Audit Committee Leadership Network

ACLN

VIEWPOINTS

Oversight of third-party risk

Companies, as well as their boards, are increasingly attuned to the risk presented by their suppliers, distributors, and other vendors due to regulatory pressure, the proliferation of third-party arrangements, and the complexity of cybersecurity. Regulation, intended to curtail risks to the public, has also brought pressure to bear. Some companies, especially those in regulated industries such as financial services, have created centralized third-party risk management programs, and even those without specialized programs are dedicating time and attention to ensure their third-party practices are consistent across the globe.

Executive summary

On October 31, 2017, members of the Audit Committee Leadership Network (ACLN) met in New York to discuss the current state of third-party risk management with two guests: Jim Connell, managing director and head of corporate third-party oversight at JPMorgan Chase, and Darlene Nicosia, vice president of commercial products supply at the Coca-Cola Company. This *ViewPoints* includes background information and synthesizes the perspectives that members shared before and during the meeting on the following topics.[1]

- **The third-party risk landscape continues to evolve** [page 2]

  The number of third parties with whom companies engage continues to grow. Many companies are using more traditional vendors, such as suppliers and distributors, within their supply chain, while also utilizing new types of partnerships. Companies derive many benefits from these relationships, but reliance on outside parties comes with increased risk. ACLN members and guests noted that associated risks present real threats to business continuity, whether through cyber breaches or reputational damage.

- **Companies use a variety of methods to manage third-party risk** [page 4]

  While there is no standard approach to structuring a third-party risk management program, members and guests shared a variety of practices for ensuring coordinated, successful oversight of these risks. Members discussed the centralized approach that some large banks are starting to use and whether that model would make sense in other sectors. In addition, members addressed practical techniques for onboarding new third parties and inspecting third-party practices for ongoing compliance.

- **Boards heighten the attention given to third-party risk** [page 7]

  Boards rely on a number of different frameworks and metrics to oversee third-party risk. In some cases, the issue is a regular item on the audit committee agenda; in others, it is delegated to another committee or is handled by the full board. In all cases, directors must understand the nature of the company's third-party relationships and how the company is managing these risks.

The third-party risk landscape continues to evolve

Third parties—whether in the supply chain, information systems, or new ventures—offer companies the ability to be more agile in a competitive environment by reducing production or delivery time while also lowering cost, and companies are working with more and more of them. A 2017 study of nearly 400 private and public companies reported that two-thirds of those companies have over 5,000 third-party relationships, with some having many more.[2]

The sheer number of these relationships adds to the challenge. *"Our organization interacts with over 28,000 third-party vendors, with 6,000 presenting some level of risk that needs monitoring,"* said Mr. Connell. In a pre-meeting conversation, one member highlighted what makes third-party risk different: *"Because they are outside of your organization, using third parties fundamentally limits the company's control."*

Key third-party relationships

In pre-meeting conversations, one member noted that the first step in managing third-party risk is defining what third parties are. One expert defines third parties as, "Any entities that are not company employees, including suppliers, vendors, subcontractors, contract manufacturers, resellers, distributors, partners, captives, and affiliates."[3]

Suppliers

Companies rely on a broad range of suppliers for the goods and services necessary to make and deliver their own products. In a recent survey of procurement executives, 36% reported having experienced a significant supplier-related risk event in the past two years. Of these executives, only 14% reported having a resilience strategy in place.[4] The survey found that companies are focused on understanding the operational risk presented by each supplier, particularly when that party is a single source for procurement, a dominant supplier, has significant intercompany relationships, works with multiple business units, requires a long lead time, or provides client-facing service.[5] Ms. Nicosia noted that manufacturing partners are essential to Coca-Cola's business, and each supplier typically goes through an audit before her company relies on them to manufacture ingredients.

