

WEDNESDAY, FEBRUARY 15, 2023
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
Juan Jose Perez
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. <i>External Audit Update – Mr. David Gagnon</i> | 12:00-12:10pm |
| 2. <i>Information Security Update – Ms. Cindy Leavitt, Mr. Rich Nagle</i> | 12:10-12:20pm |

ITEMS FOR ACTION

- | | |
|--|---------------|
| 3. Approval of November 2022 Committee Meeting Minutes – Ms. Elizabeth Kessler | 12:20-12:25pm |
|--|---------------|

Executive Session

12:25 – 2:00pm

Highlights of 2023 external audit plan and strategy

We are pleased to highlight key elements of the audit plan and strategy for the year ending June 30, 2023, which is provided under separate cover and which includes certain required communications to governance and other materials.

We would be happy to discuss questions you may have on these topics or any others.

Highlights:

- Audit timeline
- Entities within the scope of our engagement
- Significant risks and estimates
- New accounting and auditing pronouncements
- Single Audit update
- Thought leadership and other KPMG reports

The Ohio State University

**Discussion with
those charged
with governance**



Audit plan and strategy for the year ending June 30, 2023

February 15, 2023

Delivering a better audit experience drives us



With KPMG, you can expect an experience that's better for your team, your organization, and the capital markets. An experience that's built for a world that demands agility and integrity.

We aim to deliver an exceptional client experience for The Ohio State University by focusing on:



Quality



Experience



Productivity



Insights

See how.



Executive summary



KPMG Clara Technology: Bringing the audit to one place



Streamlined client experience

And deeper insights into your business, translating to a better audit experience.



Secure

A secure client portal provides centralized, efficient coordination with your audit team.



Intelligent workflow

An intelligent workflow guides audit teams through the audit using documented risk areas by ASC topic.



Increased precision

Advanced data analytics and automation facilitate a risk-based audit approach, increasing precision and reducing your burden.



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
- Clarify responsibilities for data governance across the enterprise
- Reassess how the board—through its committee structure—assigns and coordinates oversight responsibility for cybersecurity and data governance frameworks, including data privacy, ethics, and hygiene

Audit considerations:

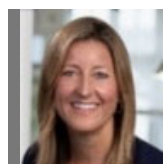
- Evaluate risks of material misstatement resulting from, among other things, unauthorized access to financial reporting systems (e.g., IT applications, databases, operating systems)
- Determine whether there is a related risk of fraud
- Develop audit approach based on risk assessment
- If a cybersecurity 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



Kim Zavislak

Account Executive
Columbus Office
Managing Partner



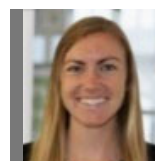
Cathy Baumann

University and Single
Audit Partner



Rosemary Meyer

University and Components
Engagement Quality Control
Review Partner



Brigid Murray

University and Single
Audit Manager



Amy Banovich

Healthcare Entities
Engagement Quality
Control Review Partner



Hilda de la Cuesta

Uniform Guidance
Senior Associate



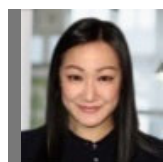
Chase Gahan

Components Managing
Director



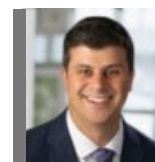
Johnny Lewis

Healthcare Entities
Partner



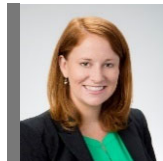
Jane Kim

Lead Senior
Manager



Robby Perry

Healthcare Entities
Senior Manager



Sarah Janka

Senior
Manager



Kody Seeger

Healthcare Entities
Manager



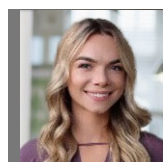
Alex Sherer

Investments
Manager



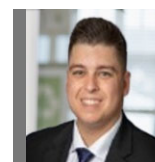
Sidney Arnold

Healthcare Entities
Senior Associate



Allie Clement

University Senior
Associate



Darryn Bradt

Investments
Senior Associate

The OSU engagement team (continued)

Parms + Company



John Parms
Managing
Partner



Tim Grant
Partner

Specialists



Susan Eickhoff
National Office Leader
Higher Education/Grants
Compliance



Jeff Markert
National Office Leader
Government/GASB



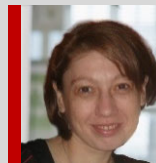
Tara D'Agostino
Tax Compliance
Managing Director



