Southeast Audit Committee Network

June 2019

SEACN

SUMMARY of THEMES

IT risk and resiliency, critical audit matters, restatement and material weakness trends, and special investigations

Southeast Audit Committee Network (SEACN) members met in Atlanta on May 30, 2019, for discussions on board oversight of IT risk and resiliency, critical audit matters, restatement and material weakness trends, and special investigations. This *Summary of Themes* synthesizes those discussions.[1] *For a list of meeting participants, please see page 8.*

Audit committees and auditors are learning from CAMs dry runs

Chuck Carver, EY Partner and Southeast Region Professional Practice Director, joined members to discuss critical audit matters (CAMs), the new auditor reporting standard issued by the Public Company Accounting Oversight Board (PCAOB) in 2017. Mr. Carver said that the new standard was intended to shed light on *"the critical matters the auditor went through during the audit"* in order to provide investors with more information from the auditor. This new section of the auditor's report is not expected to change the audit itself and it is not intended to be a list of key business risks. According to Mr. Carver, the new standard is prompting auditors to revisit their reporting to the audit committee to ensure that they are prioritizing the most challenging issues and highlighting them for the audit committee.

The discussion highlighted the following:

- **A limited number of CAMs.** Though Mr. Carver noted that some auditors are *"struggling to come up with one,"* he said that having no CAMs would be rare. There is an expectation that companies will have at least one CAM and that, on average, auditors are coming up with two to three CAMs for most companies. The most common CAMs were in the areas of income taxes, revenue recognition, and goodwill or intangible asset impairment.
- **Additional guidance.** Mr. Carver noted that identifying CAMs remains a work in progress as the deadline looms for large filers with fiscal year-ends on June 30, 2019 or later. More guidance could come from the PCAOB or CAQ; Mr. Carver recommended that audit committees discuss with the auditor newly issued regulatory guidance and emerging trends related to CAMs to make sure there is proactive discussion before the filing deadline.

- **Sensitivities around new disclosures.** Members predicted that their General Counsel and Investor Relations teams will be actively and increasingly involved with key messaging around CAMs. Some members questioned whether it was safer to identify more in the first year or fewer, and expressed concern about setting unintended precedents: specifically that, once an issue is identified as a CAM, it may be difficult to remove that item from the CAMs disclosure, with the result that the quantity will only increase over time. Mr. Carver advised flexibility, saying, *"We take a lot of the complexity in accounting as routine, but to an investor it might seem significant…some of the more routine areas might get added."* While the average this year is expected to be around two per company, he advised, *"Don't get locked into having two CAMs."*

Restatements and material weaknesses may be increasing

Mr. Carver spoke briefly about a perceived increase in restatements and material weaknesses recently identified. The most common areas of concern related to income taxes, revenue recognition, business combinations and/or significant unusual transactions. There were few clear trends, according to Mr. Carver, who said they were *"facts and circumstances-based"*, and mostly *"one-offs across the board."* He also noted that while they were seeing an increase, it did not represent *"hundreds of restatements."* Mr. Carver said that the complexity of changes and new standards in recent years meant that audit committees should be attuned to any new issues coming up and have the right resources and expertise involved in reviewing controls.

IT risk & resilience are increasingly board issues

> *"All companies are becoming tech companies. We may be distributing different things but we're all tech."* – SEACN member

Members were joined in a wide-ranging discussion of the risks related to major IT transformation by Dave Dowsett, Global Head of Technology Strategy, Digital Transformation, Emerging Technology and AI at Invesco, and Beth Ross, Principal in the Advisory Practice at EY. Virtually all SEACN members' companies are investing significantly in efforts to leverage technology to increase operational efficiency, minimize risk, and improve customer experience. Members and guests discussed strategic and operational risks demanding the attention of boards as companies grow increasingly reliant on new and interconnected systems for core business processes and customer interactions.

