Public Draft Version 1.0

Governance, Risk Management, and Compliance: An Operational Approach

A Compliance Consortium Whitepaper

Bill Zoellick
Ted Frank
May 16, 2005

Abstract

The Compliance Consortium has found that it is critically important for boards of directors and for senior management to become actively involved in setting governance, risk management, and compliance objectives. Since the range of governance, risk management, and compliance concerns is very broad, boards and management need a way to organize and prioritize objectives. This paper provides an operational approach to setting objectives and to creating and monitoring the programs to attain them. It also includes a list of key questions that board members and management can use as a way to begin assessment of an organization's governance, risk management, and compliance programs.

This paper was prepared by the Compliance Consortium with assistance from The Gilbane Report (www.gilbane.com)

Governance, Risk Management, and Compliance: An Operational Approach

A Compliance Consortium Whitepaper

Executive Summary

Boards of directors and senior management are generally aware of the need for active engagement in setting objectives and overseeing programs associated with governance, risk management, and compliance (GRC). The Compliance Consortium has found that such engagement is most successful when the board and management treat GRC as a distinct area of focus, standing on the same level as other principal organizational objectives.

The rationale for this kind of high-level attention to GRC objectives grows out of the unique nature of these objectives. Even though GRC objectives and operations are dispersed across the organization and integrated with other operational objectives and activities, they also stand apart as a distinct set of concerns. Just as important, GRC objectives share common characteristics, making it possible to manage GRC as a coherent organizational focus.

Once boards and management accept the importance of high-level management of GRC objectives, they must confront the problem of how to accomplish such management, since the range of concerns is broad. The Compliance Consortium has defined a set of seven operational concerns—drawn from the US Sentencing Commission guidelines for effective compliance and ethics programs—that can serve as a high-level framework that boards and senior management can use to organize and manage GRC operations. This paper describes the seven operational concerns.

This operational approach to GRC creates a foundation that enables directors and managers to evaluate existing GRC programs within an organization. The paper includes a list of a dozen questions that directors and managers can use to frame such an evaluation. The paper closes with a brief description of other, more detailed and specific GRC frameworks that can be used in a complementary relationship with the high-level, operational approach described in this paper.

Table of Contents

Organization, by its very nature, contains … powerful factors of misdirection. To overcome these obstacles requires more than good intentions, sermons, and exhortations. It requires policy and structure. It requires that management by objectives be purposefully organized and be made the living law of the entire management group.

– Peter F. Drucker
Management: Tasks, Responsibilities, Practices
1974

A ship in port is safe, but that's not what ships are built for.

– Grace Murray Hopper

Over the past few years board members and senior managers have been required to deal more consistently and more carefully than ever before with matters of governance, risk management, and compliance. These requirements have been particularly noticeable in mid-sized and larger public companies due to deadlines imposed by the Sarbanes-Oxley Act. But increased emphasis on governance, risk management, and compliance (GRC) has spread more broadly than that. It also includes private companies seeking debt financing as well as non-profit organizations seeking foundation support. Boards and management of any kind of organization, of almost any size, must be able to make the case that they are driving the car, know where it is going, and can keep it on the road.

Years of working with hundreds of organizations of all kinds and all sizes has led the Compliance Consortium to an insight that boards and managers can use to make governance, risk management, and compliance efforts more effective. The insight is at once simple and radical: *Governance, risk management, and compliance must be treated as a separate area of concern by boards and management. Even though GRC is part of everything the organization does, effective management requires treating GRC as a unique set of objectives and associated processes.*

Given this insight, the Compliance Consortium confronted the question of how boards and managers can put the insight to use. What does it mean operationally? That is the question addressed in this paper.

Governance, Risk Management, and Compliance: A Definition

It is worth spending a moment to talk about what "governance," "risk management," and "compliance" mean in the context of this discussion, since the terms—particularly "risk management"—are used in many different ways.

Governance

It is easy to fall into the trap of regarding governance as a strictly internal activity and as an activity that is primarily directive, rather than responsive. Governance, as most people would agree, is ***the process by which the board sets the objectives for an organization and oversees progress toward those objectives***. The "trap" consists of focusing on the

"oversees progress" part of this definition without paying enough attention to the process of setting objectives.

Governance involves not only driving the car, but also knowing where the organization needs to go and responding to hazards along the way. Governance requires understanding of the motivations and expectations of the different constituencies that the organization is responsive to—investors, capital markets, donors, business partners, governments, the public, and so on. Governance requires looking outside the organization as well as within it.

