Strengthen Your CORE

ARE YOU GETTING THE MOST FROM YOUR COMPLIANCE, OPERATIONS, RISK, AND ENTERPRISE SUPPORT FUNCTIONS?

By James Bierstaker, Kenneth K. Marshall, and Jonathan Greenwald

In setting objectives for or evaluating the performance of CEOs, most often the measures are about strategic direction, market share, revenues, profit margins, assets, new products, and similar growth indicators. Rarely would you see the question, "How do you know you are getting the most from the company's investment in its Compliance, Operations, Risk, and Enterprise (CORE) support functions?"

If you really believe the adage "You get what you measure" (regardless of whether the measure is qualitative or quantitative), how can boards of directors justify not considering CORE support functions when determining how to compensate CEOs and other business unit executives? Stated simply, the behaviors of CEOs and other senior business executives will depend on the measures applied in setting their compen-

Compliance, Operations, Risk, and Enterprise (CORE) support functions include not only risk management and compliance regimes, but also technology groups, operations support groups, finance functions, and operating personnel in business units.

sation and evaluating their performance.

The costs of not having a robust risk management and compliance system can be high. Take, for example, the case of the one trader at French bank Société Générale who made unauthorized trades that resulted in a $7.2 billion loss, despite a compliance system that was supposed to prevent this. Moreover, a lack of risk management procedures at financial institutions may have been at the root of the current economic crisis. This means that regulators will now be focused on CORE controls at financial institutions.

Legislation and Regulation: The CEO's Responsibility

In the aftermath of Enron and WorldCom, as well as industry-wide investigations of mutual funds, investment banking, investment research, and insurance, the financial services industry has had to cope with an unprecedented level of legislation and regulation. The intent is to correct corporate misconduct and force accountability higher up in the organization. Such legislation and regulations include the Sarbanes-Oxley Act of 2002 (SOX); Securities & Exchange Commission (SEC) Rules 38a-1 and 206(4)-7 of the Investment Company and Investment Advisers Acts of 1940, respectively; National Association of Securities Dealers (NASD) Rule No. 3013; and the Dodd-Frank Wall Street Reform and Consumer Protection Act. No matter the legislation and regulation, chief executive officers and chief compliance officers (CCOs) are expected to:

◆ Create policies, procedures, and processes to ensure that employees operate within all legal and regulatory boundaries;

◆ Ensure that the company communicates—and applicable employees understand—the policies and procedures that set forth the corporate principles of behavior;

◆ Design and operate a risk management and compliance program that accomplishes the stated compliance objectives;

◆ Monitor that the company follows policies and procedures; and

◆ Exercise oversight and testing of compliance programs to certify that the program is working effectively.

In addition, the Basel II accord (and now Basel III) and the Markets in Financial Instruments Directive (MiFID) are examples of regulatory drivers of a similar nature that affect non-U.S. companies and U.S. companies with international operations. Adding to the international breadth of recent regulations, companies in many countries are adopting rules similar to SOX. In the March 12, 2007, issue of *U.S. News & World Report*, for example, Ethiopis Tafara, director of the SEC's office of international affairs, explained that SOX-type reforms had been undertaken in all major international capital markets, which is one reason for their maturation.

Moreover, during the recent near meltdown of the financial markets, we witnessed:

◆ The disappearance of such prominent firms as Bear Stearns and Lehman Brothers;

◆ Government rescues of and/or assistance to American International Group (AIG), Citigroup, Bank of America Merrill Lynch, and General Electric, as well as two major automobile manufacturing companies (General Motors and Chrysler); and,

◆ The discovery of major Ponzi schemes at well-known hedge funds.

These events underscore the importance of maintaining risk management and compliance systems that were envisioned in the legislative and regulatory edicts. We probably will see additional legislative and regulatory initiatives roll out to reform banks, insurance companies, investment managers, financial intermediaries, and the regulatory framework within which these institutions operate.

The Corporate Response: Single-Point Initiatives

Addressing the avalanche of new laws and regulations has, of necessity, been undertaken through single-point initiatives directed to each particular law, rule, or regulatory body. Highly detailed and costly documentation efforts have been under way in all public and highly regulated companies, and some of these initiatives overlap each other. What was previously inferred as working by virtue of the existence of written policies and procedures must now be ensured as working through connecting the policies and procedures to governance processes, operational activities, and controls, and supervision thereof, and, finally, to the tests, observations, and other means through which the end-to-end compliance system is determined to be effective.