Distributors

Many industries depend on distributors to reach the marketplace, whether wholesalers for bottlers or agents for insurers. These third-party partners introduce regulatory and reputational

risk through their activities on the company's behalf: "For suppliers, distributors are the face of your company. They either accentuate or cloud your brand promise."[6] Some members noted the importance of strong distribution channels for large technology companies, which depend on many third-parties to sell their products. One member said, *"We have nearly 200,000 partners around the world distributing and selling our products."*

Outsourced functions and business partnerships

Outsourcing also opens the door to third-party risk. Information technology, customer service, call centers, and human resources functions like benefits processing are not traditionally defined as part of the supply chain, but as these jobs and functions are outsourced, they become sources of third-party risk, much like suppliers or distributors. In addition, shared technologies, such as cloud data storage, are necessitating new kinds of third-party arrangements, with attendant risks.

Companies will frequently join forces to serve each other's customers more effectively or to reach new customers. Examples of such partnerships include contracted ventures with marketing and cobranding partners and engagements with fee-based service providers. When these arrangements require sharing sensitive data, they become a source of risk.

Potential third-party risks

Experts and members noted several specific types of risk arising from third-party engagements:

- **Cybersecurity risk.** A recent survey of IT and security professionals found that 63% of cybersecurity breaches were linked to third parties with access to corporate applications.[7] Cybersecurity issues cut across nearly all facets of third-party engagements. Third-party access to the company's information systems or its customers requires thorough controls and monitoring. Several members identified the protection of data assets as one of the highest priorities for their companies in third-party engagements. Both guests emphasized the importance of cybersecurity.
- **Fraud and corruption risk.** The Foreign Corrupt Practices Act (FCPA) requires that companies know the relationships a third party has with foreign officials, that they understand the business rationale for working with the third party, that they undertake ongoing monitoring of third-party relationships, including periodically performing due diligence, audits, and training, and that they request annual compliance certification. Unfair or deceptive practices by third parties causing harm to customers put the company itself at risk of an FCPA violation. Many companies still have work to do in order to address anti-corruption issues. In a 2013 study, EY reported that 44% of over 1,700 respondents did not perform background checks on third parties with whom they engaged in business.[8] In the same year, more than 90% of Department of Justice investigations of FCPA violations were related to the actions of third parties.[9] One member noted that FCPA issues are a major

challenge for the audit committee: *"We perform analytics to focus on the real issues, but with over 100,000 contracts, something still comes up monthly that requires the audit committee's attention."*

- **Operational risk.** When a third party plays a key role in company operations, the company suffers if the third party's operations cease, slow down, or do not produce the expected result. Ms. Nicosia noted the benefits of having a contingency plan in place to deal with scenarios such as a recent case in which a storm shut down a supplier's factory for an extended period. Companies should also be aware of the financial health of third parties on whom they rely. The financial risk of doing business with third parties is not restricted to suppliers; shared-revenue agreements in contracts with distributors, joint venture partners, or other business partners can stand in the way of a company getting paid for its products or services.
- **Reputational risk.** In many scenarios, third parties—such as distributors, retailers, or franchisees—publicly represent a company's brand. If a third party acts in a way that does not meet the standards of the company or the expectations of its customers, reputational damage can occur. Several members identified reputational risk as a major concern for their companies in doing business with third parties. Members noted the difficulty of recovering the public's favor once damage to the brand occurs. *"Reputational risk is real,"* said Ms. Nicosia. To defend against reputational risk, Coca-Cola requires its suppliers to adhere to certain standards. One member asked, *"Are you getting pressure to extend your work to be more socially focused?"* Ms. Nicosia said, *"Yes, from environmental practices and workplace conditions to others. It runs the gamut. We have supplier guiding principles that state our expectations. Furthermore, our customers care and ask how we're addressing the issues."*

Companies use a variety of methods to manage third-party risk

Third-party risk management (TPRM) initiatives vary from company to company and from industry to industry, but often responsibility for them rests with procurement or risk functions.[10] Among member companies, some have robust plans in place while others are less prepared. The level of awareness varied by sector but is highest in financial services.

Approaches to TPRM

"[TPRM] programs are almost always homegrown, although firms often bring in outside advisers to help build up the program," said Mr. Connell. ACLN members and other experts identified three common approaches to managing third-party risk.