Once the board sets organizational objectives, it must turn to the second part of governance, which focuses on defining oversight responsibility and high-level processes to ensure that the organization actually meets the desired objectives and is, in fact, responsive to the external constituencies.

More simply, governance is the set of processes that keeps the organization alive, responding as it must to the world that it lives in and regulating the internal information flows and decision processes that ensure that its responses are timely and appropriate.

Risk Management

"Risk management" means different things in different contexts. It can mean hedging investments, buying insurance, quality control, and more. Common to all these definitions is the notion that risk management is part of the process of making decisions. Ultimately, risk management supports *risk taking* and the organization's ability to compete.

For board members and senior managers, risk management has become more visible over the past five years. In many organizations, it was not long ago that "risk management" was handled by the legal department. The understanding of risk was as something to be contained and, if possible, eliminated.

However, as Navy Admiral and computer pioneer Grace Murray Hopper noted, "A ship in port is safe, but that's not what ships are built for." Or, more bluntly, "Nothing ventured, nothing gained." Steven Root, Northrop Grumman's Chief Internal Audit Executive from 1981 to 1995 put it this way: "Risk is the degree of uncertainty accompanying a given course of action. Prudent managements will do what they can to manage that risk to tolerable levels. In the end, however, management must be willing to accept the possibility that what it intends in the way of results may not be achieved. Willing and knowledgeable risk acceptance is what risk taking is all about." [1] Risk management enables knowledgeable risk acceptance.

The old view of risk—as something that the legal department took care of or that you managed by buying insurance—is not really displaced by the view of risk as something to be accepted and managed. What has happened instead is that board members and senior management are using the language and techniques of risk management to address a much broader range of organizational concerns.

There are, of course, many kinds of risks that an organization must deal with: market risk, credit risk, foreign exchange risk, risk of catastrophic loss, and so on. Clearly, board members and senior management need some way of grouping these risks to make them manageable. The old technique of treating all relevant risk as "legal risk" was clearly too simple, but going to the other extreme and treating each risk as a separate dragon that must be slain cannot work either.

Categorizing Risk

It is important to keep two things in mind when grouping risks. The first is that risks are tied to objectives—they are a measure of the chance that the organization will not achieve its objectives. Consequently, it is useful to separate risks related to different kinds of objectives. It is useful, for example, to distinguish between strategic risks and operational risks. The differences between the two categories of objectives translate into different ways of managing risk.

The second concern in grouping risks is that it is useful to segregate risks that, apart from objectives, are managed with radically different tools. For example, even though many organizations could reasonably argue that financial risk is part of their overall operational risk, it makes sense to treat financial risks as something special. The reason is that the tools and methodologies for managing financial risk are so specialized and different from those used for most other operational risks.

Taking both sets of considerations into account, the Compliance Consortium has identified four categories of risk that boards and senior management typically attend to. These categories closely parallel the kinds of risk identified by other organizations such as the Committee of Sponsoring Organizations of the Treadway Commission (COSO).[2]

Strategic Risk

The risk of not achieving the organization's longer range, strategic objectives. Here are examples of strategic objectives for different organizations:

- Maintain an annual return on employed capital of 16%
- Expand the product line to serve the enterprise market and develop a sales channel for that market
- Obtain conservation easements or equivalent protection for at least half of the offshore islands along the coast of Maine over the next fifteen years

Operational Risk

Risk associated with the effectiveness and efficiency of operations, including profitability or other performance measures. Examples include:

- Supply chain delays or failures
- Difficulty in hiring or retaining staff
- Equipment failures
- Unanticipated defect rates

Financial Risk

The risk associated with changes in factors such as interest rates, commodity prices, stock prices, and exchange rates.

Legal and Regulatory Risk

This category includes several related kinds of risks:

- The risk that the organization is not in compliance with regulations or other compliance standards.
- The risk that regulations—or the current approach to interpreting regulations—will change to create adverse consequences for the organization.
- The risk of adverse litigation.

Given these four general categories of risk, what, then, is "risk management?" COSO offers the following definition in its *Enterprise Risk Management—Integrated Framework:*

> *Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in a strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.*[3]

Breaking this definition into its key elements, the important components of risk management are:

- Board and senior management are involved
- Risk is tied to strategy
- Risk management spans the enterprise
- Risk management reflects the organization's risk appetite
- The goal is reasonable assurance, not certainty
- The focus is primarily on objectives (and only secondarily on process)

Compliance

With the passage of the Sarbanes-Oxley Act, the Health Insurance Portability and Accountability Act (HIPAA), and dozens of industry specific regulations and initiatives, compliance has emerged as a critically important concern for boards of directors and management. Certainly, compliance is a component of regulatory risk management. But it also plays a central role in the management of operational, financial, and even strategic risks.

