protiviti®
Risk & Business Consulting.
Internal Audit.

Key questions surrounding integrated GRC

In this article Protiviti addresses four key questions related to governance, risk and compliance (GRC). Among the discussion points are its definition and the similarities and differences between integrated GRC and enterprise risk management. Protiviti also provides a comprehensive guide to the value of an integrated GRC programme and practical steps towards achieving that value.

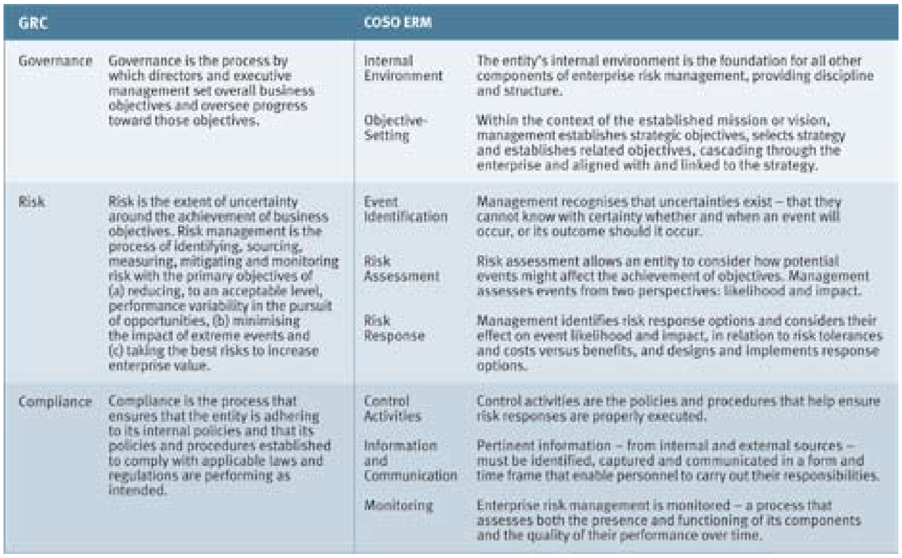
Franklin Delano Roosevelt once said: "The structure of world peace cannot be the work of one man or one party or one nation. It must be a peace which rests on the co-operative effort of the whole world." Integrated governance, risk and compliance (GRC) is a little like world peace in this way, something we can all agree upon conceptually, but requires the co-operative efforts of all groups within the enterprise. This article addresses four key questions related to GRC:

- What does it mean?
- What is the value?
- What are the barriers to success?
- What are the practical steps towards achieving value?

What is integrated GRC?

GRC means different things to different people. One perception is that integrated GRC is nothing more than enterprise risk management (ERM) repackaged by solution providers to drive a new market. Others consider ERM and GRC as distinct subsets of one another. ERM practices have traditionally focused on strategic, financial and operational risks, whereas GRC derives its origins largely from a compliance focus. GRC practices have evolved over a long period of time and place greater emphasis on integrating various risk and compliance functions. On closer review, ERM and GRC differ in terms of their moniker origins and related market practices, but are similar in definition. These similarities in definition are illustrated in Figure 1 by comparing Protiviti's definition of GRC to the Committee of Sponsoring Organizations (COSO) ERM framework.

Defining GRC as a set of aligned activities is the first step towards integrating the management of multiple risk domains into a unified programme that appropriately shares resources and knowledge to efficiently manage all aspects of GRC. Once this integration takes place, regulatory compliance is viewed as a risk to be managed and the compliance process takes on a broader context, i.e., as a process applied to the internal policies pertaining to all risks.



