Internal Audit can play a leading and unifying role in the management of governance, risk management and compliance (GRC). This article discusses how the Open Compliance and Ethics Group (OCEG) GRC Capability Model (GCM) adds value to the knowledge and skills of internal auditors working in the GRC area.

OCEG's GRC Capability Model

The Open Compliance and Ethics Group is a non-profit think tank with more than 40,000 members worldwide (see www.oceg.org). OCEG's raison d'être is to help organisations achieve 'Principled Performance', which means achieving organisational objectives, living up to stakeholders' expectations, managing risks, utilising opportunities, honouring internal promises, and operating within imposed (legal) external frameworks.

Within this context OCEG defines GRC as: "a capability that enables an organisation to reliably achieve objectives while addressing uncertainty and acting with integrity".

The GCM is all about integrated governance, management and assurance of performance, risk and compliance. GCM concerns the broad responsibilities of the CEO, the complete area of risk management and compliance – all key concerns of the internal audit function. GRC certify (www.grccertify.org) is an OCEG associated organisation which grants certifications to professionals. At present the GRC Professional (GRCP) and GRC Auditor (GRCA) certifications can be taken whereas GRC Enterprise Architect (GRCE) and GRC Master (GRCM) certifications are under development.

GRC Capability Model

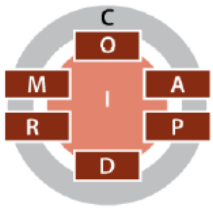
OCEG's GCM exists of eight components (with associated elements), which are explained in detail in the *Red Book*. As shown in *figure 1*, the model has a lot in common with standards such as COSO ERM, ISO 31000 and FERMA.

GRC in practice

GRC is centrally concerned with answering the question of how organisations can meet the expectations and requirements of important internal and external stakeholders. Organizational leadership achieves this through the establishment of sound management controls (setting up their own ground rules and complying with external codes), which the organisation then must abide by. In practice GRC addresses many of the same basic questions as Enterprise Risk Management (ERM):

- What rules are required? (versus leaving it to the professional discretion and common sense of managers and staff)
- Which rules should be established centrally? (versus letting local management decide for themselves)

These questions apply to all aspects of policy execution and business operations; including profit, safety, continuity, innovation, integrity, and information security. Since many functions are involved in the design, implementation, execution, monitoring and testing of these rules, GRC is essentially concerned with the effective control of the internal policy setting process. OCEG uses terms like coordination, integration and federation in this regard.



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)

Specifics of the OCEG-model

The extent to which OCEG's GCM can help internal auditors with giving assurance and recommendations is discussed later on in this article. Firstly, we examine the specifics of the GCM, also in comparison to similar standards.

1. The GCM focuses on eight outcomes – note these are entirely separate to the eight components referenced above. The salient factor is the focus on business performance.
2. The GCM pays particular attention to stakeholders and their interests, emphasising that the executive team needs to make clear decisions regarding them (prioritization). Increased stakeholder confidence is stressed as a key asset of principled performance.
3. The GCM dedicates more attention to the environment (external context) as compared to the COSO-ERM-model, for example, which puts more emphasis on the internal environment.
4. OCEG's GRC definition (capability) strongly conveys that in essence it is all about a competence. This is stronger than the COSO-ERM-definition, which is aimed at the process flow ("Risk management is a process").
5. It is interesting to see that the components Proact, Detect, and Respond emphasise not only the negative sides. They are not solely about preventive actions and measures "to reduce undesirable conduct, conditions or events", but they are also about the incentives. OCEG emphasises the promotion of desired behaviour (rewards, ethics, etc.). Not only corrective actions and measures in order "to correct undesirable conduct, conditions or events" are discussed. Attention is paid to the rewards, too. However, the latter part is still under development in the *Red Book*.
6. Many standards lack the component 'Organise'. This is a critical element though, as in practice multiple departments and functions are involved in GRC. Good orchestration relates not only to the appropriate setup of internal control, but also to the smart gathering of assurance, integrated reporting of findings, and so on.
7. OCEG recognises that many executive teams struggle with well organising their internal 'rules of the game' (policy management). And also with providing information about the already realised and intended transactions. Therefore, the *Red Book* emphasises the

importance of solid information management (definitions, 'single source data', management of master data, etc.). This is not only about historical data, but also about the available knowledge concerning the future.

