Managing Third-Party Relationship Risk

Today’s businesses must have a clear understanding of the risks inherent in their business relationships with outside parties. To address these risks, companies must implement programs using nonadversarial third-party risk management strategies that benefit all parties.
Managing Third-Party Relationship Risk

With increased regulatory scrutiny, continuing cost pressures, active investors, and a vigilant public, businesses today must have a clear understanding of the risks that are inherent in external business relationships. By recognizing and proactively addressing these third-party issues, business leaders can reduce exposure to risk and achieve stronger relationships with service providers, suppliers, and delivery partners. The end result: a nimbler, more responsive, and more profitable operation.

Trends

As enterprise risk management (ERM) takes root in more and more businesses, these companies’ executives are thinking more broadly about the risks their organizations face. Inevitably, there is growing realization that many of the most significant risks are driven by relationships with other entities. These relationships include:

- **Service providers** – such as processing, accounting, computer services, IT, service centers, internal audit, warranty processing, call centers, advertising and marketing, leasing, legal, collections, and construction services providers;
- **Supply-side partners** – such as production outsourcing, research and development, material suppliers and vendors, and software development providers;
- **Demand-side partners** – such as customers, distributors, resellers, franchisees, licensees, replicators, and original-equipment manufacturers; and
- **Other relationships** – such as alliances, consortiums, joint ventures, and investments.

Risks have always been inherent in third-party relationships, but some particularly dramatic examples of risk exposure have occurred in recent years. For example:

- **Reliance on third parties.** The March 2011 earthquake and tsunami in Japan demonstrated a significant vulnerability to sudden parts shortages and supply chain disruptions across a broad range of industries.
- **Protection of systems and data.** High-profile data breaches have shown how even businesses with robust data security systems can be at risk due to weaknesses in the security of third-party organizations entrusted with sensitive information.
- **Reputation linked to others’ actions.** Unexpected revelations about distant suppliers’ labor and environmental practices, which often catch retailers and distributors by surprise, demonstrate how quickly stakeholder confidence can be shaken, even in businesses with solid reputations for competence and integrity.
- **Continuity of operations.** Allegations of accounting fraud in one major outsource provider of IT services ultimately had global repercussions, triggering the near collapse of the business and imperiling software development strategies worldwide.
- **Financial dependency.** Highly volatile commodity prices have led to rapidly changing cost structures for vendors in virtually all industries.

Third-party risks are increasingly important to companies, given the trends of outsourcing, regulatory focus, offshoring, global supply chains, and consumer and investor expectations. All of these trends add up to a requirement for a new approach to identify and manage a broad range of risks associated with an organization’s extended relationships.
Gaps

While a growing number of organizations appear to recognize the increasingly uncertain risk picture that results from relationships with external agents and intermediaries, there is much less agreement about how to effectively identify, quantify, and mitigate associated risks.

Service Provider Risk Management

In a recent study conducted by ChainLink Research,1 nearly 50 percent of organizations indicated that risk assessment played a “critical and mandatory” role in their service provider selection. However, more than 70 percent of the surveyed organizations reported having no resilience and risk mitigation standards to which they hold their service providers.

Further, the ChainLink research noted that “the thoroughness of the risk assessment varies greatly, depending on the company.” Companies lack the ability to extend risk assessment into subcontractors and tend to focus on the easiest risks to quantify, such as financial viability or business continuity plans.

Supply-Side Partner Risk Management

In a recent study by Compliance Week magazine,2 more than 90 percent of the surveyed corporate executives said they believe conducting a vendor risk assessment is either important or very important. At the same time, though, more than half were dissatisfied or, at best, had neutral feelings about their company’s current approach to vendor risk assessments. As Compliance Week summarized, “Vendor risk assessments continue to confound many companies, even while they say that getting a handle on supply-chain risk is at the top of their priority list.”

The top difficulties cited by the survey respondents included a lack of good data on vendors, poor visibility into the use of subcontractors, and limitations in comparing vendor risks.

Demand-Side Partner Risk Management

Demand-side third-party relationship risk tends to be industry-specific and varies depending on the method of delivery to customers (direct or multichannel, for example). Often companies lack the infrastructure or technology to have adequate monitoring in place and handle the volume of demand-side relationships. It is common for companies to rely solely on the self-reporting of information.

Risk Management of Other Relationships

Companies often fail to achieve the value they had expected a relationship to yield. Many times, organizations realize only in retrospect that the foundation of a particular relationship had never been solid – because at the inception of the agreement, planning was lacking and incentives for success were not built in to the agreement.
Challenges

To address successfully this broad range of third-party relationship risks, businesses must be competent and skilful when identifying, analyzing, and assessing risk and then developing risk strategies and metrics. These efforts can be complicated by a variety of factors, both internal and external.

