Do You Need A GRC System?

A candid look at Governance, Risk and Compliance systems—and how to succeed with the right solution.

By Susanne Elizer, Shawn Martin, and Eric Knutson

Today’s Environment
Many companies are facing an increase in compliance issues, regulatory scrutiny and shareholder oversight. No company wants to be surprised by a charge of noncompliance, a troublesome audit finding, or the rise of an unforeseen crisis. Depending on the event, the repercussions can range from distracting and disruptive to devastating. A robust governance, risk and compliance (GRC) system provides several main benefits to an organization while keeping you on top of changing regulations. In addition, streamlined GRC processes can help executives save and manage resource allocation for audit and controls testing. The right system will give people across the organization the tools to eliminate redundancies, leverage previous audit work papers, schedule controls and tests systematically and allow them to reuse previous audits and data. As organizations grow, a GRC system supports the move from a tactical, check-the-box compliance approach to a more strategic approach that reduces risk by increasing visibility and control.

Point B’s Perspective
Point B works with clients across diverse industries to evaluate and implement GRC systems as part of a strategic approach to governance, risk and compliance. Not every organization needs a GRC system. But they’re increasingly valuable for promoting strong corporate governance and enterprise risk management (ERM), and for demonstrating good-faith efforts to comply with laws and regulations, which has been a growing space since 2001. GRC systems are important, even imperative, to organizations that:

• Are in a business or industry with a low-risk tolerance for fraud, other risk events or are heavily regulated.

• Must meet multiple or complex compliance requirements.

• Face a number of risk management, compliance and audit processes—often as a result of industry consolidation.

• Want to give senior executives a better way to view and evaluate risks and actions across the organization.

Finding the right fit.
Involving key stakeholders in system requirements and selection will go a long way to ensuring successful implementation. This is the time to establish common expectations in the form of your risk framework, which may address any or all of the following categories: market, operational, or credit risks. Keep in mind that a GRC system is designed to inform decision-making, assist in resource allocation, and inform your strategy in managing risk portfolio. The right GRC system will give executives a window into the health of their dashboards with drill down capabilities and automatic alerts that provide strategic insight. In establishing system requirements, consider the information required to help make informed decisions. A successful implementation will focus on ease of use and access to relevant data.
Do You Need A GRC System?

delivered in a timely fashion. The system should integrate easily with existing operational processes—augmenting existing capabilities. It should excel at the GRC functions you’re looking for, while functioning within the limitations of your organization.

Consider the product vision and vendor.

When evaluating vendors, be aware of the variability among GRC systems. Avoid outdated patchwork solutions with disparate components that have been cobbled together through acquisition. Look for seamless, streamlined enterprise solutions backed by an experienced GRC vendor’s strategic roadmap and product vision. You’ll find that all leading vendors’ systems support the Unified Compliance Framework (UCF), a GRC industry standard among other regulatory compliance standards such as COSO, SOC, PCI, etc. To meet consumer demand, most of the solutions in the market are beginning to develop mobile offerings. Allowing auditors to work more efficiently (no longer needing to carry a test plan or audit form print out, but also enabling them to work offline and sync items later. Another consideration in your vendor selection should be their ability to migrate your existing data, documented processes or previous audit and control data, and artifacts. As with any system you invest in, the vendor’s long-term viability and support are essential. Price and price structure matter, too. Consider the full implications of price and how it’s structured, from licensing costs to implementation and ongoing support. What structure best serves your company?

Focus on GRC functionality.

Most vendors are happy to provide a hands-on demo of their GRC system, loading it with data you provide in advance.

Look at the robustness of the system. How well does it accommodate your risk framework, configure to your environment, and integrate with your enterprise IT solutions? Do you have unique risks to your intellectual property that you want to protect? Consider how granular you’ll want to get with the data you collect, analyze and report. Dynamic updating is imperative. Compliance regulations change, and the value of an integrated GRC system is its ability to keep your data current for users across the organization. You’ll want the system to deliver timely and thorough updates as compliance rules change. Make ease of use a key requirement, including automatic triggers that alert users to changes in regulations and compliance matters. An intuitive system will reduce training time and boost adoption. Finally, be clear about your ongoing support requirements—and be sure that the vendor is, too.

Phased implementation may be the answer.

We often recommend a phased implementation of GRC systems. It’s an approach that respects the full scope of organizational change that’s typically required. You may want to conduct an analysis that considers the scope of the implementation and aligns your implementation plan with the magnitude of change it means for the organization: Is it rolling out across all divisions, or just one? Is it a dramatic change that will take stakeholders beyond their comfort zone? Or is it a more modest evolution for a few true believers? What are the organizational politics around this implementation? Were you able to build buy-in earlier in the process by engaging stakeholders in setting system requirements?

The Bottom Line

As risk and compliance issues and processes become more complex and dynamic, a GRC system can help you manage them efficiently and effectively. In selecting a system, know how you plan to use it and what you want to get out of it. Pay attention to change management issues and address them early on. The same transparency that benefits risk and compliance issues will serve you well as you select and implement your GRC system.