Hubèrt Aelbers RE CISA GRCP
Drs. Marinus de Pooter RA CMA CFM CIA CRMA

Internal Audit kan bij uitstek een verbindende rol spelen bij governance, risk management en compliance (GRC) vraagstukken. In dit artikel de meerwaarde van het GRC Capability Model (GCM) van de Open Compliance and Ethics Group (OCEG) voor de kennis en vaardigheden van internal auditors in die rol.

OCEG's GRC Capability Model

Open Compliance and Ethics Group is een 'open source' platform, dat momenteel ruim 40.000 aangesloten leden telt (zie www.oceg.org). Centraal staat het begrip 'principled performance'. Volgens OCEG gaat dat vooral over bedrijfsdoelstellingen behalen, verwachtingen van stakeholders waarmaken, risico's managen, kansen benutten, interne beloften nakomen en binnen de opgelegde (wettelijke) externe kaders blijven. Vanuit deze context definieert OCEG GRC als: 'a capability that enables an organization to reliably achieve objectives while addressing uncertainty and acting with integrity'.
Het GCM gaat over de geïntegreerde governance, management and assurance of performance, risk and compliance. Zo gedefinieerd betreft het de brede verantwoordelijkheid van de CEO, het complete terrein van risk management en compliance en daarmee het hele werkveld van de internal auditfunctie. GRC certify (www.grccertify.org) is een aan OCEG gelieerde organisatie, die persoonlijke certificeringen toekent. Op dit moment bestaan de GRC Professional (GRCP) en GRC Auditor (GRCA) certificeringen, waarvoor ook in Nederland trainingen kunnen worden gevolgd. In ontwikkeling zijn de GRC Enterprise Architect (GRCE) en GRC Master (GRCM) certificeringen.

GRC Capability Model
OCEG's GCM bestaat uit de volgende acht componenten (met bijbehorende elementen), die uitvoerig worden toegelicht in het *Red Book*. Uit *figuur 1* blijkt dat het model veel gemeen heeft met andere standaarden, zoals COSO ERM, ISO 31000 en FERMA.

GRC in de praktijk
GRC-vraagstukken gaan over de vraag hoe aan de verwachtingen en eisen van belangrijke interne en externe stakeholders kan worden voldaan. De organisatieleiding doet dit door te zorgen voor deugdelijke managementacties en beheersmaatregelen (het opstellen van huisregels of volgen van externe codes), die dienen te worden nageleefd. In de praktijk gaat het daarbij om dezelfde basisvragen als bij enterprise risk management (ERM):
- welke regels zijn nodig? Versus het aan het professionele inzicht en gezonde verstand van de managers en overige medewerkers zelf overlaten;
- welke regels dienen centraal te worden vastgesteld? Versus de invulling ervan aan het lokale management zelf overlaten.

Deze vragen gelden voor alle aspecten van de beleidsrealisatie en bedrijfsvoering, zoals rendement, veiligheid, continuïteit, innovatie, integriteit, informatiebeveiliging, et cetera. Omdat veel functies betrokken zijn bij het ontwerpen, implementeren, uitvoeren, monitoren en toetsen van deze regels, gaat GRC vooral ook over het effectief regelen van de regie over het interneregelgevingsproces. OCEG bezigt in dit verband termen als coordination, integration en federation.

Bijzonderheden van het OCEG-model
Later in dit artikel wordt nader ingegaan op de vraag in hoeverre OCEG's GCM internal auditors kan helpen bij het geven

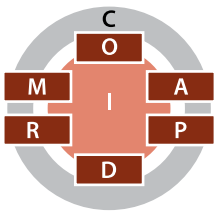
van assurance en aanbevelingen. Ter voorbereiding eerst een aantal bijzonderheden van het GCM, ook in vergelijking met andere standaarden.

