GRC IN ONTWIKKELING

Meetlat voor beheersing

Waar bevindt een onderneming zich in termen van governance, risk management & compliance? Met behulp van het GRC-ontwikkelmodel kan worden bepaald in welke fase van ontwikkeling de afzonderlijke afdelingen interne controle, risk management, compliance en internal audit zich bevinden, en de mate waarin dit de 'defensie' van de onderneming beïnvloedt.

TEKST SAN CROONENBERG, EDDY VAN DER GEEST EN MICHAEL SCHOEVAART* | BEELD CORBIS

GRC is een veelgebruikte afkorting voor governance, risk management & compliance. De term 'GRC-raamwerk' duidt op het totale beheersingskader van een organisatie. Een nieuwe term voor een oude bekende dus. Het beheersingskader wordt gebouwd rondom processen in de organisatie, met bijbehorende risico's en controls om deze te managen.

'ER IS EEN BREDE BEHOEFTE AAN EEN BENCHMARK OM TE KUNNEN ZIEN WAAR DE EIGEN ORGANISATIE 'STAAT' OP DIT GEBIED.'

THREE LINES OF DEFENSE MODEL

Binnen een GRC-raamwerk zien we veelal een 'three lines of defense-model' met de volgende 'verdedigingslinies':

- **'First line of defense'** ('eerste lijn'), zijnde het lijnmanagement. Dit is direct verantwoordelijk voor risicomanagement en control van de onder haar ressorterende processen.
- **'Second line of defense'** ('tweede lijn'), gevormd door functies en/of afdelingen die het verantwoordelijk lijnmanagement ondersteunen bij de inrichting van de organisatie en de afdelingen (bijvoorbeeld verbijzonderde (groeps-)afdelingen voor risicomanagement, compliance, en interne controle) die beleid formuleren over risicobeheersing en controls op een specifiek vlak.
- **'Third line of defense'** ('derde lijn') is de internal auditfunctie die onder andere de inrichting en werking van de eerste en tweede lijn controleert.

De introductie van de Sarbanes-Oxley Act (SOx) in de Verenigde Staten in 2002 had vergaande consequenties voor Amerikaanse ondernemingen en hun dochtermaatschappijen. Ook zogenaamde *foreign private issuers* (buitenlandse ondernemingen genoteerd aan de New York Stock Exchange) vallen onder de wetgeving. SOx bracht ons de *in control*-verklaring, door velen gezien als dé uiting van het management dat het alwetend handelt. Tegenstanders van de *in control*-verklaring noemen deze 'gebakken lucht' (zie Leen Paape in 'de Accountant' van juli/augustus 2008). Maar zeker is dat de *in control*-verklaring veel teweeg heeft gebracht en het uitgangspunt vormt voor menige organisatie om doelbewust te streven naar een beter functionerend beheersingskader.

GROTE VERSCHILLEN

In het kader van een onderzoek van het NIVRA (vakgroep INTAC) en IIA Nederland zijn in 2010 28 GRC-eindverantwoordelijken geïnterviewd over de positionering van compliance, internal control, risk management en internal audit binnen de bestaande overkoepelende governance van hun organisatie. Volgens de geïnterviewden had hun risk management niet gefaald in de aanloop naar de kredietcrisis van de afgelopen jaren. Opmerkelijk, want waar(om) zijn dan miljoenen verliezen geleden?
Een andere opvallende uitkomst betrof de brede behoefte aan een GRC-'meetlat' of benchmark om te

Groeimodel in vier fasen

Onderstaande algemene kenmerken van de vier fases van het GRC-groeimodel zijn van toepassing op elk van de afdelingen *compliance, internal control, risk management en internal audit*. De kenmerken zijn indicatief bedoeld en niet-limitatief en beschrijven de bekwaamheden (competenties) behorende bij de diverse fasen.

