March 2016

Meeting the Challenges of Third-Party Risk Management

How Manufacturing and Distribution Companies Can Control the Expanding Web of Risks

By Sam Aina, CPA, CIA, CFE, Matthew Bowser, CIA, CISA, and Lisa Domenick, CFE, CICA

Audit | Tax | Advisory | Risk | Performance

In the midst of the benefits of using third parties, there is risk. When your company outsources to a third party, the responsibility for the third party's actions and compliance remains with your company. Even when the third party outsources to its own vendor, the responsibility remains with your company. Using a third-party risk management framework will help untangle the web of risks and attain sustainable risk mitigation.

To achieve their strategies and objectives, manufacturers and distributors are increasingly relying on third parties. As these relationships become an even more integral part of how companies conduct business, it's essential that they understand – and properly manage – the risks that come along with them.

After all, when a company can't deliver on its commitments to customers or employees, they won't care if a third party is to blame. If the third party causes the company to miss a deadline, fail to satisfy expectations or quality specifications, suffer a data breach, or otherwise drop the ball, the company itself will be held responsible and accountable. The third party's reputation and business could possibly be hurt, but the company's definitely will be. For example, the public is more likely to fault automakers over the ongoing recall of millions of vehicles for air bag defects than the manufacturer of the defective products.

Managing third-party risk is critical in the manufacturing and distribution (M&D) industry. To be truly effective, it requires the involvement of not just the procurement department but also finance, internal audit, IT, operations, risk management, and, when dealing with agents or distributors, sales.

Understanding Third Parties and Their Risks

Third-party relationships encompass a vast network of relationships across the enterprise, among them:

- Suppliers (raw materials, production inputs, other goods, equipment vendors, contract manufacturers)
- Demand-side partners (distributors, advertising firms, sales representatives, social media, product resellers)
- Service providers (transportation and logistics, business services, IT services, customer-facing vendors)
- Other relationships (partnerships, agents, regulatory agencies, joint ventures, foreign-based providers)

Because many companies don't look beyond vendors in terms of relevant third parties, the level of due diligence conducted for other third parties might be less mature and, more than likely, inadequate. As a result, the existing approval and ongoing monitoring and termination processes for these relationships, including for new products and expenditures, could fail to satisfy proper risk management procedures.

Third parties often form a complex and tangled web of intertwined relationships. All of these third parties carry extended enterprise risk. In the same way that third parties are an extension of the company's business, they are also an extension of the risks affecting the company.

Some third parties have a relationship with the same company at multiple levels. A supplier could provide goods directly to both the company and a supplier of the company. This web of third parties complicates risk. For example, a company subject to conflict minerals reporting rules must bear in mind that regulators care less about the original supplier of the tin, tungsten, tantalum, or gold its products use than whether the original supplier obtained the minerals from prohibited geographic regions.

Companies with data breaches can face long-lasting damage to their reputations.

Data breaches are among the most publicized and concerning risks associated with third parties these days. Data breaches are bound to prove costly. The Ponemon Institute estimates the cost incurred for each lost or stolen record with sensitive and confidential information to be $145.[2] In addition to the direct financial costs of investigations, regulatory penalties, lawsuits, and remediation costs, companies with data breaches can face long-lasting damage to their reputations. Consumers who fall victim to identity theft, including credit card fraud, understandably feel violated. The mental and emotional trauma they sustain from the hassle and frustration of trying to resolve the situation will weigh heavily on their perceptions of the company through which the breach appears to have occurred.

Of course, the reputation damage isn't limited to affected customers. Companies hit with data breaches are likely to fall prey to intense press coverage in today's 24/7 news cycle. The media is quick to pounce when a large or well-known company's breach is uncovered but slow to follow up or explain that smaller third parties often provide the gateway for hackers to reach major companies. In the public's eye, the blame rests squarely on the company that's widely known.

Further, when a company's own confidential and proprietary information – such as contracts and agreements, trade secrets, and other intellectual property – is breached, the company can suffer untold consequences and significant financial losses.

