CHAPTER ELEVEN

11 OCEG Capability Model GRC Standards

THE OPEN COMPLIANCE AND Ethics Group (OCEG) is an industry-led nonprofit organization that develops standards guidance and helps enterprises enhance their governance, risk management, and compliance processes. OCEG is a relatively new organization and certainly did not exist at the time of our first edition of this book. With major support from the information technology (IT) systems industry, the OCEG has published several ''standards'' what it calls a governance, risk, and compliance (GRC) capability model. We have placed the word standards in quotes because the OCEG does not have the standards-setting authority that can be found in the American Institute of Certified Public Accountants' (AICPA's) standards or even in some of the ISO 31000 guidance discussed in Chapter 17.

This chapter reviews several of the currently published OCEG guidance materials, including their ''Red Book'' describing their GRC capability model, what they call their ''Burgundy Book'' on GRC capability processes, and their related materials on XML, the extensible marking language used in many Web applications. Many of these OCEG guidance materials are very similar to other GRC and ERM framework information found in other chapters, but some have a slightly different emphasis or approach. Although it is a newer organization, we feel that the OCEG will have a significant impact on GRC processes in future years.

GRC CAPABILITY MODEL ''RED BOOK''

OCEG's term ''Open'' in its name has some special meaning in an information technology (IT) sense. An open system regularly exchanges feedback with its external

environment to continuously analyze that feedback, adjust internal systems as needed to achieve the system's goals, and then transmit necessary information back out to that environment. Closed, unlike open systems, have hard boundaries through which little information is exchanged. Organizations that have closed boundaries often are unhealthy. Examples include bureaucracies, monopolies, and stagnating systems. A common term in many newer, advanced IT systems today, *open* is an appropriate word for this GRC capability model.

The OCEG's GRC guidance is found in a document called their *Capability Model "Red Book"* (www.oceg.org). This basic document, dated April 2009 at the time of our publication, is available through the Internet while an enhanced version is available to subscribing OCEG members. The basic edition contains a complete description of this GRC model but at an additional cost, an enhanced version with templates and other help aids is also available. The capability model is based around a concept called Principled Performance, an integrated GRC approach that we will discuss in the sections following.

The GRC capability model elements view, shown in Exhibit 11.1, represents the heart of the OCEG model. Many of the concepts here are very similar to Committee of