Imposing all these requirements in compressed time frames has meant adding staff and work throughout the support infrastructure of organizations. This includes not only risk management and compliance regimes, but also technology groups, operations support groups, finance functions, and operating personnel in business units. We'll refer to this extensive risk and compliance program infrastructure as Compliance, Operations, Risk, and Enterprise (CORE) support functions.

Remaining Challenges

Even after expending all this effort in response to new laws and regulations, companies still may find it difficult to maintain their risk and compliance programs. Although firms had managed to implement SOX and SEC Rules 38a-1 and 206(4)-7 by their compliance dates, according to a February 2006 article in *Risk Management*, "Audit Committees Drive Section 404 Sustainable Compliance Oversight" by Ken Daly, several challenges remained:

◆ Ensuring the sufficiency and quality of senior-management involvement in and commitment to the CORE programs;

◆ Providing an audit trail that enables a company to demonstrate the connection between policies and procedures and the actual day-to-day operating activities;

◆ Determining or selecting a manageable number of key performance indicators necessary to detect or prevent noncompliance;

◆ Ending duplication across programs and initiatives, as well as their costs;

◆ Creating a culture of transparency in reporting compliance incidents and compliance problems to senior management and boards of directors; and

◆ Obtaining maximum leverage in using technology to accomplish the organization's risk and compliance objectives, thus enabling CEOs and CCOs to fulfill their annual certification requirements.

Companies are still wrestling with these issues and may be for years to come.

In addition, information technology (IT) poses a problem regarding determining and obtaining key performance measures. IT seems to mean the technology tools that firms have latched onto for the policy components of their initiatives and, to some extent, the measurement, monitoring, and reporting components. Most managers who have endured this journey, however, have indicated that better leverage of technology should be a continued goal. This implies a separation still remains between legacy operating systems through which business transactions flow and tools that companies are adopting to support the recent control and compliance initiatives.

Compliance monitoring and testing also pose a problem. Concrete answers are needed to questions such as:

◆ How are key performance measures obtained, as well as expanded and contracted as appropriate?

◆ Does information for key performance indicators come from normal operating systems, or is it developed manually using Excel spreadsheets, which are subject to error?

◆ Who tests key performance measures? How are they tested? How much testing is enough?

Best Practices

In a recent Ernst & Young (E&Y) survey about the hedge fund industry and the potential increased regulatory scrutiny it faces, *Preparing for Increased Regulatory Scrutiny*, respondents expressed concerns and problems very similar to those we've already outlined. One of the primary purposes of the survey was to gauge the progress and evolving best practices for the hedge fund industry, which has drawn increased concern from regulators and legislators resulting from some recent highly publicized failures (e.g., Amaranth, Madoff, and others), the decreasing barriers of entry, and the greater participation of pension funds in these vehicles. The study suggests that, notwithstanding any temporary delays in having to register with the SEC and become subject to regulatory examinations, firms place more emphasis on end-to-end compliance quality to make certain they meet regulators' and investors' expectations.

We discussed recent industry trends with Alan Fish, the senior partner who sponsored the E&Y survey. He said that, in his opinion, the following issues seem to be present among most institutions: "Risk management as well as compliance and regulatory requirements are increasingly complex and intrusive and have become a growing operational and financial burden. In response to regulatory changes and market pressures, institutions have created tactical solutions within silos. This has led to the creation of multiple risk-governance processes. Institutions have spent so much time and money on regulatory changes that other important responsibilities have not been given enough attention. These include typical control functions and risk management functions that need proper attention to keep pace with business growth. Boards of directors and senior management are requiring more consolidated but understandable risk and control information."

In addition, a 2009 KPMG report, *Preparing for Regulatory Reform*, provides some practical risk management guidance for boards and management:

◆ Acknowledge your responsibilities for managing CORE activities;

◆ Review compensation structures that may drive risky behavior;

◆ Analyze and learn from past risk management failures;

◆ Develop monitoring mechanisms for CORE risks; and

◆ Create mechanisms for consistent identification and disclosure of CORE risks.

Leveraging Technology

One promising approach that some financial institutions are considering is integrating compliance programs into the enterprise risk management (ERM) function. This approach offers many benefits. In these difficult economic conditions, institutions may realize efficiencies by placing compliance risk management in the ERM function as a component of operational risk management, consistent with Basel II. By taking a combined approach to operational and compliance risk assessments, firms may conserve resources and possibly reduce the demands that risk assessments impose on a business manager's time. For example, another 2009 KPMG report, *Maintaining Your Control Environment in Turbulent Times*, included a survey of 1,000 companies and found that leading companies achieved fewer control deficiencies and better coverage while improving efficiency by automating controls.

