imagoschade dient dit project te worden getoetst.
Met andere woorden: audit en compliance gaan niet samen.
Rest nog het mogelijk samengaan van compliance en riskmanagement.
Daar gloort licht. Maar er is ook sprake van enig voorbehoud.
We zijn van oordeel dat op concernniveau afzonderlijke committees voor compliance en riskmanagement nodig zijn, mede gezien het verschil in 'opdrachtgevers'. Compliance is op de omgeving van de organisatie gericht; riskmanagement heeft te maken met bedrijfsinherente continuïteitsvraagstukken. Om die reden zijn ook op concernniveau de staffuncties riskmanagement en compliance afzonderlijk gepositioneerd. De door deze staven te ontwikkelen regelgeving dient in controlsystemen te worden geïntegreerd.

> *'Een compliance maatregel die is ingegeven door belangen van stakeholders kan haaks staan op maatregelen die bedoeld zijn om risico's te beheersen: Eumedion wenst, in het jaarverslag, volstrekte transparantie over de risico's die een onderneming loopt. De ceo daarentegen probeert juist te bereiken dat de concurrentie geen weet heeft van de uitkomsten van het interne proces van riskmanagement.'*

Deze systeemintegratie leidt op niveau van business units onvermijdelijk tot het samengaan van compliance en riskmanagement in operational riskmanagement (ORM-)groepen. Wel dienen de stafafdelingen in hun toezichthoudende en controlerende taken erop toe te zien dat die regelgeving, waarvan zij 'eigenaar' zijn op een juiste wijze wordt nageleefd.
Een bewijs uit het ongerijmde: binnen operational riskmanagement-groepen is er toch nog sprake van enig samengaan. **–C**