On the 2024 higher education audit committee agenda

January 2024

In 2023, nearly two years removed from the unprecedented disruption of the pandemic, colleges and universities confronted several emerging challenges amid a fast-changing industry landscape. A growing public distrust of higher education was reflected in an increasingly adversarial political climate; rising unrest on campuses; a backlash against diversity, equity, and inclusion (DEI) programs; and proposals that would impose additional taxes and prohibit federal student loans at institutions subject to the federal endowment excise tax.

The sector enters 2024 contending with various of other ongoing risks, including accelerating cybersecurity threats, lingering inflation, hiring and retention challenges, high interest rates, intensifying geopolitical instability, and growing regulatory burdens. Moreover, 2024 is widely considered the largest and potentially most consequential global election year in history and could further shape how these evolving issues impact institutions—from federal and state funding to achievement of environmental, social, and governance (ESG) initiatives. Once again, boards of trustees and audit committees will need to refine—or possibly even redefine—their risk-driven agendas.

Colleges and universities can expect their financial reporting, compliance, risk, and internal control environments to be tested by an array of challenges in the year ahead. The magnitude, complexity, and velocity of many institutional risks—and often their unexpected interconnectedness—will require more holistic risk management, as well as effective oversight by the audit committee. In this volatile operating environment, demands from regulators, creditors, and other stakeholders for appropriate action, disclosure, and transparency will only 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 2024 agendas:

- **Keep a watchful eye on the institution's management of cybersecurity and data governance risks.**
- **Define the audit committee's oversight responsibilities for artificial intelligence (AI).**
- **Understand how the institution is managing ESG risks and potentially applicable regulations.**
- **Monitor other emerging regulations and standards impacting the institution.**
- **Stay focused on leadership and talent in finance and other functions.**
- **Help ensure internal audit is attentive to the institution's key risks and is a valuable resource for the audit committee.**
- **Sharpen the institution's focus on—and connectivity of—ethics, culture, and compliance.**

Keep a watchful eye on the institution's management of cybersecurity and data governance risks

In United Educators' Top Risks survey of colleges and universities conducted in fall 2023, data security overtook enrollment as the top risk in higher education.[1] This risk ranking is not surprising given several recent ransomware and other cyberattacks in the sector. In many of these cases, hackers effectively blackmail institutions by threatening to release sensitive data or not allowing them to regain control of data or networks unless ransom payments are made. Indeed, in prior *On the Higher Education Audit Committee Agenda* publications, we have cited surveys indicating that cyberattacks across all industries are increasing and that education and research entities are attacked more frequently than any other industry. Cyber threats continue to proliferate, with cybercriminals using more sophisticated techniques and technologies, including AI. As institutions work diligently to enhance their cybersecurity infrastructures, bad actors are moving more quickly.

When evaluating susceptibility to cyber threats at colleges and universities—even at institutions with more mature cybersecurity programs—some common themes emerge: (1) significant endowment portfolios, research enterprises, and academic medical centers are high-value targets; (2) implementing entity-wide protective measures can be complicated in the decentralized operating environments of some larger universities, where an assortment of IT systems that are not fully up-to-date or patched may exist; (3) cyber spending, staffing, and board expertise in the sector continue to lag commercial industries; (4) numerous privacy and security regulations need to be managed, including the Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act Safeguards Rule (GLBA), National Institute of Standards and Technology (NIST) Cybersecurity Framework, and the European Union's (EU's) General Data Protection Regulation (GDPR); and (5) users connecting to or working in the institution's systems—from faculty, staff, and students to donors, grantors, and patients—are diverse and far-reaching.

