

WEDNESDAY, FEBRUARY 21, 2024
LEGAL, AUDIT, RISK AND COMPLIANCE COMMITTEE MEETING

Elizabeth P. Kessler, chair
Michael Kiggin, vice chair
Alan A. Stockmeister
Jeff M.S. Kaplan
Elizabeth A. Harsh
John Jose Perez
Bradley R. Kastan
Joshua H.B. Kerner
Amy Chronis
Hiroyuki Fujita (*ex officio*)

Location: Sanders Grand Lounge, Longaberger Alumni House
2200 Olentangy River Road, Columbus, Ohio 43210

Time: 12:00-2:00pm

Public Session

ITEMS FOR DISCUSSION

1. *External Audit Update – Mr. David Gagnon* 12:00-12:10pm
2. *Internal Audit Quality Assurance Program – Mr. Kevin Patton* 12:10-12:20pm
3. *Office of Government Affairs Update – Ms. Stacy Rastauskas* 12:20-12:30pm
4. *Information Security Update - Ms. Cindy Leavitt, Mr. Rich Nagle, Mr. Tom Bentley, Mr. Tre Smith* 12:30-12:35pm

ITEMS FOR ACTION

5. *Approval of November 2023 Committee Meeting Minutes – Ms. Elizabeth Kessler* 12:35-12:40pm

Executive Session

12:40 – 2:00pm

Meeting of the Legal, Audit, Risk and Compliance Committee (LARC), February 21, 2024

Following are highlights of our more detailed read-ahead materials

- **Fiscal 2024 audit plan**
 - Scope of entities included
 - Team and timeline
 - Risks and estimates identified
 - Other required communications
 - New accounting pronouncements
- **Results of fiscal 2023 Single Audit**
 - Unmodified opinions on six major programs
 - No noncompliance or internal control findings reported
- **Fiscal 2024 Single Audit plan**
 - Identification and selection of major programs underway
 - Significant interim testing planned
- **Industry emerging issues**



The Ohio State University

**Discussion with those charged with governance
Audit plan and strategy for the year ending June 30, 2024**

February 21, 2024

Key themes for our discussion



Modernizing the audit experience



Enhancing your experience



Scope of the audit



Required communications



Audit Committee insights



Key risks and our Audit Plan

Continuous improvement powered by transformation

Our investment: \$5B

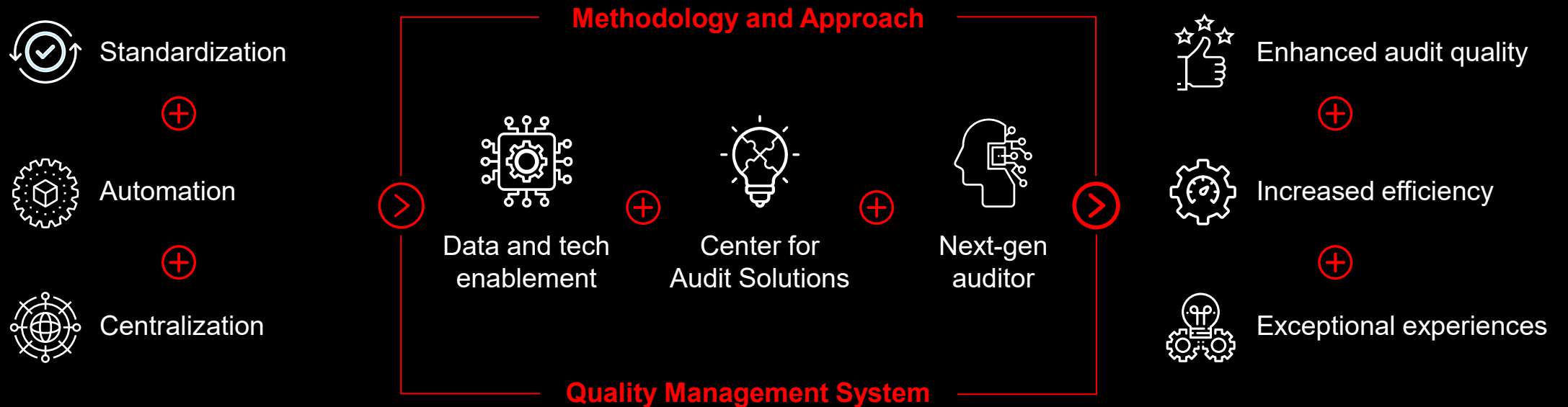
We are in the midst of a five-year investment to develop our people, digital capabilities, and advanced technology.

Responsive delivery model

Tailored to you to drive impactful outcomes around the quality and effectiveness of our audits.

Result: A better experience

Enhanced quality, reduced disruption, increased focus on areas of higher risk, and deeper insights into your business.



Cybersecurity considerations

Factors and forces elevating cybersecurity risks:

- Shifts to remote work, online customer engagement, digital finance – “remote everything”
- Acceleration of digital strategies/transformation
- Surge and sophistication of cyber attacks
- Risks, vulnerabilities posed by third-party vendors

Your considerations for robust oversight

- Focus on internal controls, access, and security protocols
- Increase diligence around third-party vendors
- Insist on a robust data governance framework
- Obtain cyber expertise at board or upper management level
- Provide ongoing cyber awareness training to leaders in the company
- Trust but verify the information reported by the Chief Information Officer function and by third-party cyber service providers

Our audit responsibilities

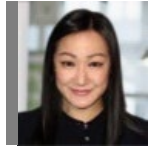
- Evaluate risks of material misstatement resulting from, among other things, unauthorized access to financial reporting systems (e.g., IT applications, databases, operating systems)
- Determine whether there is a related risk of fraud
- Develop audit approach based on risk assessment
- If a cybersecurity incident occurs, we understand and evaluate its effect on our audit approach, as well as evaluate management’s assessment of the effect on the financial statements and disclosures



The OSU engagement team



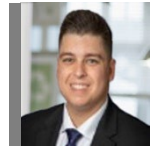
Dave Gagnon
Lead Engagement Partner
National Industry Leader –
Higher Education



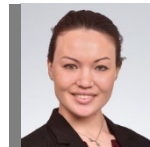
Jane Kim
Lead Senior
Manager



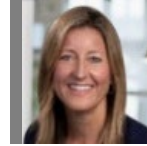
Sawyer Smith
Investments
Manager



Darryn Bradt
Investments
Senior Associate



Madelyn Fowle
University Senior
Associate



Kim Zavislak
Account Executive
Columbus Office
Managing Partner



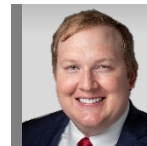
Rosemary Meyer
University and Components
Engagement Quality Control
Review Partner



