

The power of principles:

How to get back to business through
sensible integration of governance,
risk, and compliance*

Table of contents

Situation p. 2

An accelerated rate of change, greater complexity, and increased transparency have created an avalanche of new risks and opportunities. As a result, many organizations have directed significant time and resources to governance, risk, and compliance (GRC). Having stretched their oversight capabilities to the breaking point, some companies have had to divert attention from revenue-generating activities. Integration of the potentially dozens of oversight functions and committees duplicated across multiple departments and geographies can mean increased efficiency and the opportunity to drive improved performance.

Our Perspective p. 8

A principles-based approach to integrated governance, risk, and compliance (iGRC) enables companies to take incremental steps toward achieving both risk-based resource allocation and sustainable efficiencies. Anchoring the analysis in principles and systematically evaluating how people, process, technology, and information are used to apply the principles helps management focus on *what* has to be done rather than *who* reports on it or *where* it occurs. Further, organizations can take gradual steps toward iGRC. By using this approach to capitalize on their best practices, companies can reallocate business unit resources to revenue-generating roles, control skyrocketing GRC costs, and make key business decisions on a risk-reward basis.

Implications p. 14

The evolution to iGRC is based on logical integration opportunities. Once an organization has defined its scope, integration can be executed along three avenues: within oversight functions, across oversight functions, or within and across business units. This approach allows companies to move toward integration in incremental steps; establishes an efficient GRC infrastructure that enables balancing of growth, risk, and return; and lets management get back to business.

Situation

It is time to drive efficiency and improve performance.

Board and executive leadership is facing an avalanche of new risks—from financial, operational, and strategic risks, to those associated with today’s more rigorous compliance environment. While some risks bring new opportunities, others pose challenges that must be mitigated or managed. With limited resources, business leaders must evaluate and prioritize these risks to strike a balance among growth, risk, and return that is acceptable to stakeholders. Faced with steep financial and reputational consequences for failing to recognize and manage risk, and with competitors prepared to pounce on missed opportunities, many organizations have directed a significant amount of time and resources to governance, risk, and compliance (GRC).

Looking forward, business leaders’ focus on GRC will likely increase for three fundamental reasons:

- **Accelerated rate of change.** Rapid technological advances over the last several years have expedited the pace of business. As the rate of change accelerates, management must become more anticipatory and focused on the proper allocation of resources to drive business performance. This requires a GRC approach that enables organizations to be more predictive and to align risk and rewards through the efficient allocation of resources, both strategically and tactically.
- **Greater complexity.** Leaders often build flexibility into business models to accommodate the accelerated rate and volume of change. The result—from extended business models to geographic diversity—increases the complexity of managing the business. For instance, companies operate under many more regulatory regimes than they have in the past. This challenges management to understand and comply with all applicable requirements. And because of the added complexity, it is more difficult to identify and evaluate new sources of risk, whether from the political environment, from consumer expectations, or beyond.
- **Increased transparency.** Today, stakeholders and the media are likely to learn about an organization’s unmanaged risk almost instantaneously. As a result, management no longer has time to create response plans to remedy the impact of the occurrence on customers, vendors, and investors before the information is made public. This places a premium on the ability to identify, evaluate, and manage risks to the organization’s objectives.

This increased focus on governance, risk, and compliance has stretched many organizations' oversight capabilities to the breaking point. Management's response has been to ensure, often at any cost,¹ that the expectations of key stakeholders, including regulators, shareholders, the board, and rating agencies, are met. Many organizations have responded to new risks, and to the more stringent enforcement of compliance requirements, by creating or strengthening functions, layering processes and roles on top of existing functions. While well-intentioned, this effort has resulted in an infrastructure comprised of multiple independent oversight functions and committees, each focused on a specific GRC challenge. These siloed groups usually achieve their goals, but often with considerable inefficiencies and uncoordinated objectives. Consequently, business units are significantly burdened with GRC-related tasks, and distracted from their core revenue-generating activities; stakeholders and regulators are inundated with divergent information; and management lacks a clear line of sight into enterprise risk.

1 AMR Research has estimated that organizations in 2007 spend nearly \$30 billion on compliance, with 42% of that expenditure associated with the internal headcount allocation. AMR Research Alert Article. "Compliance Is Still a Priority: Total GRC Spending Approaches \$30B in 2007 and Growing," by John Hagerty and Eric Klein, February 22, 2007.