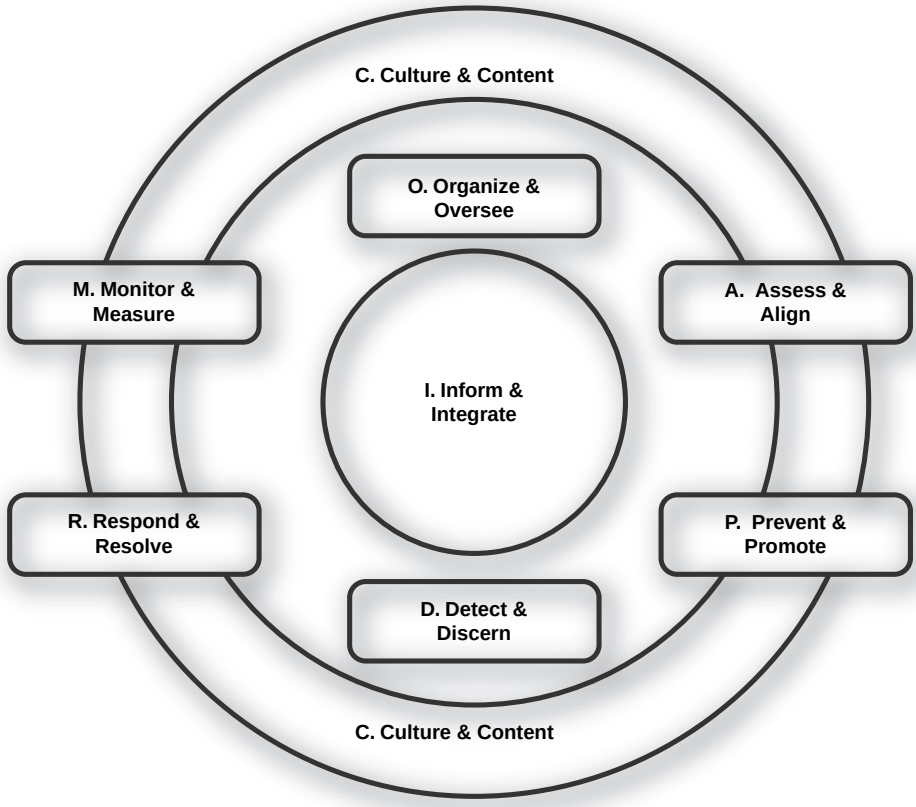

EXHIBIT 11.1 OCEG GRC Capability Model

Sponsoring Organizations (COSO) ERM and the GRC concepts discussed in other chapters, but the more recent industry- and IT-focused view of the OCEG capability model provides a different and somewhat fresh view. Applying the elements of Exhibit 11.1 to this model should help enable an enterprise to:

- Enhance business objectives.
- Enhance organization culture.
- Increase stakeholder confidence.
- Prepare and protect the enterprise.
- Prevent, detect, and reduce adversity.
- Motivate and inspire desired conduct.
- Improve responsibility and efficiency.
- Optimize economic and social value.

OCEG's Principled Performance Concept

OCEG has obtained a trademark for the term Principled Performance® and uses this concept to describe the need for an articulation of an enterprise's financial and nonfinancial objectives to achieve all of the objectives an enterprise chooses to pursue while employing an effective, efficient, and responsive approach to supporting governance, risk management, and compliance objectives. The concept here is that all enterprises must operate within defined external and internal boundaries where outside forces, such as legal and regulatory requirements, establish their mandated external boundaries. The objective here is to integrate GRC principles and objectives to help an enterprise more effectively drive performance.

For an enterprise to achieve the concept of Principled Performance®, it must clearly define its mission, vision, and values and define the objectives it seeks to achieve. It must define how it will pursue these objectives while also addressing risks and uncertainty, protecting and creating value, identifying new opportunities, and staying within defined boundaries of ethical conduct. The enterprise should make these choices transparent to appropriate internal and external stakeholders and attempt to accomplish all of this using an integrated approach to achieve the highest possible levels of performance.

In order to achieve what the OCEG calls Principled Performance®, every entity in an enterprise must define what it feels is ''right'' for it and then do these right things in what they have defined as the correct manner. We have paraphrased this concept from the OCEG materials. It is a high-level objective that goes beyond the traditional concepts of enhancing shareholder value to include desired outcomes that address enterprise stakeholder interests.

These Principled Performance concepts are key elements of the OCEG's GRC capability model as shown in Exhibit 11.1. The following sections describe the elements of that model in greater detail, particularly when they have goals and objectives different from the conventional COSO ERM framework described in other chapters. This GRC capability model outlines at a very high and extensive set of materials and concepts that are part of the OCEG model. The interested reader is encouraged to access the full model through OCEG's previously referenced Web address.

GRC Capability Context and Culture Elements

Located in the surrounding ring of the model as shown in Exhibit 11.1, the objective of this element of the OCEG model is to understand the external and internal business contexts and current culture in which the organization operates, such that the GRC system can address current realities and identify opportunities to adapt the context and culture to define the enterprise's values to better achieve desired outcomes. Using their coding letter C, there are four elements to this section of the model:

C1 External Business Context
C2 Internal Business Context
C3 Culture
C4 Values and Objectives

The GRC capability model defines a set of subelements for each of these. For example, for C3, the model contains the following subelements:

C3.1 Analyze Ethical Culture
C3.2 Analyze Ethical Leadership
C3.3 Analyze Risk Culture
C3.4 Analyze Board Involvement
C3.5 Analyze Governance Culture and Management Style
C3.6 Analyze Workforce Engagement

Each of these is supported by more detailed elements to expand the outline. In addition, the model contains a set of principles and a list of common sources of failure for each as well as guidelines and references for additional support materials.

