

AUDIT OVERSIGHT IN 2024

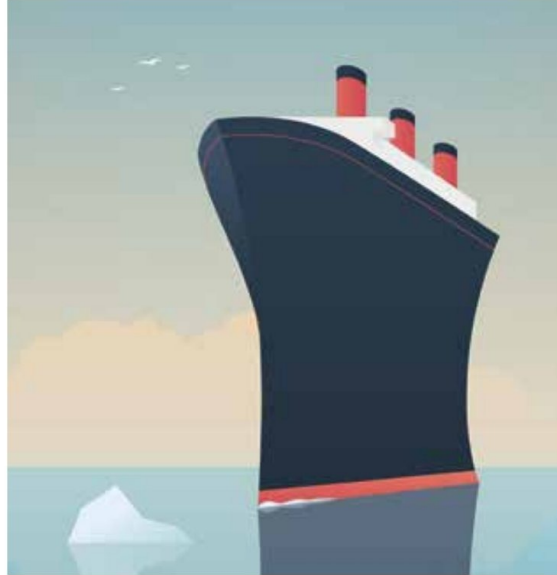
Directors share strategies on coping with heightened responsibilities and shifting priorities as an aggressive regulatory environment and emerging risks ramp up the pressure on audit committees.

CHANGING REGULATORY REQUIREMENTS,

macroeconomic uncertainty, geopolitical instability, ongoing inflation and, of course, adjusting to the advent of AI are just a few of the many areas of concern boards face heading into 2024. Charged with keeping a close eye on financial reporting, controls and disclosures, today's audit committees must navigate the monumental task of tracking and triaging a seemingly vast and ever-growing set of challenges, agreed directors participating in a *Corporate Board Member* roundtable discussion held in partnership with RSM.

"There's a lot going on, from a regulation perspective and from a macroeconomic perspective, with continued uncertainty in different areas," said Sara Lord, a partner and chief auditor at RSM US LLP. "We see higher inflation continuing, wars and other aspects of political uncertainty taking place in different areas and the SEC questioning MD&A disclosures on risks and uncertainties, supply chain issues and financial reporting. Plus, we're seeing new cyber disclosure rules coming out and watching litigation on the importance of the role of the chief information security officer unfolding." Audit committees, she advised, should be questioning management about the impact on operations, supply chains, forecasting and debt outlook, as well as pressing for proper cyber insurance and recovery policies.

For Swati Abbott, CEO of Blue Health Intelligence and a board member at the skilled nursing facilities company Ensign Group, data privacy coupled with the potential impact of regulatory activity around cybersecurity loom as large concerns. "Cybersecurity is a big issue for us in healthcare, because healthcare data is so valuable," she said, adding that the potential for unintended consequences stemming from regulators' efforts to hold CISOs accountable in the wake of cyber incidents is also worrisome. "With the SEC going after SolarWinds and their CISO, I'm wondering if that's a trend we will start seeing, and, if so, will it become hard to recruit CISOs?"



“Even if AI is not being used in your organization now, with the adoption rates we’re seeing, it will probably be in your purview as an audit committee within 12 to 18 months.”

—Troy Merkel, RSM

AUDITING AI RISK

The embrace of AI introduces a whole new area of cyber risk, added Troy Merkel, an audit partner and senior analyst in the real estate industry for RSM, who pointed out that one of the biggest cybersecurity breaches of 2023 involved Microsoft's AI engine. "As more and more AI tools come online, it's really critical that there are policies and procedures in place to protect the data and the integrity of data within organizations," he said. "Even if AI is not being used

in your organization now, with the adoption rates we're seeing, it will probably be in your purview as an audit committee within 12 to 18 months."

Several directors echoed Merkel's concern, with some noting that boards may need to take steps to ensure that attempts by a company or its partners to leverage AI don't inadvertently put its data at risk. One discussion participant recounted an outside vendor that proposed using AI to screen the company's email data and email traffic for rounded journal entries as part of a financial audit. "You have to ask questions like is that proprietary, or are you aggregating that data and exporting it somewhere?" he said. "We need to be careful that we're stepping carefully into AI, not running into AI."

Unsanctioned use of AI by overeager employees can also introduce risk. Anne McGeorge, audit chair at Dianthus Therapeutics, SOC Telemed and CltiusTech, says one of the companies on whose boards she serves is currently working on a policy on AI use for the 150 oncology physicians that it employs. "We decided that if we think they are not using AI in their practices, we are being delusional," she explained. "So we want to put a policy in place with regard to how our employees can use it and how we can monitor it so there's some consistent methodology there."

Merkel agreed that companies need to be mindful of the likelihood that employees and outside vendors will look to make use of AI capabilities. "When there's going to be use of AI by third parties and by employees, the audit committee needs to be weighing in with guardrails and also considering what that will mean for data," he said, acknowledging that audit committees may struggle with the time commitment and expertise necessary for AI oversight. "The ability to analyze AI and cybersecurity doesn't traditionally fit with the skill set of the audit committee, but it gets dumped there. The approach of most companies is, 'Anything that will be really hard and could get us in trouble with the regulator, we will throw on the audit committee.'"

