Audit Committee Excellence Series

Oversight of third-party risks

February 2016

PwC's Audit Committee Excellence Series (ACES) provides practical and actionable insights, perspectives, and ideas to help audit committees maximize committee performance.

pwc

This ACES module discusses important aspects of third-party risk mitigation oversight and the critical role audit committees play:

1. Why understanding third-party risks is critical to audit committees
2. What is so special about third-party risks
3. Getting your arms around third-party risks
4. Evaluating the company's existing standards for conducting business and contracting with outsiders
5. Long-standing relationships can bring particular challenges
6. Third-party security risks deserve special attention
7. It's a never-ending process

Appendix – Third-party risk management tool

1. Why understanding third-party risks is critical to audit committees

Today's companies are increasingly integrated with their suppliers, distributors, and other providers. Consider that third parties provide so much leverage to today's companies that as a group, 89 of the Fortune 500 average over 100,000 suppliers each – that's over 9 million total direct supplier relationships. With this leverage comes risk; companies are exposed to risk related to the actions of their third-party providers. And because of this highly-integrated world, many people don't differentiate one provider to the "value chain" from any other, but instead perceive all relevant contributors to be part of a single solution provided by the company. Consequently, they may hold the primary sponsor of the solution accountable, with no acknowledgement of the "value chain" of providers. This increases the risk that third-party providers can damage the brand of your company and create liability.

In addition to brand reputational risk are other compliance and regulatory risks. In other words, a problem created by a third-party in your "value chain" can bring a company to its knees. Areas fraught with potential issues include labor law violations, health and safety, environmental, pirated intellectual property (IP) and software, labor law compliance, and royalty payments, among others. Additionally, many third parties have access to the company's network, inviting the potential for cyber breaches and privacy violations.

The UK Bribery Act and the Foreign Corrupt Practices Act (FCPA) are examples of regulations that may be of particular concern for companies using agents, resellers, and distributors. The SEC and the Department of Justice (DOJ) have held companies liable for the acts of these types of third parties. In 2012, every bribery case prosecuted by the DOJ involved a third party. Regulators often look at a company's liability based on actual knowledge or *willful blindness* – meaning they consider whether the company has intentionally kept itself unaware of actions by the agent, reseller, or distributor to avoid liability. Unfortunately for many companies, arguing that a third-party is at fault hasn't been successful, because they could not demonstrate sufficient internal controls designed to monitor third parties.

Other regulators have also weighed-in on the consequence of actions of third parties. In 2013, the Office of the Comptroller of the Currency (OCC) gave guidance to banks for assessing and managing risks associated with these relationships. The guidance made it clear that the use of third parties does not diminish the responsibility of a bank's board of directors and senior management to ensure that the activity is performed in compliance with applicable laws.

Many boards assign coordination of risk oversight to the audit committee, since it is normally responsible for financial reporting compliance and the related internal control structures. Also, because the audit committee likely oversees the company's internal audit function, and internal audits may address the oversight of third-party risks, it is often put in the audit committee's court.

This edition of ACES focuses on the critical role of audit committees in overseeing the inevitable risks of dealing with third parties.

2. What is so special about third-party risks

Third-party risks relate to areas such as bribery, the environment, software piracy, health and safety, and labor laws, and may not be fully addressed by conventional internal controls or enterprise risk assessment processes. These risks are sometimes addressed by the full board, but often times audit committees are tasked with the assessment.

Another attribute of third-party risks is that the reputational and other risks they create all have one common denominator – they are governed and controlled by a legal contract entered into with the third party that establish the obligations, rights, and recourse of the company and its third-party providers.

Because these third-party risks are not typically covered by companies' existing risk assessment processes, the controls designed to mitigate these risks should be viewed as part of a discrete subcomponent of the company's overall internal control structure. Generally speaking, the necessary controls for monitoring third-parties are ubiquitously applicable, regardless of what type of risk is being mitigated or whether the third-party is a supplier, infrastructure provider, or distributor. Companies can design a comprehensive internal control system that covers all significant third-party relationships. Because these relationships are governed by a contract, it is particularly important to include the company's general counsel as an integral part of that process.