GRC Capability Organize and Oversee Elements

The objective of this guidance is to organize and oversee the GRC system so that it is integrated with and, when appropriate, modifies existing business processes. The set of elements, marked with the letter O, is located on the upper center of the diagram and consists of the following elements and subelements:

O1 Outcomes and Commitment
  O1.1 Define GRC System Scope
  O1.2 Define GRC System Styles and Goals
  O1.3 Obtain Commitment to the GRC System
O2 Roles and Responsibilities
  O2.1 Define and Enable GRC System Oversight Rules and Accountability
  O2.2 Define and Enable Management Roles and Responsibilities
  O2.3 Define and Enable Leadership Roles and Responsibilities
  O2.4 Define and Enable GRC System Operational Rules
  O2.5 Define and Enable Assurance Roles and Accountability (e.g., internal audit)

O3 Approach and Accountability

O3.1 to O3.5 define further system processes to build the GRC function and establish management approaches to make this an effective business function.

With an outline of detailed sub and sub-sub points, there is sufficient detail here to help an enterprise establish and organize a GRC function. There are good sets of principles and common sources of failure for each to help organize an effective GRC process for an enterprise.

Our objective here is to highlight that the OCEG GRC capability model contains some excellent materials to help an enterprise establish an effective GRC function. We are only highlighting some of the high-level attributes of this model. To further show some examples, Exhibit 11.2 outlines the detailed core subpractices for O2.4.01. This level of detail has been published for the entire model.

GRC Capability Assess and Align Elements

Moving clockwise around Exhibit 11.1, the stated goal of the A section of the GRC model is to assess risks and optimize the organization's risk profile with a portfolio of risks, tactics, and activities. The actions here include risk identification, analysis, and optimization.

The detailed guidance here is very similar to our materials in other chapters. For example, the objective of A1, Risk Identification, is to ''Identify events, forces, and factors that may affect the achievement of business objectives, including those arising with noncompliance with the requirements established by law, standards, internal policies, or other mandatory or voluntary boundaries.''

As with all other sections of the GRC capability model, this section provides outlined details for establishing an enterprise risk management function. In contrast to our materials in Chapter 5 on implementing ERM in the enterprise and others, the section of the model has perhaps a bit more of a legal focus than found in our other COSO ERM materials.

O2.4.01 Define roles and responsibilities for the following key GRC activities:

- Methodology, policy/procedures, standards, vocabulary, and maintenance.
- Risk and requirements identification, analysis, and optimization.
- Initiative implementation/project portfolio management.
- Stakeholder relations.
- Helpline/hotline.
- Investigation and resolution.
- Performance measurement.
- Communications, including public relations.
- Information management.
- Technology.

EXHIBIT 11.2 GRC Subpractices Example: O2.4 Define and Enable GRC Rules

GRC Capability Prevent and Promote Elements

The P or Prevent and Promote section of this capability model has an objective to promote and motivate desirable conduct, and prevent undesirable events and activities, using a mix of controls and incentives. This section has seven elements including codes of conduct, preventive controls, and stakeholder relations and requirements. Many of these materials are similar to materials included in other chapters, such as Chapter 9 on codes of conduct best practices.

Interestingly, P5 here covers an area that is not adequately addressed in COSO ERM, human capital incentives, with objectives to:

P5.1 Foster Ethical Leadership
P5.2 Develop Incentive-Based Evaluation and Promotion Decisions
P5.3 Develop Compensation Plans That Consider Conduct Expectations
P5.4 Develop Reward Programs

Several of these are human capital programs that are not often included in other GRC programs. For example, P5.4.05 states, ''Develop awards or other incentives for contributions by individuals or organization or extended enterprise units that result in reduced compliance failures, enforcement challenges, or other external challenges to the organizations.'' This is interesting guidance that is not often included in such plans.

GRC Capability Detect and Discern Elements

Continuing with our introduction of GRC capability elements, its D section has an objective to detect actual and potential undesirable conduct, events, GRC system weaknesses, and stakeholder concerns using a broad network of information gathering and analysis techniques. This section covers many areas discussed in our other chapters, such as a discussion of ethics hotlines from Chapter 10.

The OCEG section calls for providing multiple pathways to suspicions or incidents of noncompliance or unethical conduct, or to identify concerns about GRC system weaknesses. As part of its hotline guidance, this sections calls for the implementation of a notification system that will alert an enterprise to incidents or suspicions of noncompliance, violations of company policy, or concerns about perceived unethical conduct or GRC system weaknesses.