Internal Challenges

- **Ownership of risk responsibilities.** Clearly establishing ownership of third-party relationship risks presents a significant challenge to most businesses. Multiple layers of ownership often exist, so it might not be clear who has responsibility for the third-party risk management framework for the entire organization and who has responsibility for the review and ongoing monitoring of individual relationships.

- **Reactive approach to risk management.** In most organizations, adequate risk management involving third-party relationships is not addressed until a problem has already arisen. By that time, risk exposure has already increased and the opportunity to mitigate has already diminished. A proactive risk assessment of the relationship at the time it is established – and periodically throughout the course of the relationship – is the key.

- **Traditional metrics that don’t include risk.** The supplier scorecards that are often used for vendor selection and to reward procurement teams typically focus on metrics related to quality, cost, and delivery but give little consideration to relationship risk, including the likelihood and associated potential cost of adverse events. The metrics also don’t take into account the cost of monitoring and managing the risks.

External Challenges

- **Complex, global supply chains.** One effect of globalization has been a dramatic increase in the complexity of identifying and assessing risks. To cite just one example, under the anti-bribery, recordkeeping and internal controls provisions of the **Foreign Corrupt Practices Act (FCPA)**, U.S. companies can be held liable for the acts of foreign third parties and agents – from suppliers of raw materials and components, to international shipping providers, to overseas assembly or production facilities. At the same time, assessing and auditing compliance in such remote relationships can be costly and complex.

  Beyond globalization, today’s highly integrated supply, value, and information chains further complicate risk assessment. Traditional ways of evaluating and mitigating risk often are inadequate in an environment of shortened product life cycles, fragmentation of the supply chain, just-in-time inventory practices, and other business tools that were once considered exotic but today are the norm.

- **New disclosure expectations that increase exposure to reputational risk.** Today’s businesses are expected to disclose a much broader range of nonfinancial information to demonstrate their compliance with various environment, labor, security, privacy, and social standards. Because these disclosures are often highly dependent on the assertions and reports of third-party service providers, suppliers, and partners, the means for verifying the accuracy of third-party data can be extremely limited.

Most organizations do not adequately address risk management involving third-party relationships until a problem has already arisen.
Complex invoicing. Supplier relationships that are sensitive to prices of commodities such as raw materials and fuel often involve complex methods of invoicing. In such instances, prices are often pegged to a market index or other third-party standard, which adds another layer of complexity to monitoring and contract compliance activities. Moreover, any hedging tools must be designed carefully to take such variations into account.

Another prominent example of complex invoicing is the practice of leading big-box retailers to delay payment for inventory until it is sold off the shelf, which significantly shifts the inherent risks in the relationship. Such complications in the timing of invoicing and payment have a direct effect on the risk exposures of all parties to the contract.

Contract Considerations

In addition to internal and external challenges, special consideration must be given to any contracts governing third-party relationships. A comprehensive and carefully written contract can be the basis of a healthy relationship with a supplier, distributor, service provider, or other external party. Common contract pitfalls include:

- Lack of awareness or understanding of risk-related contract provisions. In all too many cases, procurement teams and business owners have a limited, unclear, or inaccurate understanding of important contract terms. One example is the right to audit. Often this contract provision limits a purchaser’s audit authority issues related to pricing, and it might limit the right to audit a supplier’s production processes, data, sourcing, and other criteria. If the purchasing company’s management is not fully aware of such limitations, it may be unwittingly agreeing to deprive itself of valuable opportunities for process improvement and cost reductions.

  Other examples of poorly understood contract terms include service-level agreements, volume rebates, and surcharge provisions – in particular how such provisions are to be calculated and documented and the risk consequences associated with negotiating long-term rather than short-term contracts.

- Outdated contract models in a rapidly changing environment. Outsourcing contracts that have been in place for years often fail to reflect significant trends and developments not anticipated at the time the contract was negotiated. For example, changes in technology, acquisitions, industry consolidations, or multiple layers of outsourcing (in which contracted services from a vendor are further subcontracted to unrelated suppliers rather than being handled directly) might have a considerable impact on third-party relationship risks and necessitate a revised contract.

- Complex revenue, cost, and profit-sharing models. Contracts establishing less straightforward relationships, such as demand-side relationships, alliances, and joint ventures, can also be complex. Examples include distribution, reselling, and service contracts. Variations in product mix, timing, service levels, and other factors can greatly complicate assessing the risk of the contractual relationship.
Planning for change requires cross-functional coordination, and executive leadership and oversight, with clear goals and objectives.

Solutions

The broad array of risk-related challenges today’s businesses face makes clear that an uncoordinated or case-by-case approach to third-party risk management is no longer adequate.

At a practical level, a successful third-party risk management program typically is implemented in three steps, as follows.

1. Establish ownership and buy-in. Planning for change is critical to successful third-party risk management in organizations where the ownership of such risk is dispersed among multiple stakeholders and owners. This planning requires cross-functional coordination, executive leadership and oversight, and clear goals and objectives. The mission of most organizations often includes a focus on strengthening the overall relationship with the third party.