Amy Banovich
Healthcare Entities
Engagement Quality
Control Review Partner



Chase Gahan
Components Managing
Director



Creed Rogers
Components Manager



Cathy Baumann
University and Single
Audit Partner



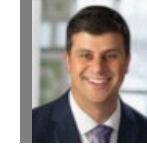
Gina Devine
Single Audit Senior
Manager



Hilda de la Cuesta
Uniform Guidance
Senior Associate



Johnny Lewis
Healthcare Entities
Partner



Robby Perry
Healthcare Entities
Senior Manager



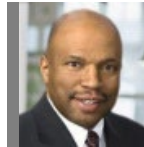
Kody Seeger
Healthcare Entities
Manager



Sidney Arnold
Healthcare Entities
Senior Associate

The OSU engagement team (continued)

Parms + Company



John Parme
Managing
Partner



Tim Grant
Partner

Specialists



Susan Eickhoff
National Office Leader
Higher Education/Grants
Compliance



Jeff Markert
National Office Leader
Government/GASB



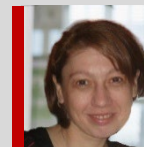
Tara D'Agostino
Tax Compliance
Managing Director



Arun Khandelwal
Director – Global
Delivery Center



Adrienne Henderson
Tech Assurance
Managing Director



Casey Shork
Actuarial Director

Required communications to those charged with governance

Prepared on: February 5, 2024

Presented on: February 21, 2024

Audit plan required communications and other matters

Our audit of the financial statements of The Ohio State University (the University) as of and for the year ended June 30, 2024, will be performed in accordance with auditing standards generally accepted in the United States of America.

Performing an audit of financial statements includes consideration of internal control over financial reporting (ICFR) as a basis for designing audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the entity's ICFR.

Additionally, we will perform a single audit in accordance with 2 CFR 200.

Matters to communicate		Response
Role and identity of engagement partner	✓	The lead audit engagement partner is Dave Gagnon. Cathy Baumann will serve as the partner on the single audit and support Dave on the University audit. Johnny Lewis will serve as the partner for the standalone reports for Wexner Medical Center Health System and Ohio State University Physicians, Inc. Chase Gahan will serve as the managing director for the stand alone component reports for The Ohio State University Foundation, Transportation Research Center Inc., and Campus Partners for Community Urban Redevelopment and Subsidiaries.
Scope of audit	✓	Our audit of the financial statements of the OSU Pool as of and for the year ended June 30, 2024, will be performed in accordance with auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in <i>Government Auditing Standards</i> , issued by the Comptroller General of the United States. Audits will also be performed on stand-alone reports prepared for the following components: <ul style="list-style-type: none"> — The Ohio State University Foundation — Campus Partners for Community and Urban Redevelopment — The Ohio State University Physicians, Inc. — Transportation Research Center, Inc. — The Ohio State University Wexner Medical Center Health System <p>Additionally, we will issue our reports on The Ohio State University Single Audit.</p>

✓ = Matters to report X = No matters to report

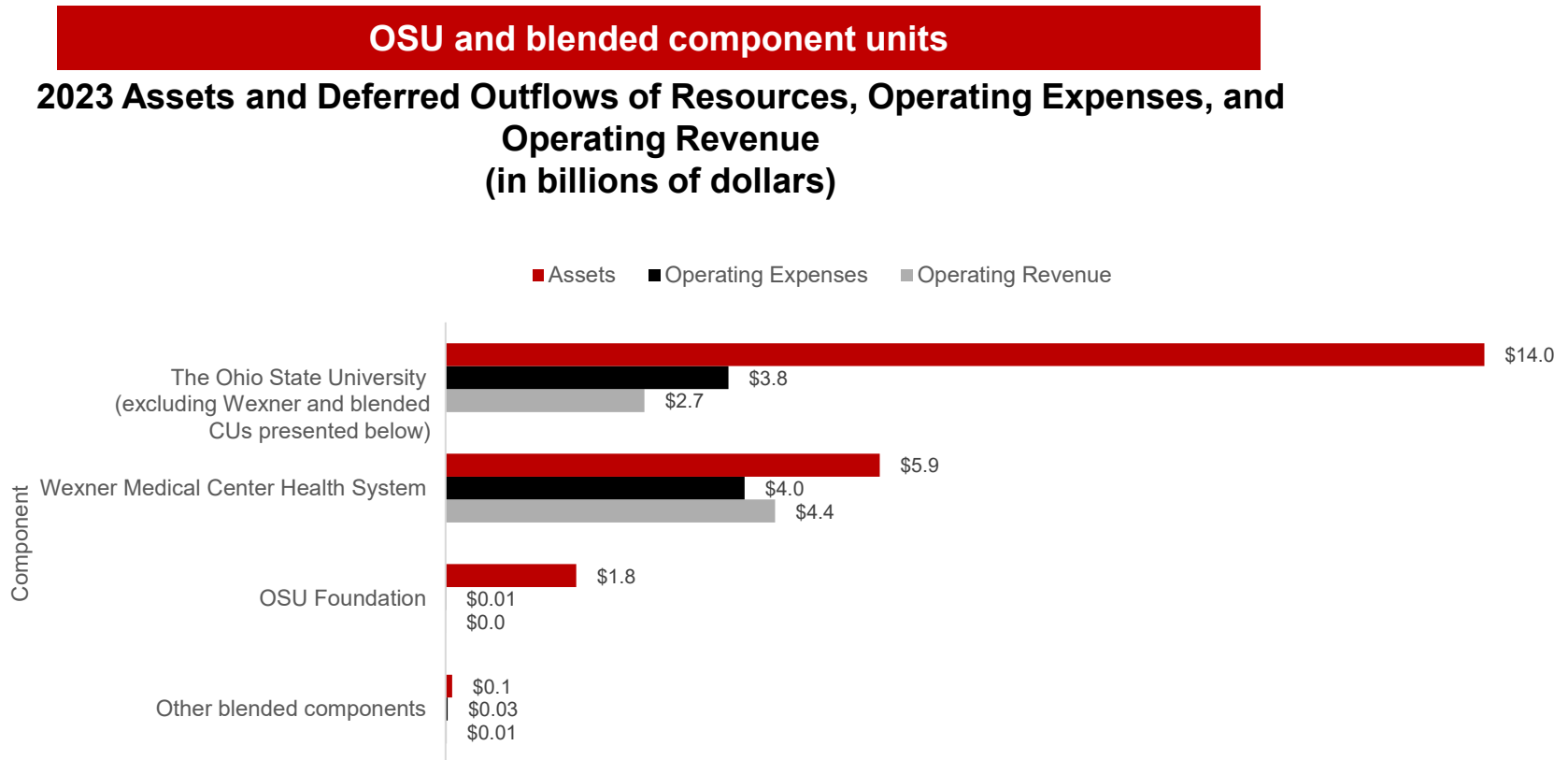
Audit plan required communications and other matters (cnt'd)

