Practice Area
briefings

sponsored content graciously presented by Miles & Stockbridge

Beyond the Fire Alarm – Integrating Governance, Risk Management, and Compliance (GRC)

By Raymond F. Monroe, William R. (Billy) Martin, and Robert Theodore (Ted) Ebert


Raymond F. Monroe


William R. Martin


Robert T. Ebert

We all know one of the many "hats" that in-house counsel wear is that of the "crisis manager." We react to frantic messages: "We've had a data breach." "We're being sued in a massive product liability class action." "Um, the Feds are here."

Crises are inevitable, and having a multidisciplinary crisis management team, including legal, management, public and government relations, and other relevant experts is a known prudent business practice. The next level of sophistication, however, focuses on how corporate governance, risk management, and compliance (GRC) proactively and efficiently interact in a system that is becoming the new normal: integrated GRC.

What is integrated GRC?

The components of GRC are not new.

- **Corporate Governance** provides fundamental structures that businesses can use to operate and achieve its objectives, including, for example, legal organization, codes of conduct, policies, systems for monitoring and implementing legal, regulatory, and contractual requirements, internal audit, and reporting processes.
- **Risk Management** focuses on identifying, analyzing, and mitigating risks through mechanisms such as contractual provisions and insurance policies. The risks can include:
  a. operational risks, including financial reporting, workplace safety, product quality/safety, cybersecurity, labor and employment, environmental, anti-corruption, supply chain management, intellectual property, and contract/government contract "doing business" requirements, as well as other requirements unique to your business; and,
  b. external risks, including technology breakthroughs, demographic shifts, and political, environmental, and social changes.
- **Compliance** focuses on understanding what legal or regulatory obligations or aspirations apply to your practice and then setting up systems for training and monitoring to ensure that the business is complying with those requirements or aspirations.[1]

Most companies have some or all of these components, as each

serves its own important function. However, operating independently, these components can overlap, leading to inefficient, siloed, reactionary, and ineffective practices. As a result, this can lead to missed opportunities to give visibility to important interrelationships and trends that allow executives, in-house counsel, and board members to identify and manage existing and evolving risks. If left unidentified or unmanaged, this can ultimately lead to crisis events with potential impacts to the company's revenues and reputation, as well as to the potential exposure for those mentioned above.

As the Open Compliance and Ethics Group (OCEG) stated in defining the concept of integrated GRC, it is:

A system of people, processes and technology that enables an organization to:

- Understand and prioritize stakeholder expectations;
- Set business objectives that are congruent with values and risks;
- Achieve objectives while optimizing risk profile and protecting value;
- Operate within legal, contractual, internal, social, and ethical boundaries;
- Provide relevant, reliable, and timely information to appropriate stakeholders; and,
- Enable the measurement of the performance and effectiveness of the system.[2]

GRC provides an "integrated, holistic approach" to ensure that an organization "acts ethically correct and in accordance with its risk appetite, internal policies, and external regulations through the alignment of strategy, processes, technology, and people, thereby improving efficiency and effectiveness.[3]"

In shaping and implementing an integrated GRC system, in-house counsel, working with the full team, can and should consider developing a system for noticing trends in the requirements and allegations of noncompliance — and adjusting its compliance and training systems to address the needs and perceptions for improvement.

Perhaps more simply and starkly: Integrated GRC is like having the visibility of an app on a smart phone with a modifiable dashboard that understands the risk environment in which your business operates, measures your performance in managing those risks against established metrics, sends alerts regarding risk metric points as they emerge, and has the ability to adapt to evolving or changing risks. Ultimately, this will establish new metrics, giving executives, in-house counsel, and board members real-time visibility into the status of the company — before, during, and after the crisis event.

In-house counsel key to shaping and implementing integrated GRC

In-house counsel can and should play a key role in structuring and implementing an integrated GRC approach, as this position is naturally central to creating governance structures; identifying and developing mechanisms (e.g., contract clauses, insurance policies, and regulatory or statutory revisions) that identify and address risks; and bringing inside and outside experts together to take a more holistic view of identification and mitigation of risks.

In-house counsel should also understand that new laws and regulations at the international, federal, state, and local levels are being modified daily — creating a legal "big data" environment. No one lawyer can keep track of all developments, integrate such developments across all legal disciplines, and then spot trends in both the requirements and in enforcement techniques that heighten risks to various product lines and/or geographical regions in which the company does business. However, by working with other in-house lawyers, outside experts, and other disciplines inside and outside of the company, in-house counsel can be integral to a team by identifying risks and developing a system to train and monitor compliance.

However, a compliance system that expects in-house counsel to parachute in to respond to one-off hot line calls is reactionary. In shaping and implementing an integrated GRC system, in-house counsel, working with the full team, can and should consider developing a system for noticing trends in the requirements and allegations of noncompliance — and adjusting its compliance and training systems to address the needs and perceptions for improvement. Crisis events and parachute drops will still likely oc-

cur, but with in-house counsel input, ongoing process improvement can and should increase operational efficiency and effectiveness. Ultimately this will reduce risk to the company, its products and its brands, and the personal exposure of senior management and board members.

An increasingly aggressive DOJ

The Department of Justice (DOJ) has made it abundantly clear that it will vigorously enforce criminal laws against corporate wrongdoing. The examples have been and will continue to be in the headlines, from accounting and obstruction of justice, to environmental violations, and to numerous financial, health care, and Medicare fraud cases.

