What GRC Could Mean to Your Organization

If you regularly follow business news and blogs, chances are you’ve seen increased occurrences of three little letters: GRC. Governance, risk, and compliance are nothing new... Actually, GRC seems as though the letters belong together and always have been grouped this way. Well, that’s half right. They do belong together. These letters represent a critical business concept that is (or should be) on the minds of everyone responsible for leading and/or governing organizations in today’s complex business arena.

WHAT IS GRC?
According to the Open Compliance and Ethics Group (OCEG), GRC 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 the risk profile and protecting value.
• Operate within legal, contractual, internal, social, and ethical boundaries.
• Provide relevant, reliable, and timely information to stakeholders.
• Enable the measurement of a system’s performance and effectiveness.

OCEG President Carole Switzer believes that GRC has the potential to provide organizations with a uniform view of information so they can align risk management with objectives, reduce complexity, diminish inconsistencies, and harness technology for optimal performance. “Today’s boards and executive management are increasingly cognizant of the need for an integrated approach that is proactive, effective, and organization-wide,” says Switzer. “When appropriately implemented, GRC is all of these.” She goes on to say that GRC accelerates risk-intelligent decisions, improves organizational agility, and reduces system costs. “Considering all these benefits, what’s not to like?” she asks.

GRC VERSUS ERM: WHAT’S THE DIFFERENCE?
Both governance, risk and compliance and enterprise risk management (ERM) are aimed at ensuring all risks facing an organization are identified, analyzed, and quantified. However, there are critical differences. ERM provides a methodology for managing the entire range of risks, and is the measurement and qualification of risk, as well as the establishment of individual risk ownership.

GRC provides a larger, over-arching framework and philosophy for communicating around governance and compliance risks by leveraging technology for reporting mechanisms such as dashboards. This technology centralizes and organizes things such as policies, procedures, documentation requirements, and risk assessments. In essence, GRC encompasses ERM.

Source: Treasury & Risk, June 2007
WHAT ARE THE BENEFITS OF GRC?
As organizations grow and evolve, often they layer new processes on top of old procedures without looking at their operations afresh to ensure optimal functionality and effectiveness. Many areas function in silos — only reacting to stimuli as they occur, rather than approaching issues proactively.

GRC, however, employs a much broader, integrated, and more proactive approach that takes full advantage of all opportunities and resources — especially information technology. When effectively deployed, GRC can help ensure controls are appropriate, operate effectively, address risks as intended, and use resources efficiently. More importantly, GRC can help provide assurance to the board and senior management that the entire system of governance, risk, and compliance is effective and high-performing.

According to Switzer, GRC is a way of thinking and acting that facilitates a paradigm shift within any organization. “The reason I am so passionate about GRC is that it can bring about true transformation in the way we do business,” she says, “the way we understand and address risk, and the way we can and will achieve a principled approach to governance and performance in both big and small companies today. This is about establishing an integrated, harmonized system of people, processes, and technology — a system that enables not only a smooth operating machine, but one that is flexible, quick, and responsive, and models both power and control.”

BEST GRC PRACTICES
OCEG’s GRC Achievement Awards honor organizations that are exemplary in integrating governance, risk management, and compliance. Recently, the 2010 awards recognized the efforts of six leading companies:

• Best Buy — Using social media to stimulate dialogue on ethical issues, Best Buy has an ethics blog that is especially popular among its younger workers and customers.
• Capital One — By simplifying and standardizing risk management processes throughout the enterprise, Capital One has enhanced its system of internal control and achieved an increased level of comfort and assurance.
• Carnival — Even in its globally decentralized environment, Carnival successfully integrated GRC, which resulted in greater balance and corporate autonomy, as well as enhanced internal control.
• DIRECTV — After addressing the inherent risks and challenges of spreadsheet data management, DIRECTV implemented entity-wide methods and programs designed to standardize the use, maintenance, and sharing of spreadsheets.
• Tawuniya — By linking GRC and performance management, Saudi Arabia’s leading general insurance agency created a corporate culture of effective risk management.
• VISA — By consolidating more than 3,400 requirements into a system that supports focused analysis, analytics, and assurance, VISA implemented a holistic, enterprise-wide approach to risk management.
Benefits of GRC include increased stakeholder confidence, improved responsiveness and readiness of the organization to address risks, and an enhanced flow of consistent information throughout the entity.