GRC		COSO ERM	
Governance	Governance is the process by which directors and executive management set overall business objectives and oversee progress toward those objectives.	Internal Environment	The entity's internal environment is the foundation for all other components of enterprise risk management, providing discipline and structure.
		Objective-Setting	Within the context of the established mission or vision, management establishes strategic objectives, selects strategy and establishes related objectives, cascading through the enterprise and aligned with and linked to the strategy.
Risk	Risk is the extent of uncertainty around the achievement of business objectives. Risk management is the process of identifying, sourcing, measuring, mitigating and monitoring risk with the primary objectives of (a) reducing, to an acceptable level, performance variability in the pursuit of opportunities, (b) minimising the impact of extreme events and (c) taking the best risks to increase enterprise value.	Event Identification	Management recognises that uncertainties exist – that they cannot know with certainty whether and when an event will occur, or its outcome should it occur.
		Risk Assessment	Risk assessment allows an entity to consider how potential events might affect the achievement of objectives. Management assesses events from two perspectives: likelihood and impact.
		Risk Response	Management identifies risk response options and considers their effect on event likelihood and impact, in relation to risk tolerances and costs versus benefits, and designs and implements response options.
Compliance	Compliance is the process that ensures that the entity is adhering to its internal policies and that its policies and procedures established to comply with applicable laws and regulations are performing as intended.	Control Activities	Control activities are the policies and procedures that help ensure risk responses are properly executed.
		Information and Communication	Pertinent information – from internal and external sources – must be identified, captured and communicated in a form and time frame that enable personnel to carry out their responsibilities.
		Monitoring	Enterprise risk management is monitored – a process that assesses both the presence and functioning of its components and the quality of their performance over time.

Figure 1: Comparison of Protiviti's definition of GRC to that of the COSO ERM framework

What is the value of integrated GRC?

Is integrated GRC an all-or-nothing proposition? The challenge of integration often relates to cultural boundaries within an organisation rather than conceptual or technical issues. GRC processes are unique in relation to operating processes. Changing markets and a continuing stream of new laws and regulations spanning decades have driven an ad hoc and reactionary evolution of new policies, procedures and controls in organisations. Often, internal and external pressures result in these changes being completed at such a pace that the 'new' policies, procedures and controls are added onto the existing structure. This ongoing spiral of change has led to complex accountabilities, the growth of silos, inefficient communications, decreasing

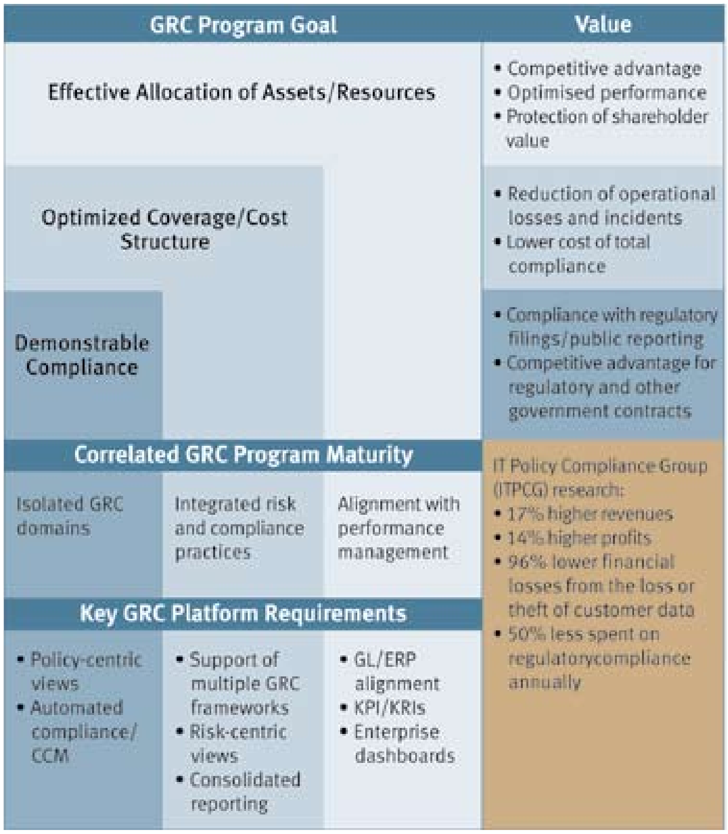

GRC Program Goal
Value
Effective Allocation of Assets/Resources
• Competitive advantage
• Optimised performance
• Protection of shareholder value
Optimized Coverage/Cost Structure
• Reduction of operational losses and incidents
• Lower cost of total compliance
Demonstrable Compliance
• Compliance with regulatory filings/public reporting
• Competitive advantage for regulatory and other government contracts
Correlated GRC Program Maturity
Isolated GRC domains
Integrated risk and compliance practices
Alignment with performance management
IT Policy Compliance Group (ITPCG) research:
• 17% higher revenues
• 14% higher profits
• 96% lower financial losses from the loss or theft of customer data
• 50% less spent on regulatorycompliance annually
Key GRC Platform Requirements
• Policy-centric views
• Automated compliance/ CCM
• Support of multiple GRC frameworks
• Risk-centric views
• Consolidated reporting
• GL/ERP alignment
• KPI/KRIs
• Enterprise dashboards

Figure 2: GRC programme maturity continuum

organisational transparency and so on – all leading to a higher cost of compliance.

