

**MARK L. FRIGO, PHD, CMA, CPA**

DIRECTOR

THE CENTER FOR STRATEGY, EXECUTION, AND VALUATION

DEPAUL UNIVERSITY

**RICHARD J. ANDERSON, CPA, CFSA**

CLINICAL PROFESSOR OF RISK MANAGEMENT

THE CENTER FOR STRATEGY, EXECUTION, AND VALUATION

DEPAUL UNIVERSITY

# 10 STRATEGIC GRC: Steps to Implementation

A structured, informed approach to governance, risk, and compliance efforts can help leverage cross-functional synergies and increase organizational efficiency.

**D**RIVEN LARGELY BY LEGAL AND REGULATORY requirements, many organizations have made significant investments in their risk and control functions during the past few years. As a consequence, areas such as compliance, legal, internal auditing, and enterprise risk management (ERM) have expanded in size and scope. Even before the current environment of cost reductions, these expansions began prompting concerns about increased

expenses and duplicative activities among the various risk and control functions, including internal auditing. Moreover, each function often maintained its own unique definition of key terms such as risk and compliance, which created the potential for confusion among stakeholders.

Borne out of these concerns was the advent of governance, risk, and compliance (GRC) initiatives, which seek to improve efficiency and effectiveness across an organization's risk and control functions. Internal auditing is often involved in these initiatives, given its role as a critical GRC function. GRC initiatives can provide internal auditors with numerous opportunities to enhance audit processes and knowledge activities, yet they can also present auditors, and the organizations they

serve, with many challenges. Accordingly, auditors need to understand GRC processes and position themselves to help the organization both achieve GRC benefits and avoid the potential pitfalls.

#### WHAT IS GRC?

GRC initiatives help enhance overall governance by leveraging common processes and increasing knowledge sharing and coordination across the organization's GRC functions. For example, GRC often seeks to integrate risk assessment processes, which are frequently performed separately by individual functions, thereby gaining efficiencies. Leveraging risk assessments cross-functionally helps eliminate gaps in processes or coverage, and it enhances effectiveness by increasing information sharing and coordination of activities such as scheduling. Additionally, GRC helps the organization ensure more consistent views of risk and prioritize issues requiring management's attention as well as its responses. GRC initiatives also provide an opportunity to rationalize and reduce some costs as well as ease the burden on business units by improving coordination and clarification of roles.

As with many new and developing initiatives, GRC can be detrimental to individual risk and control unit effectiveness if not managed carefully. GRC objectives must be clear, and those charged with establishing them need to consider what each objective should and should not include. Moreover, the initiative must focus on how GRC functions achieve their missions, rather than rethinking or blurring core roles. Any GRC program must recognize and protect the unique roles of each function

while also recognizing the potential benefits of leveraging core skill sets, common processes, and knowledge. If the initiative is designed or perceived simply as cost cutting or organizational restructuring, many potential benefits will not be achieved. GRC's underlying goal is integration of common processes and alignment of focus, not added competition or distractions among GRC units or creating infrastructure that did not exist before.

GRC is a developing concept that must be managed attentively and tailored to

fit each organization's unique environment and circumstances.

**1 COORDINATE GRC FUNCTIONS** Management should begin by forming a working team and identifying the GRC functions that should participate in the initiative. Although most of these functions should be readily known, broad consideration should be given to the selection process. Internal auditors, given their enterprisewide perspective, can help identify areas of GRC activity throughout the organization.

**Any GRC program must recognize and protect the unique roles of each function while also recognizing the potential benefits of leveraging core skill sets, common processes, and knowledge.**

each organization. It should be adapted to the organization's specific needs, control culture, and governance structures.