A time for change

Many companies recognize that they cannot cost-effectively sustain this approach, and others are concerned about the impact that future growth will have on an already fractured system. The solution is to integrate governance, risk, and compliance to seize future business opportunities while remaining adaptable to addressing new risks and compliance obligations. But with potentially dozens of oversight functions and committees duplicated across multiple departments and geographies, the task of integrating deep-rooted and widespread infrastructures is substantial—and the stakes are high. Some companies that have tried to meet this challenge have succeeded in creating pockets of improved efficiency. But companies can and must do more to create sustainable efficiencies and drive risk-based resource decisions to improve business performance.

Take incremental steps
toward risk-based
resource allocation and
sustainable change.

Our Perspective Anchor GRC integration in principles.

A principles-based approach to integrated governance, risk, and compliance (iGRC) makes it possible for companies to take the necessary incremental steps toward achieving both risk-based resource allocation and sustainable change at the enterprise level. We have defined the GRC principles essential for integrating risk and performance while enhancing business effectiveness, regardless of the company, function, risk, or regulation. The development of an iGRC framework begins by tailoring these principles to each company's unique environment. Management then determines the method for applying the principles across the organization by examining four operating levers used to execute the principles—people, process, technology, and information. The fact that the framework is based on principles rather than organizational silos enables management to focus on *what* has to be done rather than *who* reports on it or *where* it occurs. And because the framework is designed for incremental execution, gradual steps within it will advance an organization toward an iGRC platform and a more efficient allocation of resources.

By using this approach to capitalize on their best practices, companies can reallocate business unit resources to revenue-generating roles, control skyrocketing GRC costs, and make key business decisions on a risk-reward basis, thereby improving overall business performance.

Consider, for instance, the efficiencies targeted by a major organization for which the cost of GRC oversight exceeded \$200 million and was climbing between 5 and 10 percent annually. Using the principles-based iGRC framework, management conducted an assessment, exploring the root causes of inefficiencies—such as duplication of efforts across functions and unnecessary variations in processes and methods—and identified actions that could result in a 10 to 15 percent savings. In this particular example, the greatest opportunities came from integrating across functions, improving role clarity, and achieving a common understanding of risk tolerance.

Looking just at the regulatory aspect of integration, Gartner, Inc. has estimated that companies that maintain individual initiatives for each regulatory challenge spend 150 percent more on compliance and 10 times more on IT compliance than those that take a proactive approach to integration.²

2 Presentation by French Caldwell, Research VP, Gartner, “Technologies for Regulatory Compliance,” Gartner Fall Symposium, October 2006, Orlando, FL.

What you have to get right

The iGRC principles-based framework cuts across organizational hierarchies that mask potential integration points behind reporting lines and create inefficient silos. The following approach highlights critical factors in achieving an effective and efficient outcome.

Use an accepted set of principles—Regardless of the company, function, risk, or regulation, establishing an iGRC framework that enables businesses to strike the right balance between risk and reward requires the application of a set of core principles. To identify integration opportunities while also preserving those differences that are warranted, management should anchor its assessment and redesign efforts in these core principles. The principles that organizations have used successfully and that can serve as a model for other companies are shown below. These principles are common across the organizational structure and sustain focus on the work itself, enabling management to identify efficiencies in the execution of the principles.

