European Audit Committee Leadership Network

August 2018

EACLN

VIEWPOINTS

Oversight of third-party risk

Third-party relationships can be a substantial source of enterprise risk. The proliferation of third-party partners, regulatory pressure, and the complexity of cyber-related risks has led companies to dedicate more time and attention to the potential risks presented by their suppliers, distributors, vendors, and other partners. In some companies, including those in highly regulated industries like financial services, this has led to the creation of a centralized model for overseeing third-party risk.

On July 11, 2018, members of the European Audit Committee Leadership Network met in Frankfurt to discuss key third-party risks their companies face and strategies to mitigate these risks with two guests: Achim Laube, regional head of non-financial risk management–risk type control, for Germany and Europe, the Middle East, and Africa, at Deutsche Bank, and Netta Nyholm, partner and advisory risk services leader for Germany, Switzerland, and Austria at EY. *For guest biographies, see Appendix 1, on page 11. For a full list of participants, see Appendix 2, on page 12.*

Executive summary

This *ViewPoints* includes background information and synthesizes the perspectives that members shared before and during the meeting on the following topics:[1]

- **The current third-party environment** (page 2)
  Third-party relationships enable companies to be flexible and competitive in a global business environment. Large, publicly listed companies now rely on a wide range of different third parties to help with various aspects of their businesses. These relationships often allow companies to delegate important tasks so that they can focus on their core competencies. While these relationships include traditional suppliers and distributers, many companies are also entering into new types of partnerships, ventures, or similar relationships with smaller start-ups.
- **The major risks associated with third-party relationships** (page 3)
  With the benefits gained from third parties comes related risks that pose significant threats to a business, such as cyber breaches, business continuity challenges, or reputational damage. Moreover, as the regulatory landscape evolves, companies must ensure that third parties comply with legal requirements, which can be especially challenging when dealing with smaller third parties in certain risky situations.
- **How companies manage third-party risk** (page 5)
  Third-party risk management varies depending on the sector of the business and the scale of third-party relationships. For highly regulated industries like financial services or pharmaceuticals, these functions are often centralized, with specialized executive

leadership overseeing risk for the whole enterprise. Other organizations tend to have more decentralized or hybrid functions, with business units locally owning the risk or groups like compliance, procurement, or legal overseeing the risk. Regardless of the formal risk management model, it is critical for companies to grasp the scale of their third-party relationships and adopt uniform practices and processes for dealing with third parties.

- **The board's role in overseeing third-party risk** (page 7)
  Boards, specifically audit committee chairs, understand that today's global business environment requires relationships with an increasingly diverse group of third parties. EACLN members recognized that while many boards are in the early stages of overseeing third-party risk management, the issue is likely to require heightened attention in the future. Audit chairs were therefore interested in how best to advise management on these risks to ensure thorough oversight of third-party relationships from the outset.

For a list of discussion questions for audit committees, see Appendix 3, on page 13.

The current third-party environment

Third parties offer companies the ability to be more agile in a competitive environment by reducing production or delivery time, performing non-core business activities, and lowering costs. In recent years, many companies' third-party relationships have expanded as supply chains, distribution partners, business process outsourcing, information technology (IT) infrastructure providers, and new ventures have expanded and grown increasingly complex. A 2017 survey found that European companies have an average of nearly 12,000 third-party relationships across their global organizations in a typical year.[2] EACLN members said that the number of partners that their companies do business with could be even higher.

Identifying what constitutes third-party relationships is an important first step in developing an approach to manage them. One source 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 to provide the goods or services necessary to make and deliver their own goods or services. In a recent survey of procurement executives, 33% reported having experienced a significant supplier-related event in the past two years, and only 14% reported having a resilience strategy in place.[4] Another 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 or a dominant supplier, has significant inter-company relationships, works with multiple business units, requires a long lead time, or provides client-facing service.[5]