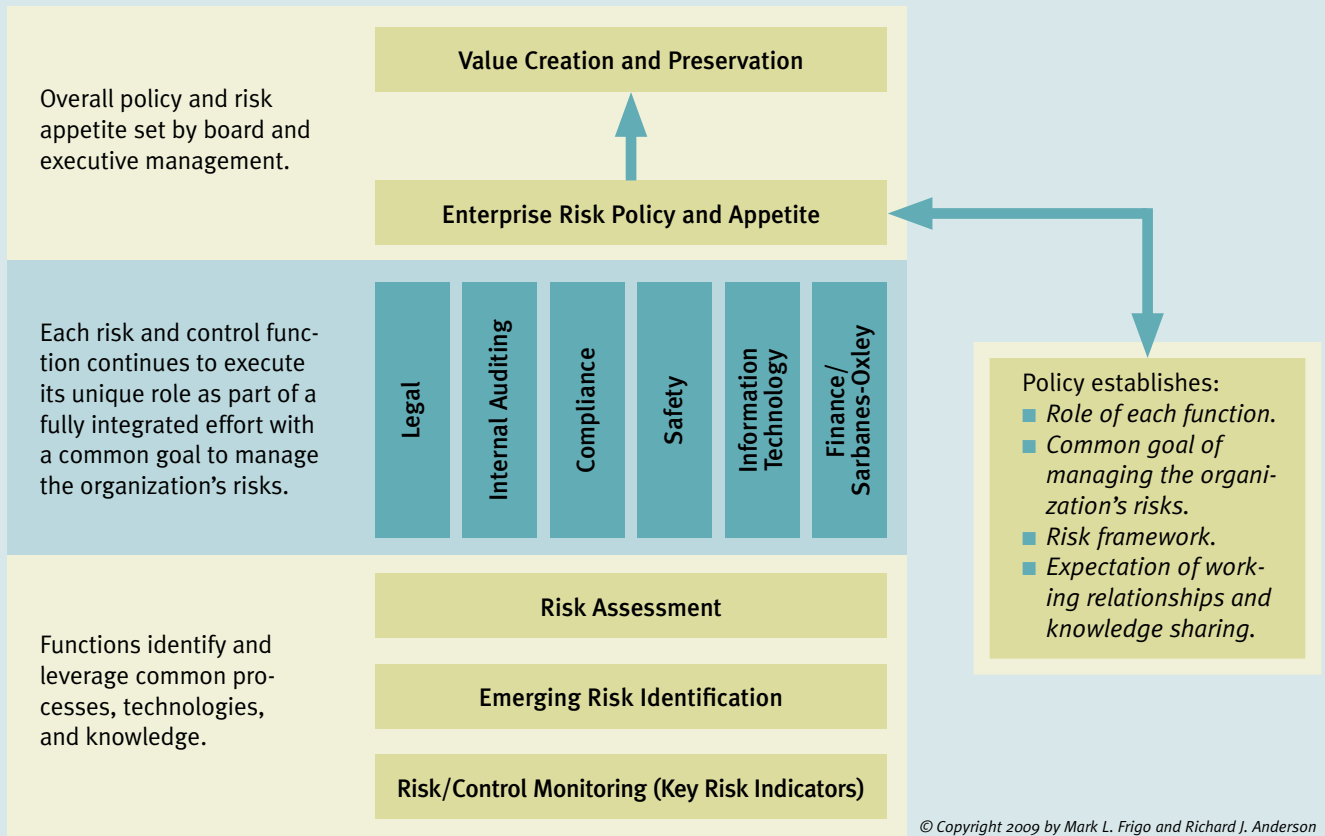
#### 10-STEP APPROACH

Strategic GRC design and implementation can be aided by a basic, 10-step approach. The steps provide a platform for learning, educating, and establishing buy-in across GRC functions, and they are designed to lead organizations through a practically oriented process where each action builds on the next. They also facilitate and support the development of tailored results that best

Next, the working team should establish a common understanding, goals, and an initial vision, including clarification on what constitutes a GRC initiative. At one U.S. financial services organization, the GRC working group developed a simple set of common objectives for its initiative:

- Agree on a common risk management concept for functions across the company that handle risk (risk management functions).
- Maintain the independence/objectivity of each risk management function.

# Strategic GRC Framework



A source of some confusion and misunderstanding related to GRC has been the lack of a basic conceptual model or framework. To address this problem, the Strategic Risk Management Lab at DePaul University developed the Strategic Governance, Risk, and Compliance Framework. The framework has three basic components:

- A strategically focused top, which ties into ultimate shareholder value.
- A middle section that represents the individual GRC functions.
- A bottom that comprises common, integrated processes.

The top, strategic section, and in particular the board-level risk policy segment, represents a key element of the framework. It requires a common view of organizational value creation and protection and provides a set of shared, high-level risk policies to ensure consistency of purpose and thinking across GRC functions. This top-down approach also drives greater communication among GRC functions and more consistent reporting. Bottom-up approaches, by contrast, can easily fail as they increase the likelihood that siloed units may continue to pursue their own goals and objectives in the absence of a policy from the top. Without this strategic umbrella in place, achieving GRC benefits can be very difficult.

The middle portion of the framework recognizes that individual functions have unique roles that must be maintained for the integrity of organizational governance. This component is especially relevant for internal auditing. Without a clear acknowledgment of each function's value, organizations simply looking to cut costs may be tempted to distort internal auditing's role or merge it with other GRC functions.