Fase 1 Verkokerd & inconsistent	• Afdelingen zijn recent gevormd en bevinden zich in een ad hoc en ongestructureerd leerproces. • Er zijn geïsoleerde controls en audits op juistheid en wettelijke compliance vereisten. • Rapportages over risico's, controls en audits zijn ongestructureerd en sterk afhankelijk van de kennis en kunde van de GRC-pioniers. • Gebruik van practices is afgeleid van beschikbare (best/good) practices van professionele organisaties. De afdelingen kennen geen eigen (best/good) practices. • Afwezigheid van professionals, structuur en beleid.
Fase 2 Georganiseerd & reactief	• Er vormt zich structuur in de organisatie van de GRC-activiteiten met periodieke herhalingen van de uit te voeren acties. • Planning is echter nog sterk gestuurd op de individuele prioriteitstellingen van het management van de organisatie. • Rapportages over risico's, controls en audits nemen vaste gestructureerde vormen aan. • De GRC-kennis verspreidt zich, maar zit nog met name bij gespecialiseerde functies.
Fase 3 Proactief & gemanaged	• Processen, procedures en policies zijn gedefinieerd, gedocumenteerd en actief gemanaged in de infrastructuur van de organisatie. • De GRC-afdelingen zijn afgestemd en gestroomlijnd met de strategische doelstellingen van de organisatie en de risico's. • De GRC-afdelingen werken samen aan een goede performance en structuur. • GRC-competenties zijn geïnstalleerd en worden vervangen/bijgehouden door kennis te delen tussen de afdelingen.
Fase 4 Geïntegreerd & geworteld	• Zelflerende afdelingen met streven naar continue verbetering van het proces en de activiteiten. • Om strategische doelstellingen te halen wordt zowel interne als externe informatie gebruikt. • Performance naar zelfontwikkelde best practices. • GRC-functies zijn kritieke onderdelen van de gehele governance structuur. • GRC-functies zijn door de gehele organisatie verankerd en bemand door professionele medewerkers. • Performance-meting van de organisatie, de afdelingen en de individuele medewerkers is gericht op verbetering en professionalisering van de gehele organisatie. • Verwachtingen van alle GRC-functies zijn op elkaar afgestemd.

kunnen zien waar de eigen organisatie 'staat' op dit gebied. Voor wat betreft de ontwikkeling van governance, risk management en compliance bestaan grote verschillen tussen organisaties, zowel in de financiële als niet-financiële sector. Een grote slag is gemaakt bij de invoering van de SOx-wetgeving en de daarop volgende implementatie van de Nederlandse Corporate Governance Code. Veel organisaties zijn toen - al dan niet vrijwillig - gestart met het bouwen van een op COSO-ERM (enterprise risk management) gebaseerd beheersingskader en het bijbehorende GRC-speelveld, bestaande uit de overkoepelende *governance, het risk management, de internal control, de compliance en de internal auditfuncties*. De inrichting van dat speelveld verschilt ook per sector.

FINANCIËLE EN NIET-FINANCIËLE SECTOR

Bij financiële instellingen is er specifieke regelgeving (Nederlandse Corporate Governance Code, Basel II, Solvency II - III in aantocht - en de Code Banken) die voorschrijft dat GRC-functies separaat dienen te worden gecreëerd en moeten functioneren. Tot aan de financiële crisis waren er geen redenen om aan te nemen dat governance, risk management, compliance en internal audit in de financiële sector onvoldoende waren geëquipeerd om grote tegenslagen te managen.

In de niet-financiële sectoren is de regelgeving over de inrichting van het GRC-speelveld minder dwingend. Daar zien we recentelijk juist een tegengestelde ontwikkeling: integratie van diverse GRC-functies in gecombineerde afdelingen.
Een van de *lessons learned* van de economische crisis is dat door onvoldoende kennisdeling als gevolg van te strikte scheidingen tussen functies (verkokering), samengestelde risico's kunnen worden gemist.
De nadelen van verkokering kunnen zo de voordelen van onafhankelijkheid teniet doen. Kennelijk vormt een te sterk doorgevoerde organisatorische onafhankelijkheid juist een valkuil voor de beoogde weerbaarheid van ondernemingen voor een economische crisis.