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: January 30, 2023

Presented on: February 15, 2023



Summary: Audit plan required communications and other matters

Our audit of the financial statements of The Ohio State University (OSU) as of and for the year ending June 30, 2023, 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	<p>The lead audit engagement partner is Dave Gagnon.</p> <p>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.</p>
Scope of audit	<p>Our audit of the financial statements of the OSU Pool as of and for the year ended June 30, 2023, 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:</p> <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>

Summary: Audit plan required communications and other matters (continued)

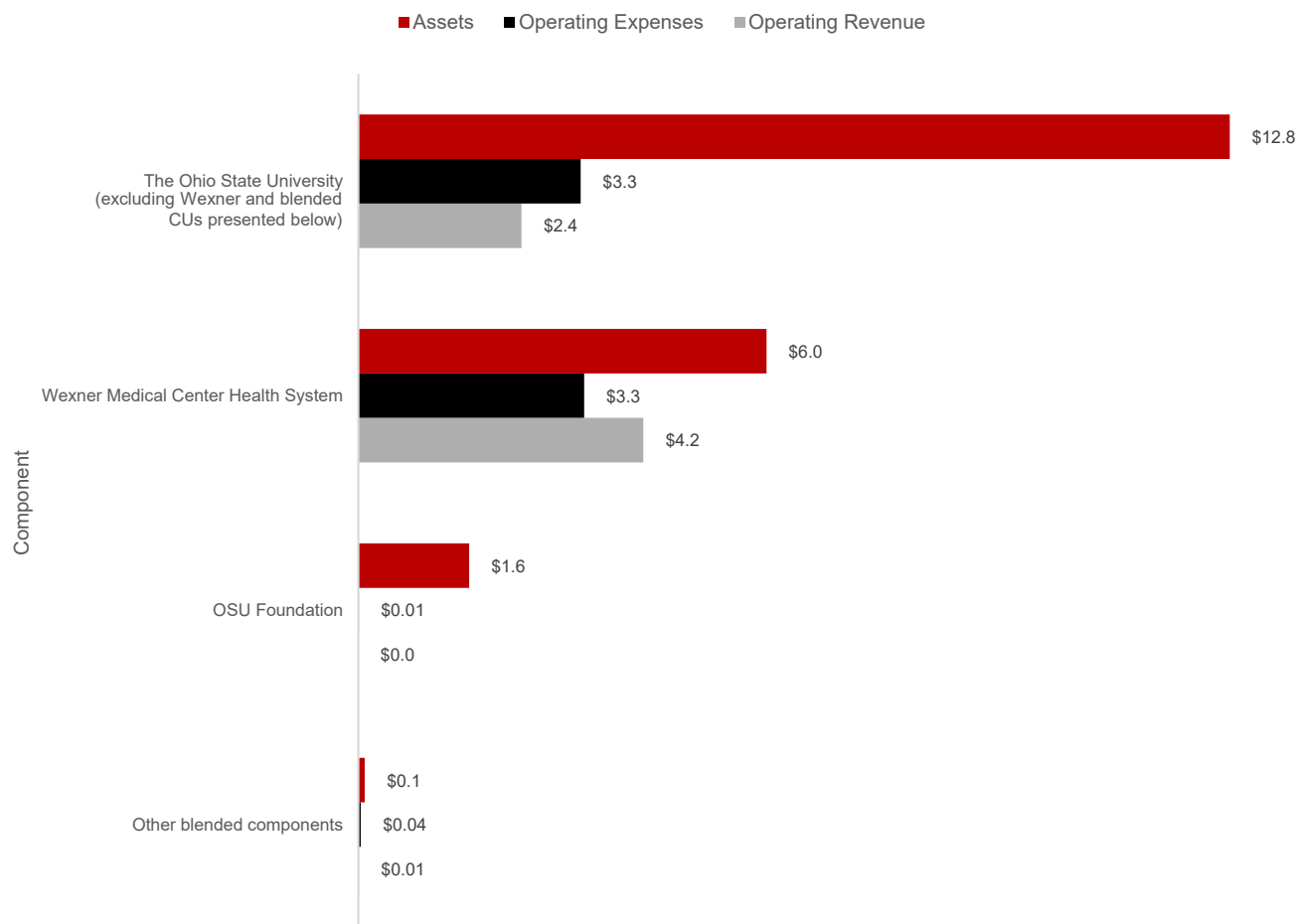
Matters to communicate	Response
Financial reporting entity	See pages 11 and 12
Materiality in the context of an audit	See page 13
Our timeline	See page 14
Risk assessment: Significant risks	See page 15
Risk assessment: Significant estimates	See page 16
Involvement of others	See page 17
Newly effective accounting standards	See pages 18 and 19
Independence	See page 20
Responsibilities	See page 21
Inquiries	See page 22

