On the 2023 higher education audit committee agenda

January 2023

As the pandemic subsided in fiscal 2022, many colleges and universities experienced a rebound in operational performance amid residual federal stimulus funding, despite headwinds from inflation, workforce disruption, and a changing political landscape. Heading into fiscal 2023, higher education institutions faced geopolitical instability, surging costs, less favorable debt markets, lingering workforce and supply chain issues, and the prospect of a global recession. Given these issues, as well as long-standing pressures around the industry business model, access, equity, affordability, and outcomes, boards and audit committees will once again need to refine their risk-driven agendas.

College and university audit committees can expect their institutions' financial reporting, compliance, risk, and internal control environments to be tested by an array of challenges in the year ahead, from cyber risks to social risks—including continued stress in attracting and retaining talent. The increasing complexity and fusion of risks—and their unexpected interconnectedness—put a premium on more holistic institutional risk management and oversight. In this volatile operating environment, demands from creditors, donors, grantors, and other stakeholders for action, as well as increased disclosure and transparency, will continue to intensify.

Drawing on insights from our interactions with higher education audit committees and senior administrators, we've highlighted several issues to keep in mind as audit committees consider and carry out their 2023 agendas:

- **Maintain a sharp focus on leadership and talent in finance and other key functions.**
- **Understand how the institution is managing and reporting on environmental, social, and governance (ESG) risks.**
- **Keep a watchful eye on the institution's management of cybersecurity risks.**
- **Sharpen the institution's focus on ethics, compliance, and culture.**
- **Help ensure internal audit is focused on the institution's key risks—beyond financial reporting and compliance—and is a valuable resource for the audit committee.**
- **Reinforce audit quality and set clear expectations for frequent, candid, and open communications with the external auditor.**
- **Take a fresh look at the audit committee's agenda, workload, and capabilities.**

Maintain a sharp focus on leadership and talent in finance and other key functions.

College and university administrators face a very challenging environment today. To make the higher education business model more efficient, many institutions are implementing new enterprise resource planning (ERP) applications to enhance a variety of core business processes, from budgeting, financial reporting, and student services to payroll, procurement, grant compliance, and endowment management, among others. At the same time, institutional leaders are contending with talent shortages in key financial, IT, risk, compliance, and internal audit roles as they try to forecast and plan for an uncertain economic environment. It is essential that the audit committee devote adequate time to understanding risks related to transformation strategies and personnel constraints—to help ensure that the finance and administration organization has the leadership, talent, and bench strength to execute those strategies while maintaining its core operating responsibilities.

In 2022, colleges and universities experienced unprecedented demands for greater workplace flexibility and equity, higher compensation costs, and in some cases, significant attrition in specialized administrative positions. The traditional campus-based work model, an aging demographic in senior administrative roles, and historically leaner staffing models have only intensified pressures on recruitment and retention. United Educators' *Top Risks Survey* of colleges and universities conducted in September 2022 affirmed that recruitment and hiring jumped from the 14th most-cited risk in 2021 to the *third* in 2022, just behind data security and enrollment.[1]

While the competition for talent in finance, accounting, internal audit, and IT roles has abated in some parts of the country—as well as in certain competing sectors—personnel turnover and unfilled positions in a sector that generally offers lower salaries and provides less work-life balance than in the past have left some institutions struggling to appropriately staff certain roles and functions. To mitigate further attrition, many colleges and universities have had to recalibrate remote work policies, find new ways to promote employee engagement and collaboration, strengthen recruiting efforts, provide stay bonuses, or renegotiate compensation.