While these users often make important financial and strategic contributions to the institutional mission, their wide-ranging interests, technical expertise, and levels of security awareness can make implementing cybersecurity protocols challenging. To mitigate these issues, institutions must be willing to embrace cutting-edge security solutions, including security awareness training, across multiple platforms. An October 2023 EDUCAUSE report[2] indicated that although 90% of college and university respondents mandate security awareness training for employees, training design and frequency vary, and only 38% say it is effective or very effective. Far fewer respondents indicated that students or other stakeholders are regularly trained or that individuals who fail phishing tests must undergo additional training. Respondents also noted that while training covers federal regulations such as FERPA and HIPAA, institutional privacy and data governance policies are often excluded.

Institutions should ensure that security awareness programs are tailored to and deployed across stakeholder groups and incorporate means to measure and monitor effectiveness. Mapping the evolving requirements of multiple security and data governance frameworks to the institution's cybersecurity program—as well as educating and monitoring compliance of applicable stakeholders—is also essential.

Colleges and universities can further enhance their cybersecurity protocols by:

- *Narrowing the scope of access to secure systems*. System access should be limited 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.
- *Deploying, tailoring, testing, and refining baseline tactics.* This may mean more frequent vulnerability assessments and penetration testing, "red teaming" (which tests how the security team responds to various threats), and system backups, as well as refreshing incident response plans more regularly.
- *Developing a comprehensive response policy for ransomware*. Institutions should have a firm stance on whether to pay—or not pay—ransom before systems are compromised. Purchasing ransomware insurance, if possible, is key to preparation, as is identifying who will make the ultimate payment decision if a breach occurs.
- *Establishing minimum cybersecurity standards for all vendors and other third parties with whom the institution does business, and regularly monitoring them*. As a practical matter, those entities may also ask about the institution's cyber program.
- *Understanding third-party vendor risks associated with cloud-based systems that create new access points to sensitive data*. Such vendors require regular vulnerability assessments, and their internal controls should have independent assurance from auditors through service organization controls (SOC) reports (which should be reviewed by the institution).

[1] United Educators, *2023 Top Risks Report: Insights for Higher Education*, 2023.

[2] EDUCAUSE *QuickPoll Results: Growing Needs and Opportunities for Security Awareness Training*, October 30, 2023.

The audit committee can help ensure the institution has a rigorous cybersecurity program by considering the following questions:

- Do we have clear insights into our cybersecurity program's current maturity, gaps, and threats, including whether the institution's most "valuable" assets are adequately protected? Does leadership have a prioritized view of additional investments needed? Measurement may be facilitated by guidance from, for example, the federal Cybersecurity and Infrastructure Security Agency (CISA) and the not-for-profit Center for Internet Security (CIS), who provide self-assessment tools such as *Stop Ransomware and the CIS Top 18 Critical Controls*, respectively. The CIS database also allows for benchmarking against other colleges and universities.
- Do we have the appropriate leadership, talent, and bench strength to manage cyber risks? In the event of unexpected turnover or inability to fill key positions, what are the risks to the institution?
- 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 and risk?
- Do we regularly test our incident response plan? Does our plan include up-to-date escalation protocols that, among other things, specify when the board is informed of an incident? What is the frequency of penetration and red team testing, 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? How does our framework intersect with our AI governance policy?
- Is security, privacy, and data governance training for students, faculty, staff, and other stakeholders regularly provided? Is training completion and effectiveness monitored and enforced? How is security awareness periodically assessed?
- Do security and privacy terms in agreements with third-party information technology (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 identifying changes to 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?

Define the audit committee's oversight responsibilities for AI

In just a few short years, AI has gone from being the purview of a select group of tech leaders to becoming nearly ubiquitous across finance teams. According to the KPMG 2023 AI in Financial Reporting survey, 65% of organizations across industries are already using AI in some aspects of their financial reporting, and 71% expect AI to become a core part of their reporting function within the next three years. Still, while business leaders are eager to explore the different capabilities that AI—and generative AI in particular—can bring to their organizations, many are taking a slow and steady approach to adoption. According to our survey, 37% of finance leaders are still in the planning stages of their generative AI journeys.

