Central Audit Committee Network

November 2018

CACN

SUMMARY of THEMES

Third-party risk, the proxy season, and workplace conduct

Members of the Central Audit Committee Network (CACN) met in Chicago on October 17, 2018, to discuss the board's oversight of third-party risk, insights from the recent proxy season, and how the board should handle issues of workplace culture and conduct in the #MeToo era.

Third-party risk

Companies now depend on third parties in almost every segment of their business. The challenge of overseeing these relationships, which can number in the thousands, is becoming acute. Information technology (IT) risks such as cyberattacks, privacy breaches, failures by cloud providers or other IT vendors, and failures in key vendors' IT systems topped the list of member concerns. Other key issues included financial and operational risk in critical suppliers, risks raised by relationships with international partners, and the reputational risks posed by distributors, sales agents, and others who represent an organization to its customers.

CACN members were joined in Chicago by Matthew Gopin, vice president of IT governance, risk, and compliance at Walgreens Boots Alliance; Jim Lentino, senior vice president and chief risk officer at Wintrust Financial; and David Shade, a partner in EY's Advisory Services practice. Together, they discussed the board's oversight of third-party risk management.

Getting the basics right remains a challenge.

Even for large organizations with relatively robust third-party risk management programs, basic aspects of vendor management can be difficult to execute—for example, maintaining a comprehensive list of vendors and identifying which are most important or pose the greatest risks. Mr. Gopin said that organizations *"have to start with the basics of the critical processes for your business, then identify third parties that support them."* Determining who within an organization is accountable for managing key third-party relationships, especially when a major vendor has multiple points of connection to the organization, can also be a challenge, as can cataloguing and identifying the terms of an organization's many third-party contracts.

Responsibility must be allocated across the organization

Members and guests agreed that individual business units need to take responsibility for third-party risk and noted the importance of infusing a culture of risk management throughout the organization. Mr. Shade said it is crucial to establish *"a culture and tone at the top that says you can outsource the function but not the responsibility. If people get that, you are going in*

the right direction." Mr. Gopin reminded members of a fundamental fact: *"The end user is the front line."*

Creating a culture of risk oversight requires establishing common risk-management procedures and frameworks, ensuring that businesses do not circumvent vendor management policies, and providing for appropriate escalation of risks. Mr. Lentino said, *"We sit down with the businesses and ask them to think about their risks. We push ownership down and give them the framework to think about their risks and ask, what are the controls?"* He added, *"If a particular contract negotiation requires an exception to our vendor policy, we use a risk-based escalation process to ensure the decision to accept the risk is held at the right level."*

The audit function plays an important role in providing an enterprise-wide view of third-party risks, whether or not an organization has adopted a formal "three lines of defense" model. Mr. Shade said, *"Internal audit absolutely needs to be part of the process. It makes sure processes, procedures, and the overall program are operating the way they should be. There are a lot of overlaps within the organization—IT, legal, finance, procurement. Internal audit can look across the organization and give perspective on how the program is operating holistically."*

Third-party relationships evolve with changing risks

Third-party risk management is a dynamic process that requires continuous monitoring of relationships. Vendor contracts, especially long-term agreements, need to be able to adapt to changes in the risk landscape. One member said, *"Take [the General Data Protection Regulation]—it's only been on the radar the last two to three years. It may not have been contemplated in contracts we have. In a world of [artificial intelligence], other things are going to come up. How do you put in place the oversight and management processes to enable ongoing evolution?"*

Mr. Gopin said that one approach is to put language in contracts that requires vendors *"to have general best practices and keep up with standards as they change."* Mr. Lentino said contracts should include a commitment to good governance and controls, or *"performance measures that say, If you fail to meet these standards that we have a right to terminate our contract or otherwise seek compensation."* Others said long-term or "evergreen" contracts that renew automatically require special attention.

Members and guests also commented on the importance of considering third-party relationships in business continuity and crisis management planning.

Critical questions for boards to ask about third-party risk management

Members and guests identified questions that boards can ask management regarding third-party risk management:

- Do you have a comprehensive inventory of all vendors?
- Are third parties tiered or ranked by level of importance and level of risk?
- For each critical vendor, do you know who is accountable for managing the relationship?
- What is the framework or process for managing each critical vendor? Is proper governance in place to maintain the process?
- Do you know where your contracts are housed and what their terms are?
- Do you have a risk acceptance process? Do you have the ability to escalate those risks and evaluate them? Is there a place to keep track of the risks you've accepted?
- For significant relationships, what is the exit strategy or contingency plan?

Proxy season review

Kellie Huennekens, associate director of EY's Center for Board Matters, joined CACN members for a discussion on trends emerging from this year's proxy season.

- **Institutional investors and other stakeholders seek a greater voice.** Large institutional investors have become more vocal through both proxy voting and direct engagement. Employees, nongovernment organizations, and other stakeholders are also increasingly active. For example, Ms. Huennekens noted that a large tech company faced strong criticism from employees when it opposed a shareholder proposal requesting that women and minority candidates be considered for future board seats. The board reversed course and said it would adopt such a policy.

