Mature Solutions Are Needed to Meet a Broader Range of Risk

Tom Willman, The Hackett Group

This essay is part of a series, ***Controllers' Corner: Two-Minute Essays on Financial Management and Control,*** which asks industry thought leaders for their opinions on critical issues facing today's finance organizations.

The worldwide economic crisis has been blamed in part on failures of government regulatory oversight, corporate governance, and risk management. As organizations prepare for the next round of growth, they are asking themselves how to prepare their governance, risk, and compliance profiles to better manage the next set of unexpected events.

Q Given that governance, risk and compliance (GRC) covers a very broad range of processes across finance, IT, and lines of business, how should organizations set their priorities for risk management?

The recession and liquidity crisis of 2008-9 have demonstrated that most organizations do not operate with the agility required to respond to the risk and volatility in today's business environment. The risk spectrum that organizations face today is much more complex than it has ever been, with both the types and intensity of risks increasing dramatically. This has generated a renewed focus on Governance, Risk Management and Compliance (GRC). As Sarbanes-Oxley compliance activities are becoming embedded in daily operations, organizations are now taking a broader view of GRC to encompass things like market, operational and geopolitical risk, to name a few.

The majority of organizations that The Hackett Group studies have, or are implementing, enterprise-wide risk management capabilities. This can include a formal organization, with the company's leadership aligned with the effort. We have found, however, that not many organizations have robust or mature processes in place to identify, monitor and manage these risks on an enterprise-wide basis. Controllers have long played a key role in the compliance aspect of GRC (e.g., internal audit, Sarbanes-Oxley compliance) and can take a leadership role in helping their companies drive improvements in their overall risk management capabilities. They can help their organizations reduce the cost associated with compliance activities while creating additional visibility to enterprise-wide risks. Specifically, Controllers can focus on the following:

1. Simplification, standardization and automation of the internal control environment
2. Collaboration with Internal Audit to move to a more risk-based approach to audits
3. Incorporation of risk-based metrics into standard management reporting
4. Evaluation of advanced GRC tools

Simplification, standardization and automation of the internal control environment

World-class finance organizations are reaping the benefits of the simplification, standardization and automation that they have driven in their finance processes and systems and the associated internal control environment. The use of Shared Services to perform finance activities and the associated compliance activities have also contributed significantly to World-class performance. These efforts have enabled World-class finance organizations to operate with compliance process costs as a percent of revenue, which includes fully loaded internal labor and outsourcing costs (e.g., external audit fees) that are 28% lower than their peers. External audit fees, which represent approximately 50% of an organization's compliance costs are almost 40% lower when normalized on revenue at world-class finance organizations, reflective of a well-run company with a strong internal control environment.

Controllers should constantly be looking for opportunities to rationalize and simplify their key control environment to reduce the number of control points that fall into the scope of SOX 404 testing. For the key controls that remain, they should leverage the functionality of their finance systems to automate as many key controls as possible and shift the balance towards preventive vs. detective controls. A strong deficiency assessment and prioritization process is also critical to enable organizations to evaluate and remediate high impact deficiencies on a timely basis.

Collaboration with Internal Audit

As GRC has become an enterprise-wide issue, Internal Audit has to shift their focus away from financial and Sarbanes-Oxley compliance and incorporate operational, IT, fraud detection and prevention and other types of audits in their programs. This has talent management implications as most internal auditors have spent the last several years heavily focused on Sarbanes-Oxley and do not necessarily have the expertise to perform these other types of audits. This has led Internal Audit organizations to evaluate their skills and capabilities and either hire in new auditors or look to co-sourcing arrangements with third parties to fill any gaps.

Controllers should collaborate with Internal Audit in a couple of areas. First, they can help Internal Audit understand where the highest-risk areas are in the Finance organization and jointly develop an audit plan that addresses those risks. This represents a shift away from the traditional time-based approach to audit plan development. Second, Controllers and Internal Audit should continue to work together to embed the responsibility for documentation and assessment of controls and testing of controls into the daily operations to allow Internal Audit to retain their independence and focus their resources on other areas.

Incorporation of Risk-Based Metrics into Standard Management Reporting

Controllers provide an integral role in the standard reporting that executive management teams receive on business performance. This represents is a real opportunity for Controllers to enhance the value that their executive management teams receive by incorporating critical risk-based metrics into that standard reporting package. They should work with senior management and the Enterprise Risk Management organization if one exists to understand the appetite for risk, identify current and emerging risks that are most critical to the business and agree on metrics and reporting schedule that can be used to monitor and manage exposure to these risks. Controllers can then work with the businesses and IT to identify and agree on sources of data that will be used to calculate the risk-based metrics and to develop the processes needed to integrate these metrics into the standard reporting package.

Evaluation of Advanced GRC Tools

Sarbanes-Oxley brought with it a plethora of vendors offering solutions to help companies manage the activities associated with SOX compliance. While the promises from these vendors were great, the early versions of these tools were focused on document management, workflow and reporting and didn't really deliver the improvement in business practices that were expected. However, the GRC application space is maturing and the solutions are becoming more comprehensive. There are applications available today to enable business process management, continuous controls monitoring, segregation of duties management and policy and procedure management. While Controllers should evaluate these tools with some skepticism, many of the vendors in this space have demonstrated they can deliver impressive customer success stories on how their applications have helped companies improve quality and reduce errors, lower costs of compliance and enhance visibility to risk information.

About Tom Willman

Tom Willman is the Global Practice Leader of the Enterprise Performance Management Executive Advisory Program for The Hackett Group. With more than 15 years of experience in finance, accounting and consulting in a wide range of industries, Mr. Willman focuses on helping CFOs and other finance executives transform their organizations by deploying more efficient and effective processes, service delivery models and enabling technologies. Mr. Willman may be contacted at twillman@thehackettgroup.com.

IBM Canada Ltd.
3600 Steeles Avenue E.
Markham, ON L3R 9Z7
Canada

Produced in Canada
March 2010

P24237

Please Recycle

Cognos. software