1. Het GCM stuurt aan op acht resultaatgebieden, die overigens geen directe link hebben met de acht componenten. Wat daarbij opvalt is de business focus.
2. Het GCM heeft aandacht voor de stakeholders en hun belangen. Het gaat erom dat de organisatieleiding hierin duidelijke keuzen moet maken (prioritization). Increase stakeholder confidence wordt genoemd als belangrijk voordeel van principled performance.
3. In het GCM is ruimere aandacht voor de omgeving (external context) vergeleken met het COSO-ERM-model, dat meer de nadruk legt op de internal environment.
4. De GRC-definitie van OCEG (capability) drukt goed uit dat het eigenlijk gaat om een competentie. Dit is sterker dan de COSO-ERM-definitie, die meer gericht is op de procesgang (process).
5. Interessant is dat bij de componenten Proact, Detect en Respond niet alleen wordt gekeken naar de negatieve kanten. Zo gaat het bijvoorbeeld niet alleen over preventive acties en maatregelen 'to reduce undesirable conduct, conditions or events', maar ook over de incentive kant. OCEG benadrukt het bevorderen van gewenst gedrag (beloningen, ethisch handelen, et cetera.). Zo komen niet alleen corrective acties en maatregelen aan de orde 'to correct undesirable conduct, conditions or events', maar wordt ook aandacht besteed aan de rewardingkant. Dat laatste onderdeel is in het *Red Book* overigens nog under development.
6. De component Organize ontbreekt bij veel standaarden. Dit blijkt dit een uitermate wezenlijk onderdeel, omdat in de praktijk meerdere afdelingen en functies bij GRC betrokken zijn. Het goed voeren van de regie betreft niet alleen het passend inrichten van de interne beheersing, maar ook het slim vergaren van assurance, het geïntegreerd rapporteren over de bevindingen, et cetera.
7. OCEG maakt inzichtelijk dat veel organisatieleidingen worstelen met het goed georganiseerd krijgen van hun interne spelregels (policy management). En met de informatievoorziening over de reeds gerealiseerde en nog beoogde transacties. Het *Red Book* benadrukt dan ook het belang van goed informatiemanagement (definities, 'single source data', beheer van stambestanden, et cetera). Daarbij gaat het dus niet alleen over historische gegevens, maar ook over de beschikbare kennis met betrekking tot de toekomst.
8. De achtergrond van OCEG is in belangrijke mate compliance management. Dat komt bijvoorbeeld naar voren in de gerichte aandacht voor requirements. Deze vereisten kunnen zowel zijn opgelegd door een externe wet- of regelgever danwel zelfgekozen richtlijnen of afspraken betreffen. Denk bij dit laatste bijvoorbeeld aan overeenkomsten met cliënten of afspraken met werknemers. Meer dan andere standaarden legt GCM ook de focus op interne en externe onderzoeken van incidenten (investigations) en herstelacties (remediation).
9. OCEG definieert het verschil tussen kansen en bedreigingen als volgt: 'Opportunities are events and conditions that, on balance, contribute to reward (which is a measure of the desirable effect of uncertainty on objectives) – while threats are events and conditions that, on balance, contribute to risk (which is a measure of the undesirable effect of uncertainty on objectives)'. Wij vinden dit expliciet kijken naar de upside, de opportunities een duidelijke plus ten opzichte van bijvoorbeeld de COSO-standaarden.
10. In het *Red Book* wordt ook het beoordelen van de aanvaardbaarheid van de risk/reward balans (inherent, current residual en planned residual) aan de orde gesteld. Daarbij zou echter duidelijker benadrukt kunnen worden wie dan die afwegingen dient te maken.
11. Risicoblootstelling is meer dan het simpelweg vermenigvuldigen van een kans met een effect. Evenals andere modellen heeft ook het GCM geen remedie tegen het gegeven dat het inschatten van risico's zowel lastig als relatief is. De mate van de risicoblootstelling blijft een (inter-)subjectieve mening. En de interconnectiviteit van risico's maakt het er niet doorgrondelijker op.

Voordelen voor de internal auditor

Welke meerwaarde heeft OCEG's GCM nu voor internal auditors? Het GCM kan een duidelijke bijdrage leveren aan het ontwikkelen van kennis en vaardigheden. De OCEG-publicaties geven de internal auditor handvatten bij het beoordelen van en adviseren over GRC. Zo geeft het *Red Book* best practiceaanbevelingen op onder meer de volgende gebieden:

1. (IT-)governance: het begrijpen van de organisatiebrede governance, risk and compliance frameworks (en de mate van integratie hierbij) die de eigen organisatie toepast. Het GCM geeft de auditor handreikingen om in kaart te brengen en te beoordelen hoe de organisatieleiding kansen benut en bedreigingen beheerst. Daarbij helpt vooral de aandacht die wordt besteed aan de regie (de component organize). We zien dat het gebrekkig coördineren, integreren en or-



CONTEXT
C1 - External Context
C2 - Internal Context
C3 - Culture
C$ - Objectives

INTERACT
I1 - Info Management
I2 - Cummunication
I3 - Tecnology

ORGANIZE
O1 - Commitment
O2 - Roles
O3 - Accountability

DETECT
D1 - Detective Actions & Controls
D2 - Notification
D3 - Inquiry

MEASURE
M1 - Context Monitoring
M2 - Performance Monitoring
M3 - Systemic Improvement
M4 - Assurance

ASSESS
A1 - Identification
A2 - Analysis
A3 - Planning

RESPOND
R1 - Responsive Actions & Controls
R2 - Internal Investigation
R3 - 3rd Party Investigation
R4 - Crisis Resonse
R5 - Remediation
R6 - Rewards

PROACT
P1 - Proactive Actions & Controls
P2 - Codes of Conduct
P3 - Policies
P4 - Educations
P5 - Incentives
P6 - Stakeholder Relations
P7 - Risk Financing

Figuur 1. GCM en de acht componenten (Copyright www.oceg.org)

kestreren van GRC in de praktijk zorgt voor suboptimale situaties.