Although the emergence of generative AI in higher education is frequently considered in an academic context—where it remains both a threat (e.g., academic dishonesty) and opportunity (e.g., online education)—AI also has tremendous potential to transform finance and other administrative processes at colleges and universities. A 2023 EDUCAUSE survey found that 83% of college and university respondents believe that "generative AI will profoundly change higher education in the next three to five years," and that 65% believe its use has "more benefits than drawbacks."[3] According to Inside Higher Ed, several institutions—in part through funding from federal, state, and private grants—have made significant investments in AI to support research, education, and workforce initiatives, with some building large-scale AI centers.[4] And while generative AI is already being used throughout the sector in various applications (for example, chatbots in IT and enrollment support systems), its potential to enhance a wide range of tasks, processes, and services is growing rapidly.

Optimizing certain AI solutions requires a robust enterprise resource planning system (ERP), as well as personnel with appropriate institutional knowledge and skill sets. Entities with legacy ERPs and siloed administrative staffing may lack the computing capacity—and skill sets—necessary to take advantage of all that AI has to offer. In addition, many higher

[3] EDUCAUSE *QuickPoll Results: Adopting and Adapting to Generative AI in Higher Ed Tech*, EDUCAUSE REVIEW, April 17, 2023.

[4] Inside Higher Ed, *Risks and Rewards as Higher Ed Invests in an AI Future*, September 5, 2023.

education institutions are currently replacing their finance, human capital management, and student information systems to transform core business processes. Such institutions may benefit from a more measured approach to AI adoption that considers how AI fits into their overall transformation strategy.

Examples of how college and university administrative teams might leverage AI moving forward include:

- Filtering and combining data sets, e.g., transactions and payment methods, to identify trends.
- Further automating processes such as payroll, purchasing, and related user-support systems.
- Combing through large swaths of public data that provide market insights and competitive intelligence to support marketing, admissions, fundraising, and other strategies.
- Analyzing anomalies to control budget variances, spot fraud, and facilitate internal audits.
- Developing dynamic budgeting and forecasting models to sensitize projections for any number of internal and external variables.

As noted in the KPMG *On the 2024 Board Agenda*, oversight of generative AI should be a priority for boards in 2024, including how to oversee generative AI at the full-board and committee levels. Handing over decision-making to a machine is no small undertaking. Any number of issues—from biased data to algorithmic errors—can result in the technology making mistakes that can affect an entity's analysis, revenue, forecasts, or even its reputation. But for leaders who make the effort to put the right controls in place around AI, the benefits can outweigh the risks.

The audit committee may end up overseeing the institution's compliance with the patchwork of differing laws and regulations currently governing generative AI, as well as the development and maintenance of related policies and internal controls. Some audit committees may have broader oversight responsibilities for generative AI, including overseeing various aspects of the entity's governance structure for the development and use of the technology. How and when is a generative AI system or model—including a third-party model—developed and deployed, and who makes that decision? What generative AI risk management framework is used? Does the institution have the necessary generative AI-related talent and resources? How do we ensure our adoption of AI is ethically responsible and aligned with the institution's culture? Do we have clear AI governance and AI security policies? Have we determined how those should link to our data governance and cybersecurity programs?

Given how fluid the situation is—with generative AI gaining rapid momentum—the allocation of oversight responsibilities to the audit committee may need to be revisited.

Understand how the institution is managing ESG risks and potentially applicable regulations

For many institutions, ESG has become a board-level imperative, reflecting and aligning with the entity's mission, values, goals, and reputation. Colleges and universities face increasing stakeholder demands—from board members, creditors, and local communities to students, faculty, and donors—for ESG data, particularly around DEI and climate impacts. In 2023, several long-simmering threats that could impact these ESG priorities emerged against the backdrop of a polarized political environment: the Supreme Court's decision to end race-conscious admissions, allegations that antisemitism is tolerated on college campuses while ideological differences are not, and a backlash against DEI resulting in the elimination of diversity offices at several public institutions. These and similar challenges are likely to continue in 2024, although the ESG reporting landscape is expanding beyond the realm of public companies to cover more entities and disclosures.