This section of the OECG guidance provides for hotline and notification processes as well as inquiry and survey processes to inquire about and survey ethics activities. As part of this process, the enterprise should define opportunities for obtaining stakeholder and workforce views about risk, the GRC system, conduct, and an organizational commitment to its stated values. There is good guidance throughout this GRC model, including a standard to establish a survey approach that reduces the burden on survey subjects and provides a consolidated view of information obtained from the workforce.

GRC Capability Response and Resolve Elements

The R or respond and resolve element of the GRC capability model has an objective to respond to and recover from noncompliance and unethical events or GRC system failures, so that the organization resolves each immediate issue and prevents or resolves similar issues more effectively and efficiently in the future. This element has five components:

R1 Internal Review and Investigation
R2 Third-Party Inquiries and Investigations
R3 Corrective Controls
R4 Crisis Response, Continuity, and Recovery
R5 Remediate the GRC System

Many of these procedures go beyond the steps described in our other chapters to investigate violations in enterprise ethics and compliance practices. For example, for R1 on internal reviews and investigations, the guidance is to review and be prepared to investigate allegations or indications of misconduct or GRC system failures to understand the facts, circumstances, root causes, and appropriate resolutions. The principle here is that the board and senior management should never be blindsided, but instead must know in a timely fashion about any issue that can significantly affect the enterprise.

The OCEG standard calls for an enterprise to establish procedures and a core team for inquiring further into and investigating complaints or reports about compliance or ethical issues, as well as for issues detected during ongoing monitoring processes or periodic evaluations of the GRC system. The standard goes on to call for strong procedures to bring certain matters to the attention of senior management or the board. Another guidance standard calls for an enterprise to periodically review any reported incidents and data to identify trends, trouble spots, or installed controls that appear to need revision. The suggested procedures here are stronger than we would expect to find in many enterprises today.

GRC Capability Monitor and Measure Elements

The OCEG component of measure and monitor is located on the upper left side of the Exhibit 11.1 diagram. This OCEG element contains guidance to assign management's specific responsibilities, decision-making authority, and the accountability for achieving system goals. Using the letter M, it consists of the elements to monitor and evaluate the performance of the GRC programs and to initiate systems improvements where necessary.

This element recognizes that the GRC system must be flexible enough to respond rapidly to internal and external changes in the environment in which it operates. The GRC system will be most effective if an enterprise identifies and evaluates anticipated changes in time to plan system alterations. The model recognizes that the failure to respond to any needed context changes may result in the failure of critical GRC system controls.

The standard calls for an enterprise to continually monitor internal and external changes that may have a direct, indirect, or cumulative effect on enterprise GRC processes. For example, the changes in external requirements may include the following:

- Laws, rules, and regulations.
- Administrative guidelines and rulings.
- Significant judicial rulings covering area of interest.
- Regulatory and prosecutorial guidance.
- Consent orders and enforcement activities.
- Industry standards developments or trade association commitments.

This extensive list points out the challenges an enterprise—particularly a large, multinational organization—will face when attempting to monitor such events and rulings. It is often too much to assign such monitoring to one group because of the breadth and diversity of information. For example, some years ago this author was responsible for a compliance committee for a large U.S.-based, 100-plus-years-old corporation with very successful activities in retail, finance, logistics, and other areas. With things like over 75-year-old legal consent decrees that still sort of applied and an ongoing raft of current regulatory issues, monitoring compliance was a major challenge and required the implementation of adequate tools. Processes should be in place that encourage managers at all levels and locations to report potential warning areas to a central GRC administrative group for further investigation and planned actions.

With the steps to perform and implement the GRC program, this element calls for monitoring and periodically evaluating the performance of the GRC system to ensure that it is designed and operated in an effective and efficient manner and is responsive to internal and external context changes. This is the concept of continuous improvement that has been referenced in many places in our chapters on effective GRC and ERM processes. The OCEG GRC capability model discussed in this chapter perhaps goes a bit further in calling for a scheduled periodic reevaluation of the appropriateness of the GRC system design in light of its identified requirements and key risks.