Broadly understood, compliance is the mechanism that makes governance work. It is compliance with the organization's own required procedures that enables management of the risks that endanger the entity. Monitoring and supporting compliance is not just a matter of keeping the regulators happy; it is the way that the organization monitors and maintains its health.

In many public companies, the substantial expenditures and attention committed to meeting Sarbanes-Oxley Section 404 deadlines has distorted this understanding of compliance, turning it into an end in itself, driven by external demands. This is a mistake. Compliance efforts will be effective and sustainable only in organizations where compliance emerges from an ongoing board-level engagement in governance and risk management, and where compliance is the means to support governance and risk management. Put more simply, governance, risk management, and compliance are a package deal.

GRC as a Distinct Enterprise Focus

As noted at the outset of this paper, the key insight emerging from the hundreds of engagements comprising the collective experience of Compliance Consortium members is that boards and senior management should address GRC as a distinct enterprise focus, standing apart from other high level concerns such as return to shareholders, market expansion, effective investment in information technology, depth of ability on the management team, and so on.

The Consortium recognizes that for many companies, placing this level of emphasis on GRC as a distinct area of activity would constitute a change from current practice. Typically, the responsibility for managing the different kinds of risk—strategic, operational, financial, and legal and regulatory risk—is dispersed across a range departments and reporting relationships. The CFO carries responsibility for the financial reporting, other risks are managed within the human resources department, yet others are the domain of the legal or compliance department, and much of the rest is spread across operating units.

What lies behind the Consortium's assertion that organizations should change these current practices? What are the advantages of bringing these different responsibilities together? And, finally, if one accepts that this really is a good idea, how would an organization go about doing it?

We will start with the "why?"—what are the reasons to treat GRC as a distinct board-level and senior management focus? Once we have some answers to "Why?", we can turn to "How."

The Characteristics of GRC

Even though the fundamental concerns and activities associated with governance, risk management, and compliance are dispersed across the organization and integrated with daily operations, these GRC activities have a different "flavor," arising from their orientation toward a different end point.

As a simple example, consider management of e-mail. In most organizations, e-mail has displaced the paper inter-office memo as the way to coordinate activities. One Fortune 50 company, for example, uses e-mails to acknowledge transactions between subsidiaries. The e-mail serves as proof that the business on the receiving end has approved the transaction and will book its end of it. From the standpoint of the people doing the accounting, the e-mails help the subsidiaries balance receivables and payables. They are a convenient way to get the job done.

From the standpoint of the corporate parent, however, the e-mails take on a different aspect. They are records—essential information required to produce and audit the consolidated financial statements. The e-mails—a small part of a massive flow that includes notices of meetings, draft correspondence, jokes, office gossip, and more—must be archived and managed just like a purchase order or a receiving report.

Making an e-mail record management system like this work requires recognizing that there are two different objectives that must be satisfied. The operational objective is to get the job done quickly and efficiently. The GRC objective is to ensure that the record is

identified, classified, and retained. The objectives are intertwined and operate in parallel and simultaneously, but they are distinct and must be managed as such.

There are thousands of examples like this in organizations of even modest size and complexity, comprised of approval cycles, cross-checks, reviews, budget comparisons, and so on. In each instance there is an operational or strategic objective wrapped together with one or more objectives related to governance, risk management, or compliance.

Even though the operational and strategic objectives are extraordinarily diverse, reflecting the broad range of activities in a complex organization, the GRC objectives and activities have a distinct flavor. The flavor arises from a set of characteristics that are common across GRC objectives and activities. It is the existence of these common characteristics that makes it possible—perhaps even necessary—to treat GRC as a distinct area of enterprise focus. The common characteristics include …

Complex Accountabilities

> *When we try to pick out anything by itself, we find it hitched to everything else in the Universe.*
>
> *-- John Muir*
> **My First Summer in the Sierra**

What is true for the universe and the Sierra Mountains is also true for governance, risk management, and compliance. This is really at the heart of what makes GRC distinct and unique. While the operational objective tied to any action is often narrowly focused ("send this email to acknowledge receipt of the shipment from the other subsidiary"), the associated GRC objectives invariably address a broader range of accountabilities ("provide the basis for quarterly reconciliation," "simplify consolidation," "provide an audit trail," "provide assurance against financial misstatement.")