Yet challenges do remain. A 2008 *Management Research News* study by Vinod Kumar, Raili Pollanen, and Bharat Maheshwari, "Challenges in Enhancing Enterprise Resource Planning Systems for Compliance with Sarbanes-Oxley Act and Analogous Canadian Legislation," found that companies had to modify ERM systems to meet control requirements and needed to address technical, process, and cultural challenges. For example, major technical challenges included systems security, logical access, segregation of duties (i.e., programming vs. production), and cultural factors, including resistance to change. Control implementations were often costly, complicated, and not fully completed.

Avoiding Pitfalls

A 2006 *Harvard Business Review* article by Stephen Wagner and Lee Dittmar, "The Unexpected Benefits of Sarbanes-Oxley," suggested that companies should consider some basic, but important, themes as a means to address common pitfalls stated previously. They include:

◆ Increasing audit committee involvement and oversight,

◆ Exploiting convergence opportunities,

◆ Standardizing processes,

◆ Increasing business managers' involvement,

◆ Reducing complexity, and

◆ Minimizing human error.

In terms of convergence, a technology company took advantage of SOX and combined its requirements with other regulatory mandates to cut costs and gain greater efficiency while it gained compliance. According to the authors: "The company convened a team to identify commonalities among the statutory regimes with which it had to comply, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Gramm-Leach-Bliley (GLB) Act, California's Security Breach Information Act, and other laws to protect privacy and combat identity theft."

As a further example, PepsiCo would get senior business management involved. Wagner and Dittmar said, "PepsiCo uses an annual survey of about 100 senior executives to demonstrate the condition of its control culture. Conducted by the company's internal auditors, the questionnaire probes hiring practices, employee evaluation, contract solicitation, incident reporting, objective setting, and other areas." Not only did PepsiCo benefit from getting upper-level management involved, but they also discovered that inefficient controls existed in some areas, such as pension accounting. If a compliance program is designed to effectively address these areas, a company has a sufficient starting point for meeting its next challenge.

There are other similar success stories as a result of increased compliance. In October 2005, the Information Technology Process Institute (ITPI) undertook a study of 98 IT organizations at a number of different companies. They found that the more compliant a company was, the more efficiently it ran. Their results pointed to the fact that there may be "an unexpected payoff to having a comprehensive set of controls that leads to process improvements for information technology groups." Another interesting finding of the study was that IT industry leaders spent less time on compliance compared to their low-performing competitors because they already had the proper controls in place. Moreover, the study found the best IT groups used a subset of controls, but the low performers didn't. These controls included monitoring systems for unauthorized changes, tracking the change success rate, and using an automated process for configuration management. Several ITPI studies since then have discussed the maturity model for IT governance and other good management practices. What's most important to take away from these studies is that all industries—not IT only—can gain the efficiencies from compliance and good governance.

In addition, a 2007 Aberdeen survey in the area of security and risk management showed that the top-performing firms shared many of the following characteristics:

◆ Consistent security and compliance policies,

◆ A responsible executive (often the CFO) or team with primary ownership for security governance and risk management,

◆ Visibility of key information required to manage security and compliance processes,

◆ Protocols to keep management accurately informed of IT-dependent risks,

◆ Controls to monitor and verify that requirements of internal policies and external regulations are being satisfied, and

◆ Processes to identify all information required for auditing and reporting.

Continuous Improvement

Returning our attention to the implementation complexities and high costs of the well-intended legislative and regulatory mandates, much debate centers on the following single universal truth: You can lay down principles of laws, but you can't mandate or legislate good behavior. Historically, employees who are going to do something wrong will find ways around the laws. The best way to prevent this from happening is to create and maintain a healthy culture of control and compliance that strives for zero defects while, at the same time, rewarding transparency and communications. Too many of the companies that get into trouble have had plenty of written policies and procedures but have had cultures that ignore problems raised or just "shoot the messengers" when they try to point out problems. Nothing can replace a strong and positive tone from the top.

Continuous improvement and rightsizing of CORE programs are imperative when evaluating their ongoing effectiveness. The following four guiding principles can be useful in ensuring the continued effectiveness of the programs:

◆ Analyze recent compliance and risk initiatives for lessons learned,

◆ Review the size and number of ongoing compliance and risk regimes,

◆ Organize ongoing compliance and risk management resources and their activities for success, and

◆ Eliminate inefficiencies resulting from multiple compliance and risk management regimes.