Matters to communicate		Response
Significant findings or issues discussed with management	X	
Financial reporting entity	✓	Pages 10 to 11
Materiality in the context of an audit	✓	Page 12
Our timeline	✓	Page 13
Risk assessment: Significant risks	✓	Page 14
Risk assessment: Additional risks identified	✓	Page 15
Involvement of others	✓	Page 16
Newly effective accounting standards	✓	Page 17
Independence	✓	Page 18
Responsibilities	✓	Page 19
Inquiries	✓	Page 20

✓ = Matters to report X = No matters to report

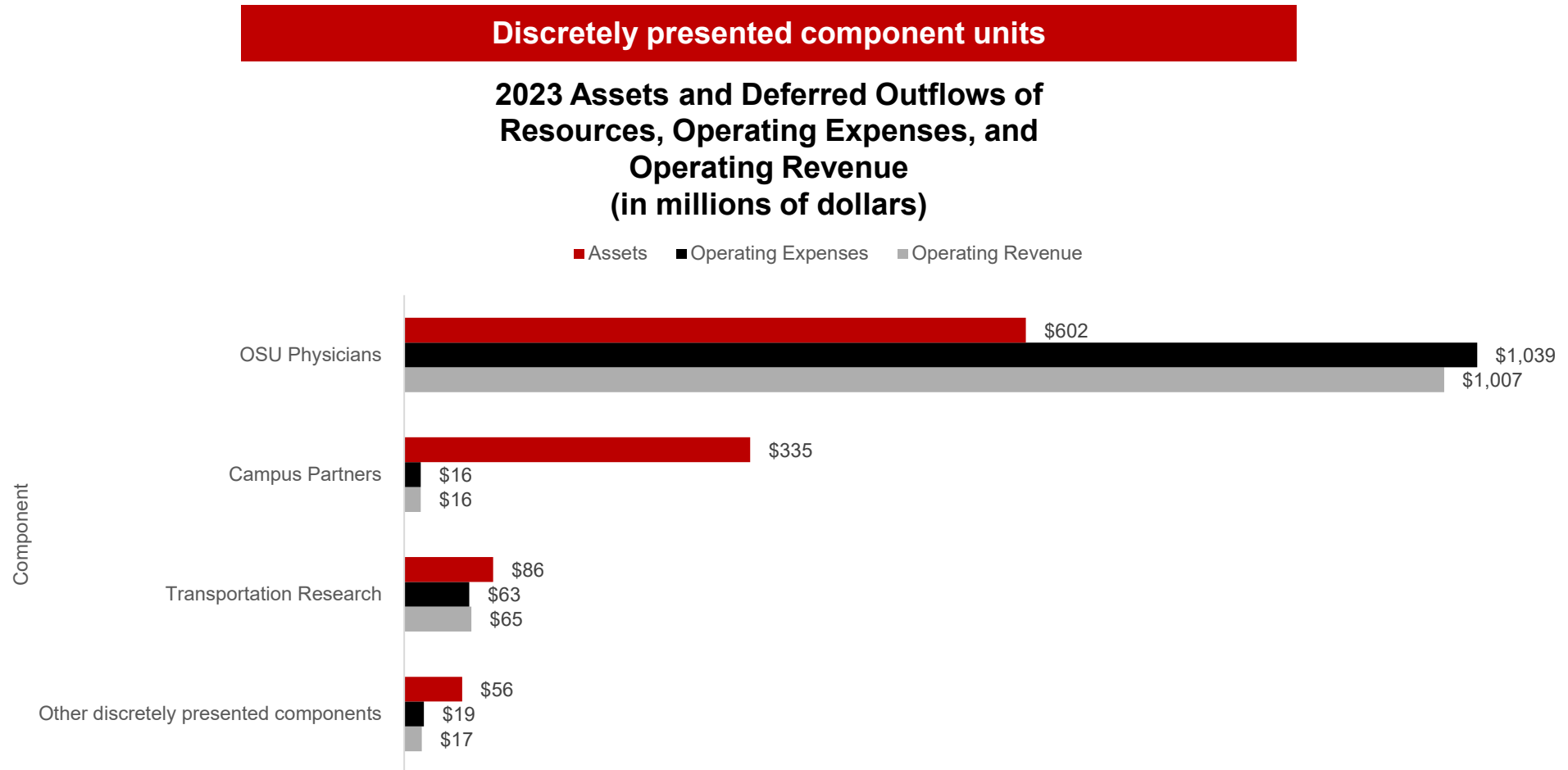
Financial reporting entity

The following illustration depicts the entities included in the Primary Government column of The Ohio State University financial statements.



Financial reporting entity (continued)

The following illustration depicts the entities included in the Discretely Presented Component Units column of The Ohio State University financial statements.



Materiality in the context of the audit

We will apply materiality in the context of the preparation and fair presentation of the financial statements, considering the following factors:

<p>Misstatements, including omissions, are considered to be material if there is a substantial likelihood that, individually or in the aggregate, they would influence the judgment made by a reasonable user based on the financial statements.</p>	<p>Judgments about materiality are made in light of surrounding circumstances and are affected by the size or nature of a misstatement, or a combination of both.</p>	<p>Judgments about materiality involve both qualitative and quantitative considerations.</p>
<p>Judgments about matters that are material to users of the financial statements are based on a consideration of the common financial information needs of users as a group. The possible effect of misstatements on specific individual users, whose needs may vary widely, is not considered.</p>	<p>Determining materiality is a matter of professional judgment and is affected by the auditor's perception of the financial information needs of users of the financial statements.</p>	<p>Judgments about the size of misstatements that will be considered material provide a basis for</p> <ol style="list-style-type: none">Determining the nature and extent of risk assessment procedures;Identifying and assessing the risks of material misstatement; andDetermining the nature, timing, and extent of further audit procedures.

Our timeline

February – March 2024

Planning and risk assessment

- Debrief and planning meeting with management
- Planning and initial risk assessment procedures, including:
 - Involvement of others
 - Identification and assessment of risks of misstatements and planned audit response for certain processes
- Obtain and update an understanding of OSU and its environment
- Inquire of those charged with governance, management and others within OSU about risks of material misstatement
- Coordinate with Internal Audit
- Communicate audit plan

May 2024

Interim

- Identify IT applications and environments
- Perform process walkthroughs and identification of process risk points
- Evaluate design and implementation (D&I) of entity level controls and process level controls for processes
- Evaluate D&I of general IT and automated controls
- Perform TOE of relevant process level, general IT, and entity-level controls, where applicable
- Perform interim substantive audit procedures over payroll, expenses, journal entries
- Perform risk assessments for direct and material compliance requirements identified for the major programs audited as part of the single audit
- Perform control and compliance testing over certain major programs

August – October 2024

Year-end

- Complete control testing for remaining process level, general IT, and entity-level controls, where applicable
- Perform remaining substantive audit procedures
- Evaluate results of audit procedures, including control deficiencies and audit misstatements identified
- Review financial statement disclosures
- Perform control and compliance testing for the single audit