Distributors

Distributors and resellers are important intermediaries between companies and end users. Whether wholesalers for manufacturers or agents for insurers, many industries depend on distributors to reach the marketplace. These third-party partners introduce regulatory and reputational risk by acting on the company's behalf. "Distributors are the face of your

company. They either accentuate or cloud your brand promise," one expert explained.[6] The risk presented by a single distributor differs by company and depends on the organization's reliance on that channel to get its product to market, noted one member: *"For one company, this risk is low because of the geographic spread and large number of distributors; however, for another company with only two paths to market, the risk is more concentrated."*

Business partnerships or joint ventures

Companies engage with other parties in a limitless range of ways to serve each other's customers more effectively or to reach new customers. In some cases, these relationships focus on co-branded marketing strategies, while others include the provision of service for an agreed-upon fee; in many cases, these agreements require sharing sensitive data. These types of business partnerships make up 80% of some business units' spending on suppliers; they "are complex arrangements in which risk-sharing is sometimes poorly specified, and some risks are unaddressed."[7] Deutsche Bank's Mr. Laube said, *"Working with small fintech companies is strategically so important for us, but we've realized that they will not be standard relationships. In one example, partnering with the company would have required us to open up sensitive customer connections to deliver information to them, so instead we decided to acquire the technology."*

Commonly outsourced functions

IT, customer service, call centers, and human resources functions such as benefits processing are not traditionally defined as aspects of the supply chain, but they are necessary adjuncts to operations and are commonly and increasingly outsourced. Shared technologies, such as cloud-service providers, also give rise to new kinds of third-party engagements and attendant risks.

The major risks associated with third-party relationships

While there are many benefits to working with third parties, companies are subject to new and different risks when they cede control to outside organizations. Third-party risks are interconnected. Experts and members commented on several specific risks arising from third-party engagements:

- **Cybersecurity risk.** A 2016 survey of IT and security professionals found that 63% of cybersecurity breaches in recent years were caused by or linked to third parties with access to corporate applications.[8] Third-party access to a company's information systems and customer data can create vulnerabilities that are of particular interest to regulators. While cybersecurity is top of mind for most members, getting a better understanding of a company's exposure to third-party cybersecurity risk remains a work in progress for some. One member noted, *"Because systems are becoming more interconnected—for example with cloud computing—this area is critical, and the audit committee should spend more time on the technology risk."* Another member said, *"Our cybersecurity team maintains an awareness of the risks presented by third parties and takes measures to avoid those. A concern that remains is whether the partners are prepared to respond to an attack."*

- **Data privacy risk.** EACLN members and experts alike noted that the recently implemented General Data Protection Regulation (GDPR) creates new risks for companies that use third parties to manage customer, employee, and other individual data. The GDPR specifically applies to data breaches caused by third parties. Since 63% of breaches involve third parties, as noted above, companies must ensure that their partners are ready to comply with its requirements.
- **Fraud and compliance risk.** In Europe, anticorruption laws differ by country, with the broad basis provided by the Organization for Economic Cooperation and Development's model. The United Kingdom's Bribery Act of 2010 applies to companies conducting business in the United Kingdom or partnering with UK-based businesses that fail to prevent bribery, including bribes offered or given. In addition, under the Bribery Act, it is an offense to request, agree to receive, or accept a bribe. The United States' Foreign Corrupt Practices Act, which is widely recognized and enforced, 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. Concerns relating to third-party fraud and corruption risk have led some companies to bring work done with foreign governments in-house. Not all companies fully understand the hazards of fraud and corruption that third parties present. In a recent EY survey, more than 25% of respondents stated that the people managing third-party relationships within their companies were not required to complete fraud and compliance risk training.[9]
- **Operational risk.** Without direct control over activities performed by third parties, companies are subject to business continuity risk when operations cease, slow down, or do not produce the expected result. Operational risk may arise when a company works with parties based in other countries, where perceptions of quality or timely delivery might differ from those of the company.
- **Reputational risk.** In many scenarios, third parties such as distributors, retailers, or franchisees publicly represent a company's brand. Reputational damage can result from third-party actions that do not meet the standards of the company or the expectations of its customers. This is especially challenging because social-media platforms offer global forums on which to air grievances and businesses have little recourse to manage brand perception as quickly as messages spread through these channels.
- **Geopolitical risk.** Different norms make managing global programs a challenge. Members agreed that certain geographies create major risks for their companies, especially regions where human rights issues like child labor are a concern. One member noted the difficulty of working with some government-owned suppliers: *"The rules used to govern differ from country to country, and some countries are unpredictable. It's important to know the political particularities of the jurisdictions in which you work."*