Financial reporting entity

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

OSU and blended component units

2022 Assets and Deferred Outflows of Resources, Operating Expenses, and Operating Revenue (in billions of dollars)

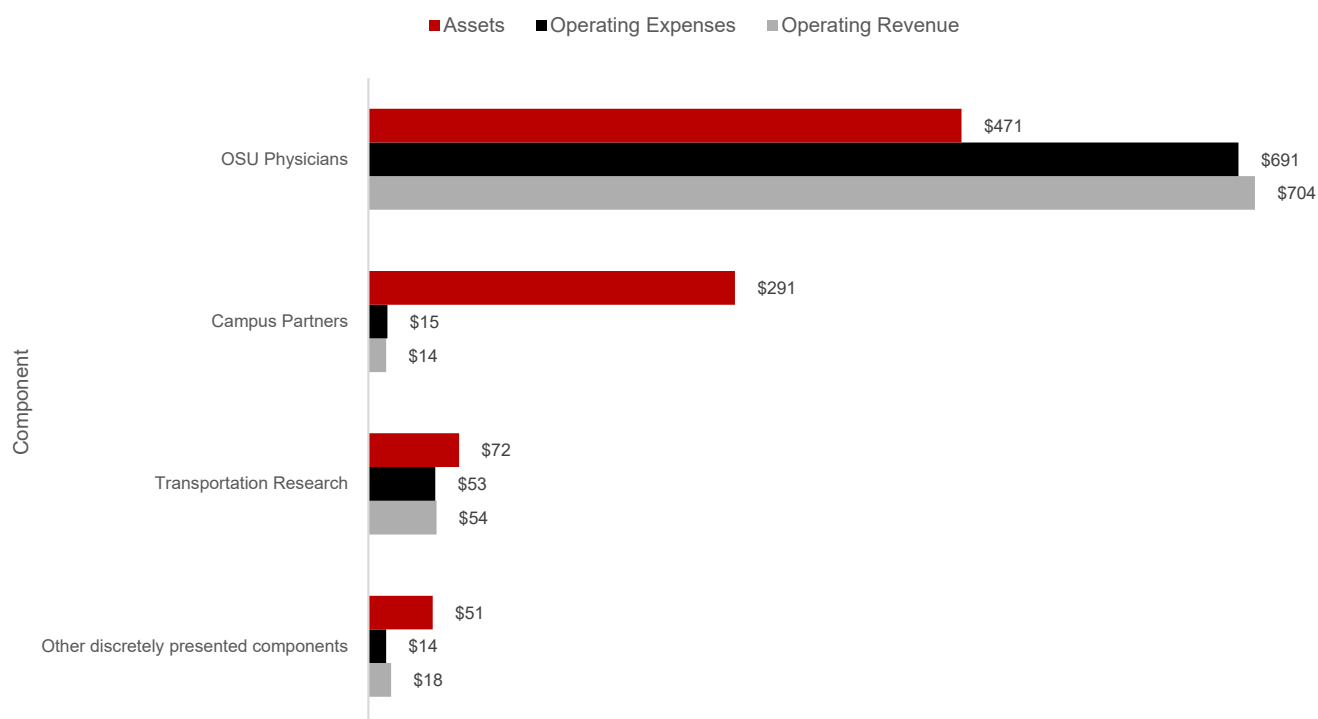


Financial reporting entity (continued)