Areas for Improvement

With third-party relationships creating such significant risks, it's not surprising that executives are interested in improving their third-party risk management. A survey conducted by the Institute of Internal Auditors Research Foundation and sponsored by Crowe[3] found that executives felt their organizations need to improve in the following areas (note that respondents were allowed to select multiple areas of concern):

- Understanding risk exposures (38 percent of the respondents)
- Defining third-party risk management responsibility (32 percent)
- Standardizing third-party risk management activities (29 percent)
- Risk management expertise (28 percent)
- Tools to support third-party risk management (28 percent)
- Third-party communication (25 percent)
- Influence over third parties' controls (19 percent)

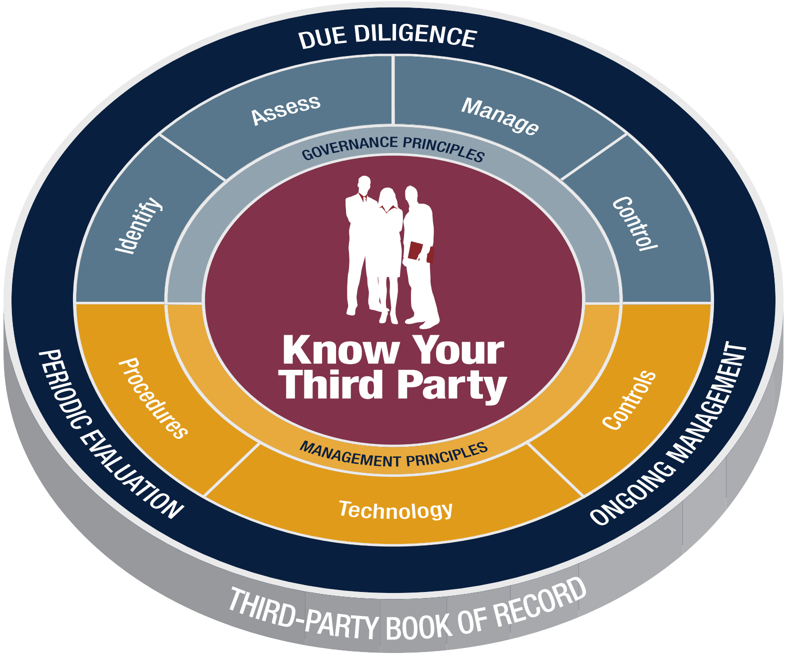
A Framework for Managing Third-Party Risk

Using an established framework can help improve management of third-party risks. A company must begin by inventorying and assessing its third parties and the risks they pose. The assessment should produce a prioritized list based on the likelihood and impact of harm to the company.

From there, the company should identify a mitigation strategy, including controls such as monitoring, audits, and compliance reviews, to manage the risks. It will also need to establish and implement appropriate procedures, tools, and technology (for example, software solutions to track and manage third-party relationships). A combination of virtual and on-site assessments will provide visibility into the operations and control structures at third-party facilities.

Naturally, a stale framework or an unmanaged program will fail to enable sustainable risk management of third parties. The exhibit illustrates how knowledge of a third party combines both the principles governing the company's third-party relationships (the identification of third-party relationships, assessment, management, and control) with the principles required to manage those third-party relationships (standards, procedures, and technology). Encompassing all of this is the company's due diligence at the onset of a relationship, ongoing management of the entire population of parties, and periodic evaluation to properly monitor the relationships. The exhibit also allows for necessary adjustments to any specific third-party risk management program.

Exhibit: Third-Party Risk Management Framework



Source: Crowe analysis

Operational and Strategic Considerations

Effective third-party risk management programs have a strong tie to their companies' operational and enterprise risk management (ERM) strategies. The concept of a third-party risk center of excellence – a cross-functional task force that coordinates its organization's third-party risk management program – helps bring together dedicated third-party resources with the subject-matter experts from departments such as procurement, IT, information security, compliance, operational risk, and privacy. The line-of-business personnel who interact with the third party on a day-to-day basis also play a vital role in the third-party risk management of the organization.

The best ERM programs integrate strategic third parties into their overall operational risk management approach. This effort can include:

- Assessment of risk management capability during a due diligence phase
- Negotiation of contracts with strategic third parties with heightened transparency and information available to manage operational risk
- Use of key risk indicators (KRIs) and "red flags" to oversee and monitor the risk management capability of the third party
- Access provided to third-party representatives to specific company risk training and ERM program awareness

The consideration of third parties and their influence is a particular challenge to effective operational risk management. Most of the world's leading companies put their reputation and financial success in the hands of third parties. Operational risks often manifest themselves beyond the boundaries of the enterprise, and most organizations are highly dependent on other organizations to not only mitigate operational risk but also to identify, assess, and report risk information.