Sample Principles

Objective setting

Risk appetite and tolerance

Roles and responsibilities

Policies and standards

Risk and control assessment

Issues management and remediation

Monitoring

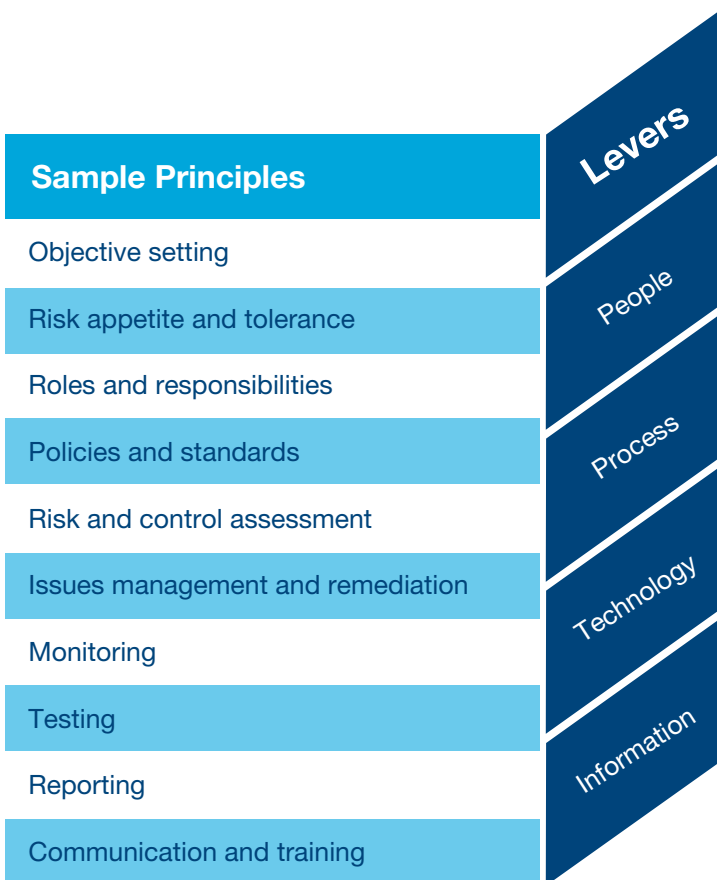
Testing

Reporting

Communication and training

Examine operating levers to identify logical integration points—Once management identifies its set of principles, it can assess the methods used to execute those principles and find the logical points for integration. To tackle this major undertaking systematically, management should evaluate the way people, process, technology, and information—the four operating levers—are used to apply each principle.

The purpose of integration is to combine common processes and information, but it is important to preserve variations in how principles are applied when it makes sense to do so. When identifying logical integration points, an essential consideration is finding those areas where differentiation should be preserved. This selectivity requires understanding the root causes of the differences in how principles



are executed, and distinguishing—based on facts—those differences that are valuable and necessary from those that have evolved simply because of ineffective and inefficient silo practices. Integration is then achieved using options ranging from coordination, combination, and shared-services platforms to co-sourced and outsourced activities.

To illustrate the power of principles, consider the principle of testing. It is a common practice to execute testing activities in multiple organizational units, spanning business and control functions. Initially, it appears as though there is limited opportunity to improve testing efficiency because of the natural inclination to think about testing efficiencies only in terms of the people lever. However, when evaluating testing in the context of the other operating levers, a more comprehensive yet practical view emerges:

- The processes that are used for testing are often inconsistent. Absence of consistency hampers communication between groups and results in a lack of common standards for test scoping, test execution, and deficiency identification.
- The testing effort is often supported by multiple systems or, in some cases, a complete lack of technology. This creates either wasted spend or leaves the organization dependent on heavily manual efforts.
- Information—the actionable product of people, process, and technology—is often uncoordinated and redundant. This impacts test reliability and prevents the organization from efficiently satisfying new or evolving demands. Viewing testing through the lens of all four operating levers can eliminate redundancies and disconnects, enabling improved efficiency and performance.

Implications
Execute along
three avenues.

The evolution to iGRC depends on taking advantage of logical integration opportunities. However, full integration into one standard set of processes is neither practical nor desirable. Instead, integration should occur at sensible points to move the organization toward a GRC platform that is focused on balancing growth, risk, and return.

Starting with a single principle, oversight function, or business unit, management must carefully determine the scope of integration based on its objectives and on the organization's capacity for change. Because integrating disparate processes and information can generate resistance, include stakeholders in the scope-setting process to garner support. Consider the following two scenarios, which illustrate the flexibility that the principles-based approach gives management to match scope to organizational needs.

Scope-setting: scenario one

A company had seen its cost of governance, risk, and compliance skyrocket and was looking to make a change. Management set the scope to include a high-level evaluation across a select number of oversight silos to identify logical points of integration. Additionally, it conducted an evaluation of a single business unit to understand how oversight functions and business units interact. This comprehensive scope enabled the company to develop sufficient information to demonstrate that enterprise change could yield efficiencies without degrading effectiveness.

Scope-setting: scenario two

By contrast, another company, whose concerns centered on only one functional area, Treasury, chose to focus on how the principles were executed within that function. They were not ready for a comprehensive overhaul or enterprise-wide integration, even if such an integration were limited to a single principle. Their goal was to establish within Treasury a set of activities that would enable the functional area to respond to all existing oversight functions without overlap or redundancy.

Take small steps, demonstrate value, and then move on to the next step.

