THE UNIVERSITY OF VERMONT AND STATE AGRICULTURAL COLLEGE
BOARD OF TRUSTEES

AUDIT COMMITTEE

Members: Chair Shap Smith, Vice Chair Jodi Goldstein, Matt Devost, Katelynn Giroux, Ed Pagano, Kristina Pisanelli, and Catherine Toll

Representatives: Faculty Representative Barbara Arel, Staff Representative Mindy Bean, Graduate Student Representative Vanessa Ballard, Alumni Representative Susan Higgins, Student Representative Matt Sorensen, and Representative Doug Hoffer of the State Auditor's Office

Thursday, April 11, 2024

3:00 p.m. – 4:00 p.m.
230 Waterman Building

AGENDA

	Item	Enclosure/ Exemption	Discussion Leader(s)	Times*
	Call to order			***3:00 p.m.**
1.	Approval of February 8, 2024 meeting minutes	Attachment 1	Shap Smith	3:00-3:05
2.	Presentation of the FY 2024 external audit engagement plan • Resolution authorizing retention of external audit firm for the FY 2024 mandatory annual audits	Attachments 2 & 3	David Gagnon and Sara Timmerman, KPMG	3:05-3:15
3.	Higher education industry update	Attachment 2	David Gagnon, KPMG	3:15-3:25
4.	Compliance update	Attachments 4 & 5	Tessa Lucey	3:25-3:35
5.	Campus Threats/Mass Casualty (*Enterprise Risk Management Risk #7 Update*)	Attachment 6	Mike Schirling	3:35-3:45
6.	Emergency Preparedness & Institutional Continuity (*Enterprise Risk Management Risk #29 Update*)	Attachment 6	Mike Schirling	3:45-3:55
7.	Other business		Shap Smith	3:55-4:00
	Motion to adjourn			**4:00 p.m.**

* Time is approximate.
** Executive session as needed.

AUDIT COMMITTEE
BOARD OF TRUSTEES
UNIVERSITY OF VERMONT AND STATE AGRICULTURAL COLLEGE

A meeting of the Audit Committee of the Board of Trustees of the University of Vermont and State Agricultural College was held on Thursday, February 8, 2024, at 3:00 p.m. in the Livak Ballroom, Room 417-419 Dudley H. Davis Center.

MEMBERS PRESENT: Chair Shap Smith, Vice Chair Jodi Goldstein[1], Otto Berkes, Kenny Nguyen, Kristina Pisanelli[2], and Catherine Toll

MEMBERS ABSENT: Ed Pagano

OTHER TRUSTEES PRESENT: Board Chair Ron Lumbra and Katelynn Briere

REPRESENTATIVES PRESENT: Faculty Representative Barbara Arel, Staff Representative Mindy Bean, Alumni Representative Susan Higgins[2], and Vermont State Deputy Auditor Tim Ashe[2] (on behalf of Vermont State Auditor Douglas Hoffer)

REPRESENTATIVES ABSENT: Graduate Student Representative Vanessa Ballard and Student Representative Matt Sorenson

PERSONS ALSO PARTICIPATING: President Suresh Garimella, Vice President for Finance & Administration Richard Cate, Vice President for Legal Affairs & General Counsel Trent Klingerman, Chief Internal Auditor Bill Harrison, University Controller Claire Burlingham, Director of Compliance Services and Chief Privacy Officer Tessa Lucey, Administrative Assistant Amy Vile and David Gagnon[2], and Sara Timmerman of KPMG

[1] Joined the meeting at 3:08 p.m.
[2] Participated by phone.

Chair Shap Smith called the meeting to order at 3:05 p.m. He began by acknowledging Otto Berkes and Kenny Nguyen for their work on the committee as they finish their term on the Board of Trustees.

Approval of minutes

A motion was made, seconded, and voted to approve the November 6, 2023, meeting minutes.