In our experience, although some 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. Many are still inventorying existing ESG activities and considering how to develop a comprehensive ESG approach. At all stages, there is ample room for agreement and alignment on ESG definitions and a critical need for quantitative, reliable data. Still, the absence of a generally accepted ESG framework in the sector (as in most other industries) 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 remains uncertain. Media reports have been dominated by the Securities and Exchange Commission's (SEC) March 2022 climate reporting proposal, under which public companies would report direct and indirect emissions, including those generated through supply chains and affiliates. The proposal has met with resistance by registrants and lawmakers, and a final ruling has not yet been issued. While the SEC does not directly regulate the higher education sector, its oversight of public debt markets includes conduit offerings by colleges and universities (although proposed rulemaking to date does not apply to such offerings). Nevertheless, many institutions have begun including sustainability data in their offering documents, issuing reports on climate and DEI factors in their endowment management, and sharing ESG information with bond rating agencies (who consider ESG risks in ratings reports).

In addition, there are other complex and extensive climate and sustainability reporting laws—applying to both public and private entities—that require consideration:

- On October 7, 2023, the governor of California signed three disclosure laws that will shape climate reporting far beyond the state's borders:
  - Effective in 2026 (2025 data), Climate Corporate Data Accountability Act (SB-253) mandates the disclosure of greenhouse gas emissions;
  - Effective on or before January 1, 2026, Climate-Related Financial Risk Act (SB-261) mandates the disclosure of climate-related financial risks and measures adopted to reduce and adapt to such risks; and
  - Effective on January 1, 2024, the Voluntary Carbon Market Disclosures Act (AB-1305) introduces disclosure obligations related to voluntary carbon offsets and emissions reduction claims.

  The laws are based on whether an entity does business or operates in California—not whether it is physically present in the state—and meets specified revenue thresholds (SB-253 and SB-261). The California Air Resources Board has been tasked with developing and adopting regulations to implement SB-253 and SB-261.
- The EU's Corporate Sustainability Reporting Directive (CSRD) amends and significantly expands existing EU requirements for sustainability reporting and has considerable ESG reporting implications for U.S. companies with physical presence and revenue in the EU meeting certain criteria. Determining which entities are in the scope of the CSRD is complex.

There is much to resolve in terms of how these laws will be implemented. Moreover, it is currently unclear whether or how colleges, universities, and other not-for-profits with activities in California or the EU could be impacted by or exempted from the requirements.

Oversight of an entity's ESG activities is a formidable undertaking for any board and its committees. In the corporate sector, the nominating or governance committee often takes the coordinating role, with the audit committee often overseeing internal controls, disclosure controls, and ESG disclosures. Although standards and practices affecting higher education institutions will continue to evolve—including as to the roles of governance and auditors in the process—audit committees should encourage management to inventory and assess the scope, quality, and consistency of ESG disclosures. In the public sector, the focus is often on determining what data needs to be collected, processes for collecting the data and ensuring the data is reliable (including related controls). This evaluation should consider available methodologies and standards; how the institution is defining metrics; understanding expectations of creditors, donors, and other stakeholders; and the appropriateness of the ESG reporting framework(s) for the institution.

The audit committee should ask:

- Does the institution have an ESG or similar strategy, and who is responsible for its execution?
- How are material ESG risks identified? Are these risks appropriately reflected in the institution's enterprise risk management (ERM) profile?
- Does or should the institution utilize an ESG reporting framework? Do we have metrics to measure progress against stated goals, and how are they defined? Who within the institution is responsible for generating and tracking ESG data and ensuring its quality and conformity with applicable standards?
- Have we enlisted faculty with ESG expertise to help us think through our strategy and framework?

