The Institute of Internal Auditors

TONE at the TOP

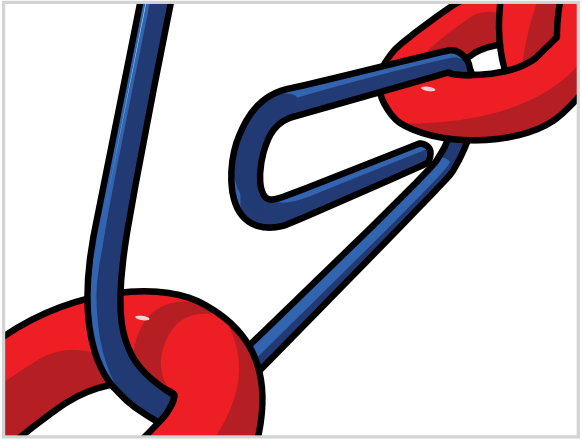
Issue 67 | April 2014

Providing senior management, boards of directors, and audit committees with concise information on governance-related topics.

Managing Third-party Risks

When your organization relies on third-party suppliers or service providers, your exposure to risk multiplies. And while the term "third-party" is often used in reference to big jobs — such as outsourced labor, data processing, or manufacturing — the associated risks can apply to every contractual relationship, no matter how small. They may even extend to include your vendors' relationships with their service providers or suppliers.

More than 65 percent of organizations rely "heavily" on third parties, according to a recent survey conducted jointly by The Institute of Internal Auditors Research Foundation and Crowe Horwath LLP. Yet, despite the prevailing belief that third-party relationships pose a significant risk to the organization, a large majority (80 percent) of organizations devote only a sliver of their internal audit resources to assessing third-party risks. Moreover, researchers discovered a lack of consensus about who in the organization actually "owns" each third-party relationship and uncertainty regarding what specific steps should be taken to reduce risk exposures.



This issue of *Tone at the Top* explores the subject of third-party risks, tapping the insights of three risk management experts who offer several tips to help company leaders grapple with this growing concern.

Moving Target

"Third-party risk is one of the greatest risks to our organization," says William Vinson, vice president and chief audit executive at Seagate Technologies, a global leader in computer hard disk drives and data storage solutions. "Whether it's manufacturing or some other service, we're handing over a lot of the typical controls we would expect to see internally to someone else."

Seagate relies heavily on third-party manufacturers and suppliers in China, Malaysia, South Korea, Thailand, Singapore, Brazil, and other countries with a wide range of cultural practices, political systems, regulations, labor laws, and quality-control expectations. Navigating this complex and shifting landscape can be a daunting challenge.

"It's important for boards and audit committees to recognize that, when you're talking about third-party risk management, you're dealing with a constantly

evolving environment," Vinson says. "Economies change. Politics and regulations change. There has to be a robust and continuing review and evaluation process."

Establishing comprehensive contract agreements is a step in the right direction. But third-party risk management programs must also include provisions for monitoring compliance and enforcing those contracts.

Fight for Rights

Although reputational risks — such as poor working conditions, corrupt practices, and product liability — tend to garner more public attention, much of third-party risk management actually involves less provocative matters such as making sure that vendor contracts are clearly written, costs are accurately identified and understood, suppliers and consultants are not padding their bills, and all parties are compliant.

One example of a common third-party risk involves channel distribution arrangements, in which a branded product passes through several checkpoints, taking on the bells and whistles of "value-added" resellers. For example, a computer manufacturer allows a channel partner to add a component, such as memory. But the part is defective or substandard, leading to problems. In such a case, the manufacturer essentially vouches for the work of an invisible third party, whose subpar work may ultimately damage sales and the brand's reputation.

Software licensing and music royalty agreements are two other common areas where failing to audit or enforce contractual provisions may lead to significant monetary losses. "It's easy for an IT shop to deploy more software than it pays for," says Robert Pink, a partner with KPMG who specializes in contract compliance services. "In channel distribution, a third party might understate sales to reduce royalties owed under a reseller agreement." Fortunately, Pink says he's seeing an upswing in the exercising of contractual audit rights and the enforcement of single-use provisions.