Presentation of the Fiscal Year (FY) 2023 uniform administrative requirements, cost principles, and audit requirements for federal awards (Uniform Guidance)

University Controller Claire Burlingham and Senior Audit Manager Sara Timmerman reported that with respect to KPMG's report on internal control and compliance based on the Uniform Guidance, -KPMG's opinion was unmodified with no material weaknesses and no significant deficiencies. On compliance and internal control at the program level, there were no material weaknesses or significant deficiencies in internal control over compliance. UVM remains a low-risk auditee.

Next, Ms. Timmerman explained that the research and development cluster, Medicaid cluster, and the Department of Education fund for improvement of postsecondary education were the major federal programs tested in FY 2023.

To finish, Lead Audit Engagement Partner David Gagnon offered an overview of the Department of Education's related-party disclosure requirements and how they may impact the university.

FY 2023 NCAA agreed-upon procedures

Claire Burlingham and Sara Timmerman reported that as it relates to the agreed upon procedures, there were no significant findings or adjustments identified.

Presentation of FY 2023 IT observations

Sara Timmerman reviewed KPMG's information technology controls assessment and discussed one observation and recommendation related to PeopleSoft. Furthermore, Claire Burlingham offered an overview of management's corrective actions. In conclusion, President Suresh Garimella commented on how Enterprise Technology Services (ETS) and Human Resource Services (HRS) were working together to prioritize and strengthen access control.

Internal audit update

Chief Internal Auditor Bill Harrison offered an overview of internal audit and follow-up activity since his last report to the committee on September 18, 2023. Mr. Harrison noted that a planned financial audit of an international sponsored project has been removed from the work plan because the sponsor has removed the audit requirement from the grant agreement.

Compliance annual survey results

Director of Compliance Services and Chief Privacy Officer Tessa Lucey presented the results of the fourteenth annual compliance awareness survey. Ms. Lucey explained that the survey provides an opportunity to demonstrate that the university's compliance program is operating effectively. Despite seeing a slight reduction in awareness and culture scores over the 2022 results, the overall awareness and culture scores continue to affirm the efficacy of the program. The results show there is strong awareness and a solid culture of compliance across the university.

Presentation of the results of the biennial Enterprise Risk Management (ERM) assessment

Tessa Lucey began by offering an overview of the ERM risk assessment biennial cycle. Every two years, a comprehensive assessment is conducted, complemented by a survey in the intervening year. In calendar year 2023, the university completed its first off-year survey.

Ms. Lucey explained that based on the survey results there were two changes to the Heat Map related to discrimination and bias, and research data.

Executive Session

At 3:50 p.m., Chair Smith entertained a motion to enter into executive session for the purpose of discussing contracts, general public knowledge of which would clearly place the university at a substantial disadvantage.

All in attendance were excused from the meeting, with the exception of Trustees, President Suresh Garimella, Vice President for Finance & Administration Richard Cate, Vice President for Legal Affairs & General Counsel Trent Klingerman, Chief Internal Auditor Bill Harrison, University Controller Claire Burlingham, and Administrative Assistant Amy Vile.

The meeting was re-opened to the public at 3:56 p.m. There being no further business, the meeting was adjourned.

Respectfully submitted,

Shap Smith, Chair

KPMG

University of Vermont State and Agricultural College

Discussion with the Audit Committee of the Board of Trustees

Prepared on: March 28, 2024
Presented on: April 11, 2024

Audit plan and strategy for the year ending June 30, 2024

Audit Committee of the Board of Trustees
University of Vermont State and Agricultural College:

We are pleased to have the opportunity to meet with you to discuss our audit plan and strategy for the University of Vermont State and Agricultural College – (the University) as of and for the year ending June 30, 2024. We continuously look to build on our strong understanding of the University, bring fresh perspectives, and focus on our service commitments.

As required by our professional standards, this report highlights our required communications with the Audit Committee, and includes other information that we believe you will find helpful. We present our scope of work, a timeline, our engagement team, audit focus areas, and our responsibilities. We have also included certain reminders with respect to independence requirements and governance considerations for audit planning.