Since the 2015 "Yates Memorandum," it is also clear that DOJ will focus on individuals. For example, the Yates Memorandum provides:

- that DOJ will use its "best efforts to hold to account the individuals responsible for illegal corporate conduct;" [4]
- that both civil and criminal investigations will "focus on individuals from the inception of the investigation;"[5] and,
- that for corporations to "be eligible for any cooperation credit, corporations must provide to the Department all relevant facts about the individuals involved in corporate misconduct."[6]

In this prosecutorial environment, and in the context of integrated GRC systems that can give executives, in-house counsel, internal auditors, and board members visibility into what is required, what is occurring, and what is being done about it, the potential risks of operating outside of the "new normal" may require a consideration for whether the absence of an integrated GRC system or an appropriate inquiry and monitoring by individual(s) armed with such a system equates to a violation of the appropriate "duty of care," justifying, for such individual(s), civil liability or criminal prosecution.

Call to action

1. **Consider adopting an integrated GRC approach.**
   The integrated GRC approach is quickly being adopted, in many forms and approaches, across various industries, and by companies of all sizes. It has been found to improve communication and information sharing, reduce overlapping and duplicative activities, and raise visibility for the importance of risk management and compliance. As a person with substantial responsibility for a company's approach in these areas, in-house counsel should encourage its client to look at GRC approaches and determine whether one fits — or can be designed to fit — the needs of the company.
2. **Put in-house counsel at the epicenter of a company's risk management and compliance structure.**
   Even if a company does not want to adopt a formal GRC program, it is critical that the structure of an organization allows for the rapid flow of information relating to the risk and compliance issues affecting in-house counsel.

   Too often, companies are organized in a manner that encourages risk or compliance issues to be moved "up the chain" through a business area or functional organization to make sure that senior management is aware of the issue before it is referred to counsel. These delays can limit the options available to in-house counsel to mitigate the risk. Likewise, a company's policies and procedures should make it clear to employees that in-house counsel should be engaged not only when an event resulting in a potential liability has happened —such as a data leak, the creation of an environmental hazard or a contract breach — but also when the risk of the event (or the potential for it) becomes apparent. In addition, in-house counsel should be included in any organization, group, or council in a company designed to review risk or compliance issues.
3. **Expand the scope of in-house counsel legal guidance.**
   A GRC program, whether integrated or not, does not work if there is insufficient information in the system. Much of the input into the GRC system comes, or should come, from in-house counsel. The task of identifying critical information, though, has become increasingly more difficult. The world is changing quickly, and each new development — whether it is a technological breakthrough; a shift in political power; or an environmen-

In those situations, without some form of integrated GRC, you will be behind the curve of best practices, putting your executives and board members at risk for allegations of civil and/or criminal misconduct.

tal, social, or economic change — has a legal impact. Reviewing the traditional summaries of case decisions and regulatory and statutory developments relevant to a particular industry may not be enough to provide adequate advice to clients.

For example, 10 years ago, the legal issues associated with the unintended use of electronic data did not exist. Now, to provide guidance, in-house counsel needs to keep up on legal developments relating to data breach in areas such as contract law, tort law, insurance law, and privacy law. Similarly, in-house counsel faces new challenges in the area of compliance. While in-house counsel generally has experience complying with a multitude of overlapping, sometimes conflicting, federal, state, and local statutes and regulations, the globalization of the economy presents a vast new set of international rules to contend with. These include export control, privacy, and anti-bribery statutes and regulations. Internal communication includ-

ing in-house counsel and external communication to relevant subject matter experts is essential to facilitate a functional, even if not fully integrated, GRC system.

The risk of doing nothing

Change is always hard, but failing to identify, analyze, and manage risks holistically, integrating them into corporate governance and compliance — while your competitors continue to move in that direction — comes with its own risks. You will not be identifying any new or existing risks, nor establishing systems and metrics for monitoring them. At best, you will be doing so in an ad hoc manner. As a result, in some critical instances, you may be reacting to problems as they arise — responding to the fire alarm, perhaps armed only with the information to fight last year's fire — sometimes surprised and unprepared for the inevitable encounters with today's auditor, investigator, reporter, suspension and debarment official, or sentencing judge. In those situations, without some form of integrated GRC, you will be behind the curve of best practices, putting your executives and board members at risk for allegations of civil and/or criminal misconduct.

Another alternative, if you have not done so already, is to provide legal input on the merits of an integrated GRC system. Your recommendation could be a long-term value-add for your company, your executives, and your board members — ultimately making you more prepared for the next crisis. **PAB**

NOTES

1 See generally Scott L. Mitchell and Carole Stern Switzer, GRC Capability Model Red Book 2.0, OPEN COMPLIANCE AND ETHICS GROUP at Intro 9-13 (2009), *https://thegrcbluebook.com/wp-content/uploads/2011/12/uploads_OCEG.RedBook2-BASIC.pdf*.
2 Id. at 8.
3 Nicolas Racz, Edgar Weippl and Andrea Seufert, A Frame of Reference for Research of Integrated GRC, HAL ARCHIVES at 8 (2010), *https://hal.archives-ouvertes.fr/hal-01056386/document*.
4 Sally Q. Yates, Individual Accountability for Corporate Wrongdoing, DOJ Memorandum at 2 (Sept. 9, 2015) (emphasis in original), *https://www.justice.gov/dag/file/769036/download*.
5 Id. at 4.
6 Id. at 3.

Ray Monroe and Billy Martin are principals and Ted Ebert is counsel in the Washington D.C. office of Miles & Stockbridge. Each has more than 30 years of experience in counseling and litigating on issues related to compliance, corporate governance, ethics, government contracting, internal investigations, and white collar crime. Martin was formerly a federal prosecutor, including serving as Executive Assistant U.S. Attorney for the District of Columbia. Ebert was formerly a senior legal counsel and executive at a Fortune 100 corporation.