8. To a large extent the origins of OCEG lie in compliance management. This is evident for example in the focus given to requirements in the framework. Requirements may be imposed by an external legislator or regulator, or they can be self-imposed guidelines or arrangements. Examples of the latter are contracts with clients or agreements with employees. More than other standards GCM focuses also on internal and external research of incidents (investigations) and remedial actions (remediation).
9. OCEG defines the difference between opportunities and threats as follows: ']"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)". In our opinion this explicit focus on the upside, the opportunities, is a clear advantage compared with, for example, COSO standards.
10. The *Red Book* also addresses the assessment of the acceptability of the risk/reward balance (inherent, current residual and planned residual). However, it could be emphasised more clearly who should make that call.
11. Risk exposure is more than simply multiplying probability with effect. Similar to other models, GCM has no solution for the fact that the assessment of risks is both difficult and relative. The level of risk exposure remains a (inter-)subjective opinion. And the interconnectivity of risks does not help to make this process more transparent.

Advantages for the internal auditor

What is the added value of OCEG's GCM for internal auditors? Evidently, the GCM can contribute to the development of their knowledge and skills. The OCEG-publications give the internal auditor guidance for assessing and advising about GRC. The *Red Book* gives best practice recommendations in the following areas:

1. (IT) governance: understanding the organisation-wide governance, risk and compliance frameworks (and their level of integration) applied by their business. The GCM provides guidance for the auditor in mapping and assessing how the executive team seizes opportunities and mitigates threats. The attention paid to direction (the 'Organise' component) is particularly valuable in this respect. It is our observation that deficient coordination, integration and orchestration of GRC will lead to suboptimal outcomes.
2. Risk management: mapping and understanding the ways in which enterprise risk management is established within the auditor's own organisation. The GCM helps the auditor assess the extent to which the executive team has established the (changes in the) chances of success and risk exposures, which determine to which extent they will achieve their organisational objectives.
3. Risk attitude/culture: understanding the way in which the executive team applies risk management in practice. The GCM is useful for the internal auditor, because the model pays explicit attention to promoting and rewarding good behaviour within the organisation.
4. Industry specific opportunities and risks: understanding the current and future chances of success and risk exposures of the organisation, in the context of the sector in which it

operates. The emphasis on the business model matches with the necessity of internal auditors to thoroughly understand the (primary) business processes of their auditees. Hence, the auditors become better sparring partners.

5. Control frameworks: applying these frameworks in assurance and consultancy assignments, and monitoring the effective operation of the controls in these frameworks. The GCM presents the internal auditor with a more holistic picture of the organisation by taking a broad perspective: not only considering risks, but also opportunities.
6. Ethics and fraud: identifying fraud risks and selecting the right tools and methods to investigate fraud cases. The GCM helps the internal auditor to investigate the possibilities of fraud, propose suitable controls, discover violations, and execute further investigations.
7. Compliance: understanding the laws and regulations applicable to the organisation and enabling a compliant corporate response. The GCM makes the internal auditor realise that compliance is not only about requirements from legislation and regulation (the mandatory boundaries), but that also business contracts (the voluntary boundaries) are relevant.

The unruly practice

Given the advantages presented above, we recommend that internal auditors study and apply the GCM, whilst always bearing in mind the restrictions of standards and models. At the end of the day it comes down to the behaviour and quality of (personal) leadership of those involved; it requires the competence to hold 'crucial conversations'; it is the ability to have discussions about difficult topics, such as overly optimistic assumptions, near incidents and identified wrongdoings; all done in a way aimed that strengthens and maintains the relationship. Then a high reliability organisation can arise.

Want to know more…

For more information on knowledge and skills of internal auditors, refer to: The IIA Global Internal Audit Competency Framework (especially the parts IV. Governance, risk and control and V. Business acumen).

Hubèrt Aelbers is director at Integrc. He has many years' experience in the delivery of complex SAP projects, and extensive knowledge of business processes and the specification and delivery of GRC solutions for continuous controls monitoring systems. Further on Hubèrt Aelbers is an experienced trainer in SAP audit, control & security, lecturer at Erasmus University, and an OCEG certified GRC professional trainer.

Marinus de Pooter is owner of MdP | Management, Consulting & Training and partner of The Perfect Fit. He is also associate of Blommaert Enterprise and DNV GL Business Assurance. De Pooter has broad international management and consulting experience in governance, risk management & compliance, internal control, Internal Audit and finance. He regularly conducts trainings, seminars and guest lectures on these topics.

The Dutch version of this article was published in Audit Magazine, issue 2, 2014.