IS GOVERNANCE, RISK MANAGEMENT & COMPLIANCE [GRC] SNAKE OIL?

Emmanuel Moore Abolo, Dr.

Available at: https://works.bepress.com/emmanuel_abolo/4/
IS GOVERNANCE, RISK MANAGEMENT & COMPLIANCE [GRC] SNAKE OIL?

GRC is a recent buzzword in the business world with no single, commonly accepted definition. However, the concept now permeates the risk management airwaves in the same way that enterprise risk management did some years back.

In its GRC Capability Model, Red Book defines GRC as 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.

Gartner defines GRC management as “the automation of the management, measurement, remediation, and reporting of controls and risks against objectives, in accordance with rules, regulations, standards and policies.”

The letters in GRC can be explained as follows:

**Governance:** Setting the policies, structure and objectives for an organization and overseeing progress toward those objectives.
**Risk Management**: This is the identification, assessment, and prioritization of risks (defined in ISO 31000 as the effect of uncertainty on objectives, whether positive or negative) followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events[1] or to maximize the realization of opportunities[ Wikipedia].

**Compliance**: The management and monitoring of compliance with the organization’s own required policies and procedures that enable management of the risks endangering the organization. It includes reporting of regulatory and policy breaches, management of their remediation, and communications between the organization and the regulator.

GRC reflects a new way of thinking in which organizations are adopting a holistic approach to these aspects of their business and encapsulates how an organization understands stakeholder expectations and then directs and manages activities to maximize performance against those expectations, while managing risks and complying with applicable laws, regulations and obligations.

Being closely related concerns, governance, risk management and compliance activities are increasingly being aligned in order to reduce conflicts, wasteful overlaps and gaps.

The main goal of GRC is to help an organization efficiently deploy policies and controls to address all its compliance obligations while at the same time leveraging information that helps proactively run the business. Done properly, GRC creates a central nervous system that helps an organization to manage its business more effectively.

To be clear, GRC is not just about complying with rules and requirements at any point in time. Rather, those who are serious about GRC, seek to create a system and culture so that compliance with external regulations, enforcement of internal policies, and risk management are automated as much as possible and can evolve in an orderly fashion as business and compliance needs change.

That’s why some would say that the C in GRC should stand for controls: controls that help make the process of compliance orderly and make process monitoring and improvement easier.

GRC processes are extensive, ranging from the activities of the board and executive management, through strategy setting, performance management, risk management and financial reporting, and including internal controls and IT security.

Adopting an effective implementation strategy for GRC can significantly increase shareholder value and empower organizations to:
• Improve strategic business decisions by clearly defining associated risks and opportunities
• Minimize operational surprises with more proactive and effective monitoring
• Protect and enhance reputation and brand by capitalizing on business opportunities while reducing the likelihood of negative events
• Increase organizational efficiency
• Avoid fines, penalties and damage to reputation

The question every company must answer is: Will we do the bare minimum to make sure that we stay out of trouble, or can GRC become an opportunity for us to find new ways of running our business better?

In other words, GRC should not be seen as snake oil; not a useless concept of some sort. A common strategic approach involving governance, risk and compliance will lead to the end of the "silo" approach that firms currently take. It also implies a new way of working for compliance and a leadership opportunity. It is the next evolutionary step beyond enterprise risk management.

By taking a more integrated approach across the three elements, and costing risks and controls, businesses can be smarter in the way that they employ resources. If an organization is spending very little on trying to contain a risk that could potentially cost them a great deal of money or spending a great deal on offsetting risks that could potentially cost very little, they are not being smart. Compliance is required to look more closely at the way risks evolve and develop and the performance of controls.

GRC is, first and foremost, a particular organizational philosophy. It requires absolute commitment at the most senior level for it to have a chance of working and it must run throughout the entire organization, from top to bottom and side to side.

Bringing a practical GRC design to fruition within a financial services organization, for instance, requires[Hegel 2014]:

• continuing resource commitment at the most senior levels;
• the creation and communication of a common set of overarching strategic business objectives which take into account the needs and wishes of stakeholders, including regulators;
• the creation and communication of relatively simple policy statements which set out the parameters within which the strategic business objectives will be achieved;
• the consolidation of a number of varying information outputs across businesses and control functions into a comprehensible set of common elements, to create valuable qualitative indicators;
• the application of financial modelling to the inputs and outputs, to identify the cost and value of risks and controls and enable rational resource allocation;
• the continuous application of expert human judgment to all consolidated information;
• effective and frequent internal communication of information, obligations and expectations;
• cohesion and cooperation rather than partisanship throughout the support functions; and
• absolutely rigorous planning and progress monitoring to integrate the new approach across all business and control areas.

The scale of effort required to bring this about is rather significant. At a time when companies are seeking to shrink their cost bases as fast and as far as possible, any programme with no immediate bottom line impact, however worthwhile, is likely to end up in the “pending” tray.

Ultimately, the final question must be: is an industry ready to move to a governance, risk and compliance approach? It is clear that majority of the industries have not yet implemented comprehensive ERM approaches, despite their obvious value. If the map now exists to drive to GRC++, however, why stop off at ERM-ville on the way? Clearly the possibility exists for any organization to evolve straight to the new approach if it chooses to, and the early implementers who see this as a rational business decision will have the resultant platform for growth sooner than later.