This year, we have also included our most recent Peer Review Report, which includes a *pass* rating (the highest rating possible), as well as the related American Institute of Certified Public Accountants' National Peer Review Committee's acceptance letter dated December 7, 2023.

We look forward to our discussion.

Best regards,

David Gagnon
Partner, Audit, U.S. Sector Leader, Higher Education & Other Not-for-Profits

We aim to deliver an exceptional client experience by focusing on:

Quality
in all that we do and how we deliver

Experience
providing an intentional and exceptional experience for our clients

Productivity
audit smarter, not harder

Insights
leading industry and topical information sharing

Required communications to the Audit Committee

Audit plan required communications and other matters

✓ = Matters to report X = No matters to report

Our audit of the financial statements of the University of Vermont (the University) as of and for the year ending June 30, 2024, will be performed in accordance with auditing standards generally accepted in the United States of America and *Government Auditing Standards*.

Performing an audit of the 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 University's ICFR. As a reminder, we do not issue an opinion on internal control.

Our compliance audit for the University's major federal program will also be performed in accordance and the audit requirements of Title 2 U.S. Code of Federal Regulations Part 200, *Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards* (Uniform Guidance).

We will perform an NCAA Agreed-Upon Procedures engagement as of June 30, 2024.

Matters to communicate		Response
Role and identity of the lead audit engagement partner	✓	David Gagnon
Significant findings or issues discussed with management	X	
Client service team	✓	Page 5
Materiality in the context of an audit	✓	Page 6
Our timeline	✓	Page 7
Risk assessment: Significant risks	✓	Page 8
Areas of focus, planned approach, newly effective accounting standards, and Single Audit overview	✓	Pages 9 to 12
Use of technology in the audit	✓	Page 13
Independence, including Peer Review report	✓	Pages 14 and 15
Responsibilities	✓	Page 16
Governance considerations and inquiries	✓	Page 17

Client Service team

University of Vermont– Audit Committee of the Board of Trustees

David Gagnon
Lead Engagement Partner

Marie Zimmerman
Engagement Quality Control Partner

Audit

Sara Timmerman
Lead Audit Senior Manager

Logan Lamothe
Senior Associate

Burlington based audit staff

Subject Matter Professionals

Tax

Shy Joseph
Exempt Tax Managing Director

IT

Kevin Sutula
IT Director

Actuarial

Alexander Smith
Actuary Director

GASB

Jeff Markert
National Office Leader, GASB Accounting and Auditing

Materiality in the context of an audit

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

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 consolidated financial statements.	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.	Judgments about materiality involve both qualitative and quantitative considerations.
Judgments about matters that are material to users of the consolidated 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.	Determining materiality is a matter of professional judgment and is affected by the auditors' perception of the financial information needs of users of the financial statements.	Judgments about the size of misstatements that will be considered material provide a basis for 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

March – April	May – July	August – November	December – February
Planning and risk assessment — Communicate audit plan — Complete initial risk assessment procedures, including: - Identification and assessment of risks of misstatements and planned audit response for certain processes — Update our understanding of key processes, information systems, and changes in internal control — Identify relevant IT applications and environments — Identify major programs for Uniform Guidance audit	**Interim** — Ongoing risk assessment procedures — Perform process walk-throughs and identification of process risk points for certain processes — Evaluate D&I of general IT and automated controls for Uniform Guidance — Perform interim substantive audit procedures — Perform interim fieldwork for Uniform Guidance audit	**Year-end** — Perform remaining substantive audit procedures relative to June 30 account balances — Evaluate results of audit procedures, including control deficiencies and audit misstatements identified — Present audit results to the Audit committee and required communications — Issue opinion on financial statements — Issue report on Compliance and on Internal Controls in accordance with *Government Auditing Standards* — Review preliminary management letter comments, if any	**Completion and reporting** — Perform remaining procedures related to Uniform Guidance audit — Issue NCAA agreed-upon procedures report — Present Uniform Guidance audit results to the Audit Committee and required communications — Debrief on audit process

Year-round liaison with University Audit Committee, Internal Audit and senior management. Continuous identification and resolution of key risks and issues.

