



One for Three

Should governance, risk management, and compliance be tackled as one problem, or is this a classic case of scope creep?

[Scott Leibs](#), CFO Magazine

September 01, 2007

The Sarbanes-Oxley Act has long had a digital doppelgänger. Almost from the day it was announced, and certainly since its Section 404 emerged as a major corporate headache, IT companies have hawked products that promise to ease the regulatory burden. Often these have been hastily retooled versions of applications that were originally designed to do something else — manage documents and workflows, for example, or provide a repository or database for business rules.

If these software vendors were hoping for a bonanza, they were soon disappointed. While many companies have, over time, come to see automation as a part of the Sarbox solution, for most it has been ancillary to retooled processes and other activities. And with recent guidance from the Securities and Exchange Commission shifting the focus of Section 404 compliance to an assessment of material risk, instead of an exhaustive cataloging of every facet of every control that organizations rely on, the need to document the minutiae of corporate life may soon abate.

But when it comes to opportunity knocking, software companies and IT consultants have a sense of hearing that a dog might envy. Even before the Section 404 playbook was being altered, vendors were altering their Sarbox applications, morphing them into more-complex and more broadly focused products that could address two related areas heavily affected by Sarbox: corporate governance and risk management.

Thus governance, risk, and compliance (GRC) software was born. At its core it remains a tracking system, capturing data on various compliance requirements as they affect a specific company and chronicling how the company does (or does not) satisfy those requirements.

But the software is now more than an automated checklist. Increasingly it aims to provide more-sophisticated decision-support capabilities. That's in large part because even as the growing list of regulatory requirements creates a new level of risk (namely, the risk that a company won't meet a requirement and will thus face penalties), other forms of risk are also receiving more attention in Corporate America. In fact, the field of enterprise risk management (ERM) is nearly synonymous with GRC, and many GRC products are touted for their ability to help companies monitor and analyze a wide range of business risks, of which regulatory compliance is merely one.

If you find this both compelling and confusing, join the club. Even companies that have embraced GRC admit that they aren't always sure exactly what it means or how far it can extend. Despite the advancing capabilities of the technology, some companies say they prefer GRC software that is limited in scope, and others are pursuing a GRC strategy that focuses on organizational structure and processes rather than IT.

Overlapping Efforts

Despite those differing approaches, however, many companies agree on two key points: there is a degree of overlap between governance, compliance, and risk-management efforts; and a failure to bring some order to bear in addressing those needs often leads to duplication of effort and higher costs.

"Companies now spend about 8.5 percent of their IT budgets on compliance needs," says French Caldwell, an analyst at Gartner. "The next step is to leverage the investments they've made in systems that simply capture data for compliance purposes, and use that data to aid decision making on operational risk and corporate performance."

But while "next step" implies a logical progression, that's not how things play out at most companies. Often, Caldwell says, companies have already purchased more than one software package to address different facets of GRC. That happens for many reasons. One, different groups are often responsible for different aspects of GRC management. Not only might the compliance staff and the risk-management staff be separate, but employees responsible for, say, financial compliance under Sarbox may have no interaction with employees responsible for health and safety compliance under the Occupational Safety and Health Administration, the Environmental Protection Agency, or some other federal regulatory body. Each group often buys a software package that meets its needs. "This often leads to companies paying for several licenses for similar products," Caldwell says. "If they bought an enterprise license for one, they could save a lot of money."

Oracle and SAP have both entered the GRC arena, offering a range of products designed around what Oracle's Chris Leone, group vice president of applications strategy, calls "an orchestration piece that documents and monitors all GRC efforts." As Gartner's Caldwell sees it, "The entrance of ERP companies indicates that the GRC market is real, and for companies that put an emphasis on operations risk management, adopting a single technology platform can be extremely useful."

Many companies prefer to start small — and stay there. At transportation services firm YRC Worldwide, general counsel Dan Churay says that while there are some potential synergies between governance, risk, and compliance, "the degree of overlap is overemphasized, both by vendors and consultants and also by people within companies who may be new to risk or compliance."

YRC worked with Pricewaterhouse-Coopers to develop a GRC strategy built around reporting relationships and risk analysis rather than software deployment. "We are also looking to expand the use of the Sarbox software we've invested in [from Certus Software]," Churay says, "to embed more controls." But the primary focus is on assessing what kinds of risks can be managed centrally versus handled by specialists.

Ahead of Its Time?

At Burger King Corp., senior vice president of finance Chris Anderson points out that the company has 12 pages of risk factors in its 10-K. "No software package could handle them all," he says. And "compliance" means many things at Burger King, from Sarbox (handled by finance) to food safety and attendant federal regulations (handled by a dedicated unit). "We did find Sarbox compliance software helpful," Anderson says, "but we went with something simple that provided a repository for documents and flowcharts."

PwC's Miles Everson, a partner who leads the company's GRC Services business in the United States, says that companies "often own a lot of the software they need. The focus should be on minimizing the number of discrete oversight functions and integrating their activities."

That, software companies counter, is why GRC software makes sense: it provides the technological underpinning needed to achieve such integration. Perhaps the software is slightly ahead of its time. As KPMG's Mark Goodburn notes, "Historically, companies had two things to manage: people and processes. Then IT came along. Now GRC is entering the picture as a fourth dimension, but it will need time to become an integral part of a company's culture."

Gartner predicts a robust 23.8 percent compound growth rate for GRC software through 2010, but AMR Research sees much slower growth in the near term (see "It's All GRC to Them" at the end of this article). Estimates differ in part because definitions of GRC are as varied as they are fluid. The big question for GRC as a software category is whether the integration that it claims to facilitate is something companies will want to undertake.

Scott Leibs is a deputy editor of CFO.

IT'S ALL GRC TO THEM

Spending on various categories of GRC suggests that this three-letter acronym covers an alphabet's worth of ground.

(TECHNOLOGY SPENDING IN \$ MILLIONS)

	2006	2007	2008
Sarbox	\$1,935	\$1,840	\$1,879
Documents/ records retention	1,038	1,169	1,172
Security/privacy	486	674	676
Operational/general risk management	n/a	638	672
Other	\$5,422	\$5,559	\$5,849

*Includes customer compliance, green compliance, manufacturing traceability, SEC regulations, FDA regulations, Basel II, legal discovery issues, import/export tracking regulations, and manufacturing process approval/certification.

Source: AMR Research, February 2007

. © CFO Publishing Corporation 2007. All rights reserved.