November – December 2024

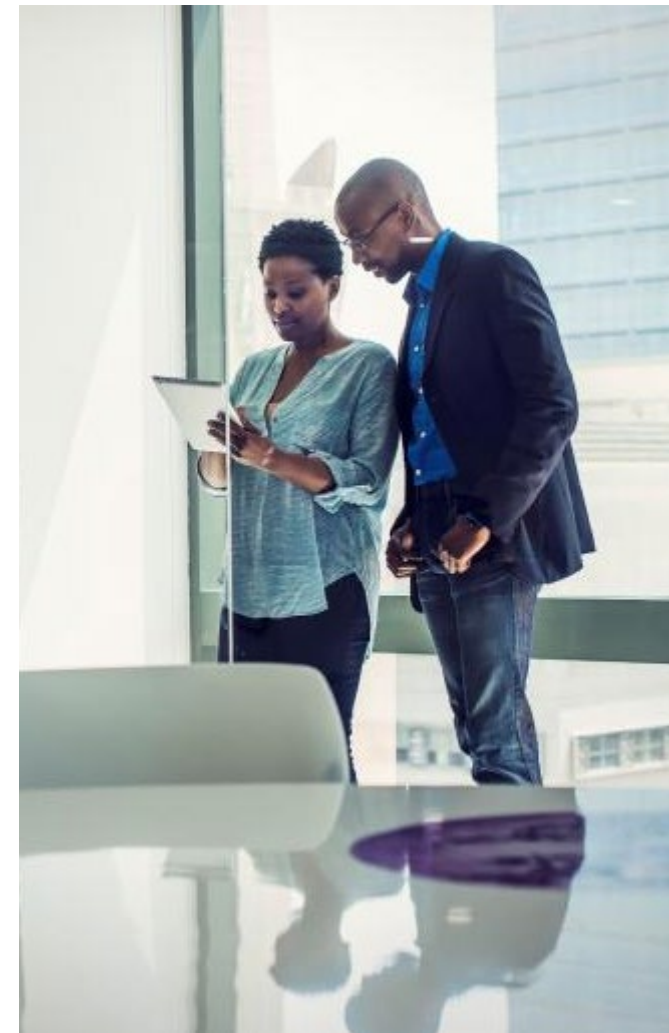
Completion

- Evaluate results of audit procedures, including control deficiencies and audit misstatements identified
- Present audit results to those charged with governance and perform required communications
- Issue audit reports

Risk Assessment: Significant Risks

Significant risk	Susceptibility to:	
Management override of controls Management is in a unique position to perpetrate fraud because of its ability to manipulate accounting records and prepare fraudulent financial statements by overriding controls that otherwise appear to be operating effectively. Although the level of risk of management override of controls will vary from entity to entity, the risk nevertheless is present in all entities.	Error	Fraud
		Yes

Significant risk	Description of significant risk	Susceptibility to:		Relevant factors affecting our risk assessment
		Error	Fraud	
Valuation of patient accounts receivable (healthcare entities)	Management's estimate of the allowances for uncollectible accounts is based on analysis of open accounts receivable, average historical collection experience, and other relevant factors to arrive at an overall assessment of collectible net accounts receivable.	Yes		Significant assumptions used that have a high degree of subjectivity: Historical collection experience is the key driver in evaluating the future collection of outstanding patient accounts receivable. Additional consideration is given for changes in aging as well as process changes year over year.



Risk assessment: Additional risks identified

Additional risks identified	Relevant factors affecting our risk assessment and planned response
Valuation of alternative investments	Due to the relative lack of transparency into the underlying assets, including that these investments are not valued on a daily basis, nor readily available, we will perform various procedures to determine whether net asset values (NAVs), as applicable, are reliable, including confirming balances and ownership percentages as of year-end, obtaining underlying audited annual financial statements and back-testing reported NAVs, evaluating NAV valuation and cash changes between the audit date and the University's fiscal year end.
Valuation of marketable securities, which are reported within current and noncurrent assets on the statement of net position	Management's estimate of the fair value of marketable securities, including stocks and fixed income assets, held directly by the University is determined based on quoted prices in active markets.
Valuation of pension and other post-employment benefit liabilities and related accounts	Management's estimates of net pension obligations reported are based on a variety of actuarial assumptions related to participant mortality, as well as interest rates, historical experience, the provisions of the related benefit programs, and desired reserve levels.

Involvement of others

Audit of financial statements	Extent of planned involvement
Internal audit	No direct assistance will be received from the University's internal audit group. Internal audit reports will be reviewed and considered as part of our risk assessments as required under <i>Government Auditing Standards</i> .
KPMG Tech Assurance	Assist the audit team in evaluating general information technology controls and IT application controls.
KPMG pension and postretirement benefit actuary	Assist the audit team in evaluating pension and postretirement benefit obligations.
KPMG Business Tax Services – Development and Exempt Organizations specialist	Assist the audit team in evaluating OSU's tax-exempt status as a governmental entity. Also will assist the audit team in evaluating tax-exempt status of component units and to assist in evaluating uncertain tax positions, if any.
Parms + Company LLC	Subcontractor firm assisting KPMG with certain audit procedures to be performed for OSU's financial statements (including OSU Physicians, Inc. and Wexner Medical Center) and Uniform Guidance audits.

New and upcoming accounting pronouncements



GASB Statement No. 99, *Omnibus 2022*

This Statement provides an extension of the use of LIBOR, clarifies provisions related to the new Statements for leases, public-private partnerships and subscription-based IT arrangements, and the classification and reporting of derivative instruments. LIBOR provisions are effective upon issuance; leases, PPPs, and SBITA provisions are effective for periods beginning after June 15, 2022 (OSU's FY23 financials); and derivative provisions are effective for periods beginning after June 15, 2023 (OSU's FY24 financials).



GASB Statement No. 101, *Compensated Absences*

The requirements of this Statement are effective for periods beginning after December 15, 2023, or OSU's FY25 financials. Establishes standards of accounting and financial reporting for compensated absences and associated salary related payments, including certain defined contribution pension and defined contribution OPEB.



GASB Statement No. 100, *Accounting Changes and Error Corrections*

The requirements of this Statement are effective for periods beginning after June 15, 2023, or OSU's FY24 financials. Establishes accounting and financial reporting requirements for accounting changes and the correction of an error in previously issued financial statements.

Shared responsibilities: Independence

Auditor independence is a shared responsibility and most effective when management, those charged with governance and audit firms work together in considering compliance with the independence rules. In order for KPMG to fulfill its professional responsibility to maintain and monitor independence, management, those charged with governance, and KPMG each play an important role.