Significant risks

Significant risk	Susceptibility to:
	Fraud
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. **Relevant factors affecting our risk assessment** – the size of the entity, the oversight and governance controls in place, and the "tone at the top" of the organization are relevant factors considered when evaluating the risk of management override of controls. Although, the level of risk of management override of controls will vary from entity to entity, the risk nevertheless is *present in all entities*. Professional standards require us to perform procedures sufficiently responsive to address the risk of management override of internal controls. Such procedures include: • Inquiring of management and governance • Assessing the effectiveness of entity-level controls • Considering potential fraud risks affecting financial reporting • Understanding and evaluating the journal entry process and the completeness of journal entry activity • Identifying and testing high-risk journal entries, if any • Considering the results of other audit procedures primarily in areas of judgment	**Yes**

Areas of focus and planned approach

The following pages discuss the results of our preliminary risk assessments, including the areas of focus and our primary planned procedures.

Areas of Focus	Primary planned procedures
Investments	— Confirm with fund managers, custodians, and banks — Test investment correspondence including statements, reports, cash activity, and audited financial statements — Independently price level 1 and 2 securities — Complete other procedures for funds stated at net asset value, as a practical expedient including review of audited financial statements and rollforward procedures from 12/31 to 6/30
Actuarially determined liabilities (OPEB)	— Review pension valuation and actuarial assumptions using a specialist — Test key underlying data used to determine the liability and valuation — Evaluate required disclosures and RSI
Compensation and benefits	— Review payroll related accrued liabilities — Test payroll expense and other related benefit costs
Net tuition and fees, auxiliary revenue and related receivables, and grants and contracts	— Test tuition, auxiliary revenue, and institutional aid on a sample basis and analytical basis — Test sponsored research funding on a sample basis of grants and contracts

Areas of focus and planned approach (continued)

Areas of Focus	Primary planned procedures
Capital assets and related depreciation	— Review a sample of fiscal 2024 fixed asset additions and construction-in-progress additions — Review reasonableness of capital interest — Review reasonableness of depreciation expense — Review third party housing transactions for accounting and reporting, as applicable
Debt and related items	— Confirm outstanding debt with financial institutions — Review reasonableness of interest expense — Review debt transactions, as applicable
Commitments and contingencies and other	— Evaluate outstanding legal and regulatory matters — Confirm with legal counsel — Evaluate financial statement presentation and disclosures, including new discretely presented component units

Single Audit overview and scope

Area of audit focus	Primary audit approach
Schedule of expenditures of federal awards (SEFA) prepared by management	We will review the SEFA, prepared by management, for appropriate presentation and accuracy of assistance listing number (ALN) references, pass-through ID, and cluster presentation.
Major program determination	We expect one major program in scope this year: Student Financial Assistance (SFA) cluster. *Finalization of major program determination is dependent on the final schedule of expenditures of federal awards and risk assessment procedures.*

2020 major programs audited	2021 major programs audited	2022 major programs audited	2023 major programs audited	2024 major programs planned
— Research and Development Cluster — Medicaid Cluster — Coronavirus Relief Fund	— Student Financial Assistance Cluster — Covid 19-Higher Education Emergency Relief Fund — Coronavirus Relief Fund	— Research and Development Cluster — Covid 19-Higher Education Emergency Relief Fund	— Research and Development Cluster — Medicaid Cluster — Department of Education-Endowment award	— Student Financial Assistance Cluster

Regulatory and accounting update: New accounting standards

New accounting standards	2024	2025
GASB 100, Accounting Change and Error Corrections	✖	
GASB 101, Compensated Absences		✖

Use of technology in the audit

Our multi-year technology plan includes the following tools.

Bolded tools have been implemented in prior year audits with the expectation of continued expansion of other tools in the future.