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

Discretely presented component units

2022 Assets and Deferred Outflows of Resources, Operating Expenses, and Operating Revenue (in millions of dollars)

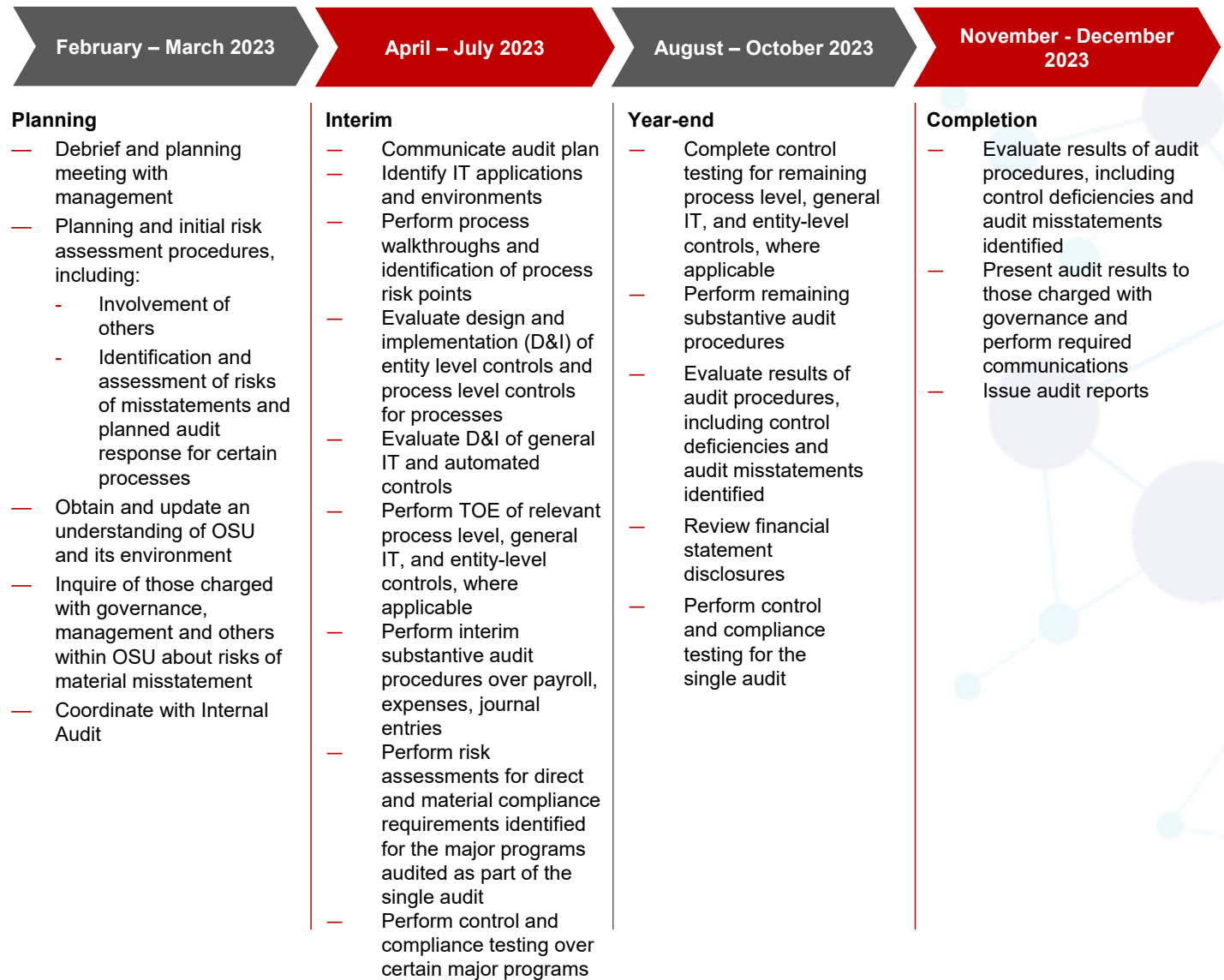


Materiality in the context of an audit

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"> a. Determining the nature and extent of risk assessment procedures; b. Identifying and assessing the risks of material misstatement; and c. Determining the nature, timing, and extent of further audit procedures.

