Subsequent to the accounting scandals in the early part of the decade and the near collapse of financial systems in the latter part of the decade, focus on enterprise risk management (ERM) has increased significantly. Concurrently, as corporations have increasingly turned to outsource suppliers and service providers to reduce operating costs and increase internal focus on core competencies, third-party risk management has also grown rapidly in importance as a subset of overall ERM initiatives. Why? Simply, liability and responsibility cannot be outsourced.

Generally, we can do a good job of identifying, quantifying, and managing risks within our own organizations. However, because our third-party business partners are managed indirectly and cannot be monitored as easily as our own employees and assets, many organizations must contend with blind spots in third-party risk management. A report titled “Third-Party Codes of Conduct: A Benchmarking Survey,” published by the Society of Corporate Compliance and Ethics (SCCE) in February 2009, noted that 83 percent of the respondent’s organizations had not established a code of conduct unique to their third-party business partners.

Further compounding this dilemma, regulators, including FDIC, SEC, FFIEC, OCC, OIG and others, are increasing their focus on potential third-party risks. They want to see organizations proactively identifying potential risks,
verifying that business partners and their employees are compliant, monitoring for changes that might create new risks or compliance gaps, and managing the investigation and remediation of incidents.

Driven by internal risk reduction initiatives and external regulatory pressures, organizations are discovering a broad array of challenges as they attempt to proactively manage their risks stemming from third-party business partners. External risks can manifest in many forms, including fraud and bribery issues, code of conduct and ethics violations, regulatory violations, privacy breaches, quality issues, and labor standards.

Managing these potential supply-chain risks can be significantly more challenging than managing similar risks that may emanate from within the organization. Often, as organizations attempt to address third-party risks, they focus on the launch of relationships (on-boarding) but fail to account for issues that can occur throughout the life of relationships. These are risks that can quietly creep into relationships over time and create exposures that are unknown until an incident occurs. The reasons that organizations often fail to manage third-party risks throughout the life of relations are two-fold:

This document is only available to subscribers. Please log in or purchase access

Purchase Login