Audit committee role considerations

- *Understand how many significant third-party relationships the company has and the nature of those relationships.*

- *Evaluate how audit committee oversight should consider these controls over third-party risks in aggregate to ensure a comprehensive process.*

- *Evaluate whether company counsel is sufficiently engaged in the third-party risk control environment. And whether they comprehend the importance of their role.*

The company's general counsel needs to be an integral part of the process.

3. Getting your arms around third-party risks

It would be difficult to name a company that doesn't have some risks in a relationship with a third party, whether that party is a business partner, supplier, distributor, contractor, service provider, or has some other relationship with the company. Essentially, any organization that has access to your company's IP or corporate network, provides IT infrastructure to the company, or is otherwise a participant in the company's "value chain," creates a third-party risk that needs to be managed in some way. It's important to embed management of third-party risks in a company's overall risk management program.

There are special challenges that differentiate overseeing third-party risks from other risks. Consider that many companies don't have an inventory of their third-party relationships. The relationships may have been developed at an operating unit or plant level and bypass any company controls that may exist. Or the company may lack policies and procedures for creating and monitoring third-party relationships. Controls cannot be effective if the list of third parties isn't complete and accurate.

To further complicate the matter, many third parties have their own third-party relationships that provide services to them – making those other parties a second-tier third party to the company. It can be important for the company to understand how its first-tier third parties manage the risks to the company presented by the second-tier third parties.

Moreover, third parties may be located overseas with different laws, practices, and business ethics. Other relationships might be long-term and/or sole-sourced, increasing the complexity of bringing definition and risk mitigation to the relationship (e.g., supplier relationships).

The Appendix hereto provides an example of an effective third-party risk management tool to:

- inventory third-party relationships,
- prioritize those that are most significant,
- assign a risk rating to each type of risk and an overall risk rating for each third party,
- identify management responsible for managing the risk,
- map risk oversight for each relationship to the board or its committee, and
- address the frequency of reporting updates about each relationship to the board.

4. Evaluating the company's existing standards for conducting business and contracting with outsiders

A standard, comprehensive practice for managing third-party risks could help the company mitigate these risks and facilitate audit committee oversight. Directors may want to understand the company's approach relative to the following best practices, both before and after contracts are finalized.

Upfront procedures

Due diligence on reputation and capabilities – A formal due diligence process is important for companies that routinely work with third parties. In its simplest form, due diligence might include searching databases and reviewing media coverage and internet sites for information about a company's reputation and capabilities. More robust due diligence could include using questionnaires to learn about compliance practices and the use of second-tier third parties, obtaining information about relationships with government officials and organizations, conducting site visits, and might even include asking for evidence of licenses for any IP the third party uses in its processes, such as software. The amount of due diligence performed on a potential third-party relationship should be based on the level of risk the party creates for the company.

Proper reporting lines for third-party compliance program from a governance standpoint – Identifying who at the company "owns" the third-party management function is important. The executive owner needs to have appropriate autonomy, authority, and resources, access to the chief executive, and access to the audit committee (or another committee if board oversight is assigned elsewhere).

Adequate contracts and policies, including protection of IP, training of their employees, and rights to audit – Relationships with third parties are generally governed by a contract. The contract should define specific terms of delivery and quality, how the party will protect the company's IP, how employees will be trained in protecting the IP, and also anti-corruption matters for employees. The company should have the right to audit compliance with these criteria and its general counsel needs to understand the importance of these types of contract provisions.

Right to terminate the relationship for violations of the agreement – Typically, a company will have the right to terminate a contract with a partner for a breach of the contract terms. With a robust third-party contract the company would have the right to terminate for noncompliance with specific metrics. These may include not only delivery and quality metrics, but also early-warning metrics on issues that could lead to reputation or brand damage. For example: labor or human rights violations; running a "third shift" to manufacture lower-quality branded goods; or leaking IP to an outside party that could undermine the company's market.

Extend employee hotlines – Create a mechanism to allow employees at key third parties access to the company's whistleblower reporting hotlines. This could give the company an early-warning about a cultural weakness at a third party that needs to be addressed. It might also be a factor in deciding when a site visit is needed, or might impact the timing for its next compliance audit.