- As the institution's reputation is on the line, understand where ESG information is currently disclosed—e.g., the institution's website, and the Sustainability Tracking, Assessment & Rating System (STARS), a higher education reporting tool used by hundreds of institutions. Do such disclosures have consistency to the extent they appear in multiple communication channels? What policies and procedures are in place to ensure the quality of data used? Are such disclosures reviewed with the same rigor as financial results? Do (or should) we obtain assurance from internal or external auditors about our ESG data to provide our stakeholders with a greater level of comfort? Who are the stakeholders accessing such information, and what mechanisms exist for them to ask questions and provide feedback about our results?
- How are we keeping pace with industry-leading practices around ESG and the plethora of regulations that could require us to make ESG disclosures in the future?
- Clarify the role of the audit committee in overseeing the institution's reporting of ESG risks and activities, particularly the scope and quality of ESG disclosures. How are the full board and other committees involved in overseeing ESG initiatives?

Monitor other emerging regulations and standards impacting the institution

U.S. Department of Education (ED) enhanced disclosures. On October 31, 2023, ED amended Title 34 Part 668 of the Code of Federal Regulations (CFR) relating to standards for institutions participating in federal student aid programs, effective July 1, 2024. Among other actions, the CFR retains and reaffirms a requirement, dating back to the 1990s, for institutions to report *all* individual related-party transactions in the audited financial statements they file with ED annually.

Over the last few years, ED has increasingly rejected annual filings deemed to have missing or incomplete related-party data. ED's requirement uses the same related-party definition as U.S. generally accepted accounting principles (GAAP). However, that definition is increasingly complex and wide-ranging, and includes, for example, officers, board members, donors, and their immediate family members, and financially interrelated entities. And whereas GAAP allows financial statement preparers to consider the materiality and specificity of related-party information to be disclosed—including the related-party's identity—ED requires, at a minimum, disclosure of the names, locations, and descriptions of all related parties and the nature and amount of any transactions, financial or otherwise, between those parties and the institution, regardless of when they occurred. The regulation states that de minimis routine transactions need not be considered for disclosure purposes. However, ED cites only lunches or meals for trustees as an example, and it is unclear which, if any, other transactions may also be de minimis.

Given ED's heightened focus on related-party reporting, the audit committee should understand and monitor how the institution will meet ED's requirements. Questions to be asked include: Do we understand the term "related party" in the context of ED's mandate and GAAP? Do we have the systems, processes, and internal controls necessary to capture and evaluate the information needed to comply? Have we considered the implications of personally identifiable information in required disclosures? Such considerations may be complicated and will need to be carefully assessed and perhaps even discussed with those who could be affected. Are we working closely with legal counsel and our auditors as we navigate the issues? Do we understand how a rejected ED filing could impact the institution? The institution should also monitor and consider any guidance provided by the American Institute of Certified Public Accountants, as well as any future clarifying guidance by ED.

Accounting for credit losses. The Financial Accounting Standards Board's (FASB) Accounting Standards Update (ASU) 2016-13—*Financial Instruments—Credit Losses (Topic 326): Measurement of Credit Losses on Financial Instruments*, as amended, is effective for private entities—including

colleges, universities, and other not-for-profits (NFPs) applying FASB guidance—for fiscal years beginning after December 15, 2022 (fiscal 2024 for most higher education institutions). While certain instruments are excluded from the scope of the ASU—such as receivables from donors and federal research sponsors accounted for as contributions under FASB Topic 958, as well as loans and receivables between entities under common control—the ASU applies to most financial assets measured at amortized cost, such as student and patient care accounts receivable, loans and notes receivable, as well as programmatic loans made by NFPs.

Under existing standards, a credit loss is recognized when it is probable it has been incurred (generally after inception of the asset). By contrast, the ASU requires—generally upon inception of the asset—recognition of losses expected over the contractual term of the asset, even if the risk of loss is currently remote. Accordingly, an entity's process for determining expected losses in accordance with the ASU considers not only historical information, but also current economic conditions and reasonable and supportable forecasts about future conditions (with reversion to historical loss information for future periods beyond those that can be reasonably forecast).

