On the 2020 higher education audit committee agenda

In the year ahead, college and university audit committees will again be challenged to effectively oversee their core responsibilities, as well as other risk-driven agenda items such as cybersecurity and compliance with laws and regulations. Prioritizing a heavy audit committee agenda is never easy, and 2020 will be particularly challenging. The audit committee is operating against a backdrop of changing student demand, demographics, and expectations; digitization and disruption; and greater regulatory complexity and scrutiny.

Drawing on insights from our work and interactions with higher education audit committees and senior executives, we have highlighted several areas that audit committees should keep in mind as they consider and carry out their 2020 agendas:

- Maintain (or regain) control of the committee's agenda
- Sharpen the focus on the institution's culture, ethics, and compliance programs
- Understand recent changes to federal Financial Responsibility Standards
- Continue to focus on cybersecurity
- Modernize and strengthen the back office.

Maintain (or regain) control of the committee agenda

Nearly half of the 1,300 audit committee members responding to our *2019 Global Audit Committee Survey* said it is "increasingly difficult" to oversee major risks on the committee's agenda in addition to its core responsibilities (overseeing financial reporting and related controls, as well as internal and external auditors). Aside from any new agenda items, the risks many higher education audit committees have had to contend with for some time—cybersecurity and information technology (IT), campus safety, regulatory compliance, international activities, etc.—have become more complex. More and more, this broadening risk purview is reflected not only in the committee's composition and charter but also in its name (e.g., "Audit and Institutional Risk Committee").

From an audit committee perspective, a focus on agenda management is critical. The focus should also consider the roles of other board committees—particularly finance, investments, academic affairs, and student affairs, wherein agenda overlap with the audit committee can occur—in the risk management process. Recognize that some agenda overlap is inevitable and desirable, and that risk perspectives are often enriched by audit committee members who serve on one or more of those other committees. The audit committee chair can take the lead to mitigate agenda overload and inefficiency by working with the board chair to ensure major institutional risks are assigned to and overseen by appropriate board committees. Do tangential discussions about matters better addressed by other committees consume or overtake audit committee meetings? Do priority agenda items such as executive sessions get short shrift due to time constraints? Is the audit committee satisfied with its effectiveness? Amid the myriad current challenges and emerging trends in higher education, the traditional board committee structure is increasingly challenged and may no longer align with the institution's enterprise risk program or strategy.

Reassess whether the audit committee has the expertise and time to oversee the growing categories of risks it has been assigned. Do these trends require greater attention from the full board—or perhaps a dedicated committee or subcommittee? Given their operating complexity, several comprehensive universities have established audit subcommittees to oversee enterprise risk management, IT, or other risk areas, as well as separate audit committees to oversee academic medical centers. Keeping the audit committee agenda focused will require discipline and vigilance in 2020.

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

Recent industry scandals related to admissions and rankings manipulations, faculty misconduct, and affiliations with tainted donors demonstrate that the reputational costs of an ethics or compliance failure are higher than ever. Fundamental to an effective compliance program is the right tone at the top and culture throughout the institution, which supports its strategy, including its commitment to its stated values, ethics, internal controls, and legal/regulatory compliance. In 2020, colleges and universities will contend with challenges in a number of policy risk areas, including revisions to the National Association for College Admissions Counseling's Code of Ethics and Professional Practice; major proposed revisions to federal Title IX regulations; and, for those institutions with academic medical centers, various policy and compliance risks at state and federal levels involving patient care, supply chain management, and price transparency. In today's complex, fast-paced operating environment, which often requires trustees, employees, and students to make rapid decisions considering a number of factors, the focus on ethics and compliance is critical.

Closely monitor the tone at the top and culture throughout the institution with a sharp focus on behavior (not just results) and yellow flags. Understand programmatic incentives and pressures that influence behavior, both in terms of threats and opportunities. Enlist internal audit's help in establishing key performance indicators, validating results, and offering recommendations. Does the institution's culture make it easy for people to do the right thing? Ensure the code of conduct and regulatory compliance and monitoring programs are up-to-date and that they clearly communicate the institution's expectations for high ethical standards. Are entity-wide ethics and sexual harassment training programs in place? How is compliance with such programs tracked, and what are the ramifications for noncompliance? Looking to interactions with external parties, do policies and procedures ensure that the institution avoids gifts, grants, or alliances that may run counter to its values or put its reputation at risk?

Focus on the effectiveness of whistle-blower reporting channels and investigation processes through a #MeToo lens. Does the audit committee see all whistle-blower complaints? If not, what is the process to filter complaints that are ultimately reported to the audit committee? As a result of the radical transparency and interconnectivity enabled by social media, the institution's culture and values, commitment to integrity and legal compliance, and its brand reputation are on full display.