'NAARMATE DE ORGANISATIE ONTWIKKELT WORDEN DE FUNCTIES LANGZAAM VOLWASSENER EN GROEIT HET GEHEEL UIT TOT EEN GEÏNTEGREERD BEWUSTZIJN.'

REGELGEVINGSREFLEX

Waarom is in de Nederlandse regelgeving voor financiële instellingen dan nu de verplichting tot functionele scheiding opgelegd? Het is al vaker vertoond: de regel-

gevingsreflex. Als er iets misloopt wordt de regelgeving aangescherpt.
Wellicht kan het GRC-vakgebied een voorbeeld nemen aan de proef in 2003 met een verkeersplein in Drachten. Bij een onveilig verkeersplein heeft de gemeente de moed gehad om alle verkeersborden en stoplichten te verwijderen. De reguliere verkeersregels gecombineerd met normaal fatsoenlijk weggedrag bleken afdoende om de veiligheid te verbeteren én de doorstroming te bevorderen. Uitzonderingen (*hufterig weggedrag*) werden niet voorkomen, maar voor het gros van de weggebruikers betekende deze proef een verbetering. Het loslaten van een rule-based-benadering voor een principle-based-benadering, waarbij ruimte wordt geboden voor een op een specifieke situatie afgestemde operationele invulling, zoals bij niet-financiële instellingen nu het geval is, zou in de financiële sector evenzeer een gunstige uitwerking kunnen hebben.