Ongoing procedures

Audit and monitor high-risk parties – "High-risk parties" might be defined in different ways depending on the company. It could be based on the dollar value of the relationship, how important the relationship is to the company, the location of the party (if it is in a high-fraud risk location), the nature of the company's IP the third party has access to, or some other measures. Defined high-risk parties should be subject to continuous monitoring.

Obtain periodic representations of compliance – Depending on the company's assessment of the risk associated with third parties, it could require third parties to periodically submit representations of compliance. The representation could be based on an audit the third party conducts on itself (possibly by its internal audit function) or for which it engages an outside party to conduct, or could simply be a warranty by the third party that no violations of IP or corruption of laws have occurred. The company's decision on which approach works for any given third party should be based on the level of risk the third party presents to the company.

Exercise the right to audit with a documented process – Inasmuch as the company might have a contractual right to audit a third party, actually taking advantage of that right is also important. The internal audit department could conduct the audit, or it could be outsourced to a third party such as an audit firm. Exercising the right to audit sends a clear message to the third party about how seriously the company takes compliance with contractual terms. They can even be a source of revenue recovery in royalty audits, which ensures the company is getting paid its share of relevant sales.

Conducting audits could aid the company if the third party is ever charged with wrongdoing, which may include violation of the FCPA, by demonstrating that the corruption occurred despite reasonable efforts by the company to monitor the behaviors of the third party. If there is an enforcement action against a third party, the government/regulator may have expected the company to perform audits of various third parties, and a company's failure to do so could suggest an inadequate monitoring process.

Monitor metrics and reporting – For each third-party agreement, meaningful metrics need to be identified and reported to the company on a regular basis. The specific metrics to be monitored will depend on the nature of the relationship between the company and each third party, as there is no "one-size-fits-all" formula.

To have an effective control environment, companies need to follow-up on reports not submitted timely, review reported metrics for anomalies, exercise its right to audit, and maintain on-going communication with the third party.

Audit committee role considerations

- *Assess whether the executive that "owns" the third-party risk oversight program has appropriate standing and visibility in the company to maximize the potential for effectiveness. Evaluate management's tone and attitude toward compliance.*

- *Assess whether the company's due diligence process is appropriate to identify the risks potential third*

parties might pose to the company, and how the company plans to mitigate and monitor those risks if it moves forward with the relationship.

- *Understand the company's activities regarding third-party relationships in high-corruption risk locations and industries. Discuss if, and why, the company is using "middle men" in corruption hot spots.*

- *Inquire whether the company exercises rights to audit, rights to terminate, and adequately monitors compliance on an ongoing basis.*

- *Understand how management identifies the metrics and reporting protocols for third-party relationships. Discuss management's process for review and follow-up on the reports.*

- *Understand the role of internal audit (or audit firm engaged) that will perform audits of significant third parties with respect to third-party risks as well as fraud prevention and detection. Consider the use of fraud monitoring software tools on outsiders.*

5. Long-standing relationships can bring particular challenges

For many companies, relationships with some suppliers have a long history. It's likely these relationships don't come with the formality that newer relationships may have. In addition, they may have evergreen provisions or may not automatically renew. Twenty years ago, there may have been less of a focus on monitoring third-party behaviors, so companies should question whether the existing contracts with these third parties meet the standards needed in the current environment. That said, transitioning a long-time business partner or supplier to a new structure needs to be managed carefully.

One approach that has been found effective is a roll-out of a comprehensive third-party relationship management program to all new and existing third-party relationships. This may be best done based on a "threats and safeguards" perspective, focusing first on those third parties located in a country with significant risk of corruption or other concerns. Rating each third party based on risk factors, including its location, interaction with government officials, and the volume of sales or fees paid helps set priorities about where the company needs to focus its efforts. Third parties representing the highest risk should be subject to the most extensive due diligence. Lower-risk third parties may warrant a less rigorous review.

6. Third-party security risks deserve special attention

Many third-party providers have access to sensitive information on the company's network. These parties may include suppliers and those responsible for credit card and payroll processing and data hosting. And the legal liabilities for third-party cyber breaches continue to increase, including those assessed by state law, the Federal Trade Commission, and HIPAA. The same considerations mentioned for other third-party risks apply to these cyber risks, with a particular focus on high-risk parties and an emphasis on the need for effective ongoing monitoring.