Decentralized management

Nearly 19% of companies responding to a recent survey described their current TPRM model as decentralized, with risk management embedded within each business unit.[11] Several members reported that their companies used a decentralized model.

ACLN members noted that third-party risk is typically integrated into the company's enterprise risk management (ERM) plan and that issues with third parties are generally brought to the board through ERM reporting, not as a separate type of risk. Some members described third-party risk as an emerging area within ERM and said that while it is currently a component of their plans, it warrants more of the audit committee's attention.

Centralized management

Some companies have designated leaders in management to oversee third-party risk. This centralized approach is a growing trend at global banks. A recent EY study of financial services organizations found that of the 49 global institutions surveyed, about a third had had TPRM programs for more than five years, a third for three to five years, and a third for fewer than three years.[12] At JPMorgan Chase, Mr. Connell oversees an end-to-end program tasked with centralizing third-party engagements across the organization's supply chain, which he undertook three years ago. A key responsibility is understanding the current risks to the organization and ensuring that suppliers meet the company's internal control standards, especially in dealing with customer data.

ACLN members said that outside of the financial services sector, it is uncommon for a company to centralize TPRM. One member said, *"Most organizations do not have someone in a role like Jim Connell's position; management of third-party risk is disaggregated."* Members were interested in whether centralized TPRM will make its way to other sectors. Vignesh Veerasamy, EY's third-party risk management leader for non-financial services, noted that although very few companies outside of financial services have mature TPRM programs, the programs are gaining momentum. He said, *"There is an increased focus on setting up programs by companies in other, more-regulated industries like healthcare, life sciences, utilities, oil, and gas. This development is newer than in financial services, but they are starting to determine the models needed to manage the risk."*

Hybrid models

Many organizations use a combination of approaches with some aspects of third-party management centralized and others remaining in the individual business units. The survey cited above found nearly 31% reporting a hybrid model with centralized components in either procurement or risk management.[13] Mr. Veerasamy noted, *"Often, third-party risk management is done in silos. Because of the silos, all are managing an aspect of third-party risk, but they are not talking to each other, nor are they executing it holistically. Some clients are realizing this need and are establishing TPRM programs at an enterprise level."*

As an example of a hybrid approach, Ms. Nicosia described her supply chain team at Coca-Cola, which is responsible for managing all third-party relationships related to manufacturing the company's products: *"We work with a tremendous number of suppliers, including agricultural, packaging, and many other types of third parties."* She added that while her team is ultimately responsible for these relationships and their associated risks, she coordinates

closely with the company's risk management team. "*Our program is part of ERM; however, of the key risks flagged last year, nearly 80% were related to third-party risk, so we have to think about whether third parties should stand alone,"* she said.

Ms. Nicosia highlighted the value of centralizing some components of a company's third-party dealings, such as through a procure-to-pay tool: *"Before centralizing the process eight years ago, we had thousands of suppliers with no centralized repository for contracts. Our biggest objective in creating a system was to communicate who our preferred suppliers are in order to prevent redundancies. When you utilize those established relationships, you reduce risk.*" A member noted the benefit of centralizing activities: *"Centralization of procurement is a cost savings. At large companies, you gain negotiating power with suppliers by doing so."*

Techniques used to onboard new third parties

Members and guests discussed a range of ways that companies minimize the risk of doing business with new third parties. A McKinsey report identified several strategies for helping companies with this challenge:[14]