To help monitor and guide the institution's progress as it refines the business model in a resource-challenged environment, we suggest the following areas of focus for the audit committee:

- To address staffing issues in the near term, higher compensation and benefit expectations and costs may place additional strain on the institution's budget or could adversely affect decisions around hiring and organizational roles. Does the audit committee understand how the institution is coping, particularly as to specialized resources needed to manage mission-critical processes and controls, and mitigation of fraud risks?
- The tax, compliance, and cultural ramifications of remote work arrangements and benefit program changes are complex and evolving. Does the institution have the appropriate infrastructure to monitor and manage these requirements, as well as potential increased cyber risks?
- As finance and internal audit functions combine strong data analytics and strategic capabilities from new ERPs with traditional financial reporting and auditing skills, their talent and skill-set requirements must change accordingly. Are these functions attracting, developing, and retaining the talent and skills necessary to match their needs? Are personnel embracing and accelerating available automation solutions—especially in traditionally labor-intensive areas such as accounts payable and payroll? Has management taken a fresh and holistic look at business processes and controls that may be overly burdensome relative to the risks involved?
- Do the chief business officer, chief compliance officer, chief audit executive, and chief information security officer have the appropriate internal authority and stature, organizational structures, resources, and succession planning to be effective moving forward?

[1] Source: United Educators, *2022 Top Risks Report: Insights for Higher Education*, 2022.

Understand how the institution is managing and reporting on ESG risks.

ESG involves integrating material environmental, social, and governance risks and opportunities into an entity's strategy to build long-term financial sustainability and value. In today's increasingly competitive and transparent operating environment, ESG has become a board-level imperative reflecting and aligning with an entity's mission, values, goals, and reputation.

The learning and research missions of many colleges and universities inherently correlate to or embed ESG goals. These institutions face increasing stakeholder demands—from board members, creditors, and local communities to students, faculty, and donors—for more visible and higher-quality information about ESG risks and opportunities, particularly around stated goals such as climate (e.g., "net zero") and student access. How is the institution addressing climate and other ESG risks and issues, particularly diversity, equity, and inclusion (DEI) efforts? Beyond students and faculty, ESG factors into virtually all institutional activities, such as endowment and facilities management, supply chain, fundraising, sports, international activities, and alliances. For universities with academic medical centers, additional considerations may include health equity and charity care.

In 2022, colleges and universities confronted no shortage of developing risks that could impact several long-standing social, climate, and governance priorities. For example, a Supreme Court case on affirmative action expected to be decided in 2023 could have far-reaching ramifications on student diversity and admissions, including recruitment, scholarships, standardized testing, and legacy preferences. Recent rule changes involving Name, Image, Likeness (NIL) opportunities for student athletes have introduced dynamics that may complicate management of athletic programs and exacerbate inequities. In addition, spiraling campus utility costs (which according to the Higher Education Price Index rose 43.1 percent during the year ended June 30, 2022[2]) have heightened expectations for institutions to demonstrate progress on climate action plans. And while cyber risk management may not jump to mind as an ESG imperative, it is considered critical to effective governance. Indeed, the integration of many ESG-related risks into the institution's enterprise risk management (ERM) profile is increasingly evident. The higher education sector is still in the early stages of the ESG reporting journey. In our experience, while many institutions do not have a formal ESG strategy (or publish formal reports), most have long had initiatives pertaining to ESG objectives that may be tracked and reported on by various departments. Several institutions have made public commitments around student access and affordability, faculty diversity, and divestment of fossil fuel holdings in their endowment portfolios. Others are just beginning to inventory existing ESG activities and considering how to develop a comprehensive ESG approach. At all stages, there is ample room for alignment on and understanding of ESG definitions and a critical need for quantitative, reliable data. Still, for most colleges and universities (and for entities in other sectors), the absence of a generally accepted ESG framework and lack of consensus around key industry performance indicators remain major obstacles to progress.

The extent to which higher education institutions will be subject to ESG disclosure requirements is uncertain. ESG reporting is a priority for public companies regulated by the SEC, which in 2022 issued rulemaking proposals for climate and cybersecurity disclosures and is anticipated to issue additional rulemaking on human capital disclosures. Although the SEC does not directly regulate the higher education sector, its oversight of public debt markets includes conduit offerings by colleges and universities. To date, the SEC's rulemaking has not applied to such offerings. Nevertheless, some institutions have begun to provide sustainability data in their offering documents, while others have published reports including DEI data on their investment managers. In addition, S&P and Moody's recently reaffirmed that ESG factors will continue to influence credit quality in the higher education sector[3,4] by incorporating ESG scoring in their methodologies and explicitly discussing ESG considerations in ratings reports. And as recently proposed in the U.S. House of Representatives, the Endowment Transparency Act of 2022 would amend the Higher Education Act of 1965 to mandate that colleges and universities annually disclose information about investments managed by women- and minority-owned firms as well as the percentage of bond issuances underwritten by such firms. Accordingly, as alignment of the institution's investment and financing strategies with its stated ESG goals likely becomes more apparent to donors and other stakeholders, accurately compiling and properly evaluating ESG data from third-party managers and advisers will be critical.