The framework's bottom section identifies core processes that can be leveraged across GRC functions. It also emphasizes that, once the strategic framework is in place and understood, the organization should consider whether future investments in knowledge capabilities and technology can be made on a collaborative basis.

The GRC framework can be a useful tool for internal auditors seeking both to foster understanding and facilitate implementation of GRC initiatives. Auditors and their clients should keep in mind, however, that while the framework helps organizations think and act with high-level consistency, it is not meant to serve as an organizational chart around which to restructure.

For further reading on the GRC Framework and its role in strategic risk management, see the forthcoming book by Mark L. Frigo and Richard J. Anderson, *Strategic Risk Management: A Primer for Directors and Management Teams*, 2009.

- Rationalize and harmonize approaches to risk across the organization.
- Increase information sharing across the risk management functions.

The organization viewed this working group as a first step in developing and evolving its view of GRC. In particular, it focused on increasing the interaction and information sharing across the company's risk functions.

**2 DISCUSS WITH MANAGEMENT AND THE BOARD** The initial vision and objectives established by the working group should be articulated and discussed with executive management and the board or audit committee. This dialogue should include a concise discussion of both the benefits and potential pitfalls of the initiative. The Strategic GRC Framework on page 35 can be used to facilitate discussion and ensure understanding among all parties. This

stage of implementation also presents a significant opportunity for internal auditing to serve as a strategic adviser to executive management and the directors.

As the working group seeks management and board support, discussions should also take place across the GRC functions to ensure a clear understanding of the initiative's goals and objectives. The group should also consider discussing the initiative with third parties such as external auditors or regulators.

**3 IDENTIFY INITIAL OPPORTUNITIES** The working group's focus should next shift to the identification of areas where initial opportunities for improvement may exist. Organizations usually start by reviewing processes involving communications, knowledge sharing, scheduling, and risk assessments. When examining communications activities,

many organizations have found that establishing common criteria for issue significance and consolidating issue tracking and reporting across GRC functions represents "low hanging fruit" and an effective way to focus management and director attention. Organizations have also found that sharing and coordinating the GRC functions' examination or audit schedules and making on-site visits to business units can reduce some of the apparent burden on those units. Moreover, organizations may be surprised by the number and variety of ways that risk assessments are performed across their GRC units. Risk assessment activities therefore may be another fruitful area to explore during the initial endeavor to reduce efforts and build consistency. Also, when examining risk management, organizations can ensure that developing topics such as *strategic risk management* are defined

## A Dual Role

Internal auditors play a dual role in GRC processes. First they are GRC participants, seeking to achieve benefits that will help them perform their internal audit role more effectively and advising management and the other GRC functions on GRC practices. Second, internal auditors are responsible for providing assurance over the adequacy of their organization's governance, risk management, and control activities. Playing a dual role is not new for internal auditors; many practitioners, for example, provided both consulting and assurance services in helping their organizations address U.S. Sarbanes-Oxley Act of 2002 requirements.

Serving as an adviser, while protecting operating independence, is not only possible but also consistent with the *International Standards for the Professional Practice of Internal Auditing*. Standard 2110: Governance, calls for internal auditors to "assess and make recommendations for improving the governance process" in accomplishing certain objectives. These objectives include several items detailed in the standard that fit well with GRC initiatives, such as communicating risk and control information to appropriate areas of the organization.

How internal auditors deploy themselves and manage their dual role depends on the particular status of their department. In some instances, internal auditing may be the lead catalyst in helping the organization understand the benefits of GRC and initiating a GRC project. In others, a different risk or control function may be the catalyst, while internal auditing provides an objective voice in advising both the GRC project team and management. In both scenarios, internal auditors help the organization realize the value of GRC and protect the overall integrity

of the risk and control environment. Their advice is particularly critical in making sure that all parties involved clearly understand what GRC is. Moreover, clarity of objectives and goals is key to the success of GRC initiatives, and internal auditing can be a powerful voice in keeping the objectives focused and ensuring that the integrity of the organization's overall GRC processes and roles are protected.

Internal auditors can also help ensure the organization seeks a solution that reflects its goals, culture, and stakeholder expectations. GRC is still in its infancy and should not be approached with a "cookie cutter" mentality. Internal auditors have the experience of working with other GRC functions and can use that experience to help shape the right solution.