System of Independence Quality Control

The firm maintains a system of quality control over compliance with independence rules and firm policies. Timely information regarding upcoming transactions or other business changes is necessary to effectively maintain the firm's independence in relation to:

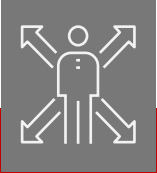
- New affiliates (which may include subsidiaries, equity method investees/investments, sister companies, and other entities that meet the definition of an affiliate under AICPA independence rules)
- New officers or trustees with the ability to affect decision-making, individuals who are beneficial owners with significant influence over the University, and persons in key positions with respect to the preparation or oversight of the financial statements

Certain relationships with KPMG

Independence rules prohibit:

- Certain employment relationships involving directors, officers, or others in an accounting or financial reporting oversight role and KPMG and KPMG covered persons.
- The University or its trustees, officers, from having certain types of business relationships with KPMG or KPMG professionals.

Responsibilities



Management responsibilities

- Communicating matters of governance interest to those charged with governance.
- The audit of the financial statements does not relieve management or those charged with governance of their responsibilities.



KPMG responsibilities – objectives

- Communicating clearly with those charged with governance the responsibilities of the auditor regarding the financial statement audit and an overview of the planned scope and timing of the audit.
- Obtaining from those charged with governance information relevant to the audit.
- Providing those charged with governance with timely observations arising from the audit that are significant and relevant to their responsibility to oversee the financial reporting process.
- Promoting effective two-way communication between the auditor and those charged with governance.
- Communicating effectively with management and third parties.



KPMG responsibilities – other

- If we conclude that no reasonable justification for a change of the terms of the audit engagement exists and we are not permitted by management to continue the original audit engagement, we should:
- Withdraw from the audit engagement when possible under applicable law or regulation;
- Communicate the circumstances to those charged with governance, and
- Determine whether any obligation, either legal contractual, or otherwise, exists to report the circumstances to other parties, such as owners, or regulators.
- Forming and expressing an opinion about whether the financial statements that have been prepared by management, with the oversight of those charged with governance, are prepared, in all material respects, in accordance with the applicable financial reporting framework.
- Establishing the overall audit strategy and the audit plan, including the nature, timing, and extent of procedures necessary to obtain sufficient appropriate audit evidence.
- Communicating any procedures performed relating to other information, and the results of those procedures.

Inquiries

Are those charged with governance aware of:

- Matters relevant to the audit, including, but not limited to, violations or possible violations of laws or regulations?
- Any significant communications with regulators?
- Any developments in financial reporting, laws, accounting standards, corporate governance, and other related matters, and the effect of such developments on, for example, the overall presentation, structure, and content of the financial statements, including the following:
 - The relevance, reliability, comparability, and understandability of the information presented in the financial statements
 - Whether all required information has been included in the financial statements, and whether such information has been appropriately classified, aggregated or disaggregated, and presented?

Do those charged with governance have knowledge of:

- Fraud, alleged fraud, or suspected fraud affecting the University?
 - If so, have the instances been appropriately addressed and how have they been addressed?

Additional inquiries:

- What are those charged with governance's views about fraud risks in the University?
- Who is the appropriate person in the governance structure for communication of audit matters during the audit?
- How are responsibilities allocated between management and those charged with governance?
- What are the University's objectives and strategies and related business risks that may result in material misstatements?
- Are there any areas that warrant particular attention during the audit and additional procedures to be undertaken?
- What are those charged with governance's attitudes, awareness, and actions concerning (a.) the University's internal controls and their importance in the entity, including oversight of effectiveness of internal controls, and (b.) detection of or possibility of fraud?
- Have there been any actions taken based on previous communications with the auditor?
- Has the University entered into any significant unusual transactions?
- Whether the entity is in compliance with other laws and regulations that have a material effect on the financial statements?
- What are the other document(s) that comprise the annual report, and what is the planned manner and timing of issuance of such documents?

Summary of Uniform Guidance audit results for June 30, 2023

Total expenditures of federal awards for the University for the year ended June 30, 2023 were \$1.085 billion.

Based on the audit procedures performed, the Summary of Results/Findings in the Single Audit Report reported the following:

- Type of reports issued on whether the financial statements were prepared in accordance with U.S. generally accepted accounting principles: **Unmodified opinions**
- Internal control deficiencies over financial reporting disclosed by the audit of the financial statements:
 - Material weaknesses: **No**
 - Significant deficiencies: **None reported**
- Noncompliance material to the financial statements: **No**
- Internal control deficiencies over major programs disclosed by the audit:
 - Material weaknesses: **No**
 - Significant deficiencies: **None reported**
- Type of report issued on compliance for major programs: **Unmodified**
- Audit findings that are required to be reported in accordance with 2 CFR 200.516(a): **No**
- Dollar threshold used to distinguish between Type A and Type B programs: **\$3,255,883**
- Auditee qualify as low-risk auditee: **Yes**

Our letter of required communications regarding our Single Audit is included in Appendix II.

The single audit reporting package was filed with the Federal Audit Clearinghouse by the University in February 2024.

Fiscal 2024 Single Audit – overview and scope

- The Single Audit in accordance with the Uniform Guidance (UG) is required annually by federal regulation and is focused on compliance and internal control over compliance for programs that are federally funded. For auditees such as the University, programs audited must cover at least 20% of federal funds expended during the fiscal year.
- Major programs are selected for audit based on quantitative and qualitative risk considerations prescribed by federal regulations. Larger programs (“Type A,” which for the University are over \$3 million, or more depending on total federal expenditures) must be audited as major programs at least once every three years; however, certain Type A programs may be required to be audited more frequently based on agency directives that they are “higher risk”.
- While risk assessments are still in progress, below is a summary of major programs recently audited for the University and the planned fiscal 2024 major programs:

FY22 Major programs – audited	FY23 Major programs – audited	FY24 Major programs – planned
<ul style="list-style-type: none"> — Research and Development Cluster — Student Financial Assistance Cluster — Education Stabilization Fund — Provider Relief Fund — Medicaid Cluster — Shuttered Venue Operators Grant — Protecting and Improving Health Globally: Building and Strengthening Public Health Impact, Systems, Capacity and Security 	<ul style="list-style-type: none"> — Research and Development Cluster — Student Financial Assistance Cluster — Education Stabilization Fund — Provider Relief Fund — Head Start Cluster — Smith-Lever Funding 	<ul style="list-style-type: none"> — Research and Development Cluster — Student Financial Assistance Cluster — Supplemental Nutritional Assistance Program Cluster — Disaster Grants – Public Assistance (Presidentially Declared Disasters:

Finalization of major program determination is dependent upon the final supplementary schedule of expenditures of federal awards, risk assessment procedures, and requirements of the 2024 Compliance Supplement (expected to be issued in the Spring). Major program compliance test work over direct and material compliance requirements is planned based upon reliance on internal control over compliance. While we may test and report on internal control over compliance, we do not express an opinion on the effectiveness of internal control over compliance.