[2] Source: *Commonfund Higher Education Price Index, 2022 Update.*

[3] Source: S&P, *Outlook for Global Not-for-Profit Higher Education*, January 20, 2022.

[4] Source: Moody's Investors Service, *Macroeconomic challenges to exacerbate ESG credit risks*, January 3, 2023.

As to other standard setters, the Financial Accounting Standards Board and Governmental Accounting Standards Board each have acknowledged and deliberated the intersection of ESG matters with financial reporting standards (although neither has established ESG disclosure requirements). In addition, the American Institute of Certified Public Accountants (AICPA) has issued guidance on sustainability reporting and related attestation by auditors, evidencing the marketplace's interest about the structure and integrity of ESG disclosures more broadly.

Although standards are still evolving, audit committees should encourage management to inventory and fully assess the scope, quality and consistency of the institution's ESG internal and external disclosures, as well as safeguards to ensure data utilized in reporting is reliable. This evaluation should include consideration of the available methodologies and standards; how the institution is defining metrics, as well as understanding the expectations of creditors, donors, and other stakeholders; and the appropriateness of the ESG reporting framework(s) for the institution.

While ESG reporting in higher education is nascent and likely to evolve over the next several years—including as it pertains to the role of governance in the process—oversight of an entity's ESG activities is a formidable undertaking for any board and its committees. The decentralized management structure of many comprehensive universities only complicates the process. In the corporate sector, the nominating or governance committee often takes the coordinating role, and the audit committee is beginning to look at the company's ESG disclosures, whether or not in SEC filings.

- Consider where ESG information is currently disclosed, e.g., sustainability and DEI reports, the institution's website, etc. Who are the stakeholders using such information? What mechanisms exist for them to provide feedback and ask questions about our data? What internal controls and procedures are in place to ensure the quality of data used, and is it reviewed with the same rigor as financial results?
- Do we understand and receive reports on the basis for the disclosures and the processes used to generate them?
- Does the institution have an ESG or similar strategy, and who is responsible for its execution? Should a disclosure committee comprising appropriate senior administrative leaders, such as the chief sustainability officer, chief diversity officer, and chief information security officer, be created to facilitate the ESG strategy?
- How are material ESG risks identified? Are these risks integrated into the ERM profile?
- Does or should the institution utilize an ESG reporting framework?
- Have we enlisted faculty with ESG expertise to help us think through our strategy and framework?
- What metrics are used to measure progress against stated goals, and how are such metrics defined? Who within the institution will be responsible for generating and tracking such data and ensuring its conformity with applicable standards?
- Clarify the role of the audit committee in overseeing the institution's reporting of ESG risks and activites, particularly the scope and quality of ESG/sustainability reports and disclosures. How are the full board and other committees involved in overseeing ESG initiatives?
- Does (or should) the institution obtain assurance from internal or external auditors about certain ESG information to provide stakeholders with a greater level of comfort?

Keep a watchful eye on the institution's management of cybersecurity risks.

Our experience suggests that cybersecurity continues to rank at or near the top of the higher education audit committee agenda. In today's increasingly distributed technology environment, it is almost inevitable for a company or institution to experience a significant cyber event. And the threat landscape is only expanding, with cybercriminals employing increasingly sophisticated tactics and technologies to wreak havoc on their targets. Their motives may vary, with some cybercriminals working on behalf of nation states to create chaos on U.S. soil, and others seeking monetary compensation, intellectual property, or other sensitive data. Moreover, cybercriminals do not adhere to an academic calendar; they work around the clock to find windows of opportunity to cause disruption. While higher education institutions are working diligently to improve their cybersecurity infrastructures, bad actors are moving more quickly.