Integrating GRC is about bringing people together to work towards managing common goals through common processes while sharing resources and co-ordinating plans. Today's business environment is too dynamic to reach a static state of integration. The goal is to develop a culture that promotes collaboration and views integrated GRC as a process, not an end state. The value returned by integrated GRC correlates to the organisation's programme goals, current maturity, technology capabilities and cost of compliance, as illustrated in Figure 2.

The irony is that many companies don't even know their total cost of risk and compliance management. That is because the management of risk and compliance is not integrated and there is a lack of transparency into how the underlying GRC processes are performing. Ultimately, an integrated GRC programme results in improved business performance by facilitating more effective allocation of assets and resources. To achieve these results, it is essential to align risk and compliance practices with performance management. Yet, value can be achieved all along the GRC programme maturity continuum. At the very least, a GRC programme, even where various GRC domain groups operate in isolation from one another, should support efficient and demonstrable compliance with specific regulatory requirements. Now, facing the prospect of additional regulations, many companies have the opportunity to take a fresh look at their risk and compliance coverage and cost structure and focus on strategies for optimisation.

Integrated GRC results in a clearer articulation of objectives, roles, responsibilities and accountabilities, leading to more effective risk and compliance process design and improved transparency into GRC performance through effective metrics, measures and monitoring. This all leads to more effective risk-based decision-making and an increased ability to anticipate issues and reduce reaction time.

What are the barriers to success?

There are significant barriers to successfully implementing an integrated GRC programme. In a survey jointly conducted by Protiviti and *OpRisk & Compliance*, the adoption of a common risk language and communication among risk management teams were cited as the two top key characteristics of an integrated GRC programme. Unfortunately, the lack of a common risk language or framework, and the required change management to support a co-ordinated effort, were respectively cited as the number two and three key barriers to successfully implementing an integrated programme. Not surprisingly, given the organisational change required to initiate the process, the number one barrier to integrating GRC practices cited by risk managers is the perceived high implementation cost with a lack of demonstrable return on investment (see Figure 3).

What are the practical steps towards achieving value?

Given the barriers to success, the journey towards integrated GRC must begin with a business case. A GRC committee with strong executive oversight and representation from multiple stakeholder groups is necessary to co-ordinate efforts. With the value understood and a change mechanism in place, the committee can begin the task of developing a unified risk framework. Ultimately, the effort should produce a consolidated reporting package that can be used for management decision-making and continuous improvement. Before delving into key considerations related to the above steps, several themes should be noted:

- Accommodate differences among GRC stakeholder requirements in order to break down barriers. For example, we believe

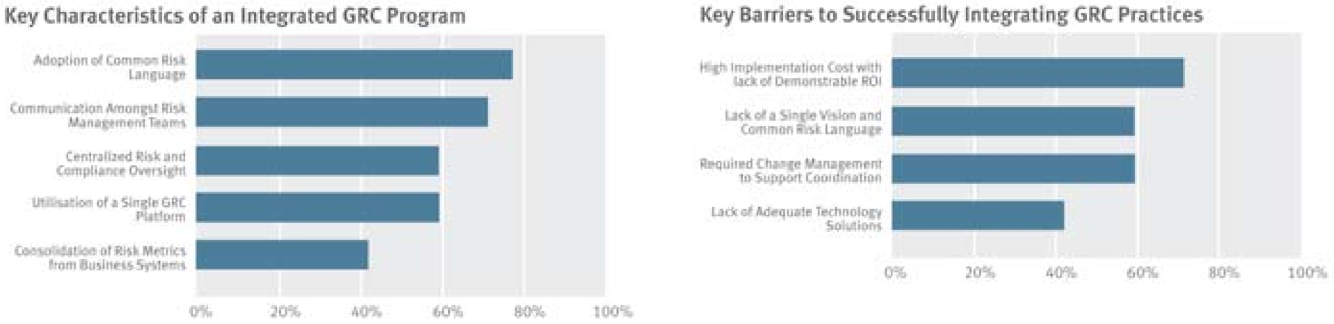


Figure 3: Characteristics of an integrated GRC programme and barriers to successfully integrating GRC practices