Strategy should guide technology investment

- **Size and scope of investment.** The threat of disruption from mavericks requires companies to consider new, technology-enabled business models to remain competitive. One member cited the examples of large tech companies, such as Apple or Amazon, for their ability to get into completely new businesses rapidly and noted how quickly that can change the competitive dynamic: *"You thought you knew who your competitors were!"*

- **Centralization vs. decentralization.** According to one member, a centralized approach is appropriate *"if you are looking to leverage scale."* Individual business units may not have the overall vision or resources to execute effective transformations; they might even be invested in protecting the status quo. Decentralization, however, also has its advantages, especially—as members pointed out—since it can offer flexibility to companies trying to ensure both opportunity for entrepreneurial initiatives and stable, ongoing operations and controls.

  Mr. Dowsett highlighted the need for balance: *"If you decentralize too much, you increase risk."* At the same time, *"big companies will not necessarily find the best solution in one location and fully centralized."*

Risks that threaten effective implementations

- **Lack of training and insufficient focus on change management.** Several members commented that the lack of attention to change management is often at the center of failed technology-transformation initiatives. *"Training people is 75%; only 25% is the tech per se."* Ms. Ross emphasized that, even in examples where the technology didn't meet the business objectives, it generally was not because the technology didn't perform as expected, but because of inadequate communication and coordination. All agreed that effective change management is critical, but some members admitted that it is sometimes an *"afterthought"* in identifying managers and in tech investments. One member said, *"Because you're so focused on the technology, you're catching up.*"

  Multiple transformative initiatives can also create what Mr. Dowsett called "*change fatigue*". He said, *"You have to watch the turnover of the team,"* and, if you hire consultants, make sure *"the knowledge is left behind"* after the consulting engagement is completed. Mr. Dowsett also noted that looking to automation to reduce the workforce can create its own risks: *"If something breaks, then what will you do? Where are the people who can fix it? Where are the experts?"*

  Another aspect is "*Who owns the algorithm [that solves] the problem?"* Ms. Ross added: *"We don't want to crush the entrepreneurial spirit, but we have to take precautions and consider internal controls implications."*

- **Reliance on third-party providers.** Members expressed concern about the small number of third parties on which companies increasingly rely for strategic infrastructure; cloud providers, for example, are now becoming more like business partners than vendors. However, Mr. Dowsett observed that many companies are not considering the full potential of tools like cloud computing, which should be used *"to compete, [and] for speed and agility, not to save money. "It is in addition an opportunity to re-architect, and not simply* *transport something broken to the cloud."* One member noted that there are finance and accounting implications to these kinds of decisions that audit committees should be attuned to*: "You are swapping [capital expenditure] with [operating expenditure]. That's hard to get right; it can run away from you."*

Effective technology transformation

Members and guests discussed effective approaches to managing risks in complex technology-transformation projects.

- **Centers of excellence:** Ms. Ross observed, *"Some companies are standing up centers of excellence around tech transformation projects, or around specific technologies"* to develop use-cases, identify and share leading practices, and implement internal control processes around the development, implementation and maintenance of emerging technologies Mr. Dowsett also emphasized the benefits of centers of excellence in creating synergies across companies that arise from technology experimentation and adoption.
- **Developing a strategic roadmap**. Mr. Dowsett emphasized that major technology investments should be about *"challenging how you do business,"* not just improving efficiency. He advised against falling into the 'trap' of enchantment with technology: he noted that *"people get caught up in tech and try to find a problem for the solution."* Mr. Dowsett said, *"The tech can do these 30 things, so … the question should be … which will give the company a competitive advantage?"* Meeting participants emphasized the need for the businesses to drive technology investment and, ultimately, retain accountability for successful transformation.
- **"Run the business, change the business."** Many members' companies are replacing legacy systems that no longer function well but must keep the business running while new technologies are incorporated. Mr. Dowsett suggested legacy systems that work should be *"left alone."* He suggested that the focus should instead be on what needs to change quickly to improve customer experience or materially increase efficiency*.* To support this approach, he advocated adopting *"two-speed technology"* by creating—as one study has recommended—an *"IT architecture [that] help[s] companies develop their customer-facing capabilities…while decoupling legacy systems."* [2] Asked whether structuring the IT function in this way might create two classes of employees, he described people as occupying one of *"three zones"*: *"those who are really up for the change; those who say, 'leave me alone'; and those in the middle, who sit in both camps."* He suggested giving all *"the chance to come on the journey. But you can't go after everyone on day one."*

The board's oversight of IT risk is evolving

Members discussed planning for outages and looking back at past tech implementations to see if the benefits of IT projects were realized, and to learn and plan for the future.