2. Risicomanagement: het in kaart brengen en doorgronden van de wijze waarop organisatiebreed risicomanagement is vormgegeven binnen de eigen organisatie. Het GCM helpt de auditor om te beoordelen in welke mate de organisatieleiding de kansrijkheid en risicoblootstelling vaststelt (alsmede de wijzigingen daarin), die bepalend zijn voor de mate waarop zij hun organisatiedoelstellingen kunnen realiseren.
3. Risicohouding/-cultuur: het begrijpen van de wijze waarop de organisatieleiding risicomanagement in de praktijk toepast. Het GCM is interessant voor de internal auditor, omdat het model expliciet aandacht schenkt aan het bevorderen en belonen van goed gedrag binnen de organisatie.
4. Branchespecifieke kansen en risico's: het begrijpen van de huidige en toekomstige kansrijkheid en risicoblootstelling van de organisatie, mede gelet op de branche waarin zij opereert. De nadruk op het businessmodel sluit aan bij de noodzaak voor internal auditors om vooral de (primaire) bedrijfsprocessen van hun auditees grondig te begrijpen. Daardoor kunnen zij betere gesprekspartners zijn.
5. Beheersingsmodellen: het toepassen van control frameworks bij audit- en consultancyopdrachten, alsmede het monitoren van een effectieve werking van de beheersmaatregelen in deze raamwerken. Het GCM geeft de internal auditor een holistischer beeld van de organisatie door het brede blikveld: niet alleen aandacht voor risico's, maar ook voor kansen.
6. Ethiek en fraude: het identificeren van frauderisico's en het selecteren van de juiste technieken en methoden om fraudes te onderzoeken. Het GCM helpt de internal auditor om de mogelijkheden voor fraude te doorgronden, passende maatregelen voor te stellen, overtredingen te ontdekken en om nadere onderzoeken uit te voeren.
7. Compliance: het begrijpen van de wet- en regelgeving die op de organisatie van toepassing is en van de mogelijkheden om daaraan te voldoen. Het GCM doet de internal auditor beseffen dat het niet alleen gaat om vereisten vanuit wet- en regelgeving (mandatory boundaries), maar dat ook contractueel overeengekomen zaken (voluntary boundaries) relevant zijn.

De weerbarstige praktijk

In het licht van de genoemde voordelen bevelen wij het bestuderen en toepassen van het GCM graag aan. Het is daarbij uiteraard goed om steeds de beperkingen van standaarden en modellen voor ogen te houden. Uiteindelijk komt het aan op het gedrag en de kwaliteit van (persoonlijk) leiderschap van alle betrokkenen. Daarvoor is het kunnen houden van 'crucial conversations' belangrijk, ook voor internal auditors. Het gaat hierbij over de vaardigheid om gesprekken te voeren over netelige onderwerpen, zoals te optimistische veronderstellingen, (bijna) incidenten en gesignaleerde misstanden. Dit alles op een manier die gericht is op het behoud van de relatie. Dan kan er een high reliability organization ontstaan. <<

Meer weten...

Zie voor meer informatie over de kennis en vaardigheden van internal auditors: The IIA Global Internal Audit Competency Framework (met name de onderdelen IV. Governance, risk and control en V. Business acumen).

Hubèrt Aelbers is director bij Integrc. Behalve zijn ervaring met complexe SAP-projecten heeft hij uitgebreide kennis van bedrijfsprocessen en GRC-applicaties voor continuous controls monitoring systems. Aelbers is tevens een ervaren trainer in SAP audit, control & security, docent aan de Erasmus Universiteit en is OCEG-gecertificeerd GRC professional trainer.

Marinus de Pooter is eigenaar van MdP | Management, Consulting & Training. Ook is hij associate partner van Blommaert Enterprise, DNV GL Business Assurance en de RedZebra Group. De Pooter heeft ruime internationale management- en consultingervaring in governance, risk management & compliance, internal control, Internal Audit en finance. Hij verzorgt regelmatig trainingen, seminars en gastcolleges over deze onderwerpen.