Indeed, several colleges and universities have succumbed to high-profile attacks, resulting in data breaches, network outages, and ransom payments to regain control of data or networks. A recent report by S&P[5] indicates average weekly cyberattacks per organization in all industries are growing, and that education and research entities experienced 1,600 weekly attacks in 2021—the highest of any industry. The report notes that the cost of insuring against such attacks is also growing, with rated colleges and universities experiencing year-over-year increases of 40–60 percent in cyber insurance rates.

At the center of higher education's cybersecurity landscape are three common themes: (1) colleges and universities—particularly those with significant research activities and academic medical centers—are high-value targets; (2) the sector continues to lag others with respect to cyber spending, staffing, and expertise at the board level; and (3) the stakeholder landscape is among the broadest of any industry—students, parents, faculty, staff, board members, alumni, donors, grantors, researchers, patients, the federal government and associated regulatory bodies, among others.

Although higher education stakeholders make important and wide-ranging financial and strategic contributions to the institutional mission, their varied interests can make quick decision-making a challenge. Fulfilling the needs and expectations of a such a complex network of stakeholders undoubtedly gives rise to more cybersecurity concerns. To mitigate these, institutions must be willing to embrace cutting-edge security solutions to manage the growing volume and sophistication of threats they face. It is therefore imperative that institutions accelerate the implementation of robust security processes and controls that continuously assess and mitigate cyber vulnerabilities. As no university wants to fall victim to a breach while cybersecurity policies await revision or proactive measures need sign-off, every second counts.

The complex and rapidly changing cybersecurity and data governance regulatory environment includes a number of different security and privacy frameworks applicable to higher education institutions, including, among others, the National Institute of Standards and Technology (NIST), which may apply to federal and other grants; the EU's General Data Protection Regulation (GDPR), a data protection law for EU citizens; and the Safeguards Rule of the Gramm-Leach Bliley Act (GLBA), which regulates the collection, disclosure, and protection of consumers' nonpublic information and applies to colleges and universities receiving federal funds. Significantly expanded GLBA requirements due to become effective on June 9, 2023 clarify that a qualified individual (typically a chief information security officer) must oversee the entity's security programs and include regular testing or monitoring, training for security personnel, periodic assessments of service providers, written incident response plans, and periodic reports from the qualified individual to the board, among other requirements. Establishing processes to monitor and map the various requirements of applicable cybersecurity and data privacy frameworks—which will continue to change and expand—to the institution's enterprise-wide cybersecurity program is essential.

In addition to approaching cybersecurity with a heightened sense of urgency and staying on top of regulatory changes, colleges and universities can enhance protocols by:

- Implementing regular training, awareness campaigns, tabletop exercises, and phishing simulations for students, faculty, staff, and other key stakeholders.
- Narrowing the scope of access to secure systems. Colleges and universities should be mindful to limit system access only to those who truly need it. For example, visiting professors should not have remote access to an institution's network once their teaching or research assignment is complete.
- Diligently deploying, tailoring, testing, and refining baseline tactics. This may mean increasing the frequency of penetration testing, "red teaming" (which tests how the security team responds to various threats), and system backups, as well as refreshing incident response playbooks on a more regular basis.

[5] Source: S&P Global, *Cyber Risk in a New Era: U.S. Colleges and Universities Go Back to School on Cyber Security Preparedness*, September 29, 2022.

- Developing a comprehensive response playbook for ransomware. It is essential that institutions have a firm stance on their willingness to pay (or not pay) ransom before their systems are compromised. Purchasing ransomware insurance is a key aspect of this preparation, as is identifying who will make the ultimate payment decision in the event of a breach.
- Establishing minimum cybersecurity standards for all vendors and regularly monitoring them.
- Understanding third-party vendor risks associated with cloud-based systems that create new access points to sensitive data. Such vendors need regular vulnerability assessments, and their internal controls require independent assurance from auditors through service organization controls (SOC) reports.

With so much data and high-value information at stake, colleges and universities are at an inflection point and should focus on adopting a Zero Trust mindset toward cybersecurity. The Zero Trust security model is increasingly viewed as a viable security approach in the postpandemic world. Zero Trust represents a significant mindset shift in which cyber teams assume their systems will be compromised and thus make security decisions based on that assumption, with a focus on the identity, device, data, and context of each entry into the system.[6] Of course, adopting such a dynamic response protocol is costly and will require institutions to allocate additional funds for cybersecurity technology and personnel. To ease this burden and allow security professionals to prioritize matters requiring human intervention, mitigation of lower-level threats and routine testing should be automated.