that integrated GRC should be bifurcated into two distinct areas: (1) integrating risk management with strategy-setting and performance management; and (2) integrated compliance. The reason for this bifurcation is that the constituencies for implementing the two areas are different in most organisations.

- Keep the integration process simple to achieve the appropriate breadth of risk and process coverage; specific areas can be drilled into further, based on the initial results and management's prioritisation.
- Enable the effort through GRC technology that facilitates collaboration among people in different silos and drives processes for integrating information for decision-making. The credibility of the integration process increases when decision-makers have just one version of the truth to work with, which is made possible through a single originating source for specific data elements.

Build a business case

There is a growing body of research that suggests integrated GRC efforts drive real value, especially as it pertains to optimising risk and compliance coverage and the underlying cost structure. However, there are no benchmarks, statistics or vision statements that compel an entire organisation to embark on the journey without understanding what benefits the organisation will specifically derive. Development of the business case starts with defining goals that correlate to the desired level of programme maturity and articulates the economic justification for moving forward. The steps for achieving value outlined in this article focus on organisations seeking to optimise their coverage and cost structure.

The first step is to assess the current coverage by establishing a complete GRC process universe, performing an enterprise risk assessment and identifying gaps or overlaps. The business' core mission and related strategies drive the business structure inclusive of its offerings, geographic footprint and legal entities, as well as the critical business processes and systems required to support the business model. Risks spanning strategic, operational, financial and compliance objectives originate within these structures, processes and systems. While events related to strategic risks often lead to significant reductions in shareholder value, it is important to note that, often, any one of these risks can have a deep impact on the business if it impairs the organisation's ability to execute its strategy successfully. That is why the essential activity in building a business case is in performing an initial enterprise risk assessment to determine where there are gaps, overlaps or overweighting in any of the risk areas described above.

The results of the assessment should be the identification of the most critical risks inherent in the business strategy as well as the consideration of such risks in establishing the key metrics and targets that drive the business. In addition, there is a value proposition around developing recommendations for efficiency or optimisation to address the identified overlaps. While quantifying the value of reducing gaps in coverage and related financial exposure may require more in-depth analysis, these initial steps begin the process of integrating GRC activities and, most important, help management gain knowledge of what they don't already know. Finally, communication should not be limited to executive management. Development of a campaign to support the integration effort is vital to socialising the new programme among key stakeholders.

Establish a GRC committee

A GRC committee should be established to promote change and co-ordinate planning efforts. It is important to recognise that the beneficiaries of integrated GRC are often executive management. Because integration requires individual silos to grant concessions on portions of their specific methodology to advance the overall effort, executive sponsorship is critical to establishing an integrated GRC programme.

The GRC committee should strive to reduce the impact on stakeholders. In this regard, a strong programme administrator to facilitate collection, management, analysis and reporting of information is essential.

Finally, the central GRC committee is responsible for co-ordinating planning efforts. It is important that a matrix of the entity structure and GRC domain classifications be used as the basis for planning. This combination helps ensure that the requisite skills are deployed to various areas of the business while reducing the likelihood that individuals with similar skill sets are duplicating efforts.

Develop a unified risk framework

Next, the organisation should develop a consolidated risk framework consisting of an agreed-upon GRC universe, inclusive of GRC contexts and a meaningful assessment model. The general ledger/ entity reporting structure should form the basis of the GRC universe to ensure relevance with respect to management's strategic and other business objectives.

