

GRC: een veelbesproken term

Bij veel organisaties ontstaat een toenemende noodzaak tot transparantie en efficiëntie in risicobeheersing en kwaliteitsverbetering. GRC wordt hiervoor vaak genoemd als oplossing. Maar wat is er met GRC te bereiken? En wat is de eerste stap? In dit artikel wordt GRC in simpele, duidelijke bewoordingen gedefinieerd. Daarnaast wordt beoogd lezers die overwegen de eerste stappen op dit terrein te zetten, of daar inmiddels al mee zijn begonnen, een duwtje in de rug te geven.

M. But en M. Groenenboom

Op verschillende fora en in vakbladen wordt uitgebreid aandacht besteed aan het onderwerp governance risk compliance (GRC). Desondanks blijft vaak onduidelijk wat de term GRC nu precies inhoudt. Wat opvalt aan de publicaties is de terugkerende belofte een definitie van GRC te geven. Hier wordt echter vaak weinig invulling aan gegeven door direct in te gaan op een bepaald aspect van GRC, zoals GRC-software, controlraamwerken of ERM. In die publicaties waarin wel een omschrijving is opgenomen, wordt GRC op verschillende manieren uitgelegd. Enkele voorbeelden:

- Buith en Van Grinsven (2009) zien GRC als een middel om het huidige silodenken te doorbreken tussen business units, functionele processen, geografie en technologie.
- Heijmans (2009) gaat verder in op de raakvlakken tussen de drie gebieden. Zij geeft in haar artikel *Taken en verantwoordelijkheden Governance, Risk & Compliance* aan dat er behoefte is om de verschillende assurancefuncties zodanig te positioneren dat zij elkaar aanvullen en er geen witte vlekken of dublures in werkzaamheden bestaan. De implementatie van een GRC-raamwerk kan dit inzichtelijk maken. Heijmans omschrijft GRC als een gestructureerde aanpak van alle governance-, risk- en compliance-initiatieven in de organisatie.
- Een definitie die gedeeltelijk overeenkomt met de voorgaande komt van Beugelaar en Van Loon (2010) en luidt: 'GRC betreft een volledig geïntegreerd denken en werken volgens een efficiënt en effectief businessmodel, waarbij eenduidigheid bestaat over alle binnen het GRC-domein uit te voeren werkzaamheden, van strategiebepaling tot en met de uiteindelijke rapportage en effectmeting en een goede samenwerking en afstemming met de activiteiten buiten dit GRC-domein'.
- Ter Heegde (2009) ziet de term GRC breder en benadrukt ook het sturingsaspect in zijn definitie: 'GRC verwijst naar het meer brede vraagstuk van control (sturing en beheersing) van de maatschappelijke onderneming, waarin begrepen de wijze waarop de maatschappelijke ondernemer sturing geeft aan afdelingen en bedrijfsprocessen, de relatie met de doelstellingen van de maatschappelijke onderneming, de samenhang met de risico's die het realiseren van doelstellingen in de weg staan, de wijze (overleg, rapportage, audits) van afleggen van verantwoording over het resultaat van het sturen op doelstellingen, de inhoud van die verantwoording en het treffen en naleven van maatregelen die zijn opgenomen in relatie tot mogelijke oorzaken van bepaalde risico's'.
- BWISE definieert GRC als 'de geïntegreerde benadering die bedrijven toepassen om sterke governance binnen een organisatie neer te zetten door middel van risicomanagement en bewezen compliance' (www.bwise.nl; 30 maart 2010).

Opvallend aan deze definities is dat in iedere beschrijving in meer of mindere mate aandacht wordt besteed aan het aspect 'integratie'. Deze integratie kan zich richten op de integratie van raamwerken, kennis of werkzaamheden. Daarnaast wordt vaak verwezen naar een gestructureerde manier van introduceren en implementeren van een bepaalde manier van denken en werken. Voordat er antwoord wordt gegeven op de vraag: wat is GRC? wordt eerst de vraag beantwoord: wat is GRC niet? Dit om te voorkomen dat de term alsnog tot verwarring leidt en een containerbegrip wordt.

Wat is GRC niet?

GRC staat voor de drie vakgebieden governance, risk en compliance. Dit geeft aan dat het om een traject gaat waar alle drie de gebieden vertegenwoordigd zijn. Een initiatief dat wordt gestart vanuit een van deze functies en waar slechts deze ene functie profijt van heeft, kan dus niet gezien worden als een GRC-traject. Een dergelijk initiatief zou wel kunnen dienen als startpunt van waaruit GRC zich als een olievlek verspreidt binnen de organisatie.