Success factors:

■ Clearly establish risk ownership.
■ Obtain cross-functional input from various stakeholders.
■ Develop a third-party risk management road map.
2. **Evaluate risks.** Understanding the risk profile of the entire organization helps focus efforts on the areas of highest risk, which allows the assignment of adequate resources to address specific clauses in an agreement or specific types of relationships or categories of risk. Developing a comprehensive risk landscape (see “Types of Risk,” p. 9) is often a helpful first step in evaluating the various risks in a relationship. This step helps avoid taking a one-size-fits-all approach and instead drives focus on the areas of risk and reward to the organization.

**Success factors:**
- Identify the high risks inherent in the third-party relationships.
- Quantify identified risks.
- Establish a plan for moving forward.

3. **Audit, monitor, and assess.** The risk landscape spurs initiatives to audit, inspect, benchmark performance and costs, verify, and gain assurance or attestation. A successful third-party risk management program has an appropriate level of:
  - Risk measurement and monitoring;
  - Performance measurement and monitoring;
  - Incident tracking; and
  - Evaluation of the value received from the relationship.

These activities are important for determining when or whether to renegotiate the terms of the agreement. The companies that are most successful in this auditing and monitoring function are those that work to enhance the data they have about their relationships so that they can predict areas of risk more accurately and automate relationship monitoring more effectively.

**Success factors:**
- Customize the assessment to the relationship.
- Use automation to streamline the process.
- Analyze trends of incidents across relationships.

Board members, as part of their corporate governance responsibilities, should be asking management about third-party risks (see “Starting the Conversation,” p. 10).
Types of Risk

Traditionally, third-party risk audits cover financial, integrity, and operational issues. In today’s environment, these domains should be defined as broadly as possible. For example, financial risk takes into account foreign exchange, currency risk, and tariffs and taxes as well as product price, markup, and rebates. Integrity issues go beyond fraud alone to include risks associated with regulatory compliance, conflicts of interest, brand, and reputation. Operational risk addresses not only cost, efficiency, and contracting issues but also business disruption risk and misalignment of supply chains. Information risk should consider the accuracy, timeliness, and relevance of data shared among parties. New technology risks will emerge as smart phones, tablets, social media, cloud computing, and new types of technology continue to develop.

Third-party relationships should also be assessed from a strategic point of view to address risk that is related to market positioning, business models, and the impact on society, the environment, and economies.
Starting the Conversation

Following are some of the questions related to third-party risks that board members should pose to management.

1. Does our company have a full inventory of its relationships and agreements?
2. Have we performed an assessment of the risks to the business or the brand for each of the relationships we have?
3. Who owns the assessment of risks?
4. What are the key relationship risks and what are the processes we have in place to manage them? Who is responsible for risk management and monitoring?
5. How do we know that our relationships are complying with the agreements in place?
6. What are the company policies related to auditing agreements for compliance?
7. How do we know our relationships are complying with laws and regulations?
8. Which of our key relationship agreements or statements of work have not been reviewed by legal counsel in the past three to five years?
9. What procedures do we follow to reassess the risks associated with a relationship prior to the renewal of a contract?
10. What types of risks are considered in the selection or renewal process? Are any significant risks not considered?
11. Do our standard agreements address the key risks of most relationships?
12. How do we know the reports we rely on from our third-party vendors are accurate?
13. Have we tested our business continuity plans with our principal third-party relationships?
14. How dependent are our third parties on subcontractors and subservicers? What risks are associated with these organizations?
Conclusion

Today, as a result of the global nature of the economy and the complexity of business relationships, the risk management efforts of every business must be more comprehensive than ever. Risks that require monitoring and managing range from financial, operational, legal, and regulatory concerns to environmental, reputational, and technology-related risks.

In the face of such complexity – and in the face of continuously increasing scrutiny from a variety of stakeholders – an effective ERM program must incorporate a proactive program of third-party risk mitigation.
Contact Information

Gregg Anderson, CIA, is a director with Crowe Horwath LLP in the Chicago office. He can be reached at 630.586.5142 or gregg.anderson@crowehorwath.com.

Mike Varney, CPA, CIA, is with Crowe Horwath LLP in the Cleveland office. He can be reached at 216.623.7553 or mike.varney@crowehorwath.com.

Rick Warren, CIA, is a principal with Crowe Horwath LLP in the Atlanta office. He can be reached at 404.442.1606 or rick.warren@crowehorwath.com.

Jill Czerwinski, CISSP, CISA, PMP, MCSA, CIPP, is with Crowe Horwath LLP in the Chicago office. She can be reached at 630.575.4317 or jill.czerwinski@crowehorwath.com.

Eric Andolina, CIA, CFE, CISA, is with Crowe Horwath LLP in the Cleveland office. He can be reached at 216.623.7510 or eric.andolina@crowehorwath.com.