Our timeline



Risk assessment: Significant risks

Significant risks	Susceptibility to:	
	Error	Fraud
<p>Management override of controls</p> <p>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.</p>		Yes

Significant risks	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		<p>Significant assumptions used that have a high degree of subjectivity:</p> <p>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.</p>

Risk assessment: Significant estimates

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

Applicable accounting pronouncements to be adopted in FY 2023:



GASB Statement No. 94, Public-Private and Public-Public Partnerships and Availability Payment Arrangements

The requirements of this Statement are effective for periods beginning after June 15, 2022, or OSU's FY23 financials. Addresses issues related to public-private and public-public partnership arrangements.

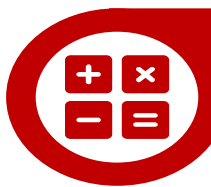


GASB Statement No. 96, Subscription-based Information Technology Arrangements

The requirements of this Statement are effective for periods beginning after June 15, 2022, or OSU's FY23 financials. This Statement provides guidance on the accounting and financial reporting for subscription-based information technology arrangements (SBITAs) for government end users (governments). This Statement (1) defines a SBITA; (2) establishes that a SBITA results in a right-to-use subscription asset – an intangible asset – and a corresponding subscription liability; (3) provides the capitalization criteria for outlays other than subscription payments, including implementation costs of a SBITA; and (4) requires note disclosures regarding a SBITA.

New and upcoming accounting pronouncements (continued)

Applicable accounting pronouncements to be adopted in FY 2023:



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).

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 component units, equity method investees/investments, 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 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 trustees, 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.

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?

Single audit update (for the year ended June 30, 2022)

The Single Audit in accordance with the Uniform Guidance (UG) is required to be filed annually by March 31st. Although we have open questions relative to the completeness and accuracy of the federal program expenditures and presentation of certain programs which may impact our major program determination, based on draft federal expenditure data as of December 20, 2022 our major programs are expected to be:

Major Programs identified in planning	New major programs identified	Other Changes
<ul style="list-style-type: none"> — Research and Development Cluster (R&D) — Student Financial Assistance Cluster (SFA) — Higher Education Emergency Relief Fund (HEERF) — Provider Relief Fund (PRF) — Medicaid Cluster 	<ul style="list-style-type: none"> — Shuttered Venue Operators Grant Program — Epidemiology and Laboratory Capacity for Infectious Diseases Program* — Protecting and Improving Health Globally: Building and Strengthening Public Health Impact, Systems, Capacity and Security <p>*Management finalizing evaluation of expenditures required to be reported</p>	<ul style="list-style-type: none"> — Coronavirus Relief Fund (CRF) was removed as there were no 2022 expenditures

- Samples have been selected and testing is progressing for all direct and material compliance requirements for the major programs identified in planning, except for the Enrollment Reporting special test for the SFA Cluster
- Our 2023 single audit is expected to commence in March 2023 or once the 2022 single audit has concluded

Update prepared as of January 30, 2023

Questions?

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.



Appendix

Appendix I – SAS 145 Adoption	Page 26
Appendix II – On the 2023 higher education audit committee agenda	Page 27
Appendix III – KPMG U.S. Transparency report and Impact plan	Page 37

SAS 145 Adoption

We will expand our risk assessment procedures, particularly in relation to the entity's use of IT.

We may modify the nature, timing, and extent of our audit procedures and request different information compared to previous audits.

SAS 145 (AU-C 315), *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement*

- SAS 145 clarifies and enhances certain aspects of the identification and assessment of the risks of material misstatement to drive better risk assessments, and therefore, enhance audit quality, such as:
 - Requirements and guidance related to the auditor's risk assessment, in particular, obtaining an understanding of the entity's system of internal control and assessing control risk
 - Guidance that addresses the economic, technological, and regulatory aspects of the markets and environment in which entities and audit firms operate
- It does not fundamentally change the key concepts underpinning audit risk, which is a function of the risks of material misstatement and detection risk. Amendments have been made to other AICPA Professional Standards
- Affects both preparers and auditors
- Applies to audits of financial statements for periods ending on or after December 15, 2023. However, KPMG is early adopting SAS 145 for audits of financial statements for periods ending on or after **December 15, 2022.**



