

The 2005 Oversight Systems Financial Executive Report on Risk Management

Like six sigma in the 1990s and total quality management in the 1980s, risk management now buzzes through corporate America as the latest initiative for better business management – and for good reason. Most financial executives say their companies faced significant operational surprises in the last five years.

Revenue, production costs, compliance, profit margins and ultimately shareholder value are at the mercy of how executives plan for and respond to the uncertainties in their business. Shareholders, creditors, regulators and bond-rating agencies are all pressuring executives to anticipate and plan for the risks and potential perils that can happen within their individual operations, in their industry or anywhere in the global economy.

This survey of financial executives provides a report card on risk management today. In summary, the emerging practice of enterprise risk management is full of good intentions but short on execution. Executives should evaluate their companies' risk management in the context of this survey and determine what specific steps they should take to manage enterprise risk.

While it's encouraging to see growing interest from business leaders in better managing corporate risk, the challenge will be for corporate America to transform that interest into action that actually helps reduce organizational risk.

Mounting Pressure and Uncertain Execution

The survey reveals that 68 percent of financial executives say their CEO is placing greater emphasis on the management of all types of risk on a holistic basis. Three out of five (60 percent) say their company has an enterprise risk management approach and philosophy that considers various interactions among different types of risk (see: *Risky Business* graph).

Risky Business... Some Hot, Some Cold

Risk – more specifically, heading off risk – is one topic the majority of financial executives surveyed had on their minds. When asked to evaluate specific behaviors of their companies, here is what they said. Our company has:



A CEO who is placing greater emphasis on the management of all types of risk on a holistic basis.



A philosophy to risk management that focuses on an enterprise-wide view of risk (i.e., an enterprise risk management or ERM approach) where interactions among various risk types are explicitly considered.



Faced significant operational surprises in the last five years.



Faced pressure from key stakeholders (e.g., creditors, bond-rating agencies) to manage all types of risk.



Designated a member of senior management with explicit responsibilities for overseeing the management of all risk across the enterprise (e.g., Chief Risk Officer, etc.).



An agreed upon and widely communicated definition of "risk" that is used across the enterprise by senior management and business line managers.



Formally trained senior management and business line managers to assess the probability (likelihood) of various types of risk.

However, the survey shows that critical elements of risk management are not in place. Only 35 percent of financial executives say their company has formally trained executives and business line managers to assess the probability of various types of risk. Most (55 percent) companies do not have a member of senior management with explicit responsibilities to manage risk. Again, the majority of those surveyed (55 percent) say their company does not have a widely communicated definition of risk.

“Corporate America faces a gap between the perception of risk management and the reality”

Dana Hermanson, Kennesaw State University

“This survey indicates that corporate America faces a gap between the perception of risk management and the reality of an effective risk management program,” said Dana Hermanson, Dinos Eminent Scholar Chair of Private Enterprise at Kennesaw State University. Hermanson is also an advisor to Oversight Systems. “CEOs are under pressure from shareholders, creditors and regulators such as the New York Stock Exchange to better manage enterprise risk, but executives are struggling to define exactly what that means for their companies.”

While proponents of risk management are thrilled to see such a high level of interest from CEOs, they also see specific breakdowns in the risk management practices that threaten the overall benefits of risk management.

“Without designated responsibility, proper training or even clear definition of risk, various line managers may be implementing their personal risk approach with varying tolerances for risk, which creates a situation where risks are managed inconsistently,” said Mark S. Beasley, professor of accounting and director of the Enterprise Risk Management Initiative at North Carolina State University. Beasley is also an advisor to Oversight Systems.

Executive Motto: Be Prepared

When asked, the majority of financial executives say their organizations are prepared to assess and manage the risk associated with most business functions. However, some fared better than others.



Enterprise Risk by Business Function

When asked, the majority of financial executives indicated their organizations were more prepared than not to assess and manage the risk associated with most business functions. However, this self-assessment shows that a third or more of financial executives say their companies are “unprepared” or “very unprepared” for various forms of risk (see: *Executive Motto* graph).