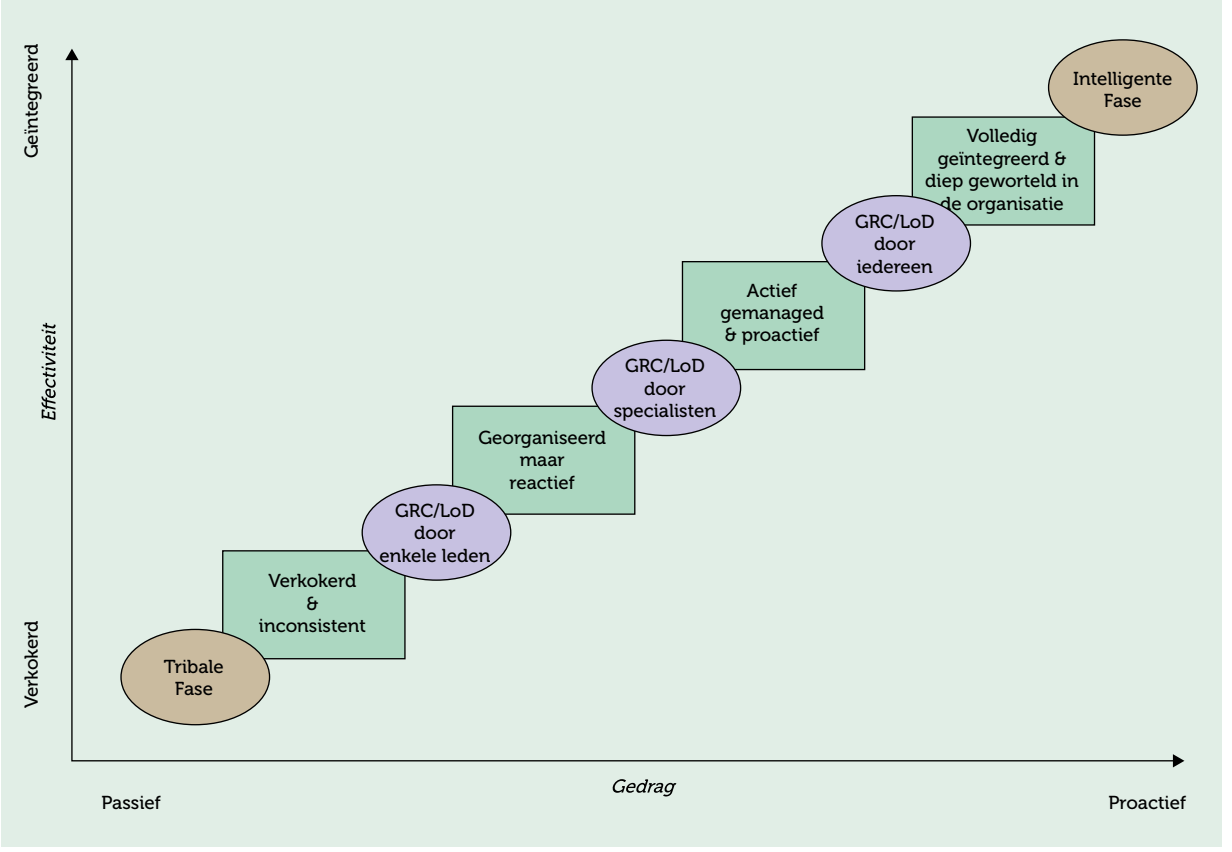
GROEIMODEL IN VIER FASEN

Zoals gezegd bleek uit het NIVRA-IIA-onderzoek dat er grote behoefte bestaat aan een 'meetlat' of benchmark voor de mate van volwassenheid van het totale beheersingskader (GRC) van een organisatie. Dit artikel geeft daartoe een eerste aanzet.
Op basis van de interviewinformatie uit het onderzoek hebben wij de verschillende aangetroffen ontwikkelstadia in beeld gebracht aan de hand van een groeimodel. Naarmate zich meer en complexere problemen én risico's voordoen, verandert de aard van het gedrag van medewerkers van de afdelingen van passief, via reactief verder groeiend naar *proactief* en dit mondt uiteindelijk uit in een *geïntegreerd* en *geworteld* systeem (*zie kader*).

'EEN DUIDELIJKE AGENDERING VAN DE VERVOLGSTAPPEN IS ESSENTIEEL.'

Voor wat betreft de afdelingen compliance, internal control, risk management en internal audit zien we bij aanvang een sterke verkokering van de taken en verantwoordelijkheden. Naarmate de organisatie verder ontwikkelt worden deze functies langzaam volwassener en groeit het geheel uit tot een geïntegreerd en ingebed bewustzijn in alle geledingen van de organisatie. In de figuur is deze ontwikkeling gevisualiseerd waarbij het bouwen van het beheersingskader, gebaseerd op COSO-ERM en het bekende *three lines of defense model* - lijnmanagement, controlfuncties, internal audit (*zie kader*) - verschuift van een probleem (c.q. proces) van enkele 'helden' in de organisatie naar *alle* medewerkers en bestuurders.

Het uiteindelijke doel is dat alle betrokkenen de algemene principes van het *in control* zijn begrijpen en van nature toepassen, zonder dat hiervoor formele beleidsregels of vragenlijstjes worden afgecheckt. GRC wordt als het ware opgenomen in het DNA van de organisatie.