- **Perform due diligence**. Before contracting with a third party, companies typically perform a review of the potential partner's financial health and reputation, as well as its operations and controls. This process varies based on the type and scale of the relationship; companies often perform more rigorous reviews of relationships that are highly visible or that involve sensitive data. Mr. Connell noted the importance of performing background checks on companies presenting a medium to high level of risk.
- **Ensure robust contracts that protect company interests**. In pre-meeting conversations, one member noted the importance of working with in-house counsel to ensure the company is adequately protected from the outset: *"Partnering with legal to get a strong contract and then managing it helps to create clear expectations between the company and the vendor. I recommend that we trust our partners but verify; there are too many instances of the third party not measuring up."*
- **Rate third parties based on their threat level.** Not all third parties introduce the same amount of risk into the company, and members said it is important to focus on those with the highest level of risk. By scoring each vendor, a company can segment its inventory and allocate resources accordingly. Mr. Connell noted, *"Using a rating system, we conduct an assessment of each supplier that shows whether they have the appropriate controls in place and in use, and if we find gaps, there is a tipping point at which we won't work with them."*
- **Add third parties to a master database**. In order to understand the universe of risks introduced by third parties, a company must know who those partners are and what risks they bring with them. The task of collecting data on third parties and entering it into a central system can be onerous, and many companies do not have key pieces of

information that would make such a database useful. While a comprehensive inventory might not be right for all organizations, experts recommend an enterprise-wide survey to begin the process.

The benefits of continuous monitoring of third parties

Evaluating third parties is an ongoing effort, and in the case of a risk like cybersecurity, what was relevant yesterday may not be today. Companies track regular metrics related to third parties' activities, controls, performance, and compliance to ensure that circumstances still warrant maintaining the business relationship.

Members noted that operational risk increases when a company works with parties based in other countries, where perceptions of quality or timely delivery might differ from those of the company: *"Over the years, a big challenge has been foreign agents because of the difficulty to police activities,"* Ms. Nicosia said. To monitor those parties, Coca-Cola utilizes auditing teams with a global presence: *"It's worthwhile to set up a protocol, auditing these third parties every two to three years. There are local customs and practices that can be difficult to detect, so it's important to be on the ground to see and listen."*

Both guests discussed the importance of robust monitoring programs that include regular audits of the riskiest third parties. Ms. Nicosia explained that to ensure an unbiased assessment, Coca-Cola often uses independent parties to assess whether a third party's environmental and workplace conditions meet Coca-Cola's standards. She added that in at least one case, her company is partnering with one of its customers to conduct joint audits to streamline the process for its suppliers. Mr. Connell said that JPMorgan Chase is partnering with three other financial services firms to execute third-party risk assessments.

Addressing the issue of cybersecurity, Mr. Connell said that when his team audits a supplier, 80% of the focus is on cyber controls and only 20% is on other operational issues. He further noted, *"A big part of our job is understanding what goes out the door. Anyone that holds our data we view as an extension of our bank, and we hold them to the same standard that we hold ourselves."* Ms. Nicosia noted that because of the high level of risk associated with cybersecurity, Coca-Cola audits almost all of the third parties that interact with the company's IT systems.

Members and guests debated using outside organizations to audit third-party compliance with a company's operating standards and codes of conduct. One member said, *"Running an audit by an outside party is not the same as running your own audit. It's difficult to assess the credibility of that audit."*

Boards heighten the attention given to third-party risk

ACLN members noted that in most cases, third-party risk is reviewed at the board level as a component of ERM. However, given the importance of this risk, members questioned what boards might do to improve oversight of this risk. Members and guests discussed new techniques for helping the board's understanding of the issue.

Using risk assessment frameworks

Often, it is the audit committee that tracks major risks, often by reviewing progress against a particular framework. EY principal Matt Moog, with the firm's IT Advisory Services practice, said, *"Frameworks are a good starting point but can be cumbersome. Aligning third-party risk with whatever framework is currently in use for security, such as [the framework from] NIST [National Institute of Standards and Technology], can help an organization establish the baseline criteria."* While frameworks can be useful guides, programs are generally particular to the organization.

At JPMorgan Chase, Mr. Connell's team uses a five-tier framework to assess supplier risk, categorizing each vendor as critical, high, medium, low, or nominal risk. *"Out of the 6,000 suppliers we rate, about 100 are critical; however, any between critical and low are subject to our assessment,"* he said.

Reporting third-party risk to the board

At members' companies, third-party risk is reported to varying committees and discussed with varying levels of intensity.