Analytics

Analytics tools:

- Operating Expense Solution
- Journal Entry Insights
- Data Visualization
- Account Analysis
- Journal Entry Analysis
- Planning Analytics
- Compare Engine
- Matching Engine
- MindBridge

Automation

Automation tools:

- Data extraction scripts
- DataSnipper
- Automated Industry Routines
- Confirmation
- IT Automation

Collaboration

Collaboration tools:

- KPMG Clara for clients
- DocuSign™

Workflow

Workflow tools:

- KPMG Clara workflow

KPMG Clara Expansion

Alteryx

PowerBI

KPMG Audit Chat

Automated Vouching Tool

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 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, 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 with significant influence over the University, and persons in key positions with respect to the preparation or oversight of the consolidated financial statements

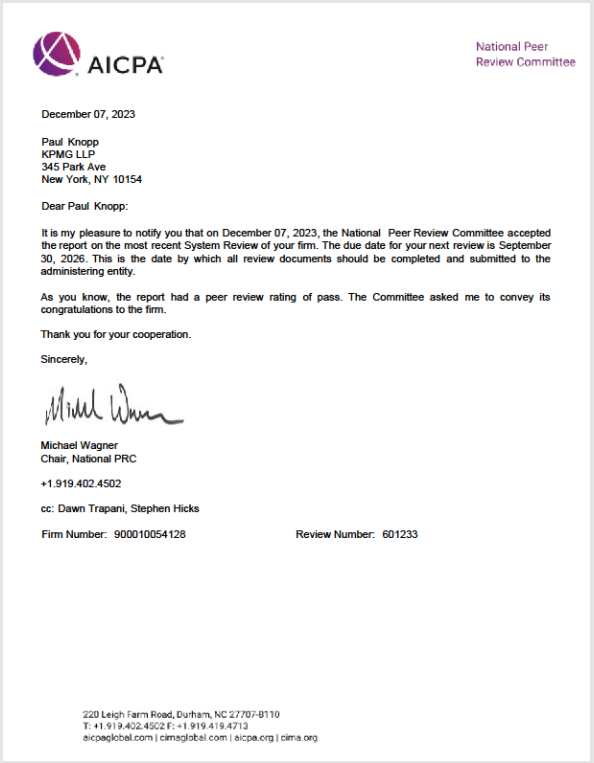
Certain relationships with KPMG

Independence rules prohibit:

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

Peer Review

Our most recent peer review report was accepted by the AICPA's National Peer Review Committee (NPRC) on December 7, 2023. **The peer review report had a rating of pass, which is the highest rating possible.** The 2023 peer review report was unmodified and therefore did not require a KPMG response letter. As a reminder, the peer review covers our firm's system of quality control for the accounting and auditing practice applicable to those not subject to Public Company Accounting Oversight Board permanent inspection for the year ended March 31, 2023 (i.e. non-public company practice).



AICPA

National Peer Review Committee

December 07, 2023

Paul Knopp
KPMG LLP
345 Park Ave
New York, NY 10154

Dear Paul Knopp:

It is my pleasure to notify you that on December 07, 2023, the National Peer Review Committee accepted the report on the most recent System Review of your firm. The due date for your next review is September 30, 2026. This is the date by which all review documents should be completed and submitted to the administering entity.

As you know, the report had a peer review rating of pass. The Committee asked me to convey its congratulations to the firm.

Thank you for your cooperation.

Sincerely,

Michael Wagner
Chair, National PRC

+1.919.402.4502

cc: Dawn Trapani, Stephen Hicks

Firm Number: 900010054128 Review Number: 601233

220 Leigh Farm Road, Durham, NC 27707-8110
T: +1.919.402.4502 F: +1.919.419.4713
aicpaglobal.com | cimaglobal.com | aicpa.org | cima.org

Responsibilities

Management responsibilities

- Communicating matters of governance interest to those charged with governance.
- Preparing the consolidated financial statements and maintaining a system of internal control over financial reporting and compliance.
- The audit of the consolidated financial statements or compliance 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 consolidated financial statement audit and compliance 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.