Best-in-class ERM programs have well-established operational risk management processes that recognize that an organization's risk profile extends well beyond the enterprise. Operational risks that cut across an entity's organizational structure, or extend beyond the enterprise, are the most challenging to manage. Internal control, risk ownership, and risk accountability might not follow the entity's organizational structure. Operational risks often require other mitigating responses beyond internal controls, such as transference or sharing with a business partner.

An ERM program should look past direct third parties, with broad focus across the extended enterprise (that is, third parties of third parties). Clear expectations should be established for operational risk owners so their responsibility for assessing, mitigating, and monitoring risk extends beyond the enterprise.

Best Practices for Managing Third-Party Relationships

Prior to entering any third-party relationship, a company's senior management should develop a plan for managing that relationship, taking into account the relationship's level of risk and complexity. To best do so, management should:

- Outline the strategic purposes of the relationship (for example, reduce costs, tap specialized expertise or technology, or augment resources or operations), the legal and compliance aspects, and the inherent risks related to using third parties.
- Discuss how the arrangement aligns with the company's overall strategic goals, objectives, and risk appetite.
- Consider whether the selection of the third party is consistent with the company's broader policies and practices (including its diversity policies and practices).
- Assess the nature and potential effect of customer interaction with the third party – including access to or use of those customers' confidential information, joint marketing and franchising arrangements, and handling of customer complaints – and outline plans to manage these effects.
- Evaluate potential information security implications, including access to the company's systems and confidential information.
- Consider contingency plans in the event the company must transition the activity that is the subject of the relationship to another third party or bring it in-house.
- Assess the extent to which the activity is subject to specific laws, regulations, and industry standards (for example, information security, conflict minerals, and Payment Card Industry Data Security Standard).
- Establish plans for ongoing monitoring of the third party's compliance with the contract (including supply side and demand side, such as supplier agreements and licensing agreements).
- Determine the need for involvement by the board of directors (for example, requiring board approval for critical third-party activities that could pose a high level of risk, such as outsourcing IT).

Act Now to Protect Your Company

Third-party relationships in the M&D industry require continuous risk management. For each such relationship considered or entered, the company must identify and assess the risks and develop and implement mitigation strategies. Failure to stay on top of the risks could have costly consequences.

Crowe

Contact Information

Sam Aina is with Crowe and can be reached at +1 818 325 8607 or sam.aina@crowe.com.

Matthew Bowser is a principal with Crowe and can be reached at +1 317 208 2432 or matthew.bowser@crowe.com.

Lisa Domenick is with Crowe and can be reached at +1 312 606 7125 or lisa.domenick@crowe.com.

[1] "Everything You Need to Know About the Takata Airbag Recall," Consumer Reports, Dec. 23, 2015, http://www.consumerreports.org/cro/news/2014/10/everything-you-need-to-know-about-the-takata-air-bag-recall/index.htm

[2] "2015 Cost of Data Breach: Global," Ponemon Institute, May 25, 2015, http://www.ponemon.org/library/2015-cost-of-data-breach-global

[3] "Closing the Gaps in Third-Party Risk Management: Defining a Larger Role for Internal Audit," The Institute of Internal Auditors Research Foundation, December 2013, http://www.crowe.com/ContentDetails.aspx?id=8109

www.crowe.com

Text created in and current as of March 2016; Cover and artwork updated in May 2018.

The information in this document is not – and is not intended to be – audit, tax, accounting, advisory, risk, performance, consulting, business, financial, investment, legal, or other professional advice. Some firm services may not be available to attest clients. The information is general in nature, based on existing authorities, and is subject to change. The information is not a substitute for professional advice or services, and you should consult a qualified professional adviser before taking any action based on the information. Crowe is not responsible for any loss incurred by any person who relies on the information discussed in this document. Visit www.crowe.com/disclosure for more information about Crowe LLP, its subsidiaries, and Crowe Global.