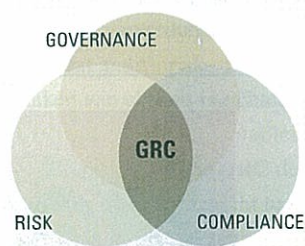
Hoewel in de definitie de nadruk ligt op de integratie van de functies, betekent dit niet dat de drie functies samengevoegd dienen te worden tot één functie. De nadruk ligt op de samenwerking tussen deze functies terwijl deze onafhankelijk van elkaar blijven opereren. In financiële instellingen is het zelfs een eis dat de functies onafhankelijk blijven.

Er zijn verschillende leveranciers die pretenderen GRC-software te leveren. Echter, na een verdieping in de functionaliteiten blijkt vaak dat deze zich slechts richten op een beperkt aandachtsgebied zoals procesbeschrijvingen, documentmanagement of performancemanagement. De implementatie van een dergelijk pakket maakt het daarmee nog geen implementatie van GRC.

Definitie GRC

Om tot een omschrijving te komen van de term GRC is gebruikgemaakt van de hiervoor genoemde definities. Daarnaast zijn de discussies en het onderzoek van de themadag 'Auditing, compliance en riskmanagement: een drie-eenheid of ieder voor zich?' als input gebruikt. Tot slot hebben onze ervaringen vanuit opdrachten bij verschillende organisaties een bijdrage geleverd. Op basis hiervan is het volgende antwoord geformuleerd op de vraag: wat is

GRC? 'GRC is een verzameling activiteiten die zich richt op de integratie van de visievorming op governance, risk en compliance en de integratie van de uitvoering van deze functies binnen een organisatie. Dit met als doel efficiëntie, effectiviteit en transparantie te creëren om te komen tot



Figuur 1. GRC

continue interne beheersing' (zie *figuur 1*).

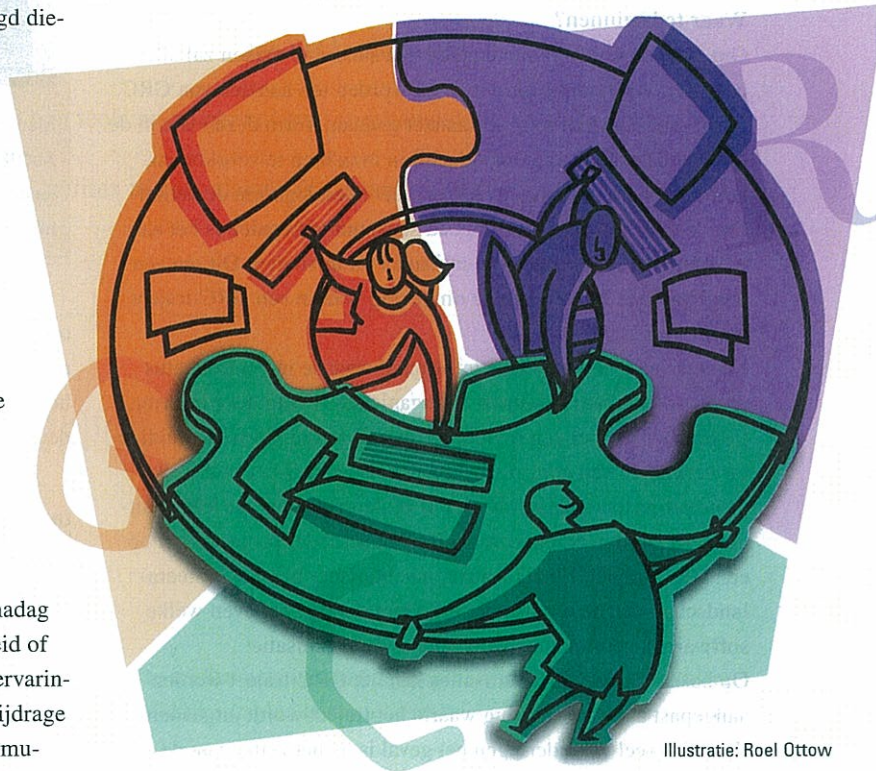
Onder integratie van de uitvoering verstaan wij niet het samenvoegen van de drie functies, maar een betere afstemming van werkzaamheden met behoud van de three lines of defence.

Wat levert GRC op?

Nu er een duidelijk beeld is van hetgeen wel en niet onder GRC wordt verstaan, is de volgende vraag wat dit oplevert voor organisaties. In de nabije toekomst zal de roep om efficiëntie alleen nog maar sterker worden. Dit geldt niet alleen voor het bedrijfsleven, maar wordt ook vanuit de overheid uitgedragen aan bij-

voorbeeld instanties in de zorgsector. Zo wordt in het rapport *Zorg voor minder last* gepleit voor een betere regulering van de regeldruk. Verantwoordelijkheden voor de uitvoering van controls worden door de implementatie van GRC duidelijker belegd in de lijnfuncties. Hierdoor worden de controleigenaren niet meerdere keren bevraagd over hetzelfde onderwerp door verschillende functionarissen.