The breadth of accountability, in itself, presents an implementation and management challenge. But the situation is made even more complex by the way that the accountabilities point in different directions. Reporting and accountability for GRC objectives typically cuts across departments, roles, and operating units. As a corollary, administration of these cross-organization objectives is necessarily decentralized. The decentralization, in turn, increases the requirement for sophisticated security.

Complex accountabilities also affect reporting requirements, demanding more flexibility to meet the needs of a more diverse set of users.

All of this—the complex groupings of organizational entities creating and depending on information related to GRC objectives, the necessarily decentralized administration of the GRC objectives and operations, and the more demanding security and reporting requirements—differentiates GRC objectives from associated operational objectives, which usually enjoy a more direct, simply hierarchical accountability structure.

At the same time, the complex accountabilities are a common element cutting across apparently diverse sets of GRC objectives, such as compliance with financial reporting regulations and risk management to safeguard organizational information assets.

Complex accountabilities are an initial, strong indication that GRC objectives and associated operations should be managed as a distinct enterprise focus.

A Minority Element Within a Majority of Organization Processes

This characteristic is, in some ways, an artifact of the complex accountabilities. GRC objectives and processes tend to be embedded within more general operational and strategic processes.

For example, financial cross-checks and safeguards are an integral part of the financial reporting process. Similarly, budget controls are integrated into operating decisions. But, as noted above, these control and risk management objectives tend to be more like each other than they are like the operations that they are a part of.

This characteristic of being a "little bit everywhere" is one of the things that GRC processes share. Because this characteristic can make management of GRC operations particularly difficult, it is worth calling out as a special attribute that can require special planning and attention.

Rapid Evolution

The processes and even the objectives associated with governance, risk management, and compliance change very rapidly. In some areas, such as legal and regulatory risk management, this change is "by design."

Of course, rapid change is a characteristic of any area of the organization that is tied to technology; new technology applications and new technology-based threats and problems drive change across the organization. GRC is no exception.

But the rate of change and the course of evolution for GRC objectives is driven by forces that are even less predictable than the course of technology development. The objectives of risk management and compliance are responsive in large part to decisions made by lawmakers, courts, and regulatory bodies. In complying with laws and regulations associated with Sarbanes-Oxley, HIPAA, 21 CFR Part 11, or any one of the many other industry and government regulatory initiatives, the expectation of change needs to be built in from the start.

The Sarbanes-Oxley legislation and accompanying regulations serve as a good illustration how change is "designed into" regulatory compliance. As is true for most legislation, the actual language of the bill passed by Congress is relatively broad. The SEC gave the law specific shape through its regulations—and the regulations change over time. Just recently, for example, the SEC decided to extend Section 404 deadlines for European firms and smaller firms. There will be yet more change as lawsuits generated around Sarbanes-Oxley come to trial and as the regulations are interpreted in the courts. This is the way that regulations are intended to work, but the end result is a regulatory environment that changes year to year, and sometimes even month to month.

As with the complex accountabilities associated with GRC, the pace and the potential range of evolution pushes organizations in the direction of managing GRC objectives with tools and techniques that are fundamentally different than those used for operational objectives.

Externally Measured

The yardstick for GRC objectives comes from outside the organization. This is, of course, true to some extent for other key board and management concerns such as earnings performance. But, even for something as closely watched as earnings, the organization can take steps to manage expectations. That ability to manage and shift the yardstick tends to disappear as the organization deals with regulators, prosecutors, and the courts.

As noted regarding the definition of "governance," these external expectations and requirements come from different sources and can point in different directions. Consequently, the task of responding to these external expectations requires a kind of prismatic measurement capability and understanding.

Unique Implementation Requirements

GRC is also differentiated from other areas of organizational concern and activity by the tools and techniques used to reach the objectives. This differences grow from the factors identified in the preceding paragraphs—the complex accountabilities, existence as a minority component within a majority of processes, the pace and variety of evolutionary change, and the need to measure up to somebody else's yardstick. But the implementation differences are more then just an outcome—the implementation requirements associated with GRC are sufficiently different from other things going on in the organization that they have the effect of becoming yet another reason why GRC should be treated as a separate area of focus.

Consider, for example, the reach of a GRC program intended to implement whistle-blower protection across an organization, or a program implementing policies to guard against and detect harassment. These implementations must scale to worldwide reach, must be very easy to use, must be consistently applied, and must be implemented with little or no footprint on client machines. They must also be adaptable to meet unique local requirements while still meeting global objectives.

GRC implementations also tend to touch many different systems within the organization, drawing upon many different kinds of data and information maintained in a variety of information structures and formats.

