Central Audit Committee Network

October 2019

CACN

SUMMARY of THEMES

Oversight of internal audit and data privacy; pros and cons of being a listed firm

Audit chairs are eager to learn about strategies for supporting their evolving internal audit organizations. They also seek effective approaches to overseeing data management and the regulatory and reputational aspects of data privacy. Central Audit Committee Network (CACN) members met on October 10 in Chicago to discuss these issues as well as the dynamics surrounding the decline in the number of public companies in the United States.

Evolving internal audit roles

Members were joined by Lisa Hartkopf, Partner, Americas Internal Audit Leader, EY and Troy Kelly, Chief Audit Executive, Walgreens Boots Alliance (WBA) to discuss how boards work with internal audit. Key themes included the following:

- **Companies seek to balance assurance and advisory functions.** Regulatory pressure, technological developments, and shifts in the risk environment have led to a wider scope for internal audit and new capabilities, including advisory skills. *"The disruption is real,"* Ms. Hartkopf said, *"and we need to look holistically at new risks."* Rather than viewing assurance and advisory as separate, Ms. Hartkopf described *"a spectrum of assurance."* At one end is a focus on *"historical data looking at policy, helping the business understand what's not working."* At the other end is *"proactive assurance—a seat at the table to share in real time a view on risk and controls."* One member referred to these as *"detective"* and *"preventive"* aspects of assurance, and several members agreed that engaging internal audit early in new projects has benefits.

  Firms have different approaches to balancing internal audit's assurance and advising roles. WBA focuses on assurance, said Mr. Kelly. *"We cover all appropriate procedures, test compliance, identify risks and controls … find the chinks in the armor."* He noted, *"Some internal audit organizations have an entirely different group of folks within internal audit who have the advisory role.* One member's company limits consultative activity to 20% of internal audit hours; this member noted that thus far, the function has *"not yet come close."* By contrast, another firm has the same target limit and is fast approaching it.

- **Coordination and cooperation with other functions is key.** Several members said that internal audit took the lead in coordinating enterprise risk management (ERM) in order to generate a cohesive view of risk across the organization. *"Internal audit works with the chief risk officer … there are a lot of synergies,"* said one. Ms. Hartkopf confirmed a trend

toward collaboration between Internal audit and compliance on ERM. She noted that her clients who managed risk most successfully look at it *"holistically across the organization and focus on risks related to the strategy. The ones who are further along are those with a chief risk officer or distinct management committee looking across all the risks of the business."*

- **Forge strong relationships with the audit committee and management.** Mr. Kelly stressed the importance of clear governance structure and lines of reporting, which can promote candor and preserve the independence of internal audit. *"Some constantly struggle with 'who is my boss?' but my CFO tells me every day: 'That's between you and the audit committee chair.'"* Mr. Kelly supports his directors in *"building relationships across the business."* Ms. Hartkopf said that success comes down to the *"brand of internal audit within the organization and the culture around controls. If those are positive, it's easier to have a dotted line to management and a straight line to the audit committee chair."*
- **Cosourcing and outsourcing can enhance internal audit**. CACN members agreed that cosourcing and outsourcing models allow companies to access cutting-edge information technology (IT) skills and foreign-language or other geographic expertise that they might not be able to afford to keep on staff. Some organizations, Ms. Hartkopf explained, decide to have the in-house function *"be the rotation piece and have the cosource provider be the continuity … Others say, 'We'll outsource [to start] and then cosource or shift to in-house as we move along the journey.'"* Mr. Kelly said that at WBA he has tried to build a culture in which cosourced providers are fully integrated with the in-house internal audit team.

Managing data and protecting privacy

Companies face significant challenges in balancing opportunities to capitalize on vast quantities of data with the legal and reputational consequences of misusing it. Members discussed these and related challenges with Sheila Colclasure, Senior Vice President, Information Policy Leadership, Interpublic Group; Scott Margolis, Managing Director of Americas data privacy and protection at EY; and Kelly Welsh, President of the Civic Committee and of the Commercial Club of Chicago.

A challenging privacy landscape

In the absence of federal data-protection legislation in the United States, and as states explore legislation of their own, there is potential for confusion and conflict. Even when firms are fully compliant with applicable laws and regulations, they must be sensitive to consumers' perceptions of the ways they are using data. The reputational stakes are high.

- **New and emerging privacy laws create uncertainty and risk.** The combination of the European Union's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and potential additional state and federal privacy laws is creating considerable uncertainty. Mr. Margolis noted that the relative *"lack of broad-scale*

enforcement" of GDPR thus far is surprising, but he said that the data protection authorities are still gearing up, and some companies *"will have significant actions taken against them."* Ms. Colclasure warned of potential conflicts among legal requirements. *"Next year we're going to have a very challenging state legislative situation and may get our knees cut out from under us at the state level; about 23 states are looking at CCPA-like regulations … In the digital era, where everything is driven with data, how will corporations survive if our technology and processing capabilities have to be bespoke on a state-by-state basis?"* Members and guests agreed that federal privacy legislation is unlikely in the next two years, despite growing support. Ms. Colclasure argued that business leaders *"must collaborate to support a federal privacy vehicle of some sort."*

In addition to enforcement actions, Ms. Colclasure warned of class-action lawsuits. One member agreed: *"Nothing right now will stop the momentum of massive litigation. This could be something like asbestos litigation; it could be going on for years."*

- **Reputational risk remains a key consideration.** Privacy is about much more than just compliance: there are thorny reputational issues to consider as well. Even explicit consent from customers and employees to use data in a manner fully compliant with regulations is not always sufficient. Furthermore, it can be difficult for firms to anticipate public perception of any new or unusual use of data.