Historically, that hasn't been the case. Matthew Behan, principal for KPMG Contract Compliance, says that, in the more than 20 years he has been conducting contract compliance audits, he is often surprised by the hiring company's lack of follow-up after a contractual agreement is established. Once the contract is signed, it seems no one ever looks at it again, he says.

Still, more often than not, breakdowns in third-party risk management result from a failure to keep close tabs on vendors and to verify that contract terms are

Third-party Risk Roster

Third-party risks can be found in every corner of an organization. Patrick Warren, principal with the risk consulting unit of Crowe Horwath, groups these risks into the following six categories:

1. **Financial** – Foreign exchange, currency risk, tariffs, taxes, product price, markup, and rebates.
2. **Information** – Accuracy, timeliness, relevance, and security of data shared by multiple parties.
3. **Integrity** – Fraud, regulatory compliance, conflicts of interest, brand, and reputation.
4. **Operational** – Cost, efficiency, contract concerns, business disruption, and supply chain concerns.
5. **Strategic** – Big-picture issues, including social responsibility, environmental conscience, and economic impact of third parties.
6. **Technology** – Computers, data-storage devices, networks, and emerging technologies.

*Adapted from Warren's article, "Closing the Gaps in Third-party Risk Management," *Internal Auditor* magazine, February 2014.

Qualified Professionals

Internal auditors and risk managers, particularly those who hold The IIA's Certification in Risk Management Assurance, are uniquely qualified to identify potential third-party risk exposures and to make recommendations on policies and procedures to manage those risks.

being met. "We know that third parties make errors," Behan says. "They take advantage of situations. And yet, very often we hear, 'That's just how business is done.' Well, okay — but if that's the way you're going to conduct business, why even have a contract?"

Reining In Risk

The rapid and accelerating pace of technological advancement and the digitization and monetization of information makes keeping a tight rein on third parties increasingly difficult. Still, with so much at stake, it is critical that organizations document and adequately monitor third-party risks.

Seagate's Vinson offers the following tips for managing the effort:

1. Conduct a complete inventory of third-party activities ranked by risk factors, including contract value, corruption potential, financial risk, and regulation.
2. Assign an appropriate and proportionate process to manage each identified third-party risk/relationship.
3. Establish clear and unequivocal rules to hold vendors accountable and measure performance.
4. Ensure that controls and risk-assessment tools adapt to changes in the risk profile.

In many organizations, the responsibility for performing these tasks falls to risk managers and internal audit professionals, who work in tandem to ensure the organization's many risk exposures are identified and addressed appropriately. Risk managers establish controls and procedures to minimize risks, while internal auditors provide an objective assessment of the controls, recommend improvements, and offer assurance to executive management and the board that risks are addressed appropriately.

Ultimately, it is incumbent upon executives and board audit committees to ensure that third-party risk management is on their radar. Company leaders must understand and be able to quantify these risks to determine whether sufficient resources are allocated to provide assurance that third-party relationships are properly managed.

Quick Poll Question

How confident are you that your organization's third-party risks are being addressed adequately?

Visit **www.theiia.org/goto/quickpoll** to answer the question and see how others are responding.

Questions Boards Should Ask

- Are third-party risks considered in the organization's overall approach to enterprise risk management?
- Has an inventory and ranking of third-party risks been performed?
- Are third-party risk management roles and responsibilities clearly defined within the organization?
- Are appropriate resources allocated to address third-party risks?
- Do risk managers and internal auditors consider third-party risk in their risk assessments and audit plans?

About The IIA

The Institute of Internal Auditors Inc. (IIA) is a global professional association with 180,000 members in 190 countries. The IIA serves as the internal audit profession's chief advocate, international standard-setter, and principal researcher and educator. www.globaliia.org

Complimentary Subscriptions

Visit **www.globaliia.org/Tone-at-the-Top** or call +1-407-937-1111 to order your complimentary subscription.

Reader Feedback

Send questions/comments to **tone@theiia.org**.

Content Advisory Council

With decades of senior management and corporate board experience, the following esteemed professionals provide direction on this publication's content:

Martin M. Coyne II
Michele J. Hooper
Nancy A. Eckl
Kenton J. Sicchitano

The Institute of Internal Auditors | TONE at the TOP

247 Maitland Ave.
Altamonte Springs, FL 32701-4201 USA