While it is important to agree on the core entity structure to co-ordinate planning and ongoing rationalisation efforts, compromises can be made in order to develop a set of inclusive GRC contexts. Defining the appropriate GRC contexts is the way the GRC committee defines the scope of the integration effort. For example, compliance-focused context (e.g., financial reporting assertions, specific regulatory requirements), frameworks promulgated by standards-setting bodies (e.g., ISO, COBIT) and enterprise risk types all share a common quality: they are primarily used to categorise specific risks, incidents, events and/or required controls. When developing a unified risk language, similarities among these different contexts should be mapped so that differences can be accommodated. The business owns the specific risk, not the process owner or business function. Similar to the way an enterprise resource planning system rolls up transactions into various reporting structures, risks can be documented once, tagged to multiple contexts and aggregated into an integrated GRC framework to support appropriate oversight by various stakeholder groups.

Finally, it is vital to develop techniques to uniformly assess risk across the enterprise. Remember to keep the process as simple as possible. Several suggestions to consider in developing a uniform assessment model are:

- **Inherent risk** – Develop an assessment model that accommodates both qualitative (e.g., impact on business continuity, reputation, human resources, regulatory compliance) and quantitative (e.g., financial loss) impacts. This model accounts for impacts that are not easily quantifiable, but could affect the business significantly.
- **Tolerances** – Attempts to establish tolerable, or target, risk can prove to be an academic exercise unless using specific metrics against established objectives. Traditional models have rated inherent, tolerable and residual risk across a 'high, medium, low' scale. This 'numerology' assessment is highly subjective and its usefulness is questionable at best, since risks are often measured in different units of measurement, just as different objectives are measured. An alternative is to employ key risk indicators, which can account for different units of measurement across risk types.
- **Residual risk** – Consider a scoring model that implies the action to be taken or required to monitor a particular risk (e.g., more efforts to quantify, active monitoring, continuous review, periodic review, no further action required) versus traditional high, medium, low scales. A residual scale that implies an action bias avoids the subjective assessments of residual value through arbitrary numerology, providing management and GRC teams with direction on how to improve the management of the risk.

Establish centralised oversight and reporting

Centralised oversight and reporting should be established to aggregate information by GRC context and deliver a single board-level GRC reporting package. This reporting package should provide a single source of the truth to executive management, yet be aggregated into different contexts for specific use by individual stakeholder groups. In this regard, the package supports management's decision-making with respect to resource allocation and pursuit of strategies. It also helps management apply lessons learned across the business, which results in reduced losses and fewer near-misses. Most importantly, the consolidated package provides a means for further rationalising the GRC programme, tightening the effort to a core set of activities that can be 'fanned' to manage multiple risk and compliance issues, both as they exist today and as they emerge tomorrow.

Summary

"One day we must come to see that peace is not merely a distant goal that we seek, but that it is a means by which we arrive at that goal. We must pursue peaceful ends through peaceful means." (Martin Luther King, Jr.) The process of integrating GRC practices also is a means rather than an end. Real value can be achieved, as long as all stakeholders work with one another and take practical, measured steps toward integration. Ultimately, the journey leads to aligning risk management with enterprise performance management and the effective integration of compliance activities.

Protiviti's Technology Offering

Protiviti's Governance Portal (www.protiviti.com/grc-software) integrates content and commonly accepted and proprietary frameworks with world-class consulting expertise into a comprehensive platform, giving organisations the visibility and insight needed to manage and mitigate critical risk and compliance issues today and in the future. The Governance Portal will provide you the targeted GRC solutions you need today, and help you converge multiple GRC practices into a single enterprise platform that aligns sound governance with business performance.

About Protiviti

Protiviti (**www.protiviti.com**) is a global consulting and internal audit firm composed of experts specialising in risk, advisory and transaction services. The firm helps solve problems in finance, operations, technology, litigation and GRC. Protiviti's highly trained, results-oriented professionals provide a unique perspective on a wide range of critical business issues for clients in the Americas, Asia-Pacific, Europe and the Middle East.

Protiviti has more than 60 locations worldwide and is a wholly owned subsidiary of Robert Half International Inc. (NYSE symbol: RHI). Founded in 1948, Robert Half International is a member of the S&P 500 index.

Contacts

Scott Gracyalny, Managing Director,
Risk Technology Solutions
T: +1 312 476 6381
E: scott.gracyalny@protiviti.com

Scott Wisniewski, Director, Product Management
T: +1 321 476 6302
E: scott.wisniewski@protiviti.com