

Internal Auditing REPORT

APRIL 2008 VOL. 8 NO. 10



Practical Perspectives

A New Risk Management Program for 2008

Jennifer Meiselman Salzman, Managing Director with the Risk Advisory Services Group of BDO Consulting, predicts that businesses will continue to align the activities and objectives of their risk, governance, compliance, privacy, and fraud areas into a fully integrated risk management program.

As companies move away from “siloes” risk management programs, which are reactive in nature, towards proactive programs that assess risk on an enterprise-wide basis, what trends can we expect to see in 2008? In addition to the emphasis on Sarbanes-Oxley compliance, there will be

increased demand for integrated worldwide risk management, fraud prevention, enterprise resource planning (ERP), and privacy protection plans.

Integrated Worldwide Risk Management Plans

In 2008, companies with overseas operations will move

toward a singular operational risk management plan encompassing internal audit, Sarbanes-Oxley, and compliance programs. Operational processes across international locations will be integrated strategically in 2008, as mitigation of operational and financial risk becomes more

Practical Perspectives

process-oriented than location-oriented.

Many companies are also consolidating their operational risk functions into a combined entity. This new operational risk entity helps avoid duplication of efforts (e.g., when one area is reviewed by three groups). A single entity also allows for rapid adjustment of resources as the companies' objectives change during the year. An acquisition may require additional resources that can be more effectively deployed from a cross-functional team than three separate groups.

The combined operational risk entity can also improve its efficiency and effectiveness with the use of technology. Many companies are implementing risk management software to integrate their risk assessment, controls documentation, testing, issue management, and reporting processes. These packages are also critical to assist with the monitoring of the companies' operational risk management programs.

The software packages are primarily Web-based, allowing accessibility from all company locations, and are available in numerous languages. The software allows the auditor to link multiple risks to multiple functional audits and locations (a many-to-many relationship), making integration among the teams more efficient. Reporting audit results

is also made easier using software, as it facilitates a consolidated repository for all risk management findings.

Leveraging ERP Software

As companies automate risk management functions, they will leverage existing ERP software and evaluate third-party software to enable them to efficiently automate processes where higher risk is prevalent.

Companies can improve their internal controls by evaluating their ERP security strategy, which significantly impacts the effectiveness of their segregation of duties. In many instances, the security strategy can be streamlined to provide more effective assignment of users and monitoring of the security program. In one company, for example, the number of security groups was reduced by a third, thereby reducing the time spent for monthly security reviews and the chance of errors during new account establishment.

Third-party software can aggressively monitor risk in real time through the identification of anomalous transactions designed to prevent fraud and material errors. For example, within the fixed asset area, depreciation calculations or asset categorization can be reviewed in real time. This can help companies avoid violations that could lead to financial restatements or Sar-

banes-Oxley internal control deficiencies.

Moving From Fraud Detection to Fraud Prevention

Previously, companies relied heavily on codes of conduct and whistleblower hotlines as their primary anti-fraud mechanisms. In 2008, companies will further develop comprehensive fraud prevention programs across all business lines and operations. These programs will encompass fraud risk assessments, fraud education for employees and management, and background checks on new employees and employees promoted to positions of trust.

As the focus on anti-fraud programs continues, companies should integrate fraud brainstorming sessions into their fraud risk assessment. During the session, management works with fraud experts to identify the scenarios at their company where fraud could occur. For each scenario, questions are asked, such as:

- Who could perpetrate the fraud?
- Who else could be involved?
- How could they execute the fraud?
- What incentives do they have to commit the fraud?
- What information would they need?

Practical Perspectives

The risk assessment should also include interviews with key management, members of the board and audit committee, and independent auditors. The company then identifies both entity-level and transaction-level controls that would mitigate the risk of the fraud occurring.

At the entity level, the trend is toward increased board and audit committee oversight. Audit committees are increasingly willing to ask difficult questions and gain a more detailed understanding of a company's fraud prevention and ethics program. The audit committee should also evaluate whether the anti-fraud program is operating effectively to prevent, deter, and detect fraud.

The Next Step in Privacy Protection

As privacy protection technology continues to advance, companies will reassess their

anti-identify theft, anti-money laundering, anti-credit card fraud, and privacy systems to meet regulatory and customer expectations.

Regardless of size, an identify theft incident can pose a serious threat to an organization's reputation and increase the risk of litigation or regulatory penalties. While financial institutions have more stringent regulatory requirements with the passage of the Fair and Accurate Credit Transactions Act of 2003, all companies should be looking to improve their identify theft programs. This should start with a risk assessment and include detailed policies and procedures, training, independent testing, incident response, and program monitoring.

Whether implementing an identify theft program or other privacy protection system, companies will seek to balance the organization's risk

tolerance with the increasing costs and complexity of privacy protection.

Conclusion

Overall, 2008 will see businesses continue to more closely align the activities and objectives of their risk, governance, compliance, privacy, and fraud areas into a fully integrated risk management program. Though this will likely take several years to achieve, the outcome will enable the risk management group to better assist the organization in meeting its business objectives. ■

JENNIFER MEISELMAN SALZMAN is a Managing Director with the Risk Advisory Services Group of BDO Consulting, a dedicated risk consulting practice that provides enterprise risk management, internal audit, business process enhancement, technology risk, and security and compliance services. BDO Consulting is a division of BDO Seidman, LLP. Jennifer can be reached at jsalzman@bdo.com.