In this manner, internal auditing can provide assurance on the overall integrity of risk and control functions while also realizing benefits for itself. Potential benefits include enhanced risk assessments and risk monitoring, access to additional data and knowledge resident in other functions, and enhanced communications. Moreover, the organization and its directors can benefit from a common definition of *significance* for issues and a common issue reporting and tracking process across GRC units. In the long run, increased effectiveness coupled with greater consistency and alignment around the organization's view of risk will lead to greater stakeholder satisfaction with internal auditing. Auditors, then, should not look at participation in a GRC initiative as a threat to their independence, but rather as an opportunity to serve as a strategic player, assisting the organization with a major initiative that aligns with their expertise.

consistently across the organization and that competencies for this area exist where necessary.

**4 DEVELOP INITIAL PROJECT PLAN** Following the identification of initial opportunities, detailed plans should be developed to tackle the inception projects. Resourcing needs, in particular, should be considered carefully. The organization should consider enlisting proven team players who are well-suited to nontraditional assignments. Moreover, the plan should include

The organization should also take this opportunity to establish its risk appetite. Defining risk appetite is an evolving area, and one that many boards have not yet undertaken. The risk policy development process provides a perfect inroad for addressing this often-neglected area.

Internal auditors can contribute to policy development, and they can help educate others involved in the process. Depending on the organization, for example, some higher level education may help board members understand the

**8 FINALIZE BOARD RISK POLICY** The organization should be able to finalize its board risk policy at this point, including the GRC vision and goals, using the output from the working group re-assessment. Depending on what the group learned as a result of the initial projects, this process may entail a simple validation or a more substantial rewrite of the policy.

**9 APPROVE RISK POLICY AND GRC STRUCTURE** Formal approval by the board or audit committee will be required. Internal auditors again have an opportunity to display their expertise during this step, as directors may look to them for assurance on both the design and implementation of the GRC structure. By taking the lead in interacting with directors and management at a strategic level, internal auditors can not only improve GRC efforts but also help increase their visibility and stature in the organization.

**Once the final plan is complete and the risk policy and structure are approved, the organization should be positioned to execute the plan and achieve the established vision.**

feedback mechanisms to capture what worked well for the project team as well as any impediments it encountered.

Internal auditors can play a significant role in these initial projects. They should assess carefully how their expertise and knowledge can be leveraged or further developed, if necessary, to participate fully in the GRC initiative. For example, with their enterprisewide perspective, internal auditors are well-positioned to help identify and rationalize duplicative processes such as issue tracking. Internal auditors also can bring the perspective of the audit committee to bear on these initial projects.

**5 DRAFT A RISK POLICY** The organization's overall risk policy represents a critical component of any GRC initiative. Policy development must be approached thoughtfully, and the right players need to be involved to ensure the appropriate legal, technical, and corporate governance perspectives. For some organizations, development involves simply updating or revising an existing policy. For others, the process will entail creation of a new policy subject to significant high-level visibility and discussion.

developing area of risk and risk management or its growing importance to parties such as rating agencies.

**6 EXECUTE INITIAL PROJECT PLAN** As with any effective project management process, measurement points and success factors should be defined, and processes should be developed to implement them. This stage should include implementing the feedback mechanisms created during GRC plan development to capture lessons learned.

**7 REVISE VISION AND PROJECT PLAN** At this point, the working group will have gained practical experience and obtained results from its initial projects. The team should next conduct working sessions to re-assess the GRC vision, goals, and approach based on those experiences. This process will enable the team to articulate a final vision and develop goals that are tailored to the organization. Attention should also be given to ongoing processes for continuous improvement, as GRC practices will likely evolve over time. Lastly, the final vision and goals should be validated with the GRC functions and key stakeholders.

**10 EXECUTE FINAL PROJECT PLAN** Once the final plan is complete and the risk policy and structure are approved, the organization should be positioned to execute the plan and achieve the established vision. Resourcing needs should be well-understood at this stage, as should the related measurement points and overall definition of success.

#### MOVING FORWARD

By serving as strategic advisers to executive management and the board, auditors can help the organization realize the benefits of enhanced GRC. Furthermore, internal auditors can help stakeholders understand that with the relative newness of GRC, a simple, iterative approach should be used to implement the initiative, giving all GRC functions opportunities to understand fully the objectives and goals. Accordingly, internal auditors are uniquely positioned to help ensure that GRC efforts are effective, produce the expected benefits, and result in a GRC process that strengthens the organization's overall governance program.

*To comment on this article, e-mail the authors at [mark.frigo@theiia.org](mailto:mark.frigo@theiia.org).*