- **Which board committee oversees third-party risk?** Several members reported that on their boards, the audit committee handles issues related to third-party risk. The audit committee has the advantage of working with the internal audit function, which makes development of a comprehensive control system to oversee third-party risk easier.[15] At financial service organizations, the risk committee typically oversees third-party risk, and some boards outside of financial services have also placed third-party risk oversight with the risk committee or with another committee that has oversight of at least some components of risk management. One member said, *"Third-party interaction is such an important part of the business that we created a separate compliance committee. It helps prevent audit committee overload and ensures [third-party risk] gets the attention it deserves."* One member differentiated the roles of the risk and audit committees in managing third-party risk thus: *"The audit committee remains responsible for financial processes, but risk mapping, beyond financial-reporting risk, goes to the risk committee, which is responsible for the entire risk landscape and delegation to other committees."* On one member's board, the audit committee does not directly oversee third-party activities, but it reviews information from other committees: *"For our industry, safety is first. Internal*

audit performs the audit on third-party data [and] reports to the public-responsibility committee, but the audit committee reviews the data."

- **How often does the board address third-party risk?** Most members said that their boards or relevant supervising committees do not address third-party risk at each meeting. In some cases, it only comes up as a small piece of a broader risk review. One member said, *"I am feeling like our practice might be inadequate. It's often episodic if there's a serious issue. Otherwise, it's a 15-minute review once a year."*
- **What information related to third-party risk do boards receive?** In a 2015 survey, EY found that 43% of organizations reported critical third parties to the board, which was up from 26% in 2014, but only 35% reported third-party breaches to the board.[16] Many executives who oversee third-party risk find effective reporting a challenge. Among the tools and techniques respondents to a recent survey mentioned using were key risk indicators and third-party performance scorecards.[17] Additionally, incident reporting has moved beyond solely alerting the board to bringing up issues of cost. Using the five-tier framework described earlier, Mr. Connell shows the audit committee the overall health and use of different third parties across the organization. He also uses key metrics to outline trends: *"For the audit committee, our reporting uses a high-level view focused on each individual business. We are also transparent about the limitations in seeing the full risk environment of our third parties."*

Conclusion

Third-party relationships are important for ACLN members. Depending on the industry, companies manage the risks introduced by third parties in different ways. As companies' relationships with third parties evolve, boards and audit committees must ensure they continue to manage those risks adequately, and a number of members feel that may mean having audit committees spend more time on the matter. One said, *"I can't help but think about the amount of time we're spending with people in your positions as audit committee chairs. We're not spending much time, in my experience."* Other members agreed: *"We dabble on the board with this issue, but we need to get deeper. It's an area we need more time on."*

About this document

The Audit Committee Leadership Network is a group of audit committee chairs drawn from leading North American companies committed to improving the performance of audit committees and enhancing trust in financial markets. The network is organized and led by Tapestry Networks with the support of EY as part of its continuing commitment to board effectiveness and good governance.

ViewPoints is produced by Tapestry Networks to stimulate timely, substantive board discussions about the choices confronting audit committee members, management, and their advisers as they endeavor to fulfill their respective responsibilities to the investing public. The ultimate value of *ViewPoints* lies in its power to help all constituencies develop their own informed points of view on these important issues. Those who receive *ViewPoints* are encouraged to share it with others in their own networks. The more board members, members of management, and advisers who become systematically engaged in this dialogue, the more value will be created for all.

Appendix 1: Participants

Members participating in all or part of the meeting sit on the boards of 38 public companies:

- Mark Blinn, Audit Committee Chair, Texas Instruments
- Pam Craig, Audit Committee Chair, Merck
- Dave Dillon, Audit Committee Chair, 3M and Union Pacific
- Carolyn Dittmeier, Audit Committee Chair, Generali†
- Ellen Kullman, Audit Committee Chair, Dell Technologies
- Mike Losh, Audit Committee Chair, Aon
- Blythe McGarvie, Audit Committee Chair, LKQ*
- Heidi Miller, Audit Committee Chair, General Mills
- Chuck Noski, Audit Committee Chair, Microsoft
- Guylaine Saucier, Audit Committee Chair, Wendel‡
- Tom Schoewe, Audit Committee Chair, General Motors
- Dick Swift, Audit Committee Chair, CVS
- Jim Turley, Audit Committee Chair, Citigroup
- David Vitale, Audit Committee Chair, United Continental