Of course, vendors need to fulfill certain security requirements before allowing access, but technology changes every day and so does the sophistication of cyber attackers. A one-time assessment of a third-party's cybersecurity may not be relevant for very long. Certainly an initial evaluation is important, but communicating the company's ongoing security expectations is critical in this evolving environment. And metrics should be established, monitored, and revised as necessary to determine if the third party's cyber program maintains compliance with required controls. It is not uncommon for companies, including the third parties, to curb spending on the latest bug fixes, upgrades, and enhancements to their software programs, which increases the opportunity for a potential breach.

Directors may also be interested in the company's attention toward limiting the amount of data that outside providers can access to only that which is necessary. And third parties should be contractually obligated to alert the company to a breach and to accommodate security audits.

Audit committee role considerations

- *Inquire if the company knows what critical data third parties have access to and whether data access is confined to only necessary information.*

- *Ask about vendors who support the company's IT infrastructure and how they are monitored.*

- *Inquire if contracts provide for rights to security audits and breach notification.*

- *Evaluate if the company has an ongoing process to monitor compliance with contractual cybersecurity mandates.*

7. It's a never-ending process

It's important that third-party relationships be periodically reviewed. As new relationships are made and existing relationships change, updates will need to be made to the third-party risk management program to reflect these changes. As the company's IP expands with new products, or new technologies are adopted, third-party relationships will inevitably be created. Also, if the company goes through a merger or acquisition, significant changes to the program may need to be made.

Audit committee role considerations

- *Understand management's plans to continually update and periodically renew the third-party controls to ensure its completeness and appropriateness.*

- *Consider the impact of any changes to the company's operating environment, and how these changes may impact its third-party relationships.*

A one-time assessment of a third-party's cybersecurity may not be relevant for very long.

Appendix

Sample of a Risk Assessment Matrix to catalog and assess third-party relationships

Third-party provider[1]	Risk Rating (assess a risk score from 1 to 5)						Overall Rating	Management Responsibility	Board Oversight	Frequency of Review[2]
	Bribery	Revenue	Cyber	Environmental	Piracy	Other				
Supplier	X	X	X	X	X		X	Internal Audit	Full Board	Annually
Distributor	X	X	X	X	X		X	CFO	Audit Com.	Quarterly
Cloud provider	X	X	X	X	X		X	CCO	Audit Com.	Quarterly
Reseller	X	X	X	X	X		X	CISO	Audit Com.	Annually
Agent	X	X	X	X	X		X	Business Unit	Full Board	Annually
(continue for all third-party providers)										

[1]Third-party providers should be presented in order of significance
[2]Represents frequency of reporting to board members responsible for oversight

How PwC can help

To have a deeper discussion about how this topic might impact your business, please contact your engagement partner or a member of PwC's Governance Insights Center.

Paula Loop
Leader, Governance Insights Center
(646) 471 1881
paula.loop@pwc.com

Catherine Bromilow
Partner, Governance Insights Center
(973) 236 4120
catherine.bromilow@pwc.com

Don Keller
Partner, Governance Insights Center
(512) 695 4468
don.keller@pwc.com

Terry Ward
Partner, Governance Insights Center
(651) 261 3763
terrence.j.ward@pwc.com

Paul DeNicola
Managing Director, Governance Insights Center
(646) 471 8897
paul.denicola@pwc.com

Other "Audit Committee Excellence Series" topics include:

- The audit committee's role in deterring fraud (December 2015)
- Dealing with investigations (June 2015)
- Role, composition, and performance (May 2015)
- Overseeing accounting changes—including the new revenue recognition standard (February 2015)
- Overseeing external auditors (September 2014)
- Overseeing internal audit (July 2014)
- Financial reporting oversight (May 2014)
- Assessing the company's forward-looking guidance practices and the potential risks of consensus estimates (March 2014)

Find more information at www.pwc.com/us/GovernanceInsightsCenter

Download our mobile app at http://pwc.to/Get365

pwc.com