Challenges for boards

- **Setting risk tolerances and conducting disaster-planning exercises.** Boards help management determine how much to invest up front, to ensure that companies can avoid lengthy system breakdowns and recover quickly if they should occur. Members said that their boards were not *"setting the risk appetite by system but asking how the company tests it."* One member described a context in which a company had determined that they had zero tolerance for system downtime, because it was a critical service; as a result, they invested huge sums to ensure they had multiple backups in multiple countries to account for risks such as natural disasters, terrorism, and cyberattacks.

- Members are keenly aware that, in the age of social media, any adverse event can quickly take on a life of its own. They spoke of 'drills' and 'battle plans' with PR firms. One recalled that, after a natural disaster, *"we did several tabletop exercises, but until you go live, you just can't know,"* to which another member responded: *"but imagine having tried to do it without a tabletop!"* A third member urged companies to mimic the military's after-action review process: *"Do a precise analysis and debrief, and then get right back on it if the desktop exercise has failed or you're not satisfied."*

- **Determining return on investment.** A common challenge several members raised is estimating ROI for major IT projects. They lamented how often these projects take longer than expected, run over budget, and deliver less than was projected. To help address this, some participants suggested trying to break up larger projects into smaller pieces and measure success based on incremental improvements. One member summed up a view shared by many: *"Where there is an operating necessity, it is hard to put a dollar benefit on it. So, we try to identify the process benefit."* In other cases, the investment may be necessary to remain competitive.

How does the board organize its oversight of technology?

While the full board generally has responsibility for oversight of major IT investments, oversight of the risks often falls to the audit committee. But more companies are adding technology committees as a response to the central role of technology in driving business models and the related risks. Members debated the pros and cons of technology committees and how to define their mandates.

- **The role of tech committees is not yet well defined.** Some boards have added or are considering adding technology committees, but the scope of oversight responsibilities continues to evolve. Where technology committees have been formed, members noted that their mandates vary, with some oversight of IT risk remaining with the audit committee (e.g., that related to internal controls) or—where one exists—with the risk committee. One member commented that *"If we had audit committee charters in front of us, we could not, probably, tell the difference between them,"* but that tech committee charters would vary significantly. Another member said their board established a tech committee *"because the* *audit committee didn't have the time, and at the board level it ate up our strategy time. An unintended benefit is that our IT group likes it a lot. They can interact with people who really understand them,"* because they have populated the committee with technology experts.

Not everyone was convinced of the need for technology committees and bringing specialized expertise onto boards. Members agreed that *"the ability to deal with tech people requires a certain level of understanding and expertise,"* but not all agreed that a new committee was necessary to achieve that objective.

Some members cautioned against the board starting to *"act like management"* by having technology experts delve into the details of technology issues. Others were concerned that the board dialogue around tech could degenerate into just *"tech talking to tech,"* without the benefit of a full board perspective that might highlight different kinds of risks or different approaches.

- **Outside expertise**. *"Audit committees have the independent audit firms. Tech committees need to have independent advisers as well,"* asserted one member. More directors are asking whether they might get outside advice at the board level on tech issues.

Special investigations

Sally Yates, Partner, Special Matters and Government Investigations at King & Spalding, joined members to discuss circumstances under which special investigations can arise, and how boards can best oversee them.