GRC Capability Inform and Integrate Elements

The letter I or what OCEG calls inform and integrate is the last element in out description of the GRC model. In Exhibit 11.1, it is located in the center of the system and has an overall objective to capture, document, and manage GRC information so that it efficiently flows up, down, and across the extended enterprise and to external stakeholders. This calls for the enterprise to develop and implement a wide range of GRC information systems to classify, capture, store, and report processes and activities. While it is not necessary for an enterprise to have one system throughout, all systems in place should be consistent in terms of their taxonomies, formats, and communications abilities.

The construction of a set of GRC supporting systems can be a key factor in the success of any total GRC information and may be one of the key challenges to achieving

success. Similar to many COSO ERM concepts discussed in other chapters, an enterprise must capture and classify a wide variety of disparate data and information and also must have the ability to capture those materials for analysis and to respond to inquiries.

We have not yet reached the point where an interested manager can Google a request for ''OCEG GRC Compliance Control Systems'' and receive a list of appropriate offering vendors in return. There are many approaches for solutions here but few obvious single solutions. A possible area of solutions can be found through the example of hospital electronic medical record systems (EMRS) that capture every activity of a medical patient, from laboratory test results, to doctor's notes, prescribed medications, and more, for later retrieval on the EMRS for both current use and archival purposes. An effective GRC capability model information system will have many of these elements.

This and the preceding sections have outlined the elements of the OCEG GRC capability model on a very high level. Some are very similar to the GRC and COSO ERM processes discussed in other chapters. Others call for a more detailed and sometimes more administrative controls–oriented approach. Our high-level description, however, does not do justice to the full study that can be found in the 240-page publication, in its basic form, describing the OCEG GRC model with much more detail in the extended document. The interested reader is encouraged to further investigate the OCEG GRC model.

OTHER OCEG MATERIALS: THE ''BURGUNDY BOOK''

A visit to the OCEG Web site allows open access to a variety of related OCEG materials, with some for general review and others for subscribers. Of particular interest may be what is called their ''Burgundy Book,'' an assessment document to support their GRC capability model guidance discussed in these previous sections. The informal name for the OCEG capability model publication is called the ''Red Book'' although we have referred to it here as the GRC Capability Model.

Another OCEG release, the purpose of the ''Burgundy Book'' is to provide GRC professionals with a common set of assessment procedures that align with the previously outlined OCEG GRC capability model as well as guidance on what can be expected during an assessment of any GRC system. The goals of this publication are to help an enterprise to evaluate the design and operating effectiveness of their GRC system and to reduce the cost of such evaluations by providing procedures to aid in any such evaluation. A further goal of this publication is to raise the overall level of maturity and quality of an enterprise's GRC processes by helping to create prioritized improvement plans and to provide an external source for the judgment and recognition of these practices.

The Burgundy Book publication includes other procedures and templates for evaluating a GRC system. Although these materials are based on the GRC capability models described previously, they can be useful reference tools for any similar evaluation. Both the ''Burgundy Book'' and other materials found on the OCEG Web site provide a good set of GRC reference materials.

LEVEL AND SCOPE OF THE OCEG STANDARDS-SETTING AUTHORITY

As we have emphasized throughout this chapter, the OCEG at present does not have the standards-setting authority found in the PCAOB, ISO, or many others. In addition, although the OCEG has released some strong guidance materials, that information still does not have the level of recognition that is found through the IIA's or ISACA's professional internal audit standards. Nevertheless, we feel that the importance of the OCEG and its guidance materials will only grow in future years and as concerns and need for effective GRC processes grow.

A major strength of the OCEG is that it is totally a volunteer organization managed by staff members from sponsoring organizations and formed into an OCEG leadership council. Sponsors here include the major public accounting firms such as PricewaterhouseCoopers (PwC) and Grant Thornton. In addition, there are many major IT-industry leadership sponsors from such firms as Oracle and SAP as well as primarily U.S. industry sponsors from such firms as AON, the major insurance company, and the retailer Wal-Mart. If there is any concern here, it appears that the OCEG is more of a United States–based and not truly international organization based on its sponsoring organizations and committee members. In our global world today, we need more of an international focus.

The interested professional may want to use this OCEG material as an additional source of reference beyond our previously referenced COSO ERM materials. It is an extensive set of guidance materials that we can only expect will grow in importance in future years.