Such implementation concerns are not, of course, a direct concern for boards of directors and for senior management. On the other hand, they are an operational reality that should shape the ways that boards and management approach the articulation and management of GRC objectives.

The Reasons for High-Level Focus

Given these arguments for treating governance, risk management, and compliance as a coherent, distinct group of organizational objectives, there still remains the question of why this should be a board-level concern and a primary focus for senior management.

One important answer ties back to the definition of governance. The board of directors really does need to set the course and see that it is being followed, and senior management really does need to drive the car.

A more complete answer emerges from consideration of the objectives of risk management. The past five years have produced a sobering range of examples of companies in which the board of directors failed to ensure that risks were managed. In some of these examples the problems have resulted from simple negligence or incompetence, such as in companies that failed to hedge against currency fluctuations when making significant international investments. In other cases such as, most infamously, Enron, the board failed to control the risk of fraud. The lesson is a simple one: Risk management and exercise of independent judgment are among the most fundamental responsibilities of board members.

There is, in addition, the need to ensure that an organization's focus on risk management and compliance is efficient and sustainable. Ultimately, making such judgments requires a company-wide perspective available only to senior management and boards of directors.

An Operational Approach to GRC

Given the insight that governance, risk management, and compliance comprise an internally coherent, unique area of organizational activity, and accepting the assertion that an organization gains advantage when directors and senior management take on GRC as a principal focus, how does an organization set about making that happen?

Put another way, how does an organization's board and senior management organize the many detailed concerns and objectives associated with the different kinds of risk management, coupled with compliance and governance, to create a workable, operational approach to GRC?

Focusing Attention: the US Sentencing Commission Guidelines

In 2004 the United States Sentencing Commission (USSC) issued revised guidelines regarding the USSC's definition of an "effective compliance and ethics program." Federal courts use these guidelines to determine the severity of the sentence that a organization receives if a court determines that fraud or other criminal conduct has occurred in the course of the organization's operations. The guidelines apply to organizations of all kinds—public and private companies, partnerships, pension funds, non-profit entities, and so on.

The reason that the USSC's guidelines for an effective compliance and ethics program are important is that adherence to the guidelines—being able to show that your organization has an effective program in place—makes an enormous difference in the severity of a sentence. Existence of an effective compliance and ethics program, coupled with self-reporting of the violation, can reduce fines by up to 95%. From the court's point of view, existence of an effective program is evidence that the criminal violation is an aberration within an otherwise law-abiding community. On the other hand, failure to have an effective program in place may imply organizational responsibility for the violation.

The opportunity to reduce potential liability by 95% is, from a risk management standpoint, is reason enough to take a look at the USSC's guidelines. But the advantages also extend beyond the reduction of legal risk: The USSC guidelines turn out to be a reasonable, workable basis for building an operational approach to GRC. The guidelines enumerate the following seven high level program requirements.

1. *Standards and procedures to prevent and detect criminal conduct*

2. *Clearly assigned responsibility at all levels (including senior management), adequate resources, and clear lines of program authority*

3. *Personnel screening related to program goals*

4. *Training at all levels*

5. *Auditing, monitoring, and evaluating program effectiveness coupled with non-retaliatory internal reporting systems*

6. *Incentives and discipline to promote compliance*

7. *Reasonable steps to respond to and prevent further similar offenses upon detection of a violation*[4]

Translating Requirements Into Operations

Strictly speaking, the USSC guidelines for an effective compliance and ethics program are focused on the problem of preventing and detecting criminal activity within an organization. Although this is certainly a central concern and objective for management and boards of directors, it is just one element within the larger governance, risk management, and compliance agenda for an organization. Directors and managers must also focus on strategic risks ("Can we expand our presence in Europe?"), operational risks ("Will we be ready to launch the new product next year?"), financial risks ("How do we protect ourselves against possible continued weakness of the dollar?), and broadly defined legal and regulatory risks ("What is our exposure due to e-mail communications and how do we begin to manage it?").

Stating the problem in a slightly different way, it is clear that the immediate focus of the USSC guidelines is relatively narrow. At the same time, it is clear that the substance of the USSC message is that these guidelines cannot simply be handled by the legal department, off in one corner of the organization. To be effective, the guidelines must become a part of the fabric of the organization's operations. Will it be difficult to balance these narrowly defined objectives against the broader concerns within an organization-wide GRC program?