Understand recent changes to federal Financial Responsibility Standards

In late 2019, the U.S. Department of Education (ED) issued new Financial Responsibility Standards (FRS) that establish triggering event reporting for all institutions participating in Title IV federal student financial aid programs, revise ratios used to assess financial health of private not-for-profit institutions, and establish federal standards under which borrower defense claims may be made for direct loans. The new rules become effective July 1, 2020. Previously, public colleges and universities were exempt from FRS. However, *all* institutions participating in Title IV programs will now be required to inform ED of certain specified triggering events (e.g., judgment or settlement arising from an action by a state or federal entity), generally within 10 days of their occurrence. Importantly, there is *no* materiality threshold for such events. Accordingly, all institutions should familiarize themselves with the triggering events. The audit committee should ensure that the institution implements protocols to timely identify and communicate such events and that general counsel is involved.

The impetus for revising the ratios—which result in a composite financial score for each private institution—stems from erroneous or manipulated ratio calculations in prior years, as well as the effects of certain accounting standards issued since ED originally established FRS in 1998. Those standards include the Financial Accounting Standards Board's Accounting Standards Update (ASU) 2016-14, *Presentation of Financial Statements of Not-for-Profit Entities* (adopted in 2019 by most institutions) and ASU 2016-02, *Leases* (effective in fiscal 2020 for most institutions), which we have discussed extensively in prior agenda publications. In addition, changes in accounting for endowments and defined benefit obligations have occurred over time.

For each ratio, the regulation requires the use of certain financial elements—some of which may not currently be reported in the institution's audited financial statements—to be presented in a supplemental schedule that is cross-referenced to the financial statement line items or notes containing the elements. Both the schedule and any expanded financial statement information must be covered by the independent auditors' report. Accordingly, private institutions should review their current financial statements and related notes to completely and accurately determine information that will need to be added for FRS purposes. Instead of revising their general-distribution annual financial reports to meet ED's new requirements, institutions may consider incorporating the required additional information and schedule in the financial statement section of the reporting package submitted annually to the federal government under the Uniform Guidance.

ED's new rules exemplify the heightened regulatory focus on higher education amid recent closures and mergers in the industry. In January 2020, the Massachusetts Board of Higher Education approved a new set of regulations governing how the state screens private colleges and universities for indications of financial stress and potential closure. The rules require, among other things, that trustees at private institutions in the state receive training in higher education metrics, legal/fiduciary responsibilities, and accreditation standards. It remains to be seen whether other states will institute requirements similar to those in Massachusetts. Nevertheless, calls for greater financial transparency are likely to increase expectations about what college and university trustees should know, as well as the ongoing regulatory burden for all institutions (regardless of financial profile). The audit committee can play a role by ensuring management stays on top of any new requirements to facilitate compliance.

Continue to focus on cybersecurity

Audit committees have made strides in monitoring management's cybersecurity effectiveness—for example, through greater IT expertise on the committee, institution-specific dashboard reporting highlighting critical risks, and more robust conversations with senior executives about cybersecurity risks, operational resilience, and the strategies and capabilities that management has deployed to minimize the duration and impact of a serious cyber breach. Despite these efforts, amid the growing sophistication, motivation, and prevalence of cyber attackers, cybersecurity will continue to be a key challenge. Audit committees should understand the areas in which the institution is most vulnerable and the processes in place to respond to a cyberattack.

In higher education, there is a continuing focus on virtual as well as physical privacy and security. While significant progress has been made, the industry as a whole continues to lag some others in terms of information security resources, spend, and policy authority and administration; compatible technologies that can be centrally supported; and contemporary security protocols (e.g., two-factor authentication, which is still relatively new to some institutions). This is complicated by the traditionally more open and decentralized IT environments at many college and university campuses, where students, faculty, and others share information and various systems and devices are outside the domain of the central IT function: depending on the environment, a single rogue laptop lacking up-to-date security software can cause major disruption to an institution's network capabilities. Also adding to the complexity are a number of recent regulations, e.g., GDPR, NIST, etc., making cybersecurity a compliance management challenge. In the virtual arena, we believe audit committees should focus on five key areas:

1. Digital extortion/ransomware
2. General cyberattacks
3. Accidental mishandling of data and security training
4. Third-party cyber risk from vendors, joint ventures, and affiliated organizations
5. Medical device security (for those with clinical or academic medical center activities).