“This survey suggests that businesses today face significant risks throughout their operations but lack a corporate infrastructure to proactively address these risks. While executives say they are moving toward a holistic approach to managing risk – enterprise risk management – they are not yet prepared to actually deal with all types of risk,” Beasley said.

In keeping with the high demands of Sarbanes-Oxley, financial execs said they were best prepared for financial reporting risks.

The Role of Technology in Risk Management

Although more than a quarter of executives (28 percent) say technology has no role in their company's overall risk management, the majority see technology as helpful to their risk management objectives. A full quarter (25 percent) say they use technology to identify existing risk, project future risk and reduce risk; 32 percent say technology is used in their organizations to identify existing risk; and 15 percent say technology is used to identify existing risk and project future risk (see: *Techno Phobic* graph).

"The use of technology in risk management appears to be in its infancy, with only a quarter of companies using technology to identify existing risk, project future risk and reduce risk. More than a quarter of the survey's respondents don't leverage technology to enhance risk management," Hermanson said. "As the practice and implementation of risk management mature, more executives will recognize and rely upon technology solutions to provide the infrastructure of risk management."

SOX 404 Compliance Year Two

When asked how they expect their external audits of internal controls to change in year two of complying with Sarbanes-Oxley's Section 404, 42 percent of financial executives said they were focusing more on changes to controls as opposed to what was already documented in year one, and 40 percent said they would increase their use of a risk-based approach to auditing internal controls (see: *SOX Part Deux* graphic).

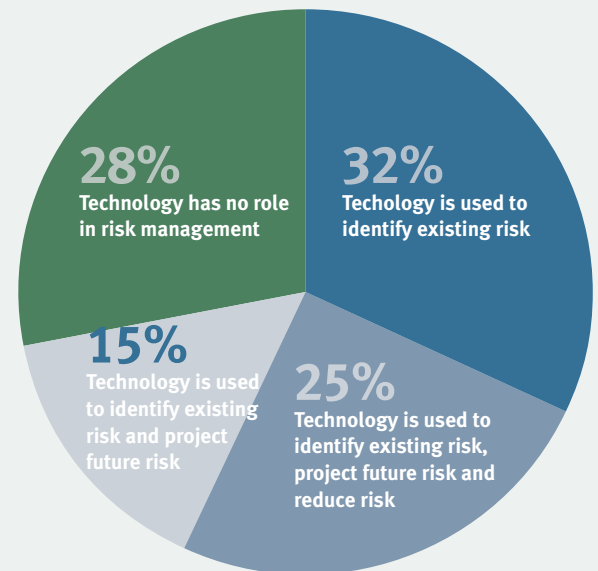
Twenty-three percent expect to have a greater reliance on technology to monitor the effectiveness of internal controls; 21 percent predict a greater reliance on internal auditors to test controls; and 21 percent plan to reduce the number of key control activities.

However, 21 percent of the financial executives surveyed are predicting no significant change in the role of external audits and internal controls in year two of SOX. Twenty-two percent are predicting less testing of internal controls that are not directly tied to financial reporting, and 15 percent say there will be less testing of automated controls due to the presence of good IT general controls.

"In the second year of SOX 404 compliance, auditors are moving toward audit efficiency by focusing on changes in controls and incorporating a risk-based approach to auditing internal controls. These changes are consistent with the theme of recent PCAOB guidance that suggests auditors went a little overboard in year one," Hermanson said.