KPMG responsibilities – Other

- Forming and expressing an opinion about whether the consolidated financial statements that have been prepared by management, with the oversight of governance, are prepared, in all material respects, in accordance with U.S generally accepted accounting principles.
- Forming and expressing an opinion on compliance for each of the University's major federal programs.
- 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, if any.
- 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.

Governance considerations and inquiries

In accordance with auditing standards, the following topics are included for the consideration of the Audit Committee. These risks are relevant to our audit planning and execution. We are not asking for specific responses, unless there is a matter that warrants particular attention that management has not communicated. Please know that we have robust discussions with management throughout the audit about these risk areas, among other considerations, and do so for every audit we perform.

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, governance, and other related matters, and the effect of such developments on, for example, the overall presentation, structure, and content of the consolidated financial statements, including the following:
  - The relevance, reliability, comparability, and understandability of the information presented in the consolidated financial statements?
  - Whether all required information has been included in the consolidated 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 considerations, as applicable:

- 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?

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 the Audit Committee is intended solely for the information and use of the Audit Committee 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.

---

kpmg.com/socialmedia

Appendix I
On the 2024 Higher Education Audit Committee Agenda

On the 2024 higher education audit committee agenda

January 2024

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

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

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

Drawing on insights from our interactions with higher education audit committees and senior administrators, we've highlighted several issues to keep in mind as audit committees consider and carry out their 2024 agendas:

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

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

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

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

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

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

Colleges and universities can further enhance their cybersecurity protocols by:

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

---

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

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

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

- Do we have clear insights into our cybersecurity program's current maturity, gaps, and threats, including whether the institution's most "valuable" assets are adequately protected? Does leadership have a prioritized view of additional investments needed? Measurement may be facilitated by guidance from, for example, the federal Cybersecurity and Infrastructure Security Agency (CISA) and the not-for-profit Center for Internet Security (CIS), who provide self-assessment tools such as *Stop Ransomware and the CIS Top 18 Critical Controls*, respectively. The CIS database also allows for benchmarking against other colleges and universities.
- Do we have the appropriate leadership, talent, and bench strength to manage cyber risks? In the event of unexpected turnover or inability to fill key positions, what are the risks to the institution?
- Who reports on cyber to the audit committee and board? Is it a chief information security officer or similar position who speaks in business terms and understands that cyber is an enabler and risk?
- Do we regularly test our incident response plan? Does our plan include up-to-date escalation protocols that, among other things, specify when the board is informed of an incident? What is the frequency of penetration and red team testing, and is there a formal process to address findings? How often are data and systems backed up, and how accessible are the backups? Resilience is vital to restoring operations after an attack.
- Do we have a robust institution-wide data governance framework that makes clear how and what data is collected, stored, managed, and used, and who makes related decisions? How does our framework intersect with our AI governance policy?
- Is security, privacy, and data governance training for students, faculty, staff, and other stakeholders regularly provided? Is training completion and effectiveness monitored and enforced? How is security awareness periodically assessed?
- Do security and privacy terms in agreements with third-party information technology (IT) providers meet the institution's criteria for adequate protections? Does management regularly review SOC reports and evaluate the institution's complementary controls to flag possible issues? Do such vendors carry cyber insurance?
- How are we identifying changes to federal, foreign, and other regulations governing data security and privacy to ensure our cybersecurity program and data governance framework reflect the latest requirements?
- Do we understand the coverages, limits, and underwriting criteria of our cyber insurance policy?

Define the audit committee's oversight responsibilities for AI

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

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

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

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

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

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

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

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

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

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

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

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

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

In our experience, although some institutions do not have a formal ESG strategy or publish formal reports, most have long had initiatives pertaining to ESG objectives that may be tracked and reported on by various departments. Many are still inventorying existing ESG activities and considering how to develop a comprehensive ESG approach. At all stages, there is ample room for agreement and alignment on ESG definitions and a critical need for quantitative, reliable data. Still, the absence of a generally accepted ESG framework in the sector (as in most other industries) and lack of consensus around key industry performance indicators remain major obstacles to progress.