In terms of physical security and the increasing number and type of facilities maintained, especially at larger universities, focus on visitor management and related crisis response planning. Understand how management is protecting server-based technologies and data and whether systems are moving to the cloud where feasible. Is the audit committee reassessing the institution's changing risk profile—and the adequacy of risk controls—on a regular basis? Remember that cybersecurity is as much a people issue—for whom awareness and education are key—as it is a technology issue. Lastly, ensure that cybersecurity is always a function of the *institutional strategy* and not merely an IT function.

Modernize and strengthen the back office

Driven by the continued need to improve efficiency, productivity, and performance—ultimately to enhance mission-centric objectives involving the student experience, research enterprise, and patient care—institutions are looking to modernize back office functions across many areas, including finance, procurement, human resources (HR), IT, supply chain, and internal audit. These initiatives are affected by advancements in technology and data governance, new regulations, and changing work force expectations. In addition, more institutions are looking outside the higher education and healthcare industries for models to provide data to internal and external stakeholders better, faster, and cheaper. What are the core tenets of technology investment and deployment that management is leveraging? How are institutions changing the structure of the workforce to enable agile working? What is the approach to enhancing the employee experience? Is the institution committed to modernizing consistently across the back office and not just in silos to support real-time decision-making?

The audit committee should understand how technology is impacting finance and internal audit's efficiency and ability to add value. As opposed to merely enhancing the institution's legacy business practices, the latest enterprise resource planning solutions for HR, payroll, finance, and student management are designed to dramatically alter how the institution does business. Do senior administrators have plans to (a) deal with the disruption and transformation that process owners around the institution will experience during the

implementation and (b) take full advantage of new system functionalities provided to automate, centralize, and control key activities? Understand how the "day jobs" of employees directly involved in the implementation will be impacted. How are historical policies, procedures, and controls affected by revised or new business processes resulting from the implementation? The chief business officer (CBO) can take the lead to inventory and update these items as changes occur, and the chief audit executive (CAE) can review the results to assure policy consistency and a smooth workflow moving forward. As no implementation is perfect, continue to ask for periodic reports on system and process performance well after the implementation goes live.

As audit committees monitor and help guide progress in the area of technology transformation moving forward, we suggest three areas of focus. First, recognizing that as much as 60 to 80 percent of finance's work involves data gathering, what are the institution's plans to leverage intelligent and cloud technologies to automate manual activities? Second, how will data analytics and artificial intelligence (AI) be used to develop sharper predictive insights, better deployment of capital, and more effective audits? The finance and internal audit functions are well-positioned to guide the institution's data and analytics agenda and to consider the implications of new transaction-related technologies. Do finance and internal audit have the tools and training to identify anomalies or other meaningful trends in analyzed data? Third, as the finance function combines strong analytics and strategic capabilities with traditional financial reporting, accounting, and auditing skills, its talent and skillset requirements must change accordingly. Is finance attracting, developing, and retaining the talent and skills necessary to match its evolving needs?

Finally, we would be remiss not to mention the continuing importance of having the right people and succession planning in place in finance and internal audit. Despite efficiency gains from enabling technologies, today's vastly more competitive, fast-changing, and data-driven higher education environment means college administrators will continue to have more on their plates and require the assistance of staff who are able to leverage the institution's new business capabilities. Accordingly, as mundane tasks fall by the wayside, expect the personnel compliment to be more specialized and adaptable. The audit committee can help by asking the CBO and CAE about the depth of talent and experience in the organization chart, especially under key positions, and plans to address any gaps. If the CBO or CAE were no longer in their roles, who would be ready to assume their responsibilities?

Contact us

KPMG's Higher Education, Research & Other Not-for-Profits Audit Practice

David Gagnon
National Industry Leader
T: 617-988-1326
E: dgagnon@kpmg.com

Rosemary Meyer
Deputy National Industry Leader
T: 410-949-8425
E: rameyer@kpmg.com

Regional Leaders

Renee Bourget-Place
Northeast
T: 802-651-5634
E: rbourgetplace@kpmg.com

Joseph Giordano
Metro New York and New Jersey
T: 212-872-4382
E: jagiordano@kpmg.com

Rosemary Meyer
Mid-Atlantic
T: 410-949-8425
E: rameyer@kpmg.com

Jennifer Hall
Southeast
T: 336-433-7117
E: jchall@kpmg.com

Kurt Gabouer
Midwest
T: 312-665-3308
E: kgabouer@kpmg.com

Drew Corrigan
Pacific Northwest
T: 503-820-6629
E: dcorrigan@kpmg.com

Mark Thomas
West
T: 949-885-5630
E: mtthomas@kpmg.com

David Harwood
Southwest
T: 214-840-6404
E: dharwood@kpmg.com

kpmg.com/socialmedia