**INTERNAL AUDITING’S ROLE**

Internal auditors play a critical role in guiding their organization beyond traditional risk management toward a proactive integrated governance, risk, and compliance capability. Therefore, of all the functions in a company or agency, there is no activity better positioned to assess the effectiveness of GRC than internal auditing.

When the board and executive management make a commitment to GRC, and take measurable action towards effective implementation, their internal auditors have an opportunity to provide assurance that there is a system in place that offers greater transparency and a stronger platform for risk-aware decision-making.

“Boards can no longer simply delegate to management every aspect of strategic planning and decision-making about how the organization will operate,” says Switzer, “by blindly approving decisions after listening to reports.” She goes on to say that today’s boards have the obligation and the opportunity to define the boundaries within which an organization operates. “To truly govern, they must establish an organizational mission and vision and ensure a measurable GRC system is in place,” she says. “And with appropriate involvement of the internal auditors, boards can rest assured that they know what they need to know to truly govern.”

Certainly, there is no one way to ensure governance is 100 percent effective, each and every risk is mitigated, and compliance efforts leave nothing to be desired. However, GRC provides a thoughtful and thorough system for addressing risk and compliance issues.

According to Switzer, GRC does this with a level of maturity that can only be gained by establishing repeatable, documented, consistent, and harmonized processes. “The issue is not about mitigating every risk; it is about recognizing what the risks are in the first place, and understanding how they change under different circumstances,” she says. “It’s about establishing meaningful controls based on real analysis of risk impacts — not just guesses — and harmonizing processes so that they are integrated into operations in a way that facilitates desired outcomes, rather than being a detriment to the business.”

Improving GRC does not mean eliminating all of our processes and technologies and starting from scratch; nor does it mean spending more and creating extra layers of bureaucracy. Every organization must evaluate its current state, determine the key points of integration where successes can be gained, and identify priorities for improvement.

Boards of directors — especially those that govern publicly traded companies with global operations — are under scrutiny today as never before. Not only are they entrusted to make strategic governance decisions on behalf of stakeholders, but those decisions can even affect society as a whole. Because, in some cases, their decisions can alter market economies and physical environments, the obligation for boards to ensure they have a true understanding of potential outcomes is a serious and daunting one.

In the absence of an integrated GRC system — one that provides clear and accurate information on which to base risk-intelligent decisions — boards can be essentially constrained. Maturing the GRC system, integrating and balancing risk and compliance processes across the enterprise, and gaining transparency through improved application of technology must be a top priority.
**Mission**
To provide executive management, boards of directors, and audit committees with concise, leading-edge information on such issues as ethics, internal control, governance, and the changing role of internal auditing; and guidance relative to their roles in, and responsibilities for, the internal audit activity.

E-mail your comments about *Tone at the Top* to:
PR@theiia.org
+1-407-937-1247

**Complimentary Subscriptions Available**
You, your colleagues, and your audit committee and board members are invited to receive complimentary subscriptions to *Tone at the Top*. Visit the online subscription request form at: [www.theiia.org/periodicals/newsletters/tone-at-the-top](http://www.theiia.org/periodicals/newsletters/tone-at-the-top) or write to us at:
The Institute of Internal Auditors
Corporate Communications
247 Maitland Ave.
Altamonte Springs, FL 32701-4201 USA
Fax: +1-407-937-1101

*Tone at the Top* is also archived online. To reprint, translate, or post this edition of *Tone at the Top*, contact PR@theiia.org.

---

**The Institute of Internal Auditors** ([www.theiia.org](http://www.theiia.org)) is dedicated to the global promotion and development of internal auditing.

Established in 1941, The IIA is an international professional association with global headquarters in Altamonte Springs, Fla. The IIA has more than 160,000 members in internal auditing, risk management, governance, internal control, IT auditing, education, and security.

The IIA is the global voice, recognized authority, chief advocate, principal educator, and acknowledged leader in certification, research, and technological guidance for the internal audit profession worldwide. The IIA enhances the professionalism of internal auditors and is internationally recognized as a trustworthy guidance-setting body. It fosters professional development, certifies qualified audit professionals, provides benchmarking, and through The IIA Research Foundation, conducts research projects and produces educational products.