The extent to which higher education institutions will be subject to ESG disclosure requirements remains uncertain. Media reports have been dominated by the Securities and Exchange Commission's (SEC) March 2022 climate reporting proposal, under which public companies would report direct and indirect emissions, including those generated through supply chains and affiliates. The proposal has met with resistance by registrants and lawmakers, and a final ruling has not yet been issued. While the SEC does not directly regulate the higher education sector, its oversight of public debt markets includes conduit offerings by colleges and universities (although proposed

rulemaking to date does not apply to such offerings). Nevertheless, many institutions have begun including sustainability data in their offering documents, issuing reports on climate and DEI factors in their endowment management, and sharing ESG information with bond rating agencies (who consider ESG risks in ratings reports).

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

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

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

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

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

The audit committee should ask:

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

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

Monitor other emerging regulations and standards impacting the institution

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

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

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

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

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

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

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

- Under Topic 958, in-scope crypto assets may qualify to be presented as part of investments in the institution's statement of financial position and related investment return in the statement of activities, subject to certain disclosures. However, in-scope crypto assets cannot be combined with other intangible assets and related changes therein if the institution reports such line items in the statements of financial position and activities, respectively. The ASU does not address classification of fair value changes of in-scope crypto assets in the statement of activities. Accordingly, institutions may present such changes within operating or nonoperating activities depending on the institution's policy and consistent with whether such changes are presented as part of investment return.
- In the statement of cash flows, cash receipts from the near-immediate liquidation of donated crypto assets are classified as financing activities if donor-restricted for long-term investment or capital purposes, or as operating activities if no 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:

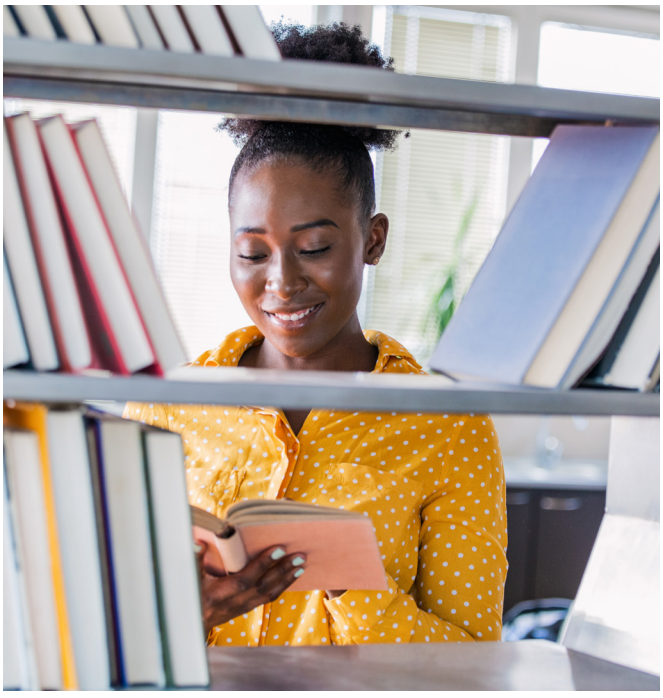
- Although changes to modes of working (i.e., remote, hybrid, and in-person) have largely stabilized in the industry, competition for talent in some functions and regions remains challenging, especially at institutions limited by traditional compensation structures. While bolstering recruitment and retention 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