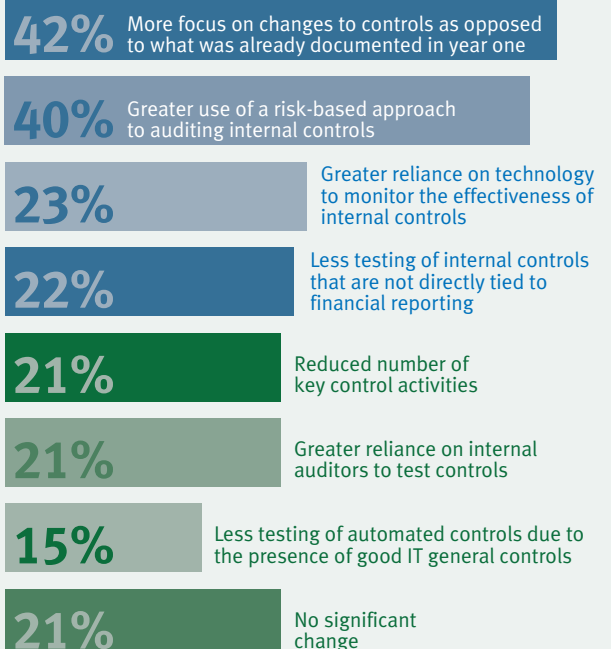
Techno Phobic or Techno Geek?

Most financial executives say technology has some role in their company's overall risk management efforts. When asked for the best description of the role of technology in risk management, they said...



SOX Part Deux

With year one of Sarbanes-Oxley (SOX) 404 compliance behind them, the majority of financial executives are bullish on not repeating year one efforts, greater consideration of risk and increased reliance on technology. Expectations for year two of SOX 404 compliance include:



Extending SOX to Risk Management

Sarbanes-Oxley and enterprise risk management are natural allies. SOX compliance efforts and investments can be leveraged to build an ERM program and drive value from a complex, expensive and mandatory process. The challenges of integrating SOX into ERM is to manage that risk as part of your day-to-day operations without adding costs.

Companies are successfully integrating SOX compliance and ERM by focusing on three areas: documentation, people and technology. After meeting first-year SOX requirements, companies have spent millions to document financial reporting risks, which becomes a valuable asset within any ERM program. Initial SOX compliance involved people throughout many areas of a company – internal controls, production controls, sales and marketing, engineering, and purchasing, to name a few. Everyone involved required some form of training to identify financial risks, and those people can apply that training to identify risk throughout all areas of operation.

The biggest challenge is then defining responsibilities for monitoring risk and maintaining consistent monitoring throughout the organization. Technology can be applied to continuously monitor operations and identify the transactions and activities that introduce risk. Technology can automate the rote and manual monitoring efforts and empower individuals to mitigate risk. By integrating SOX compliance and ERM, companies can successfully maintain compliance throughout the year in a way that drives down recurring compliance costs and avoids the quarterly fire drill to prove compliance. And in the process, ERM allows a company to make better decisions, recognize opportunities for improvement, and attain an ROI on compliance.

About the 2005 Oversight Systems Financial Executive Report on Risk Management

This survey of financial executives was conducted at the FEI Summit 2005, a Financial Executive International conference held in May 2005 to explore the evolution of the role of financial executives from financial to policy. Titles of those surveyed included chief financial officer, chief audit executive, controller and treasurer.

Other Oversight Systems Reports

The 2005 Oversight Systems Financial Executive Report on Sarbanes-Oxley, which was released in April of 2005, found that nearly half of financial executives feel the biggest issue related to compliance is the need to maintain the morale of the employees responsible for compliance.

The 2004 Oversight Systems Financial Executive Report on Sarbanes-Oxley, released in December 2004, showed that most financial executives were torn on the cost vs. benefits of Sarbanes-Oxley compliance, and it has been cited in the *Public Company Accounting Oversight Board (PCAOB) Release No. 2005-009*, a policy statement regarding implementations of auditing standards.

All Oversight Systems reports can be downloaded for free at www.oversightsystems.com/survey.

About Oversight Systems

Oversight Systems is the leading provider of independent, continuous monitoring solutions for real-time transaction inspection. By combining the expertise and experience of security, fraud, audit and enterprise software development professionals, Oversight Systems is redefining how enterprises satisfy Sarbanes-Oxley compliance requirements, and enabling corporations to gain substantial returns from their compliance investments. For more information, visit www.oversightsystems.com.

Contact: Brian Moran
brian.moran@oversightsystems.com

Oversight Systems, Inc.
75 5th Street, NW, Second Floor
Atlanta, Georgia 30308
404-920-2030
www.oversightsystems.com