Accounting for crypto assets. Crypto assets have gradually gained acceptance in higher education, particularly as a mode for donor payments and as investments. Colleges and universities applying FASB guidance may already reflect such assets held directly—or indirectly through underlying investment funds—at fair value in their financial statements. FASB's ASU 2023-08, *Accounting for and Disclosure of Crypto Assets*, introduces Subtopic 350-60, which addresses accounting and disclosure requirements for certain crypto assets. The guidance is effective for all entities in fiscal years beginning after December 15, 2024 (fiscal 2026 for most higher education institutions). Under the ASU, holdings of crypto assets that are within the scope of the ASU, such as bitcoin and ether, are measured at fair value and subject to certain presentation and disclosure requirements.

- Under Topic 958, in-scope crypto assets may qualify to be presented as part of investments in the institution's statement of financial position and related investment return in the statement of activities, subject to certain disclosures. However, in-scope crypto assets cannot be combined with other intangible assets and related changes therein if the institution reports such line items in the statements of financial position and activities, respectively. The ASU does not address classification of fair value changes of in-scope crypto assets in the statement of activities. Accordingly, institutions may present such changes within operating or nonoperating activities depending on the institution's policy and consistent with whether such changes are presented as part of investment return.
- In the statement of cash flows, cash receipts from the near-immediate liquidation of donated crypto assets are classified as financing activities if donor-restricted for long-term investment or capital purposes, or as operating activities if no such donor restrictions are imposed.
- Required disclosures for each significant crypto asset holding include name, cost basis and method used, fair value, and number of units, and, subject to certain exceptions, information about changes in such holdings during the year. Additional disclosures are also required for holdings subject to contractual sale restrictions as of the statement of financial position date. For holdings that are not individually significant, aggregate cost basis and fair value information can be presented.

Stay focused on leadership and talent in finance and other functions

For the second year in a row, recruitment and hiring ranked third in United Educators' Top Risks Survey of higher education institutions in 2023.[5] At some institutions, budget constraints, in-person staffing models, and an aging demographic in senior roles continue to contribute to this risk. While pressures

[5] United Educators, *2023 Top Risks Report: Insights for Higher Education*, 2023.

have abated somewhat, in 2024 college and university leaders may be contending with talent shortages in certain finance, IT, risk, compliance, and internal audit roles just as they refocus on strategies to transform the institution's business processes. The audit committee can help ensure that finance and administrative executives have the leadership, talent, and bench strength to support those strategies while maintaining their core operating responsibilities.

To help monitor and guide the institution's progress, we suggest the audit committee consider the following questions:

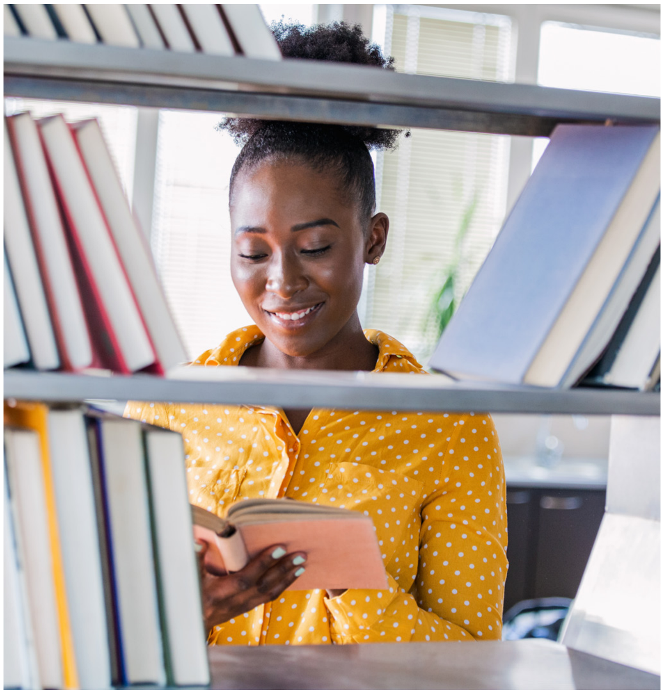
- Although changes to modes of working (i.e., remote, hybrid, and in-person) have largely stabilized in the industry, competition for talent in some functions and regions remains challenging, especially at institutions limited by traditional compensation structures. While bolstering recruitment and retention efforts may result in higher costs—which could add financial strain to the institution—employee workloads and morale, as well as internal controls, could be adversely impacted if vacant positions are not filled. Does the audit committee understand how the institution is managing, particularly as to specialized roles in IT, compliance, and other areas?
- Do we have the appropriate infrastructure to monitor and manage the tax, compliance, culture, and cybersecurity ramifications of remote work arrangements?
- Are finance and other administrative functions attracting, developing, and retaining the talent and skills we need to match their increasingly sophisticated digitization and other transformational strategies?
- Do our 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?