On the 2023 higher education audit committee agenda

January 2023



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

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

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

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



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

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

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

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

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

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



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

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

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

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

In 2022, colleges and universities confronted no shortage of developing risks that could impact several long-standing social, climate, and governance priorities. For example, a Supreme Court case on affirmative action expected to be decided in 2023 could have far-reaching ramifications on student diversity and admissions, including recruitment, scholarships, standardized testing, and legacy preferences. Recent rule changes involving Name, Image, Likeness (NIL) opportunities for student athletes have introduced dynamics that may complicate management of athletic programs and exacerbate inequities. In addition, spiraling campus utility costs (which according to the Higher Education Price Index rose 43.1 percent during the year ended June 30, 2022²) have heightened expectations for institutions to demonstrate progress on climate action plans. And while cyber risk management may not jump to mind as an ESG imperative, it is considered critical to effective governance. Indeed, the integration of many ESG-related risks into the institution's enterprise risk management (ERM)

profile is increasingly evident. The higher education sector is still in the early stages of the ESG reporting journey. In our experience, while many institutions do not have a formal ESG strategy (or publish formal reports), most have long had initiatives pertaining to ESG objectives that may be tracked and reported on by various departments. Several institutions have made public commitments around student access and affordability, faculty diversity, and divestment of fossil fuel holdings in their endowment portfolios. Others are just beginning to inventory existing ESG activities and considering how to develop a comprehensive ESG approach. At all stages, there is ample room for alignment on and understanding of ESG definitions and a critical need for quantitative, reliable data. Still, for most colleges and universities (and for entities in other sectors), the absence of a generally accepted ESG framework and lack of consensus around key industry performance indicators remain major obstacles to progress.

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

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

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

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

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

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

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

- Consider where ESG information is currently disclosed, e.g., sustainability and DEI reports, the institution's website, etc. Who are the stakeholders using such information? What mechanisms exist for them to provide feedback and ask questions about our data? What internal controls and procedures are in place to ensure the quality of data used, and is it reviewed with the same rigor as financial results?
- Do we understand and receive reports on the basis for the disclosures and the processes used to generate them?
- Does the institution have an ESG or similar strategy, and who is responsible for its execution? Should a disclosure committee comprising appropriate senior administrative leaders, such as the chief sustainability officer, chief diversity officer, and chief information security officer, be created to facilitate the ESG strategy?
- How are material ESG risks identified? Are these risks integrated into the ERM profile?

- Does or should the institution utilize an ESG reporting framework?
- Have we enlisted faculty with ESG expertise to help us think through our strategy and framework?
- What metrics are used to measure progress against stated goals, and how are such metrics defined? Who within the institution will be responsible for generating and tracking such data and ensuring its conformity with applicable standards?
- Clarify the role of the audit committee in overseeing the institution's reporting of ESG risks and activities, particularly the scope and quality of ESG/sustainability reports and disclosures. How are the full board and other committees involved in overseeing ESG initiatives?
- Does (or should) the institution obtain assurance from internal or external auditors about certain ESG information to provide stakeholders with a greater level of comfort?



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

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

Indeed, several colleges and universities have succumbed to high-profile attacks, resulting in data breaches, network outages, and ransom payments to regain control of data or networks. A recent report by S&P⁵ indicates average weekly cyberattacks per organization in all industries are growing, and that education and research entities experienced 1,600 weekly attacks in 2021—the highest of any industry. The report notes that the cost of insuring against such attacks is also growing, with rated colleges and universities experiencing year-over-year increases of 40–60 percent in cyber insurance rates.

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

Although higher education stakeholders make important and wide-ranging financial and strategic contributions to the institutional mission, their varied interests can make quick decision-making a challenge. Fulfilling the needs and expectations of a such a complex network of stakeholders undoubtedly gives rise to more cybersecurity concerns. To mitigate these, institutions must be willing to embrace cutting-edge security solutions to manage the growing volume and sophistication of threats they face. It is

therefore imperative that institutions accelerate the implementation of robust security processes and controls that continuously assess and mitigate cyber vulnerabilities. As no university wants to fall victim to a breach while cybersecurity policies await revision or proactive measures need sign-off, every second counts.