To help ensure the institution has a rigorous cybersecurity program, the audit committee should consider the following questions:

- Do we have clear insights into our cybersecurity program's maturity, gaps, and threats? Does leadership have a prioritized view of additional investments needed? Are the institution's most "valuable" assets adequately protected?
- Do we have the appropriate leadership, talent, and bench strength to manage cyber risks? What are the risks to the institution in the event of unexpected turnover or inability to fill key positions?
- Does the institution regularly test its incident response plan? How frequently are penetration and red team testing performed, and is there a formal process to address findings?
- How often are data and systems backed up, and how accessible are the backups? Resilience is vital to restoring operations after an attack.
- Do we have a robust institution-wide data governance framework that makes clear how and what data is collected, stored, managed, and used and who makes related decisions?
- Is security training for students, faculty, and staff regularly provided? Is training completion monitored and enforced? How is security awareness periodically assessed?
- Do security and privacy terms in agreements with third-party IT providers meet the institution's criteria for adequate protections? Does management regularly review SOC reports and evaluate the institution's complementary controls to flag possible issues? Do such vendors carry cyber insurance?
- How are we monitoring evolving and expanding federal, foreign, and other regulations governing data security and privacy to ensure our cybersecurity program and data governance framework reflect the latest requirements?
- Do we understand the coverages, limits, and underwriting criteria of our cyber insurance policy?
- Who reports on cyber to the audit committee and board? Is it a chief information security officer or similar position who speaks in business terms and understands that cyber is an enabler as well as a risk?

[6] Source: *Cyber security considerations 2022*, KPMG International, November 2021. https://home.kpmg/xx/en/home/insights/2021/11/cyber-security-considerations-2022.html

Sharpen the institution's focus on ethics, compliance, and culture.

The reputational costs of an ethics or compliance failure are higher than ever, particularly given the increased fraud risk due to employee financial hardship, pressures on management to meet enrollment and other budgetary goals—as well as rankings and other nonfinancial targets—and increased vulnerability to cyberattacks. Fundamental to an effective compliance program is the right tone at the top and culture throughout the institution, including its commitment to stated values, ethics, and legal and regulatory compliance. Reinforcement of these imperatives is especially critical in the decentralized operating environments of comprehensive universities, where navigating the myriad of regulatory and ethical considerations around research activities, technology innovation and commercialization, and intercollegiate athletics is increasingly complicated.

With the radical transparency enabled by social media, the institution's culture and values, commitment to integrity and legal compliance, and brand reputation are on full display. The audit committee should closely monitor the tone at the top and culture throughout the institution with a sharp focus on behaviors (not just results) and yellow flags, considering the following:

- As we've learned, leadership and communications are key, and understanding, transparency, and empathy are more important than ever. Does the institution's culture make it safe for people to do the right thing? It can be helpful for board members to get out into the field and meet employees to get a better feel for the culture.
- Help ensure that regulatory compliance and monitoring programs remain up to date, cover all vendors in the global supply chain, and clearly communicate expectations for high ethical standards. Does the institution have a clear and current code of conduct, and are annual acknowledgments or certifications of the code required for faculty and staff?
- Focus on the effectiveness of the institution's whistleblower reporting channels and investigation processes. Are all available reporting channels clearly and regularly communicated to the campus community to ensure awareness and use? Does the community utilize those channels? Does the audit committee receive regular information about whistleblower complaints, understand how such complaints are resolved, and receive data that enables the committee to understand trends? What is the process to filter complaints that are ultimately reported to the audit committee?

Help ensure internal audit is focused on the institution's key risks—beyond financial reporting and compliance—and is a valuable resource for the audit committee.