First, in implementing the different initiatives, have we done some things better in one initiative than in others, and should we transport such best practice across all initiatives? For example, if we've leveraged technology extremely well to manage the lifecycle of policies and procedures in our implementation of SEC Rules 38a-1 and 206(4)-7 but are using hard copies and other antiquated means of policy and procedure management in our SOX program, shouldn't we adopt the best practice for both programs? Similarly, one initiative may have resulted in defining and measuring the most appropriate key performance indicators, but in other programs we've tracked either too many or inappropriate performance measures.

Second, have we allowed project teams, which were needed to implement and/or upgrade responsive compliance programs, to remain in place and serve as program management teams? This can result in numerous compliance regimes making demands on the business and support units that might be redundant. Furthermore, personnel and program management teams may require different skills than did the personnel who drove the project.

Third, given the possibility that the numerous single-point initiatives have led to multiple corporate compliance regimes, should we examine whether all of our compliance and risk activities are currently organized in the most advantageous way? The possible convergence of the several single-point initiatives may have led to a lack of clarity of roles and responsibilities across the higher-level control functions of companies so that an organizational review might be of value.

Fourth, are there redundancies and/or inefficiencies in our implementations of the multiple laws? One audit committee chairman stated that he was disappointed that his external audit firm didn't offer suggestions to make SOX compliance more efficient. As an example, he wondered why both the company's management and its external accounting firm found it acceptable to have nine different payroll systems and not mention to the audit committee that they should consider asking management to consolidate them. In other words, he wondered why the testing of controls didn't appear to also focus on possible improvements to the business process. Prior to the acquisition of Salomon Brothers by The Travelers and Smith Barney, Salomon's approach to clearing and settling trades on a product basis (rather than a functional basis) led to its using more than 14 separate money-wiring systems. Although this probably is no longer the case, just imagine the complexity of applying SOX Section 404 or the Patriot Act's antimoney-laundering requirements in environments with such numerous systems that are designed to perform essentially the same function.

Reassessing Your CORE Functions

Connections among policy makers, implementers, overseers, and the reporting on the programs are still fairly informal, so it isn't easy to see a distinct connection. Single-point initiatives to hurriedly implement a particular rule, regulation, or law may have been appropriate because the requirements were driven by separate and distinct regulators and involved a variety of deadlines. Consequently, an unprecedented amount of time and money has been expended on policies and programs just to make sure they're working. In a recent E&Y survey titled *Risk Convergence*, a chief auditor of a commercial bank said: "Most organizations are like us: They got to where they got to not by design, they just morphed into it. The whole risk control self-assessment thing has really evolved recently at a fairly rapid pace. No one actually stood back and said if we were going to design an ideal organization from scratch, knowing that we had to do all these things, what would it look like? I guarantee you nobody's got that organization in place."

Companies need to take certain measures to address the redundancies, convergences, sustainability, and other issues associated with such approaches. For enhanced risk and compliance programs that would mitigate these problems, there needs to be a focus on a systematic and efficient verification process. Through combining and consolidating, program costs can be better managed. Companies also need to assess whether they created a sustainable and repeatable process as opposed to a one-time event. The point should be to avoid reinventing the wheel by adjusting the existing programs so that they have longevity and can be continuously and incrementally improved. To achieve this result, companies need to constantly explore, embrace, and adopt new technology to better manage information for their compliance and risk objectives.

We believe that good corporate governance and behavior can't be legislated; rather, behavioral principles can be laid down against which individuals and cases can be adjudicated. Inherent in this principle is rewarding good behavior and punishing bad behavior. Moreover, now that much of the heavy lifting has been done, we recommend that companies continue to seek ways to streamline and improve the risk and compliance systems they've installed to ensure the systems produce the desired results in a cost-effective manner. **SF**

James Bierstaker, Ph.D., is an associate professor in the Department of Accounting and Information Systems at the Villanova School of Business at Villanova University in Villanova, Pa. You can reach Jim at (610) 519-6101 or james.bierstaker@villanova.edu.

Kenneth K. Marshall is CEO and president of KK Advisory Services, LLC. You can reach Ken at kennethmarshall@kkadvisory.com.

Jonathan Greenwald is a member of the U.S. Navy. You can reach Jonathan at jonathan.greenwald@villanova.edu.