Thank you

David Gagnon

Lead Engagement Partner

978-404-9869

dgagnon@kpmg.com

For additional information and audit committee resources, including National Audit Committee Peer Exchange series, a Quarterly webcast, and suggested publications, visit the KPMG Audit Committee Institute (ACI) at www.kpmg.com/ACI

This presentation to those charged with governance is intended solely for the information and use of those charged with governance and management and is not intended to be and should not be used by anyone other than these specified parties. This presentation is not intended for general use, circulation or publication and should not be published, circulated, reproduced or used for any purpose without our prior written permission in each specific instance.

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.

© 2023 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. NDP384400-1A

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

Appendix

Appendix I – New AICPA Group Audit Standard	Page 25
Appendix II – KPMG U.S. Transparency report and Impact plan	Page 26
Appendix III – On the 2024 higher education audit committee agenda	Page 27

New AICPA Group Audit Standard



What is new?

AU-C 600, *Special Considerations—Audits of Group Financial Statements (Including the Work of Component Auditors and Audits of Referred-to Auditors)*



When is this effective?

Effective for audits of fiscal years ending on or after December 15, 2026, however KPMG is early adopting to align with effective dates of IAASB and PCAOB group audit standards



What are the changes to the audit?

1. Risk based approach for scoping with a greater focus on the group auditor's responsibility, with assistance from component auditors, when needed
2. Involvement in the work of the component auditor including:
 - Emphasizes two-way communication between the group auditor and component auditors
 - Strengthens and clarifies various aspects of the group auditor's interaction with component auditors related to communicating ethical requirements, determining competence and capabilities of the component auditor, and determining the appropriate nature, timing and extent of involvement by the group auditor in the work of the component auditor.
 - When determining extent of supervision, consider areas of higher assessed risk, including significant risk and significant judgment
3. More audits will meet the definition of a group audit, which will impact audit committee communications and the auditor's report

U.S. Audit Quality, Transparency, and Impact reports



- Interactive dashboard highlights key quality metrics
- Details KPMG's investment in our audit approach, people, technology, quality management system and the future of audit

Audit Quality Report



- Provides more granular detail on our commitment to continually enhance audit quality
- Outlines KPMG LLP's structure, governance and approach to audit quality
- Discusses how the firm aligns with the requirements and intent of applicable professional standards

Transparency Report



- Provides annual update on our progress on meeting goals aligned to People, Planet, Prosperity, and Governance
- Our goals reflect a materiality assessment and our aspiration to be an employer of choice

KPMG Impact Plan

In addition to this report, we are providing you with our Transparency Report Supplement: Assisting audit committees in meeting NYSE rules on auditor communications Reports and supplements available at: audit.kpmg.us/auditquality





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 report² 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 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?

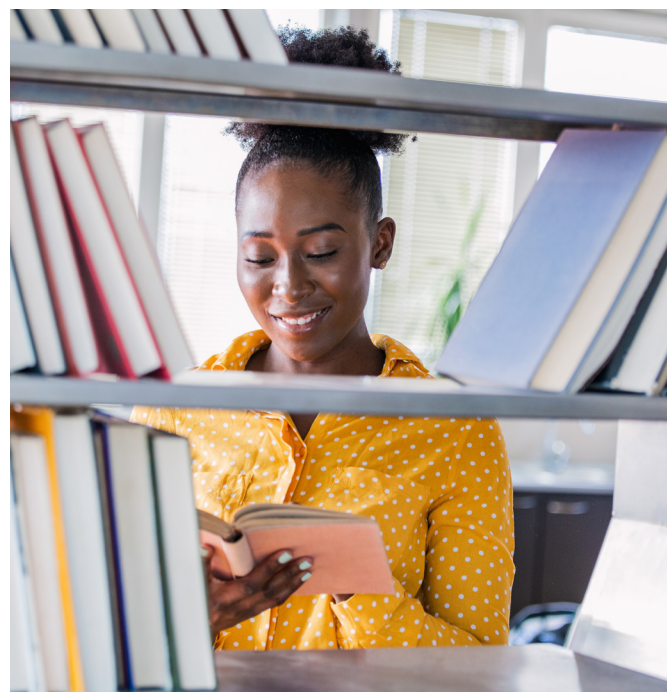
Help ensure internal audit is attentive to the institution’s key risks and is a valuable resource for the audit committee

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 is 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

Joseph Giordano

Metro New York and New Jersey

E: jagiordano@kpmg.com

Rosemary Meyer

Midatlantic

E: rameyer@kpmg.com

Jennifer Hall

Southeast

E: jchall@kpmg.com

Cathy Baumann

Midwest

E: cbaumann@kpmg.com

Drew Corrigan

Pacific Northwest

E: dcorrigan@kpmg.com

Christopher Ray

West

E: cray@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:



[kpmg.com](https://www.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.

© 2024 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization. USCS01189-1A



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.

© 2023 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. NDP421957-1A

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.



**Department of Internal Audit
Quality Assurance and Improvement Program**

Kevin Patton, Chief Audit Executive

Legal, Audit, Risk and Compliance Committee

February 2024



What is a Quality Assurance and Improvement Program?

As defined by the *Institute of Internal Auditors*:

- Incorporates both internal and external assessments of the Department.
- External Assessments are required every five years – last received and presented to the Audit, Finance, and Investment Committee in February 2021.
- Internal Assessments are required periodically when not undergoing an external assessment.



External Quality Assurance Review Results from 2021

The external validators confirmed the Department generally conforms to the Institute of Internal Auditors (IIA) – *International Standards for the Professional Practice of Internal Auditing*.

The external validators were chief audit executives from University of Washington, University of Illinois, University of Michigan and State of Ohio Office of Budget and Management - Internal Audit.

The term “generally conforms” is the highest rating available from the IIA.

Departmental Independence

To maintain independent stature, the Department of Internal Audit currently:

- Reports functionally to the Legal, Audit, Risk and Compliance Committee, and University President; and
- Reports administratively to the Senior Vice President for Business and Finance.
- Has no direct operational responsibility or authority over any activities audited.



Quality Assurance and Improvement Program

Internal Assessments – On-going Monitoring:

- **Monitoring Audits** – progress is tracked for each project-by-project phase and assigned auditor, all audit workpapers are reviewed for quality and accuracy by the Director and Chief Audit Executive (CAE), review notes are provided to assist in strengthening performance for future audits, all audit reports and related communications are reviewed by the Director and CAE before issuance.
- **Performance Metrics** – auditor productivity, project management, and audit efficiency is monitored on a weekly basis for each auditor.
- **Professional Development and Training** – each auditor receives approximately 40 hours of continuing professional development annually.
- **Feedback** – each staff member receives coaching and feedback, written review notes are provided for each audit project, customer feedback is obtained at the end of each audit engagement.