At a time when audit committees are wrestling with weighty agendas—and issues like cybersecurity and burgeoning regulations are putting risk management to the test—internal audit should be a valuable resource for the audit committee and a crucial voice on risk and control matters. This means focusing not just on financial reporting and compliance risks, but also on critical operational and technology risks and controls. Is the internal audit plan risk based and flexible, and does it adjust to changing business and risk conditions? This is an increasingly common question that audit committees are (or should be) asking the chief audit executive. The internal audit function must be able to effectively pivot to address unanticipated issues and risks as well as ongoing institutional risks highlighted in the original audit plan.

The audit committee should work with the chief audit executive and chief risk officer to help identify those risks that pose the greatest threats to the institution's reputation, strategy, and operations, such as tone at the top and culture; workforce issues; ERP implementations and enhancements; data governance; research compliance and conflict risks; international activities; third-party risks; and integrity of data used in ESG, rankings, and other reporting. Expect the latest internal audit plan to reflect these emerging risks and reaffirm that the plan can adjust to changing operational or risk conditions. Mapping internal audit's areas of focus to the institution's key business processes and risks, how does the current plan compare to last year's plan? What has changed or is expected to change in the institution's operating, data, and related control environments? What is internal audit doing to be a valued business adviser to other departments?

Set clear expectations and ask whether internal audit has the resources, skills, and expertise to succeed—especially as the tight labor market may impact recruitment and retention. Clarify internal audit's role in connection with ERM and ESG risks more generally—which is not to manage risk, but to provide added assurance regarding the adequacy of risk management processes. With the tight labor market, does internal audit have the talent it needs? Recognize that internal audit is not immune to talent pressures. In addition, help the chief audit executive think through the impacts of digital technologies—including routines and dashboards used by internal audit for risk assessment and real-time auditing, as well as systems used by the institution generally—on internal audit's workload and effectiveness.

Reinforce audit quality and set clear expectations for frequent, candid, and open communications with the external auditor.

Audit quality is enhanced by a fully engaged audit committee that sets the tone and clear expectations for the external auditor and monitors auditor performance rigorously through frequent, quality communications and a robust performance assessment.

In setting expectations for 2023, audit committees should discuss with the auditor how the institution's financial reporting and related internal control risks have changed in light of changes in the macroeconomic, industry, and institutional risk landscape. Regulatory and federal funding changes, workplace and supply chain disruptions, inflation, higher interest rates, executive transitions, endowment volatility, changes in donor credit profiles, the risk of a global recession, and other factors all have the potential to affect the institution's significant judgments, estimates, and disclosures, as well as related controls.

Set clear expectations for frequent, open, candid communications between the auditor and the audit committee—beyond what's required. The list of required communications is extensive, and includes matters about the auditor's independence as well as matters related to the planning and results of the audit. Taking the conversation beyond what's required can enhance the audit committee's oversight, particularly regarding the institution's culture, tone at the top, and quality of talent in the finance and compliance functions.

Audit committees should also probe the audit firm on its quality control systems that are intended to drive sustainable, improved audit quality—including the firm's implementation and use of new technologies. In discussions with the external auditor regarding the firm's internal quality control system, consider the results of external and internal inspections and efforts to address any deficiencies.

Remember that audit quality is a team effort, requiring the commitment and engagement of everyone involved in the process—the auditor, audit committee, internal audit, and management.

Take a fresh look at the audit committee's agenda, workload, and capabilities.

Keeping the audit committee's agenda focused on its core responsibilities—oversight of financial reporting and compliance, internal controls, and internal and external auditors—is essential to the committee's effectiveness. Beyond these duties, audit committees at colleges and universities oversee a growing plethora of other institutional risks, compounding the workload challenge and making efficiency paramount. As the role and responsibilities of the audit committee continue to expand and evolve, the committee should regularly reassess its composition, independence, and leadership to ensure they are keeping pace and to mitigate the risk of "agenda overload." The committee—with input from management and auditors, as appropriate— should conduct self-evaluations annually.