OVER-SPECIALIZING OVERSIGHT

Eric Brandt, former CFO of Broadcom and chair of the audit company at Gen Digital, pointed out that piling more responsibilities on the audit committee's plate invariably leads to less time spent on fundamentals like financials and strategy. "Now, audit committees have to measure ESG; we have to pay attention to cyber—which is actually a very significant issue—and then you start adding in AI," he said. "As we get caught up in all these specializations, audit committees and boards are being pulled toward regulatory oversight and away from the things that actually make companies successful, such as helping the management team compete and delivering value for shareholders."

For example, regulatory requirements that require robust and timely disclosure of cyber incidents essentially equate to "government choosing to prosecute the victim," Brandt said, noting that the many layers sophisticated cyberattacks often have make reporting incidents a complicated endeavor. "Maybe in some cases people have been remiss in what they're supposed to do, but I worry that we're chasing a series of expertises on boards and on audit committees that are making us not necessarily good or deep on any one of them."

The proliferation of responsibilities falling on audit committees is leading some companies to review committee charters and consider hiving off areas of focus. "We're creating a new board committee devoted to technology and digital and moving cyber there," reported Steve Shepsman, audit chair at real estate company Howard Hughes Corporation and a board member at Werber Real Estate. "When you really look at all the interfaces between customers and the company from digital and technology, it's not just an audit thing—it's how companies are operating now. It's more business-strategic."

Erie Insurance formed a dedicated risk committee focused on areas like cyber, ESG and AI in order to free up the audit committee to focus on financials and compliance, said Gene Connell, a board member at the homeowners insurance company. "We have some overlap between the two committees and joint meetings, but it was done out of a recognition that the audit committee needs to have enough time to spend on the core elements," he explained. "Things like cyber, ESG and AI are now handled by the risk committee."

Some directors expressed reservations about the notion of dividing committees to manage an increased workload. "I worry about committee pro-

"If you have the same number of board members and more committees, that doesn't necessarily create capacity."

—Sara Lord, RSM

liferation, because whether you do a four-hour audit committee or create two new committees, you're still substantially increasing the work of the individual board members," said Brandt, who is also a board member at Macerich. "I don't know how we're going to manage it all, and I'm also, quite frankly, worried whether capable people will want to be on boards."

Adding a committee singularly dedicated to technology, ESG or emerging risks may not resolve issues around the increasing workload and time commitment currently falling on directors, agreed Lord. "If you have the same number of board members and more committees, that doesn't necessarily create capacity," she said. "So you also need to be a little realistic and honest with yourself about what that looks like. Or, if you're considering adding more board members, that changes the dynamic, so what does that do for governance overall? Sometimes it's about not being afraid to have those conversations, and it's not always something you can solve in two or three meetings."

Shepsman's company, which created a separate risk committee and is now in the process of adding a technology committee, increased the size of its board to accommodate the additional responsibilities. "As more and more responsibilities are laid on the board, we have to find a way to lay that off to more people," he said. "Having five committees and extra people to [share the workload] makes it more palatable to be on the audit committee."

A CASE FOR COMPOSITION

For some directors, a lack of expertise in emerging areas of risk within the boardroom is another top concern. Kim Wales, founder and CEO of CrowdBureau and a former director at Investors Bank, referenced formidable changes taking place in banking and financial services and questioned whether the boards of financial institutions need to rethink director recruitment practices that have traditionally focused on

seeking out retirees with leadership experience. "Does anyone sitting on board today have an understanding of blockchains and regulatory restrictions?" she asked. "Should we be thinking a bit more clearly about balance with board composition? You don't want everyone to be a siloed expert, but you also don't want all people who retired out of business and maybe don't have an awareness of what's taking place in the current technologies and current regulatory frameworks because they've been removed from the day-to-day."

Rather than recruiting for expertise, several directors reported that their boards address skill gaps by bringing in specialists to educate directors on topics like cybersecurity, AI, risk disclosure and transparency in financial statements and new accounting standards. "We don't want a cyber expert actually sitting on the committee," explained Connell. "We don't want the board to get down into the weeds. Also, your ability to manage a meeting depends on the size of a committee. So we bring in the expertise we need, and we've not had any trouble finding that expertise to come in and talk to the board."

Commitment to ongoing education also helps boards keep directors up to speed on new developments at Erie Insurance, said Thomas Palmer, another board member at the company. Erie holds one or two full-board educational sessions each year, and each of the board's committees also has at least one educational session annually. The board's risk committee typically invites all sitting directors to attend meetings that provide an educational session or plan to drill down on an issue that would be helpful for the full board to better understand, explained Palmer. "For example, we held a session on director responsibility in regard to cybersecurity," he recounted. "Every board member shared his or her relevant experience, and those with a greater skill set in a particular area would raise more questions or do more probing. The point there is that you want directors to assist in framing the issue; you're not looking to someone and saying, 'Tell us what we ought to think.'"

Ultimately, the right strategy for managing the changing landscape of audit committee responsibilities will also vary by industry, by company and by size, noted Merkel. "What is clear is that there's so much coming at companies and their boards today that the status quo or the charter created 10 years ago may no longer be right for your company and your board," he said. "Taking a fresh look at the roles and responsibilities of the audit committee can ensure the audit committee is helping the company make the right business decisions, not just dealing with all of the regulatory compliance being thrown your way."