Members and guests noted that supplier concentration, or relying on a limited number of vendors, is an important emerging risk. Mr. Laube explained that companies may consolidate

supply to drive down costs, but that may increase certain risks: *"We set up outsourcing operations in India and the Philippines—but there are certain political risks, so we have spread out the work across multiple centers in those regions."* A member emphasized the need to diversify a company's supplier base to reduce risk concentration, which can bring production to a halt in the case of a natural disaster or geopolitical crisis that shuts down a single supplier's operations. Diversification of sources or suppliers, however, presents another challenge in that companies derive value from long-standing, trusted partnerships with established third parties.

How companies manage third-party risk

Corporate third-party risk management (TPRM) initiatives vary from company to company and industry to industry. At some companies, management responsibility falls to individual business unit heads while at others it is within the jurisdiction of the finance, procurement, compliance, or risk functions.[10] TPRM programs provide a "function for management to identify, evaluate, monitor, and manage the risks associated with third parties and contracts."[11] A 2015 EY survey of 49 global financial services organizations found that about a third had maintained TPRM programs for more than five years, a third for three to five years, and a third for fewer than three years.[12]

While financial services organizations have been at the forefront of developing mature TPRM programs, companies in other sectors are now taking significant steps to get ahead of these threats.[13] One expert, speaking to the Audit Committee Leadership Network in North America, 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."[14]

Three approaches to third-party risk management

Members and other experts identified three ways that companies govern third-party risk:

- **Decentralized.** In many companies, ownership of third-party risk is shared among business units. A 2016 survey found that about 19% of companies described their current model as decentralized, with risk management embedded within each business unit.[15] Ms. Nyholm observed that for most companies, third-party risk management was extremely decentralized. She cautioned, however, that this approach might leave a company without the processes and tools to manage relationships in a consistent way. *"We see that the legal department is playing a bigger role in managing third-party relationships because when something goes wrong, that's who people turn to,"* she said.
- **Centralized.** Some companies use a centralized model in which third-party oversight is assigned to a single group. In the aforementioned survey, around 36% of respondents reported using a centralized model with oversight responsibility in either procurement or risk management.[16] At Deutsche Bank, a centralized group focused on non-financial risk manages third-party risk, ensuring that business units meet the bank's standards. Several members noted the role that procurement departments play in coordinating third-party

relationships across the enterprise. *"Procurement has a central role. They have the expertise to focus on the important issues, like vetting a third party's willingness to take on our code of conduct and its cybersecurity readiness. Procurement works with the business units, so they should be sensitive to the issues that could be embedded in an arrangement,"* said one member.

- **Hybrid.** Many organizations use a hybrid approach: some aspects of third-party management are centralized, while others remain with individual business units. The survey cited above found nearly 31% reporting a hybrid model with centralized components in either procurement or risk management.[17]

Techniques used to manage third-party risk

It is one thing to establish good business practices and another to implement them across complex organizations spanning multiple business lines, functions, countries, and cultures. A McKinsey report,[18] along with member and guest discussions, identified several strategies for helping companies mitigate third-party risks:

- **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 with relationships that are highly visible or involve sensitive data. Some members noted that they have observed an increase in the practice of auditing potential partners before contracting with the third party.
- **Ensure robust contracts that protect company interests.** In pre-meeting conversations, one member noted the importance of working with counsel to ensure the company is adequately protected from the outset. Ms. Nyholm recommended that contracts be understandable to those working in the business and that ownership be clearly defined: *"Companies need to translate contracts into operational language and give access to the full contracts, so that operational dependencies are understood. There needs to be consideration of the quality of the contract, or how success is measured; this should be defined very clearly. Truthfully, this is just good project management, but if you don't have an owner, it's not going to work."*
- **Maintain a complete inventory of all third parties and associated risks.** A company must know its partners and the risks associated with each of them. The task of collecting this data into a central system can be onerous, and many companies do not have the information to make this database useful. While a comprehensive inventory might not be the right fit for all organizations, experts recommend an enterprise-wide survey to begin the process. Mr. Laube and Ms. Nyholm highlighted that some companies utilize software tools to consolidate enterprise-wide vendor inventory.
- **Rate third parties based on their risk level.** Members with active programs generally agreed that third parties should not all be treated equally and that thresholds were important to ensuring the right level of focus on each partner. A 2017 EY survey of third-party risk in financial services noted that respondents largely defined critical third parties

based on the "potential to impact critical business processes" and the "sensitivity of data involved in providing the service."[19] By scoring each partner, a company can segment its inventory and allocate resources accordingly. *"Organizations should consider which relationships need to be managed closely, are important for the business, or are high risk. It's exhausting to manage all these relationships the same way; companies need to focus their energy on those that are high priority,"* said Ms. Nyholm.

- **Verify GDPR compliance.** To ensure data privacy, experts recommend that companies "clearly define all of the areas and activities in which GDPR is in scope, and have your third-party vendors agree and provide signed contractual assurances they will achieve all the GDPR compliance intricacies."[20] In addition, companies should require that third parties request approval from the company for any outsourced activities involving sensitive data.
- **Practice continuous monitoring.** Evaluating third parties is an ongoing effort—and in the case of a risk like cybersecurity, what is relevant today may not be relevant tomorrow. EACLN members were concerned that, in some cases, TPRM focuses too much on initial vetting. By tracking regular metrics on the parties' activities, controls, and compliance standards, companies come closer to ensuring that obligations are continually being met. One member's company conducts annual audits of third parties with whom they have a significant relationship; for others, the audit is performed every three years. At most member companies, internal audit plays a significant role in providing this assurance. Ms. Nyholm advised that companies exercise their right to audit vendors: *"In contract negotiation, companies should consider how they monitor third-party relationships, and if you have an audit or open-book clause in the contract, you should do it in order to not risk losing the right to audit in the future, depending on the jurisdiction."* Companies often hire external firms to inspect their third parties' practices for compliance with both the corporate code of conduct and local laws. These inspections ensure that vendors adequately address issues such as workplace and environmental compliance.

The board's role in overseeing third-party risk

Members noted that third-party risk management is increasingly important given heightened concerns about companies' reliance on outside sources. EACLN members considered what their oversight role should be and how new techniques might help the board understand the issue. A 2018 EY report noted that while few specific third-party issues make it to the board right now, as companies elevate their TPRM programs, boards will see these items featured on their agendas.[21]

As third-party relationships continue to evolve, directors play a key role in overseeing this risk. But how are board members, and specifically audit committee chairs, getting the information they need to determine the company's risk coverage? EACLN members discussed questions for boards to consider.

Which board committee oversees third-party risk?

Oversight of third-party risk takes various forms. While some members' audit committees regularly review this risk, others said that the full board is responsible for its oversight. For

Deutsche Bank, as is typical with many large banks, third-party risk is a part of the risk committee's agenda. Members emphasized the importance of the audit committee's oversight and expressed interest in hearing how others incorporate the discussion into the committee agenda. *"The audit committee needs to take on a governance role in overseeing this risk,"* one member said. Another member expressed a concern: *"Frequently, the audit committee doesn't know how to ask the right questions about third-party contracts to understand what they say and how the company monitors them."*

Who reports to the board on third-party risk, and how often?

At some member companies, the chief financial officer, chief operating officer, chief compliance officer, chief risk officer, or individual business unit heads present to the board on these issues. They may be reviewed on an annual basis in conjunction with the enterprise risk management process, although some members commented that a change in the business environment, such as a major contract renewal, would prompt the board to take a closer or more frequent look. At Deutsche Bank, third-party risk is included in broader discussions with the group's global head of non-financial risk. *"For the board, we focus on explaining the risks from a strategic point of view and from a mitigation perspective. In reality, to get to the supervisory board, something would have to go very wrong,"* Mr. Laube explained.