In our interactions with institutions across the country, we sometimes hear that evaluating the audit committee's effectiveness in a sector as specialized as higher education and in the context of each institution's unique operating environment can be difficult. Compared with corporate audit committees—which are often highly regulated and for whom industry benchmarking, executive education, and networking opportunities are commonplace—college and university audit committees have a nontraditional focus and scope (e.g., not-for-profit accounting, research compliance, etc.) and are generally unregulated and more insular, complicating the determination of what is "optimal." External and internal auditors, as well as industry organizations such as the Association of Governing Boards of Universities and Colleges (AGB) and the AICPA, may offer relevant and objective guidance. Moreover, the higher education sector is perhaps the most collegial in the U.S., with peer institutions frequently sharing insights, so there may be opportunities to learn from and collaborate with similar institutions.

We recommend the following areas to probe as part of the committee's annual self-evaluation:

- Does the committee's charter align with and reflect the actual goals and work of the committee?
- How many members have direct experience with financial reporting, compliance, and internal controls? Is the committee relying too heavily on one member to do the "heavy lifting" in overseeing these areas?
- Does the committee include members with the experience necessary to oversee emerging areas of risk that the audit committee has been assigned—such as cyber and data security? Is there a need for a fresh set of eyes or deeper (or different) skill sets? Should other board committees take on or be created to address certain risks?

- Does the committee spread the workload by allocating oversight duties to each audit committee member, rather than relying on the committee chair to shoulder most of the work?
- Are committee meetings streamlined by insisting on quality premeeting materials (with expectations they have been read), using consent agendas, and reaching a level of comfort with management and auditors so that certain activities can become routinized (freeing up time for more substantive issues facing the institution)?
- Is sufficient time spent with management and auditors outside the boardroom—to get a fuller picture of the issues and enhance the productiveness of committee meeting time?
- Are executive (nonpublic) sessions with management, internal and external auditors, and members only at the beginning or end of meetings scheduled? Establishing a regular cadence of such meetings helps ensure that sensitive matters, if any, can be addressed and allows for more open sharing of ideas and perspectives.
- Do members have access to robust orientation and continuing education programs? Are they provided with relevant industry information sourced from outside the institution? Are mechanisms available to network with counterparts at comparable institutions?

About the KPMG Board Leadership Center

The KPMG Board Leadership Center (BLC) champions outstanding corporate governance to drive long-term value and enhance stakeholder confidence. Through an array of insights, perspectives, and programs, the BLC—which includes the KPMG Audit Committee Institute (ACI) and close collaboration with other leading trustee and director organizations—promotes continuous education and improvement of public- and private-entity governance. BLC engages with board members and business leaders on the critical issues driving board agendas—from strategy, risk, talent, and ESG to data governance, audit quality, proxy trends, and more. Learn more at kpmg.com/us/blc.

About the KPMG Audit Committee Institute

As part of the BLC, the ACI provides audit committee and board members with practical insights, resources, and peer-exchange opportunities focused on strengthening oversight of financial reporting and audit quality and the array of challenges facing boards and businesses today—from risk management and emerging technologies to strategy, talent, and global compliance. Learn more at kpmg.com/us/aci.

About the KPMG Higher Education practice

The KPMG Higher Education, Research & Other Not-for-Profits (HERON) practice is committed to helping colleges, universities, and a variety of other not-for-profits carry out their missions. Our experience serving private and public higher education institutions and other charitable organizations across the U.S. allows our professionals to provide deep insights on emerging issues and trends—from financial reporting, tax, compliance, and internal controls to leading strategic, operational, technology, risk management, and governance practices. Learn more at institutes. https://institutes.kpmg.us/government/campaigns/higher-education.html

Contact us:

The KPMG HERON Audit practice

David Gagnon
National Industry Leader
E: dgagnon@kpmg.com

Rosemary Meyer
Deputy National Industry Leader
E: rameyer@kpmg.com

Regional leaders

Renee Bourget-Place
Northeast
E: rbourgetplace@kpmg.com

Rosemary Meyer
Midatlantic
E: rameyer@kpmg.com

Kurt Gabouer
Midwest
E: kgabouer@kpmg.com

Christopher Ray
West
E: cray@kpmg.com

Joseph Giordano
Metro New York and New Jersey
E: jagiordano@kpmg.com

Jennifer Hall
Southeast
E: jchall@kpmg.com

Drew Corrigan
Pacific Northwest
E: dcorrigan@kpmg.com

David Harwood
Southwest
E: dharwood@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.