Avenues to integration

Once an organization has defined its scope, integration can be executed along the following three avenues. Each avenue yields distinct benefits. Therefore, depending on an organization's appetite for change and desire for efficiency, integration can be achieved along any one or a combination of these avenues. Keep in mind that execution is an iterative process that involves taking a small step, demonstrating value, and then moving on to the next step.

Avenues to Integration



Integrate within oversight functions. Efficiency is achieved by integrating activities within those oversight functions responsible for multiple programs—such as compliance or information security. Once management has identified the logical integration points, it can begin to define the people, process, technology, and information that can be leveraged to achieve each principle. This process establishes an operating model for each principle within the oversight functions.

To illustrate the potential benefits of this, consider the changes made in the Operational Risk department at a large U.S. financial institution. The department used multiple, disparate databases across geographies and businesses to capture and report deficiencies. Therefore, it was not uncommon for a single deficiency to be reported several times. And it was not always clear which business unit had responsibility for correcting these deficiencies. Additionally, differing standards across products and regions were used to report risk and control assessments, to record deficiencies, and to track remediation efforts. As a result, management had difficulty determining which risks were the most substantial to the organization, a situation that compromised its ability to make decisions and meet regulatory requirements.

To remedy the situation, Operational Risk integrated the databases, created a standard process by which to report and record deficiencies, established ownership of each issue, and instituted a common reporting structure to disseminate information to business and corporate management. Concurrently, the number of senior officers involved in deficiency oversight committees was reduced to create greater efficiency, clarify ownership of issues, and enable officers to return to business unit responsibilities.

Integrate across oversight functions. In addition to integration within oversight functions, management should consider logical integration points across those functions. Drawing on people, process, technology, and information practices used in individual functions, management should establish an operating model for each principle across oversight functions. Again, the focus is on what is being done, not on the associated function.

A case in point is a global financial services company that used multiple systems to assess and control operational risk. The policy that guided these risk-assessment activities was loosely enforced and interpreted differently across the risk and control assessment (RCA) units. As a result, it took months to aggregate reports at the corporate level. Additionally, the fragmented systems were expensive and produced unreliable information.

By applying the iGRC framework, a standard risk and control assessment program was implemented across the organization. The company used the framework to identify the common principles underlying the RCA process and examined the levers of people, process, technology, and information for efficiency opportunities.

As a result, the time frame for producing RCA reports was reduced from months to weeks, and the reports' accuracy, consistency, and coherence were substantially improved.

Integrate within and across business units. From a business unit perspective, the iGRC framework is critical to driving enhanced performance through risk-based decision making and to improving efficiency by integrating business unit actions into operating models for each principle. Management uses the GRC principles to help make decisions regarding risk and return, which, in turn, help drive improved business performance. The application of the principles in strategy setting and business planning is an example of this use.

At this point management can also assess interdependencies among principles. For instance, a lower risk appetite puts greater strain on risk identification and assessment activities. When management recognizes this interdependency, it can place the appropriate focus on risk identification and assessment to ensure that the operating model is sufficiently robust.

Consider the case of an international financial services company that set out to create a standard report to strengthen its network of committees charged with overseeing risk management and compliance. The committees existed in business units, functional areas, and internal audit. The reporting methodology utilized disparate databases and manual processes. Reports had differing taxonomies, were slow to be produced, and were heavy on data and light on analysis. The goal was to create consistency throughout the enterprise by using similar reports containing sections for local or specific responsibilities. The reports would be based on enterprise-wide control metrics and would aggregate information from all oversight functions, identifying the most important issues and the appropriate response strategies.

The company created a prototype for one business unit. Next they developed uniform methodologies for entering and maintaining the information, as well as a procedure for transforming the desktop-supported system into one that would be supported by a single database. This resulted in a consistent, coherent basis for management to assess its risk management and compliance priorities. The solution eliminated reporting redundancies, reduced workloads, accelerated reporting timelines, and enabled risk-based decision making.

Getting back to business

With the increasingly complex and fast-paced business environment, management must act now to build a sustainable, efficient GRC infrastructure that enables organizations to balance growth, risk, and return. The principles-based iGRC framework provides the means to achieve this goal in incremental steps, enabling companies to move toward integration at a speed that matches their appetite and risk tolerance—allowing management to get back to business.

For further information, please visit:
www.pwc.com/igrc

or call:
1.800.639.7576

Performance Improvement
Integrated Governance, Risk, and Compliance