The complex and rapidly changing cybersecurity and data governance regulatory environment includes a number of different security and privacy frameworks applicable to higher education institutions, including, among others, the National Institute of Standards and Technology (NIST), which may apply to federal and other grants; the EU's General Data Protection Regulation (GDPR), a data protection law for EU citizens; and the Safeguards Rule of the Gramm-Leach Bliley Act (GLBA), which regulates the collection, disclosure, and protection of consumers' nonpublic information and applies to colleges and universities receiving federal funds. Significantly expanded GLBA requirements that became effective on December 9, 2022, clarify that a qualified individual (typically a chief information security officer) must oversee the entity's security programs and include mandatory annual penetration testing and vulnerability assessments, training for security personnel, periodic assessments of service providers, written incident response plans, and periodic reports from the qualified individual to the board, among other requirements. Establishing processes to monitor and map the various requirements of applicable cybersecurity and data privacy frameworks—which will continue to change and expand—to the institution's enterprise-wide cybersecurity program is essential.

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

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

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

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

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

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

- Do we have clear insights into our cybersecurity program’s maturity, gaps, and threats? Does leadership have a prioritized view of additional investments needed? Are the institution’s most “valuable” assets adequately protected?
- Do we have the appropriate leadership, talent, and bench strength to manage cyber risks? What are the risks to the institution in the event of unexpected turnover or inability to fill key positions?
- Does the institution regularly test its incident response plan? How frequently are penetration and red team testing performed, and is there a formal process to address findings?
- How often are data and systems backed up, and how accessible are the backups? Resilience is vital to restoring operations after an attack.

- Do we have a robust institution-wide data governance framework that makes clear how and what data is collected, stored, managed, and used and who makes related decisions?
- Is security training for students, faculty, and staff regularly provided? Is training completion monitored and enforced? How is security awareness periodically assessed?
- Do security and privacy terms in agreements with third-party IT providers meet the institution’s criteria for adequate protections? Does management regularly review SOC reports and evaluate the institution’s complementary controls to flag possible issues? Do such vendors carry cyber insurance?
- How are we monitoring evolving and expanding federal, foreign, and other regulations governing data security and privacy to ensure our cybersecurity program and data governance framework reflect the latest requirements?
- Do we understand the coverages, limits, and underwriting criteria of our cyber insurance policy?
- Who reports on cyber to the audit committee and board? Is it a chief information security officer or similar position who speaks in business terms and understands that cyber is an enabler as well as a risk?



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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



About the KPMG Board Leadership Center

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

About the KPMG Audit Committee Institute

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

About the KPMG Higher Education practice

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

Contact us:

The KPMG HERON Audit practice

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

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

Regional leaders

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

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

Kurt Gabouer
Midwest
E: kgabouer@kpmg.com

Drew Corrigan
Pacific Northwest
E: dcorrigan@kpmg.com

Christopher Ray
West
E: cray@kpmg.com

David Harwood
Southwest
E: dharwood@kpmg.com

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

kpmg.com/socialmedia



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

© 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. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization. NDP417993-1A

U.S. Transparency report and Impact plan



2022 U.S. Transparency report

- Provides more granular detail on our commitment to continually enhance audit quality
- Outlines KPMG LLP's structure, governance and approach to audit quality

2022 U.S. Impact plan

- U.S. Impact Plan spotlights
 - Audit quality
 - Accelerate 2025
 - Reducing our carbon footprint
 - Community impact

Reports and supplements available at:

[Transparency Report and Supplements \(kpmg.us\)](#)
[2022 KPMG U.S. Impact Plan](#)



Thank you

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.

© 2022 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. NDP409981-1A

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



Information Security Update: Cybersecurity 4 You (C4U) Awareness Platform

Cindy Leavitt, Vice President & Chief Information Officer

Rich Nagle, Associate Vice President & Chief Information Security Officer

Legal, Audit, Risk, and Compliance Committee

Public Session

February 2023

cybersecurity
FOR YOU

Ohio State and C4U

- Per Proofpoint's 2022 State of Phish report, "Cybersecurity skills are life skills, not work skills".
- A lack of easily accessible, effective cybersecurity awareness training for university and medical center employees led to the creation of C4U in 2019.
- By engaging users in both personally-relevant content and compliance training for work activities, C4U enlists users to be part of the solution by:
 - Changing the culture of Ohio State to be more security aware
 - Changing the perception of security as being burdensome
 - Promoting users to be more self-interested in security
 - Changing habits and behaviors of users, not just compliance
 - Making security more fun and approachable



C4U

Metrics of Success

- Since its launch, C4U has seen **18,881** individual employees *voluntarily* utilize it, with **77.9%** return visitors.
- In 2022 alone, there was **66% increase in new users**. Much of 2022's increase can be traced to the inclusion of the Institutional Data Policy Awareness (IDPA) training into C4U.
- Many of these new users first visited C4U between February and April (the IDPA window). Users were asked at that time to complete a *single* piece of IDPA content.
- Of these new users in 2022, 811, or 15%, went on to achieve a full level in C4U
- Effectively, C4U was able to present users with a single awareness training and the content engaged them enough that **15%** began an optional, self-directed cybersecurity education journey.