GRC-groeimodel

Groeimodel per deelfunctie

	Fase 1	Fase 2	Fase 3	Fase 4
	Verkokerd & inconsistent	Georganiseerd & reactief	Proactief & gemanaged	Geïntegreerd & geworteld
Compliance	• Per deelgebied policies. • Pre-SOx-fase. • Compliance gedreven vanuit juridische zaken.	• Steeds meer policies. • Periodieke toetsing van controls (als aparte activiteit). • Afzonderlijke compliance functionarissen in de lijn.	• Periodieke toetsing is onderdeel van reguliere controls (niet toegevoegd). • Lijn rapporteert periodiek (Letter of Representation) over naleving van wet/regelgeving/policies aan hoger management.	• Compliance-taak geheel in de lijn verankerd. • Organisatie is zelf in staat compliance met interne en externe regels te toetsen en te borgen. • Alleen uitzonderingen worden gerapporteerd.
Internal control	• Per operationeel en financieel deelgebied policies. • Pre-SOx-fase. • Controls op compliance gedreven vanuit juridische zaken.	• Steeds meer relevante policies. • Periodieke toetsing van controls (als aparte activiteit) voor operatiën en financiële processen. • Afzonderlijke compliance functionarissen in de lijn.	• Periodieke toetsing is onderdeel van reguliere controls (niet toegevoegd). • Lijn rapporteert periodiek (Letter of Representation) over naleving van operationele en financiële policies aan hoger management.	• Testen van controls en monitoring van geheel terug in de lijn. • Organisatie is zelf in staat operationele en financiële controls met interne en externe regels te toetsen en te borgen. • Alleen uitzonderingen worden gerapporteerd.
Riskmanagement	• Vaste set risico's welke jaarlijks worden geëvalueerd in relatie tot bestaande controls (matrices). • Nog geen vooruitziende blik op risico's (het overkomt de organisatie).	• Vaste set risico's welke jaarlijks worden geëvalueerd. • Incidenten worden gedeeld. • Risicobestrijding is vaak nog *damage control.*	• Focus op top 10-risico's. • Periodieke rapportering met focus op mitigerende maatregelen. • Ook aandacht voor positieve risico's (kansen). • Best practices worden gedeeld.	• Risicomanagement weer terug in de normale lijn. • Elk proces/ afdeling/functie brengt uit zichzelf risico's (+/-) in kaart en beheerst deze of mitigeert gevolgen. • Alleen incidenten worden gerapporteerd.
Internal audit	• Vaste auditplanning op basis van rotatie en vooraf vastgesteld schema. • Controls op compliance wet- en regelgeving vormt aanzienlijk onderdeel van het geheel.	• Vaste auditplanning op basis van rotatie en vooraf vastgesteld schema. • Reagerend op incidenten en deze ad hoc mee auditen op basis van beschikbare capaciteit.	• Risicoanalyse is de basis voor de auditplanning en richt zich op de risico's met de hoogste impact (inclusief compliance en key-controls). • Voldoende ruimte voor flexibiliteit in planning en capaciteit.	• Risicoanalyse is continue proces en vormt basis voor auditplanning. • Continuous auditing op basis van goedwerkend ERM-systeem en XRBL rapportages. • Continue flexibiliteit in planning en capaciteit.

PER DEELFUNCTIE

Naast het algemene groeimodel zijn voor de afdelingen compliance, interne controle, risk management en internal audit per fase kenmerken van de hoofdactiviteiten van de afdelingen in kaart te brengen. Zie daarvoor het kader 'Groeimodel per deelfunctie' bij dit artikel. Dit overzicht met kenmerken is niet limitatief bedoeld maar richtinggevend en dient als referentiemodel voor organisaties om hun afdelingen aan te meten.De beide tabellen helpen een onderneming te benchmarken aan de hand van de kenmerken die behoren bij het 'groeien' naar een meer volwassen organisatie. Meer volwassen betekent dat een organisatie vlekkelozer en flexibeler kan inspelen op een snel veranderende omgeving, waar nieuwe risico's zich plotseling kunnen voordoen. Hoe verder een onderneming is verwijderd van fase vier, hoe groter de kwetsbaarheid voor tegenvallers en *downturns* zoals de recente kredietcrisis.

Bestuurders van ondernemingen doen er daarom goed aan niet te lang te blijven stil staan bij de gerealiseerde fases en momentum vast te houden bij de doorontwikkeling van GRC. Een duidelijke agendering van de vervolgstappen is daarbij essentieel. □

Noot

* San Croonenberg is coördinator internal audit bij de NBA. Eddy van der Geest is senior auditor bij Tata Steel. Michael Schoevaart is directeur kennismanagement bij Balance, bureau voor project- en interim-management sinds 2008. Inspiratie over *GRC-maturity* hebben de schrijvers opgedaan aan de hand van het Red Book van de Open Compliance & Ethics Group (zie www.oceg.org).
Het *Internal Audit Capability Model for the public sector* kan worden gedownload van de webpagina van The IIA Research Foundation, www.theiia.org.