Help ensure internal audit is attentive to the institution's key risks and is a valuable resource for the audit committee

Internal audit can and should be a valuable resource for the audit committee and a critical voice throughout the institution on risk and control matters. This requires focusing not only on financial reporting, compliance, and technology risks, but also key strategic, operational, and reputational risks and controls. Just as the audit committee is grappling with increasingly weighty and rapidly changing agendas, the scope and urgency of internal audit's areas of focus are growing. Is internal audit's annual plan risk-based and flexible, and does it adjust to changing business and risk conditions? Internal audit must be able to effectively pivot to address unanticipated issues and risks as well as ongoing institutional risks highlighted in the 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, including culture and tone at the top; cybersecurity, data governance, and IT enhancement; emergent uses for AI, including generative AI, in administrative and academic processes; workforce and wellness issues; research compliance and conflict risks; international activities; third-party risks; integrity of data used for ESG and ranking purposes; and other risks. Expect the latest internal audit plan to reflect these emerging issues and reaffirm that the plan can adjust to changing conditions. Mapping internal audit's areas of focus to the institution's 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. Clarify internal audit's role in connection with the ERM program—which is not to manage risk, but to help the institution assess the adequacy of its risk management processes. Does internal audit have the talent it needs in IT and other focus areas? Recognize that internal audit is not immune to talent pressures. In addition, help the chief audit executive think through the impacts of new technologies, including AI—such as generative routines and dashboards used for risk assessment and real-time auditing—on internal audit's workload and effectiveness.



Sharpen the institution's focus on—and connectivity of—ethics, culture, and compliance

In the current higher education environment, the reputational costs of an ethical breach or compliance failure are higher than ever. In addition, fraud risks caused by financial and operational pressures—from employee hardships and phishing scams to unrealistic goals involving enrollment or rankings targets—are expanding. Fundamental to an effective compliance program is the right tone at the top and culture. In the decentralized operating environments of comprehensive universities, where navigating myriad regulatory and ethical considerations related to research and patient care, innovation and commercialization, and intercollegiate athletics is increasingly complicated, reinforcement of these imperatives throughout the institution is essential.

With the radical transparency enabled by social media, the institution's commitments to integrity and other core values, legal compliance, and brand reputation are on full display. The audit committee should closely monitor tone at the top and 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 faculty and staff 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 all employees?
- 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 evaluate complaints that are ultimately reported to the audit committee?

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 various 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 https://institutes.kpmg.us/government/campaigns/higher-education.html

Contact us

The KPMG HERON Audit practice

David Gagnon
U.S. Sector Leader
E: dgagnon@kpmg.com

Rosemary Meyer
Deputy U.S. Sector Leader
E: rameyer@kpmg.com

Regional leaders

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

Rosemary Meyer
Midatlantic
E: rameyer@kpmg.com

Cathy Baumann
Midwest
E: cbaumann@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

Susan Warren
Southwest
E: smwarren@kpmg.com

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

Learn about us: in | **kpmg.com**

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.