Future Development

- Present state, C4U strictly promotes cybersecurity awareness and encourages **staff and faculty** to change their behaviors to be more secure.
- In our first 4 years of C4U, we have been recognized as a leader in Big Ten cybersecurity awareness platforms.
- The ultimate goal is long-term sustainment and culture change within the *entire* university community.
- **The platform will be opened to students this fall.**
 - Student groups will be engaged to test the platform and its content during the Spring Semester.
 - Will be promoted at summer student orientations.
 - Marketing campaigns will promote the wide release of the platform in the fall.
- Expanded reward options to include digital rewards and donation options to the James' Fund for Life and The Ohio State Fund for Scholarships.



Impact of C4U

Awareness of Reporting Phish Increasing Year to Year:

- Per Proofpoint, 47% of their polled users either do not know what phishing is or answer incorrectly.
- Within the Ohio State community, there has been a month over month increase in reporting of phish at the university since C4U's implementation (from March 2020 to January 2023).



User Personal Testimonials:

- “Right after I read the article, I went on my phone to check/adjust my privacy settings.”
- “It was easy to check my settings while I went through this training!”
- “Thanks for the tips - I was making some mistakes on public Wi-Fi for sure!”



Student Impact



Izaiah Steenrod



Kate Goertz



SUMMARY OF ACTIONS TAKEN

November 16, 2022 – Legal, Audit, Risk & Compliance Committee Meeting

Voting Members Present:

Alan A. Stockmeister
Jeff M.S. Kaplan

Elizabeth A. Harsh
Taylor A. Schwein

Hiroyuki Fujita (ex officio)

Members Present via Zoom:

Elizabeth P. Kessler
Amy Chronis

Members Absent:

Michael Kiggin

The Legal, Audit, Risk & Compliance Committee of The Ohio State University Board of Trustees convened on Wednesday, November 16, 2022, in person at Longaberger Alumni House on the Columbus campus and virtually over Zoom. Committee Chair Elizabeth Kessler called the meeting to order at 12:02 p.m.

PUBLIC SESSION***Items for Discussion:***

1. Audit Update: Mr. Michael Papadakis, Ms. Kris Devine, Mr. Vincent Tamaro and Mr. Dave Gagnon, the university's external auditor from KPMG, presented an audit update to discuss the draft of the university's audited consolidated financials prior to its submission to the Auditor of State.

(See Attachment X for background information, page XX)

2. Annual Affiliated Entities Report: Senior Associate Vice President and Deputy General Counsel Matt Albers and Senior Assistant Vice President and Senior Associate General Counsel Heidi McCabe shared the annual report on Ohio State's affiliated entities. Dr. Wondwossen Gebreyes, leader of Ohio State's Global One Health initiative, also joined to discuss the work of Global One Health, LLC, which was established in 2016.

(See Attachment X for background information, page XX)

Items for Action:

3. Approval of Minutes: No changes were requested to the August 17, 2022, meeting minutes; therefore, a formal vote was not required, and the minutes were considered approved.
4. Resolution No. 2023-55: Approval to Submit 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 operates on a fiscal year ending June 30 of each year; and

WHEREAS the university has produced consolidated financial statements for the 2021 and 2022 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 2021 and 2022 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 2021 and 2022 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.

(See Appendix X for background information, page XX)

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

EXECUTIVE SESSION

It was moved by Ms. Kessler, and seconded by Mr. Kaplan, that the committee recess into executive session to consult with legal counsel regarding pending or imminent litigation, to consider business-sensitive trade secrets that are 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 go into executive session with the following members present and voting: Ms. Kessler, Mr. Stockmeister, Mr. Kaplan, Mrs. Harsh, Ms. Schwein, Ms. Chronis, and Dr. Fujita

The committee entered executive session at 12:36 p.m. and the meeting adjourned at 2:00 p.m.