Quality Assurance and Improvement Program

Internal Assessments – On-going Monitoring:

- **Audit Plan** – developed based on a prioritization of the audit universe using a risk-based methodology, including input from the Legal, Audit, Risk and Compliance Committee Chair and senior management. The Fiscal Year 2025 audit work plan will be presented and agreed upon by the Legal, Audit, Risk, and Compliance Committee at the May 2024 Committee meeting.
- **Follow-up** – disposition of audit recommendations are followed up and reported on until resolved.



Quality Assurance and Improvement Program

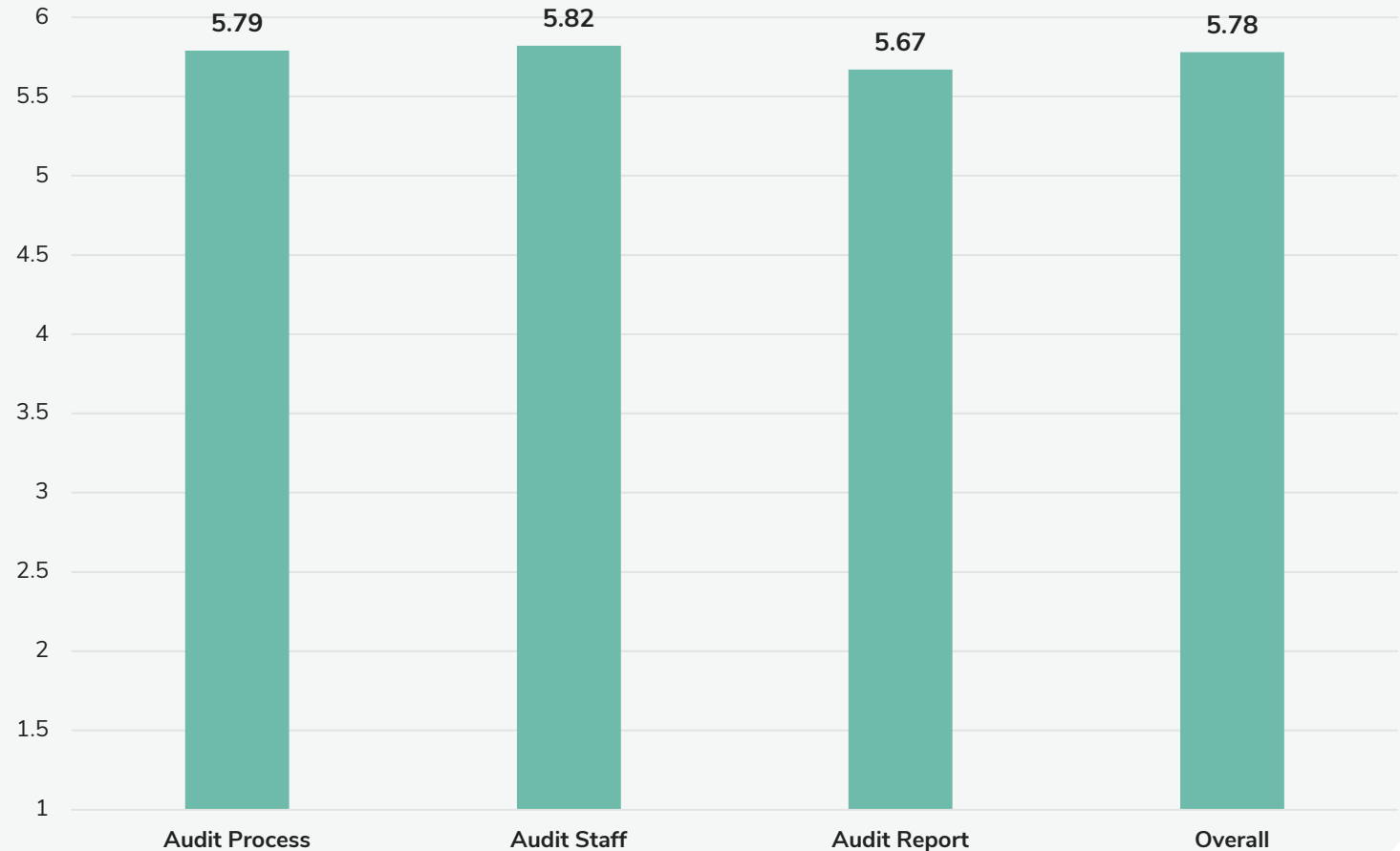
Periodic Self-Assessments:

- **Annual Governance Review** – Internal Audit Charter and Legal, Audit, Risk and Compliance Committee Guidelines are reviewed annually and updated as needed. Last updated August 2022; no update necessary to the Internal Audit Charter at this time.
- **Annual Workpaper Review** – sample of audit workpapers are reviewed by Internal Audit management to make sure work is performed in accordance with departmental practices and *IIA Standards*.
- **Audit Staff Review** – job descriptions for each audit position have been reviewed and are appropriate. Formal, written performance feedback is performed for each staff member two times/year.
- **Audit Process/Scope Review** – reviewed and modified as necessary.
- **Customer Satisfaction Surveys** – distributed to those involved in the audit process at the end of each audit.

Customer Satisfaction Survey Results

- Results are based on a six-point scale.
- Results presented are for calendar years 2022 and 2023.

Internal Audit Survey Averages Calendar Year 2022-2023
(Score from 1 to 6)



Results of the Quality Assurance and Improvement Program

1. Confirmation that Department of Internal Audit is independent – no impairments to our independence.
2. Confirmation that our work is performed in accordance with *IIA Standards* and that we abide by the *IIA Code of Ethics*.
3. Internal Audit Charter and Legal, Audit, Risk, and Compliance Committee Charter are appropriate related to internal audit activities, at this time.
4. 88% of our staff possess professional credentials or have advanced degrees.
5. Continuous Improvement - we continue to refine audit processes and staff productivity.



On the Horizon

1. Updated Internal Audit Standards were recently released by the Institute of Internal Auditors now named *Global Internal Audit Standards*.
2. We plan to evaluate and address the changes during 2024. This will be a big lift for the Department.
3. New governance terminology for LARC and IA.
4. Implementation date is January 2025.
5. Next External Quality Assurance Review is targeted for 2026.





Office of Government Affairs Update

Stacy Rastauskas, Vice President for Government Affairs

Legal, Audit, Risk and Compliance Committee
February 2024





At a glance

- Federal, State, Local and Community, Advocacy
- Offices located in Columbus, Ohio and Washington, D.C.
- 18 team members
 - Wexner Medical Center
 - College of Food, Agricultural, and Environmental Sciences

By the Numbers

\$1.53

BILLION

Annual government
investment in Ohio
State

67%

TURNOVER

Out of 165 key public
offices since 2018

58

ENGAGEMENTS

By President Carter in
January 2024

2024 Forecast – January - June

MARCH

Federal FY24 CR Expires

The continuing resolutions (CR) providing appropriations to all federal agencies expire March 1 and March 8.