  Ownership concentration in public companies continues to reshape the governance landscape. With the shift from retail to institutional investment and the increasing prominence of "active passives"—passive funds that are vocal on governance issues—a few large players, such as BlackRock, State Street, and Vanguard, wield significant influence on governance issues. Engagement conversations between investors and companies and their boards remains high and continues to grow. These conversations often take place behind the scenes, and some members noted that some governance organizations are overwhelmed with engagement requests.

- **Investment managers continue to drive environmental, social, and governance issues onto board agendas**. Ms. Huennekens noted that proxy season *"started off with a bang"* when BlackRock CEO Larry Fink's annual letter to CEOs put issues of social purpose on the table. The letter received wide attention although these matters may remain lower priorities for some boards. Ms. Huennekens also acknowledged the consensus around the importance of board diversity—of skills, gender, ethnicity, age, and tenure—not simply for reasons of equity, but also because research suggests that diverse boards function better and make better decisions. Board gender diversity is a particular focus.
- **Disclosure expectations continue to increase**. Investors, the Securities and Exchange Commission, and other stakeholders are looking for more disclosure related to the activities of the audit committee and the board's oversight of cybersecurity risks and policies. Ms. Huennekens noted that since 2012, voluntary disclosure of matters related to the audit committee—such as key focus areas and auditor tenure—have increased dramatically. Investors also seek more information on succession plans. Members commented on the sensitive nature of this information and the time boards spend on talent, including deep dives on leadership development, several levels into organizational hierarchies.

The board's oversight of workplace conduct

Over dinner, members discussed the issue of workplace sexual misconduct with Tina Tchen, a partner at Buckley Sandler and leader of its Workplace Cultural Compliance Practice.

- **Thirty years of attention have not solved the problem.** Since 1986, sexual harassment in the workplace has been deemed illegal under Title VII of the Civil Rights Act of 1964. Firms have spent significant time and resource training employees, executives, and even boards. Yet, as Ms. Tchen pointed out, recent high-profile instances of sexual misconduct and the growth of the #MeToo movement confirm that there is a long way to go before workplace environments are widely experienced as safe for everyone.
- **Ending sexual harassment is inseparable from diversity and inclusion.** Companies will not be able to make headway on eradicating sexual harassment and misconduct without making progress on diversity and inclusion. Ms. Tchen said, *"We need to look at this holistically. Our mistake is siloing diversity and inclusion from harassment. If you increase diversity, organizations make better decisions and create better workplace cultures. You have to solve both problems together."* It is a mistake, she insisted, to treat sexual harassment as *"a cost to be limited,"* by settling claims on a case-by-case basis rather than looking for patterns that may indicate deeper problems with organizational culture.
- **Organizations need to move from compliance to culture**. Many behaviors that leaders see as undesirable are not in themselves illegal—for example, bullying that does not discriminate by sex. Cultures often need to be reformed. Ms. Tchen said, *"All companies*

have sexual harassment policies, and training is based on that. It's legal compliance training, not culture training. There is a lot of behavior that is legal, but it is also toxic." In particular, those who experience or witness harassment need to be encouraged to come forward, and organizations need to establish reporting and nonretaliation policies and procedures to protect them. Ms. Tchen noted that three-fourths of those who are subject to sexual harassment in the workplace do not report it, and of those who do, three-fourths are subject to retaliation.[1]

- **Sharply reducing contact between men and women is a step backward**. Members feared that further exclusion of women could be a negative unintended consequence of efforts to combat sexual harassment. One member said, *"I think about the male mentors I've had. It's impossible to have that if men and women can't meet privately. If men step back, we will go backwards."* Another member said, *"I was not just mentored, but sponsored. Without that, women won't get the special project, line job, or promotion to get them to the C-suite."* Members also noted that zero tolerance policies can leave executives and boards with little room for maneuver in cases where mitigating circumstances exist.

About this document

The Central Audit Committee Network is a select group of audit committee chairs from leading 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.

Summary of Themes 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 *Summary of Themes* lies in its power to help all constituencies develop their own informed points of view on these important issues. Those who receive *Summary of Themes* 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.

Endnotes

[1] The study Ms. Tchen noted can be found here: Tara Golshan, "Study Finds 75 Percent of Workplace Harassment Victims Experienced Retaliation When They Spoke Up," *Vox,* October 15, 2017.

Meeting participants

- Howard Carver, Assurant
- Dick Gabrys, TriMas
- Marla Gottschalk, Big Lots
- Mike Hanley, BorgWarner
- Harry Harczak, Tech Data
- Sandy Helton, Principal Financial
- John Holland, Cooper Tire
- Mike Merriman, Regis
- Sherry Smith, Deere & Company
- Ingrid Stafford, Wintrust Financial
- Steve Strobel, Newell Brands
- Phoebe Wood, Invesco
- Donna Zarcone, CDW

EY was represented by the following:

- Julie Boland, Vice Chair and Central Region Managing Partner
- Rich Bonahoom, Partner, Business Development Leader, Central Region