Fortunately, the Compliance Consortium has found that this "problem" is not really a problem at all. Recall that GRC objectives tend to have a distinct character and flavor—that they tend to group together and interconnect with each other. As The Compliance Consortium has worked with companies to implement the USSC guidelines, it has found that this "connectedness" of GRC objectives makes it possible to translate the USSC guidelines into something broader and even more useful. The guidelines, expanded and restated, can be the basis for an operational approach to GRC.

What follows is a list of the core GRC operations that have emerged from the Consortium's efforts. Notice that there is a close correspondence between these operations and the USSC requirements, but that the scope has expanded. These seven fund-

amental GRC operations can support a full GRC program, covering all four categories of risk management.

1. Establish and Support Policies, Procedures, and Controls

The operations related to policies, procedures, and controls create the foundation for the GRC program and ensure that the rest of the program works. The operations include:

- Identifying internal and external demands, risks, and expectations, including government regulations, public opinion, customer expectations, internal risk management goals, quality standards, and so on.
- Identifying common elements across risks, requirements and expectations.
- Mapping relationships and dependencies between risks, requirements and expectations.
- Breaking complex sets of requirements into components that are relevant for particular organizational sub-units and individuals.
- Identifying existing controls that support the requirements and goals.
- Establishing, as necessary, new controls if there are objectives that are not covered by controls.
- Documenting the purpose and operation of all controls

Much of this work may be already underway in many public companies since some of these operations have been started as part of Sarbanes-Oxley compliance. In most cases, however, expanding beyond the Sarbanes-Oxley focus on financial reporting to the full range of policies, procedures, and controls that address enterprise risk will require continued attention to this operational objective.

2. Maintain Centralized Oversight

Centralized, high-level oversight and management of GRC is what this paper is all about. After the organization has identified risks, requirements, and expectations, has mapped them to each other, and finally has separated them into components that can be assigned to groups and to individuals, it should then be possible for the organization to obtain new visibility across GRC goals and operations. What follows are suggestions gathered from observation of the most successful programs:

- Commitment from top-level management must be consistent and must be clearly evident.
- GRC must be managed like any other part of the business, with an emphasis on clearly stated objectives and consistent expectation that those objectives will be met.

3. Maintain Decentralized Administration and Accountability

The requirement for centralized oversight, with its emphasis on meeting objectives, leads to a corollary requirement that accountability must be well-defined for every unit, and in some cases, every individual within the organization.

The focus on pushing responsibility for managing and executing GRC programs as far down within the organization as possible is also consistent with the complex, detailed nature of many of the regulatory requirements and of the control systems that manage risk. Risk management is all about attending to details. This can succeed only when responsibility and accountability resides at low levels within the organization as well as at the top levels.

The experience that organizations had with Total Quality Management a decade ago provides useful lessons for GRC. Although these initiatives absolutely require support and commitment from the highest levels within the organization, they cannot be made to work from the top down. Organizations learned that quality must be everyone's job. The same is true for risk management and compliance.

4. Establish Communication Channels Across All Organization Levels

Once administrative and tactical requirements have been defined, these requirements must be consistently and efficiently communicated to the appropriate people. As already noted, one of the characteristics of GRC objectives is that this communication is made more challenging by the requirement for both great breadth and great specificity within the communication. What follows are a few other considerations that should shape these communication operations.

- Communications will include policies, policy reviews and interpretations, training materials, support materials, audit information, and more.
- Communications should be at once consistent and tailored to specific tasks, requirements, and situations.
- The volume of information can be substantial.
- It is critically important to ensure that everyone is looking at the most recent versions of policies, procedures, and control mechanisms.
- Access must be simple and straightforward.
- There should be a mechanism that the organization can use to confirm that the information has been received, understood, and put into use.

5. Audit, Monitor, and Report

"Management" implies that you know whether policies and procedures are being employed and that they are effective in achieving objectives. In short, management implies monitoring and auditing. The organization should support a variety of different auditing and monitoring operations:

- Internal audits, particularly of manual processes.

- Monitoring and periodic checks of automated procedures.
- Support for efficient external audits.
- Routine, distributed reporting to employees responsible for GRC operations and objectives
- Routine and appropriate reporting from these distributed areas of responsibility up through the organization

The monitoring and reporting requirements for GRC objectives and processes are made more complex by GRC's peculiar characteristics, in particular, the complex accountabilities and the presence of GRC processes as a minority component within a majority of broader activities. The result is that GRC control must be distributed to be manageable and effective. At the same time, there must be mechanisms to report exceptions up through the control hierarchy. As a simple example, the process of monitoring supply chain risk factors is appropriately distributed to the production group within an organization, but evidence of elevated supply chain risk must be signaled upward and to other affected groups.