JUNE

State Capital Bill

Legislation to provide capital funding to state agencies, colleges and universities, and communities is anticipated to be completed by June 30.

JANUARY

Congress, Statehouse, City Council Reconvene

Legislative bodies begin work for the calendar year. Columbus City Council grows from 7 to 9 members. Mayor Ginther sworn in for 3rd term.

MARCH

State of the Union & Federal FY25 Budget

President Biden will deliver the State of the Union to the U.S. Congress on Thursday, March 7. On March 11, the federal FY25 budget is expected to be introduced.

MARCH

Ohio Primary March 19

Political parties will select candidates for local, state, and federal offices, including the U.S. presidential election. Ohio's U.S. Senate race is expected to be one of the most competitive in the country.

2024 Forecast – July - December

OCTOBER

Federal FY25 begins

Congress will need to finalize work on the FY25 budget or pass a continuing resolution by October 1.

DECEMBER

Lame Duck Sessions

Legislative sessions occurring after the election will be busy as lawmakers wrap up unfinished business before the end of the calendar year.

JULY

State FY25 begins

Ohio will begin a new fiscal year. State agencies will begin the process of preparing the next 2-year state operating budget.

NOVEMBER

General election November 5

In 2024 Ohio will elect one U.S. Senator, 15 members of Congress, 99 members of the Ohio House, and 16 state senators, 3 Ohio Supreme Court justices and the U.S. President, as well as other local judicial positions.

Information Security

Cindy Leavitt Chief Information Officer

Rich Nagle Chief Information Security Officer

Tom Bentley Chief Information & Digital Technology Officer – Wexner Medical Center

Tre Smith Chief Information Security Officer – Wexner Medical Center

Legal, Audit, Risk, and Compliance Committee

February 2024



Overview

- ✓ Industry Risk Drivers
- ✓ Recent Actions



Higher Education: External & Internal Risk Drivers

External

- Economic challenges & global conflicts
- National security through compliance
- Third-party vendor attacks

Internal

- Leadership/organizational changes
- System enhancements
- Resource prioritization challenges

Success, Despite Challenges



ADVANCED SECURITY
EFFORTS



EXTENDED OUTREACH &
PREVENTION



MET INCREASED REGULATORY
REQUIREMENTS



WORKFORCE
STABILIZATION



SUMMARY OF ACTIONS TAKEN

November 15, 2023 – Legal, Audit, Risk & Compliance Committee Meeting

Voting Members Present:

Elizabeth P. Kessler
Alan A. Stockmeister
Jeff M.S. Kaplan

Elizabeth A. Harsh
Juan Jose Perez
Bradley R. Kastan

Joshua H.B. Kerner
Amy Chronis
Hiroyuki Fujita (ex officio)

Members Present via Zoom: N/A

Members Absent:

Michael F. Kiggin

PUBLIC SESSION

The Legal, Audit, Risk & Compliance Committee of The Ohio State University Board of Trustees convened on Wednesday, November 15, 2023, in person at Longaberger Alumni House on the Columbus campus. Committee Chair Elizabeth Kessler called the meeting to order at 12:03 p.m.

Items for Discussion:

1. Committee Chair's Remarks: Ms. Liza Kessler started the meeting by welcoming Trustee Brad Kastan to the committee.
2. Audit Update: Mr. Michael Papadakis, Ms. Kris Devine, Mr. Vincent Tammaro and Mr. David Gagnon, the university's external auditor from KPMG, presented an audit update to discuss the draft of the university's audited consolidated financial statements and audit results for the year ended on June 30, 2023 prior to its submission to the auditor of state.

(See Attachment X for background information, page XX)

3. Annual Affiliated Entities Report: Senior Assistant Vice President and Senior Associate General Counsel Heidi McCabe shared the annual report on Ohio State's affiliated entities. Dean Cathann Kress, vice president for agriculture administration, and dean, College of Food, Agricultural, and Environmental Sciences, also joined to discuss and highlight one of our affiliated entities: 4-H affiliated camps.

(See Attachment X for background information, page XX)

Items for Action:

4. Approval of Minutes: No changes were requested to the August 16, 2023, meeting minutes; therefore, a formal vote was not required, and the minutes were considered approved.
5. Resolution No. 2024-45: Approval to Submit the Audited Consolidated Financial Statements (Draft) to the Auditor of State:

Synopsis: Approval to submit the draft audited consolidated financial statements to the Auditor of State, is proposed.



THE OHIO STATE UNIVERSITY

WHEREAS The Ohio State University annually seeks an independent audit of the consolidated financial statements as a matter of strong financial oversight; and

WHEREAS the Auditor of State is required under Ohio law to audit each public office; and

WHEREAS the university is a public office and is required under Ohio law to file a financial report with the Auditor of State for each fiscal year; and

WHEREAS the university has produced consolidated financial statements for the 2022 and 2023 fiscal years, in accordance with accounting principles, generally accepted in the United States of America; and

WHEREAS the university engages an outside auditing firm, currently KPMG LLP, to audit its consolidated financial statements; and

WHEREAS the university management and KPMG have produced a final draft of the audited consolidated financial statements for the 2022 and 2023 fiscal years; and

WHEREAS the Auditor of State may accept the audited consolidated financial statements in lieu of the audit required by Ohio law; and

WHEREAS the audited consolidated financial statements will not be final until approved by the Auditor of State:

NOW THEREFORE

BE IT RESOLVED, That the Board of Trustees hereby accepts the draft audited consolidated financial statements for the 2022 and 2023 fiscal years; and

BE IT FURTHER RESOLVED, That the Board of Trustees hereby approves the submission of these consolidated financial statements to the Auditor of State for review and approval.

Action: Upon the motion of Ms. Kessler, seconded by Mr. Kaplan, the foregoing resolutions were adopted by unanimous voice vote with the following members present and voting: Ms. Kessler, Mr. Stockmeister, Mr. Kaplan, Mrs. Harsh, Mr. Perez, Mr. Kastan, Mr. Kerner, Ms. Chronis, Dr. Fujita.

EXECUTIVE SESSION

It was moved by Ms. Kessler and seconded by Mrs. Harsh that the committee recess into executive session to consult with legal counsel regarding pending or imminent litigation, to consider business-sensitive trade secrets required to be kept confidential by federal and state statutes, and to discuss personnel matters regarding the appointment, employment and compensation of public employees.

A roll-call vote was taken, and the committee voted to move into executive session with the following members present and voting: Ms. Kessler, Mr. Stockmeister, Mr. Kaplan, Mrs. Harsh, Mr. Perez, Mr. Kastan, Mr. Kerner, Ms. Chronis, Dr. Fujita.

The committee entered executive session at 12:29 p.m., and the meeting adjourned at 2:05 p.m.