What information related to third-party risk do boards receive?

For many executives overseeing third-party risk, effective reporting presents a challenge. The 2017 EY survey of TPRM found that only 41% of organizations reported critical third-party information to the board, and only 26% reported third-party breaches or incidents to the board.[22] Another survey on TPRM practices found that nearly half of respondents reported on third-party risk to the board; others used key risk indicators, third-party performance scorecards, and reports to the senior operating committee.[23] Although most members reported that they look at key vendors or suppliers, not all members said they receive a comprehensive update on third-party relationships. Members also noted that their audit committees might receive more details about high-risk third parties, such as a sole supplier of a critical component. *"Exceptions are immediately brought to the audit committee in a monthly meeting with internal audit. They report on what was found and how the team is working to mitigate the risk,"* said one member.

One member noted the importance of getting the right level of detail from management on third-party risk: *"If the data you receive is rough, ask for more detail. The audit committee needs to have good material for a strong discussion, and sometimes management is not willing to give the details. They want to present a nice picture of the risk environment, but that doesn't help put the right questions on the table."*

At one member's company, the board reviews relationships with new types of suppliers, like start-ups: *"When setting up an agreement with an innovative supplier with little governance structure, decisions go to the board because of the level of risk being accepted in this partnership."* Mr. Laube noted how the board can help management align third-party relationships with the company's broader strategy: *"Boards should ask their management*

teams to explain the business rationale for third-party relationships to make sure that this agreement makes sense for the company as a whole."

Conclusion

As relationships with third parties evolve, boards must ensure they continue to oversee those risks adequately. To do so, some EACLN members said that audit committees would need to spend more time on the matter in the future. One member noted that good third-party risk management should be part of a robust enterprise risk management process: *"Risk is changing. Doing an annual risk matrix just isn't enough. If you have a good process that really thinks about the individual risks, then you should manage third-party risk in the same way. A good, dynamic risk management system identifies when these relationships present significant risk to the company."*

About this document

The European Audit Committee Leadership Network (EACLN) is a group of audit committee chairs drawn from leading European 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: Guest biographies

Achim Laube

Achim Laube is a Non-Financial Risk Manager at Deutsche Bank. He is Regional Head of Non-Financial Risk Management (NFRM) Risk Type Control, and in addition, he heads the regional supplier risk team and the operational resilience team for Europe, Middle East, and Africa.

Achim started his career at Deutsche Bank in 1985 as an apprentice and started again after he finished university as a corporate banking trainee. He held different roles in corporate banking with a focus on process management, as well as on the internet as a banking channel. Afterwards, he worked for three years in human resources to build a web-based HR self-service tool for the bank. Since 2006, Achim has worked in the area of non-financial risk, first as Operational Risk Relationship Manager, and later as Regional Head of Business Continuity Management, and Vendor Risk Management before he took over additional responsibility for all NFRM Risk Types in the region.

Achim holds a diploma in economics from Christian-Albrechts-Universität, Kiel, and a master of business administration from Ashridge, Berkhamsted.

Netta Nyholm

Netta Nyholm heads the German, Austrian, and Swiss RISK Advisory practice. She is also leader of EMEIA and GSA Third Party Risk Management. She joined EY in 2008 and is based in the Cologne, Germany, office. Netta has over 18 years of experience in consulting various industries and has expertise in third-party risk management, contract risk and life cycle management, strategic partnering, contract compliance, co-sourcing and full-sourcing, internal control systems, and industry focuses on pharmaceuticals and life sciences.

Netta holds a master's degree in media and communication from Växjö University, Sweden.