Another important part of this reporting system should be "whistleblower" capability mandated by the Sarbanes-Oxley Act. There must be a way for employees to report suspected criminal activities without fear of retribution.

Reporting should not be limited to emergency situations. Many aspects of risk management involve making judgments; it is critically important that the reporting system can also serve as a support system, providing employees with the guidance and with the contextual information they need to make sound judgments and to manage risk effectively.

6. Provide Uniform Support, Remediation, and Enforcement

The USSC guidelines emphasize the need for consistent administration of incentives for employees who comply with program objectives, coupled with consistent disciplinary measures for those who engage in criminal conduct or who fail to take steps to prevent criminal conduct. The USSC's goal is ensure that the organization sends a clear message that criminal activity will not be tolerated.

Expanding the program beyond this core focus on prevention of criminal activity to include a broader view of governance, risk management, and compliance, the organization must create a more comprehensive incentive structure, coupled with constraints on behavior, that consistently underscores the importance of reaching GRC objectives.

It is important that that concepts of uniformity and consistency extend beyond incentives and discipline to include the reporting and management processes. Use of consistent reporting conventions, terminology, and approaches across the different operations within an organization enables the distributed auditing and monitoring capability described as part of the preceding, "Audit, Monitor, and Report" operational objective. Communication laterally and vertically within the organization is facilitated by use of standard, uniform processes.

As we have already noted, the GRC program must work from the bottom up as well as from the top down, and the individual risk management activities often require

making judgments. The incentive and enforcement mechanisms must be supported by the reporting, inquiry, and communications systems.

7. Implement Continuous Process Improvement

As noted at the outset, governance is all about creating a responsive organization that thrives in its environment, as defined by investors, capital markets, competition, the government, and other forces and constituencies. It follows that the successful GRC operations focus on process improvement, business intelligence, and competitive advantage.

Certainly, as the USSC requires, if criminal activity is uncovered, it should be reported immediately. Control systems should be reviewed and, if necessary, modified to do a better job of preventing such activity. But this is just one part of what should be an overall program of process improvement. The program should include:

- Full monitoring of risk management and compliance in terms of defined responsibilities and accountability.
- Monitoring of operational risk and compliance focused toward improvement.
- Real-time escalation and reporting of critical issues.
- Benchmarking.
- Overall and discrete process analysis to facilitate process improvement.

The monitoring, reporting, benchmarking, and process analysis should, of course, be interpreted in terms of the organization's GRC objectives, tying everything back to the constituencies and to the risks that the GRC effort is designed to address. The monitoring and improvement is ultimately the responsibility of the board of directors and of senior management.

Putting the Operational Approach to Use

Returning to the questions raised at this paper's outset, the member organizations within the Compliance Consortium have learned that it is important to treat governance, risk management, and compliance objectives as a distinct organizational concern, standing apart from and on the same level as the other fundamental organizational issues that are the business of boards of directors and senior management. The reasons for according GRC objectives and operations this status emerge from the nature of the GRC objectives themselves. Even though GRC objectives cut across the entire organization and tie into everything else, they are unlike other operational and strategic objectives. At the same time, GRC objectives share common characteristics that make it possible, perhaps even necessary, to manage them as a distinct organizational concern. Finally, and perhaps most importantly, the substance of GRC objectives is closely connected to the well-being of the entity. Governance, risk management, and compliance are appropriately a board level concern.

Given this insight, the Consortium addressed the question of what it means from an operational standpoint. The Consortium has found that the US Sentencing Commission guidelines regarding an effective compliance and ethics program provide a useful starting point for defining an operational approach to GRC. One obvious reason for the appeal of

the USSC guidelines is that the ability to demonstrate guideline conformance can translate into substantial reductions of legal liability in the event of criminal activity within the organization. But the USSC guidelines are attractive for reasons that go beyond legal liability: They comprise a simple, manageable set of requirements that an organization can use as the foundation for GRC operations. Over the preceding pages this paper has described the core operational elements of such a program—these are the things that your organization should be doing.

Some board members and managers have undoubtedly enjoyed a sense of recognition in reading this list of seven operational elements. For others, however, the list may stimulate important questions about how things stand within their particular organizations. It is useful to anticipate and articulate some of these questions.

A Dozen Questions for Board Members and Senior Management

Here, then, are a dozen questions that arise from the preceding description of GRC objectives and operations. Even if your organization has GRC operations in place, it might be useful to review these questions and match them against your organization's programs.