Audit, risk en compliance zullen, onder andere om de onafhankelijkheid te waarborgen, zelfstandig blijven bestaan als functies



Illustratie: Roel Ottow

binnen organisaties. Echter, om de beheersing op een efficiënte en effectieve manier te waarborgen, zullen de werkzaamheden beter moeten worden afgestemd. Door gebruik te maken van elkaars inzichten, resultaten en expertise kunnen de drie functies zich meer gaan richten op de eigen kerntaken.

Verantwoordelijkheden die in de organisatie duidelijker belegd zijn en werkzaamheden die niet meer dubbel worden uitgevoerd zullen leiden tot een effectievere en efficiëntere manier van werken. En dit zal uiteindelijk leiden tot kostenbesparing in de beheersing. Zo moet het merendeel van de organisaties voldoen aan zowel de Wet bescherming persoonsgegevens (Wbp) als aan de richtlijnen ten aanzien van informatiebeveiliging. Hier is sprake van doublures. Het realiseren van een geïntegreerd controlraamwerk zorgt voor een efficiëntieslag van minimaal 30 procent. GRC-implementaties en GRC-tooling zorgen ervoor dat inzichtelijk wordt gemaakt waar sprake is van redundantie en hiaten in de werkzaamheden. Daarnaast kan met behulp van GRC-tooling realtime integraal inzicht worden verkregen over de in control-status van de organisatie op ieder willekeurig moment. Met deze inzichten kunnen directie en hoger management waar nodig sturing geven. De gerealiseerde doelen van GRC hebben hiermee

GRC-resultaten

- Realtime inzicht in de in controlstatus
- GRC-functies terug naar kerntaken
- Duidelijk belegde verantwoordelijkheden in de lijn

Figuur 2. Resultaten GRC

effect op zowel het uitvoerend, tactisch als strategisch niveau binnen organisaties (zie *figuur 2*).

Waar te beginnen?

Om van een GRC-implementatie een succes te maken zal allereerst een visie ontwikkeld moeten worden ten aanzien van GRC. In dit artikel is hiervoor een aanzet gedaan. Vorm deze visie in de top van de organisatie om verschil in inzichten te voorkomen, betrokkenheid op hoog niveau te creëren en legitiem de verzuiling te doorbreken. Om een goed startpunt te bepalen is het aan te raden om een aantal inventarisaties uit te voeren. Dit om een goed beeld te krijgen van de omgeving waarin een GRC-traject wordt gestart.

Inventariseer vooraf welke informatie over de in controlstatus reeds beschikbaar is binnen de organisatie. Vraag deze informatie op en voer hier een review op uit om de status van de huidige uitwerkingen van controls te bepalen. Inventariseer ook welke grote projecten, zoals Solvency II of de invoering van VMS, uitgevoerd worden en benoem welke impact ieder project heeft op een GRC-traject. En als laatste, inventariseer hoe het systeemlandschap van de organisatie eruit ziet om aan te geven welke software is geïmplementeerd binnen de organisatie.

Op basis van deze inventarisaties kan het GRC-traject worden aangepast aan de omgeving waarin het traject wordt uitgevoerd. Zoals bij veel veranderingen het geval is, is het zetten van de eerste stap tevens de moeilijkste. Iedere verandering levert weerstand



Marvin But en Merlijn Groenenboom zijn beiden werkzaam bij AuditMatch en GRC.nl. In de rol van consultant hebben zij bij verschillende organisaties ervaring opgedaan met governance-, risk- en compliancevraagstukken.

op, ook al betekent dit op termijn vooruitgang. Door te verhelderen wat onder GRC wordt verstaan en welk resultaat het oplevert, hopen we dat de drempel om deze stap te nemen kleiner is geworden en de invulling ervan de kwaliteit krijgt die het verdient.

Literatuur

- Buith, J. en J. van Grinsven, 'GRC nader verklaard', *financieel-management.nl*, 15-12-2009.
- Heijmans, J.M., 'Governance, Risk & Compliance', *Finance & Control*, p. 30, december 2009.
- Beugelaar, B. en W.A.J. van Loon, 'Geslaagd GRC binnen handbereik', p. 11 *Compact.nl*, januari 2010.
- Groenenboom, M. en S. Arnhem, 'Auditing, compliance en riskmanagement: een drie-eenheid of ieder voor zich?' *Audit Magazine*, p. 46-47, maart 2009.
- Heegde, J. ter, 'De maatschappelijke onderneming in zwaar weer', *zbc.nu*, ZBC kennisbank, 27 november 2009.
- *Zorg voor minder last* (rapport), ministerie van Financiën, p. 2, juli 2007.