- **How does the Department of Justice (DOJ) determine it will open an investigation?** Ms. Yates listed factors that could lead to an investigation, including a *"whistleblower and false claims actions."* The DOJ will consider whether the allegations involve criminal wrongdoing, and whether the issue *"looks pervasive, not just a case of rogue employees: 'Is this how the company does business?' 'How high does the alleged misconduct go?' 'How bad is it?'"* She noted that *"the Department will have priorities, where they're trying to make an impact from a deterrence perspective,"* and added that *"civil investigations can morph into criminal."*

- **How do you decide whether to self-report?** *"This is a complex issue,"* said Ms. Yates, but self-reporting is *"often a good idea."* Some specific factors to think about include distinguishing *"whether it's aberrational conduct; and whether you tried to remediate it and have no history of wrongdoing. In [such] cases I might suggest doing so, with the caveat that if it goes to the very top level of the organization, you won't get a pass."* Ms. Yates said that by self-reporting, *"you can craft the narrative in a way that you wouldn't otherwise be able to."*

- **Who should lead the investigation?** *"There's no magic theory about when an investigation should be led by the audit committee, a special committee, or the full board,"* said Ms. Yates, *"or when outside counsel is required."* Some factors to consider include whether *"the company has great exposure, if the allegations are against company executives or the board;" also "when there is potential criminal activity, or if multiple governmental agencies are involved."* She also said the board needs to be involved if the issue is something *"brand-defining, such as the #MeToo movement."* Ms. Yates advised cooperation with the DOJ, rather than just compliance. The DOJ *"does assume good intent",* so companies should "*interact in good faith, and then your lawyers can also learn about the investigation."* Ms. Yates recommended that boards have discussions in 'peacetime', before a crisis hits, and that boards should have *"teed up"* 2-3 external law firms and other advisors to whom they can turn in the event of an investigation, since on short notice it can be difficult to identify a major firm *"of any size or resources that has never done any business with you."*

Ms. Yates concluded by saying, *"Most serious fraud cases start with a flawed corporate culture*.*"* She advised members to *"think about the information you're getting about problems that could metastasize. Any sizeable organization will have issues; so have discussions about what information is coming to you and what isn't."* A member added that *"it's a good idea to meet with the chief compliance officer a few times a year*,*"* and Ms. Yates agreed, adding: *"a dotted line to the chief compliance officer shows good faith to regulators*.*"*

The perspectives presented in this document are the sole responsibility of Tapestry Networks and do not necessarily reflect the views of network members or participants, their affiliated organizations, or EY. Please consult your counselors for specific advice. EY refers to the global organization and may refer to one or more of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Tapestry Networks and EY are independently owned and controlled organizations. This material is prepared and copyrighted by Tapestry Networks with all rights reserved. It may be reproduced and redistributed, but only in its entirety, including all copyright and trademark legends. Tapestry Networks and the associated logos are trademarks of Tapestry Networks, Inc. and EY and the associated logos are trademarks of EYGM Ltd.

Meeting participants:

The following SEACN members attended all or part of the meeting:

- Eddie Adair, Rayonier Advanced Materials
- Maureen Breakiron-Evans, Cognizant
- Dallas Clement, SunTrust
- John Davidson, Allergan and Legg Mason Inc.
- Cynthia Day, Aaron's, Inc.
- Juan Figuereo, PVH
- Tom Hough, Equifax
- Jim Hunt, Brown & Brown
- Scott Kuechle, Kaman Corporation
- Rich Macchia, Fleetcor
- Connie McDaniel, TSYS
- Rick Mills, Commercial Metals Company

EY was represented by the following:

- Cigdem Oktem, Director, Southeast Region, Center for Board Matters
- Dave Sewell, Partner
- Bryan Yokley, Georgia/Alabama/Tennessee Market Segment Leader, Assurance Partner

Endnotes

[1] *Summary of Themes* reflects the network's use of a modified version of the Chatham House Rule whereby names of network participants 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] Oliver Bossert, Chris Ip, and Jürgen Laartz, *A two-speed IT architecture for the digital enterprise*, McKinsey Digital, December 2014.