1. Do we have a shared understanding of the principal strategic, operational, financial, and regulatory risks facing the organization?
2. Do we have a consistent approach to managing these risks? Or are we fragmented in our approach?
3. Do we have clarity regarding roles and responsibilities for risk and compliance requirements?
4. Is the board of directors really "driving the car" when it comes to compliance and risk management? Do we know where the car is headed?
5. Who are the various constituencies that have an interest in the performance of compliance and risk management? What are the key metrics for these constituencies?
6. Who should we get involved in the definition of our enterprise approach and what should their roles be in the risk identification and risk management process?
7. Does the variability of our compliance processes create risk of prosecution or penalty according to the sentencing guidelines?
8. How can we initiate a comprehensive program to not only improve efficiency but also improve effectiveness?
9. How do we measure efficiency and effectiveness? What confidence do we have in our understanding of effectiveness?
10. How are we supporting employees as they make risk management judgments and report back on risks and issues?
11. What are the systems that are currently used to manage compliance and risk management activities? What other systems are dependent on compliance and risk management, or constrain our GRC activities?
12. How can we leverage the operational approach detailed in this white paper?

Other Frameworks and Resources

The Compliance Consortium's intent in this paper has been to:

- focus attention on the problems and opportunities associated with governance, risk management, and compliance.
- identify a set of key GRC operations that boards of directors and senior management can use to organize and understand the state of governance, risk management, and compliance within an organization.
- provide management and directors with an initial list of questions that they can use to begin an evaluation of GRC operations.

Stated more simply, this paper provides a high-level view of the issues and a high-level approach to addressing them. As responsibility for these efforts moves downward through the organization there is a need for increasingly detailed, comprehensive guidebooks, frameworks, and benchmarks.

Directors and senior management should be familiar with two important resources that provide these kinds of more comprehensive tools. The first is COSO—The Committee of Sponsoring Organizations of the Treadway Commission—which published an integrated framework for internal control in 1992 and 1994[5], followed by a more comprehensive enterprise risk management framework in 2004. The COSO frameworks are complementary to each other and to the approach described in this paper. They provide an organization with evaluation tools for internal control and application techniques for enterprise risk management.

A second and, once again, complementary resource comes from OCEG—The Open Compliance and Ethics Group. OCEG has developed a framework that is both broader and more detailed than the one described in this paper, intended to integrate governance, risk management, compliance, and integrity into everyday business procedures in the fullest sense.[6] The OCEG Framework is comprised of two broad components: the Foundation and the Domains. The Foundation addresses the full lifecycle of planning, implementing, managing, evaluating, and improving integrated compliance and ethics programs. The Domains provide additional guidelines that are specific to a particular risk area such as employment compliance, financial assurance, or anti-corruption controls. Domains may also include guidelines designed to support different industries, business functions, operations in certain geographic locations, or organizations of various sizes (e.g., small businesses) or structures. Through its benchmarking studies, OCEG also provides assistance in comparing an individual company's activities to industry benchmarks.[7]

About the Compliance Consortium

The Compliance Consortium™ is an international membership organization designed to promote effective and efficient enterprise governance, risk and compliance management. Technology, content and services companies participating in the consortium work to identify best practices for applying technology to compliance business processes and to exploiting those best practices to improve overall business performance.

Areas of interest

The Compliance Consortium will work to

- publish governance, risk and compliance (GRC) technology and implementation best practices and reference architectures
- influence and contribute to GRC-related industry and computing standards
- establish and influence conferences and other professional events focused on GRC-centric topics

The consortium will work independently as well as in collaboration with established independent organizations as appropriate.

For more information, visit www.thecomplianceconsortium.org.

Notes

[1] Steven J. Root, *Beyond COSO* (New York: John Wiley and Sons, 1998), 190.

[2] *Enterprise Risk Management—Integrated Framework*. The Committee of Sponsoring Organizations of the Treadway Commission, 2004.

[3] Ibid., Volume 1, p 16.

[4] Paula Desio, "An Overview of the Organizational Guidelines", United States Sentencing Commission, 2004. See also Chapter 8, Part B of the 2004 USSC Sentencing Guidelines, "Remedying Harm from Criminal Conduct, and Effective Compliance and Ethics Program."

[5] *Internal Control—Integrated Framework*. The Committee of Sponsoring Organizations of the Treadway Commission. Published in two volumes, 1992 and 1994.

[6] Open Compliance and Ethics Group, *Foundation Guidelines "Red Book, Application Draft* (www.oceg.org: Open Compliance and Ethics Group, May, 2005)..

[7] Open Compliance and Ethics Group, Benchmarking Study (http://www.oceg.org/benchmarking.asp).