EY was represented in all or part of the meeting by the following:

- Steve Howe, US Chairman and Americas Managing Partner
- Frank Mahoney, Americas Vice Chair of Assurance Services

Appendix 2: Discussion questions for audit committees

- Is your company relying more heavily on third parties now than it was five years ago? Why or why not?
- What types of third-party relationships are most important to your company's success?
- How does your company identify the types of risks introduced by your third-party partners?
- Which risks are the biggest threat to your company? How is the company mitigating those risks?
- What techniques does your company use to ensure proper third-party risk management? How centralized is your company's approach?
- Absent a centralized model, how does your company ensure that third-party risk management processes and standards are consistent across the business units? If a centralized model is present, how are problems escalated?
- How does the company monitor and assess third-party relationships? Does your company track all third parties in a central inventory? Does your company use a rating system to monitor the threat level presented by each party?
- What frameworks does your company use to manage third-party risk?
- Which board committee oversees third-party risk?
- How is third-party risk reported to the board? How often and by whom?

Endnotes

[1] *ViewPoints* reflects the network's use of a modified version of the Chatham House Rule whereby names of members and their company affiliations are a matter of public record, but comments are not attributed to individuals or corporations. Quotations in italics are drawn directly from conversations with network members in connection with the meeting.

[2] Kroll and Ethisphere, *Anti-Bribery and Corruption Benchmarking Report* (New York: Kroll, 2017), 7, 38.

[3] Marie Patterson, interview with *Compliance Week,* "The Complexity of Third-Party Management," Hiperos, accessed on November 9, 2017.

[4] RapidRatings, "New Research from ProcureCon and RapidRatings Reveals over a Third of Procurement Professionals Experienced a Serious Supplier Risk Event in the Past 18 Months," news release, June 29, 2017.

[5] Jaclyn Jaeger, "Building a Resilient Supply Chain," *Compliance Week*, August 1, 2017.

[6] Jordan Katz, "How Suppliers Should Manage Their Distributors," Gallup, April 17, 2013.

[7] Carin Hughes, "Why Third Party Cybersecurity Matters," CSO, December 7, 2016.

[8] EY, *Growing Beyond: A Place for Integrity* (London: EYGM Limited, 2013), 1, 2.

[9] Ibid., 8.

[10] EY, *Shifting toward Maturity: Key Findings from EY's 2016 Financial Services Third-Party Risk Management Survey* (London: EGYM Limited, 2016), 14.

[11] Compliance Week and RSA, *Working toward a Solution: Third-Party Risk Management* (Round Rock, TX: Dell, 2017), 15. Available for download here.

[12] EY, *Shifting toward Maturity: Key Findings from EY's 2016 Financial Services Third-Party Risk Management Survey*, 2.

[13] Compliance Week and RSA, *Working toward a Solution: Third-Party Risk Management,* 15.

[14] See Dmitry Krivin, Hamid Samandari, John Walsh, and Emily Yueh, *Managing Third-Party Risk in a Changing Regulatory Environment,* McKinsey Working Papers on Risk no. 46 (New York: McKinsey & Company, 2013), available for download here.

[15] ERM Initiative Faculty and Nilisha Patel, "The Audit Committee's Role in Third-Party Risk Oversight," abstract, June 3, 2016.

[16] EY, *Shifting toward Maturity: Key Findings from EY's 2016 Financial Services Third-Party Risk Management Survey*, 17.

[17] Compliance Week and RSA, *Working toward a Solution: Third-Party Risk Management,* 13.

† Member of the European Audit Committee Leadership Network

* Alumna of the Audit Committee Leadership Network

‡ Member of the European Audit Committee Leadership Network