Appendix 2: Participants

EACLN members participating in all or part of the meeting sit on the boards of over 20 public companies:

- Werner Brandt, Siemens
- Aldo Cardoso, ENGIE
- Carolyn Dittmeier, Generali
- Ángel Durández, Repsol
- Renato Fassbind, Nestlé and Swiss Re
- Margarete Haase, OSRAM Licht
- Shonaid Jemmett Page, MS Amlin
- Nasser Munjee, Tata Motors
- Guylaine Saucier, Wendel
- Carla Smits-Nusteling, Nokia

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

- Andy Baldwin, EMEIA Area Managing Partner
- Jean-Yves Jégourel, EMEIA Assurance Leader
- Julie Teigland, Regional Managing Partner, Germany, Switzerland, and Austria

Appendix 3: Discussion questions for audit committees

- Is your company relying more heavily on third parties now than five years ago? Why?
- What types of third parties are most critical to your company's success?
- How does your company identify the risks introduced by your third-party partners?
- Which third-party risks are the biggest threats to your company?
- Do you use a decentralized, centralized, or hybrid approach to monitor and assess third-party relationships?
- How does your company ensure consistent third-party risk management processes and standards? How are problems associated with third-party risk escalated?
- 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 third party?
- How does your company balance a rigorous approach to risk management with the needs of the business to partner with certain riskier parties? Who has the ultimate say on whether the company can do business with a vendor?
- How does your company audit the practices of the third parties with which it does business? What roles does internal audit play in the process?
- What framework, if any, 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. Italicized quotations reflect comments made in connection with the meeting by network members and other meeting participants.

[2] Thomson Reuters, *Third Party Risk: Exposing the Gaps from a European Point of View* (Thomson Reuters, 2017), 2.

[3] "OCEG Integrated Third Party Management Visual Overview," Opus, June 12, 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 28, 2017.

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

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

[7] Dmitry Krivin et al., *Managing Third-Party Risk in a Changing Regulatory Environment*, McKinsey Working Papers on Risk, no. 46 (McKinsey & Company, May 2013), 3.

[8] SOHA Systems, "Soha Systems' Survey Reveals Only Two Percent of IT Experts Consider Third-Party Secure Access a Top Priority, Despite the Growing Number of Security Threats Linked to Supplier and Contractor Access," news release, May 17, 2016.

[9] EY, *Integrity in the Spotlight: the Future of Compliance; 15th Global Fraud Survey 2018* (London: EYGM Limited, 2018), 15.

[10] EY, *Shifting Toward Maturity: 2016 Financial Services Third-Party Risk Management Survey* (London: EYGM Limited, 2016), 14.

[11] EY, *Can You Transform Your Third Parties' Risk Into a Competitive Advantage?* (London: EYGM Limited, 2018), 5.

[12] EY, *Shifting Toward Maturity: 2016 Financial Services Third-Party Risk Management Survey*, 2.

[13] EY, *Can You Transform Your Third Parties' Risk Into a Competitive Advantage?* 3.

[14] Audit Committee Leadership Network in North America, *Oversight of Third-Party Risk*, ViewPoints (Waltham, MA: Tapestry Networks, 2017), 5.

[15] Jaclyn Jaeger, "Survey: Trials, Tribulations of Third-Party Risk Management," *Compliance Week*, November 1, 2016.

[16] Jaeger, "Survey: Trials, Tribulations of Third-Party Risk Management."

[17] Jaeger, "Survey: Trials, Tribulations of Third-Party Risk Management."

[18] Krivin, "Managing Third-Party Risk in a Changing Regulatory Environment."

[19] EY, *Global Financial Services Third-Party Risk Management Survey: Is it Time to Shift Your Perspective of Third-Party Risk?* (London: EYGM Limited, 2018), 12.

[20] Mike McAlpin, "Why Third-Party Vendors Are About to Become a Significant Risk to Your Business," 8x8, November 15, 2017.

[21] EY, *Can You Transform Your Third Parties' Risk Into a Competitive Advantage?* 13.

[22] EY, *Global Financial Services Third-Party Risk Management Survey*, 25.

[23] Jaclyn Jaeger, "Survey: Trials, Tribulations of Third-Party Risk Management."