Companies' responses to the challenges and opportunities

Firms are grappling with questions about what and how much data they need, how to manage and protect the data they have, and how to organize oversight of both data use and privacy.

- **Principles like privacy by design can help companies strike a balance.** Responding to both regulatory and reputational concerns, some companies build privacy into new products or services from the outset. Ms. Colclasure stressed the need to *"build privacy into each job role, to create a culture of accountability".* Mr. Margolis added, *"You need to ask whether you're acquiring the right data and keeping the right amount. Part of privacy by design is data minimization up front."*

- **Data governance requires major updates to systems, processes, and policies**. The new privacy environment means that data will, increasingly, need a verifiable provenance, a well-articulated purpose, and policies not only for access but also for retention. One member remarked, *"I feel like we're going to be replumbing our data, as we did with Sarbanes-Oxley."* Both guests emphatically agreed. Mr. Margolis dubbed *"know thy data"* the *"11th commandment,"* while Ms. Colclasure said, *"There will be more data, we will want more data, we will use more data, and so yes, this is the time you have to replumb. You need your data under control: its ingress, egress, classification, and use."* Mr. Margolis advised, *"If you don't need the data anymore, it's a bigger exposure point than it's worth. If you keep it, anonymize it."* Ms. Colclasure said, *"If you have no purpose for it, don't keep it.*

If you can articulate how you're ethically innovating—and you have guardrails—then keep it."

- **Structures and processes for privacy oversight are evolving.** Firms are still working out how to structure privacy oversight. Given the growing importance of the issue, cross-function collaboration is critical to success. A lot depends on a company's size and its risk profile. Not every firm needs a chief privacy officer (CPO), but all companies need to think about how functions like IT, compliance, risk, legal, and human resources engage with one another on these issues. Mr. Margolis said that the role of chief data officer (CDO) is emerging: *"Sometimes we now have the CIO [chief information officer] running operations, and the CISO [chief information security officer] is part of the risk organization, which provides a counterbalance. But if there's a tie, who will break it? The CDO now has stewardship of the data and represents the business, but sometimes the consumer."* Mr. Margolis added, *"The CPO often sits in the CIO organization, under the CISO. But the right place is really outside of IT."*

- **Privacy is becoming a focus for boards**, **but board engagement varies considerably**. At some companies, privacy is now a regular item on board or audit committee agendas. For others, it is just starting to receive board-level attention, and on some, it remains exclusively a legal and compliance issue. While many members felt that privacy deserves more discussion at their board meetings, one member reported, *"It pervades our board discussions. It's the whole board. The company embarked on a digital transformation of its business a few years ago, and now data privacy is a huge part of it."*

  Ms. Colclasure and Mr. Margolis offered a to-do list to boards:

  - **Gauge security threats.** Ms. Colclasure said, *"Security first. If you're not measuring and reacting to the perpetual security threats, that's a problem."*
  - **Train.** Mr. Margolis quoted the head of a regulator in charge of data protection who said, *"There are just three things I want you to do: train, train, train. The IT and risk organizations have to know their responsibilities."*
  - **Develop data governance reporting metrics.** Ms. Colclasure noted, *"For a corporation to be accountable, the board has to have metrics so it can review the program; there has to be a measurement of the different components of the program and metrics and measurement must be reported at every board meeting."*
  - **Let business needs drive technology purchases.** Mr. Margolis advised members, *"Don't authorize your organizations to go buy tools. If you don't have the appropriate processes in place, all the tool will do is let the organization do bad things faster. The process should define business requirements for what we're trying to do. THEN you can look into new technology."*

- **Obtain insurance.** Ms. Colclasure stated, *"You need GDPR and CCPA insurance. It's costly, but you need it."*

Public vs. private: the pros and cons of being a listed firm

Members discussed historical and contemporary factors contributing to the secular decline in the number of public companies, focusing particularly on more recent forces making it difficult to be a public company and more attractive to be a private one, such as investor pressures, the widespread availability of private capital, and the cost of regulatory compliance. Members suggested that different firms are suited to different ownership structures and contrasted the flexibility of private firms with the discipline imposed by the public markets.

Many were of the opinion that the downward trend in the number of public companies could lead to a segmented, inefficient market, further shut out retail investors, and increase overall risk, but others shared examples to illustrate that, under some circumstances, the flexibility of private firms can lead to better performance.

Meeting participants

- Kapila Anand, Elanco Animal Health
- Anne Arvia, GATX
- Howard Carver, Assurant
- Cheryl Francis, Morningstar
- Dick Gabrys, TriMas
- Mike Hanley, BorgWarner
- Sandy Helton, Principal Financial Group
- Frank Jaehnert, Nordson
- Neil Novich, Hillenbrand
- Al Smith, Simon Property Group
- Ingrid Stafford, Wintrust Financial
- Pam Strobel, Illinois Tool Works
- Michael Todman, Brown-Forman
- Phoebe Wood, Invesco
- Ray Young, International Paper

EY was represented by the following:

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