Rosemary Meyer
Midatlantic
E: rameyer@kpmg.com

Cathy Baumann
Midwest
E: cbaumann@kpmg.com

Christopher Ray
West
E: cray@kpmg.com

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

Jennifer Hall
Southeast
E: jchall@kpmg.com

Drew Corrigan
Pacific Northwest
E: dcorrigan@kpmg.com

Susan Warren
Southwest
E: smwarren@kpmg.com

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

Learn about us: **kpmg.com**

Appendix II
2024 Higher Education Industry Update

2024 higher education industry update

University of Vermont

March 2024

CONFIDENTIAL

Topics

01
Higher education audit committee and internal audit focus areas in 2024

02
Cybersecurity in higher education: security awareness and training

03
AI in higher education and in the audit

04
ESG in higher education

05
2023 *NACUBO-Commonfund Study of Endowments*

06
Related party disclosures required by U.S. Department of Education

07
Other developments affecting federal grants and contracts

08
Update to Government Auditing Standards

09
Presentation of discounts to student services revenues (GASB institutions)

01

Higher education audit committee and internal audit focus areas in 2024

Higher education audit committee focus areas in 2024

The risk agendas of higher education audit committees will continue to expand in 2024. Accordingly, taking a fresh look at the audit committee's agenda, workload, and capabilities will be important. We've highlighted several potential areas of expected focus below, many of which overlap with risks in the sector more broadly.

- Keep a watchful eye on the institution's cybersecurity and data governance risks.
- Understand how the institution is considering and deploying artificial intelligence (AI), and help define the board's oversight responsibilities.
- Understand how the institution is managing and reporting on sustainability and diversity, equity, and inclusion (DEI) risks and potentially applicable regulations.
- Monitor other emerging regulations and standards impacting the institution, such as related party disclosure requirements from the U.S. Department of Education effective in fiscal 2024.
- Stay focused on leadership and talent in finance and other key functions as the institution refines its business model.
- Monitor protocols to ensure research compliance and integrity, including as to grant administration, conflicts of interest and commitment, foreign influence, and misconduct.
- Ask about management's processes to ensure integrity and consistency of data provided or available to creditors, ranking and rating agencies, grantors, and other third parties.
- Sharpen the institution's focus on ethics, compliance, and culture.
- Understand risks of and changes to the institution's international activities and alliances.
- Help internal audit stay focused on critical risks while adding value to the institution.

*United Educators' Top 10 Risks of 2023**

1. Data Security
2. Enrollment
3. Recruitment and Hiring
4. Operational Pressures
5. Student Mental Health
6. Funding
7. Facilities and Deferred Maintenance
8. Regulatory and Legal Compliance (non-VAWA/Title IX)
9. Title IX
10. External Pressures

* Based on survey responses in September and October 2023.

Higher education internal audit focus areas in 2024

The opportunity for internal audit (IA) to maximize its influence within the institution and help respond to risk is ever-increasing. College and university IA functions can challenge the status quo to reduce risk, improve controls, and identify efficiencies and cost benefits across the institution. We've highlighted several risks and other focus areas to help maximize IA's value to the institution in 2024.

- Cybersecurity, data governance, and distributed enterprise threats amid hybrid working and patient care environments and growing geopolitical instability.
- Sufficiency of management's compliance with evolving cybersecurity and data governance regulations and grantor requirements.
- Appropriateness and extent of the institution's use and governance of AI.
- Adequacy of safeguards to ensure proper migration of data and systems to the cloud.
- Continuing changes to workforce modes, recruitment, and retention, all of which could impact internal controls and fraud risks.
- How digitization–including routines, dashboards, and AI to enable risk assessment and real-time auditing–can help mitigate IA's workload and improve efficiency.
- Integrity and consistency of data used for sustainability and DEI, rankings, and other external disclosures.
- Adequacy of key performance indicators to measure compliance, training, and other imperatives.
- Appropriateness of and compliance with gift acceptance policies and processes for complying with donor restrictions.
- Given their significance to donor compliance and liquidity, effectiveness of policies and procedures in endowment and treasury management.
- Strength of protocols around research compliance and integrity, including as it pertains to grant administration, identification and disclosure of potential conflicts of interest and commitment, foreign influence, and misconduct.
- Management, monitoring, and verification of construction costs for major capital projects.
- As to significant NCAA programs, adequacy of Name, Image, Likeness (NIL) policies and procedures.
- Ways to elevate internal audit's profile as a valued advisor to the board, senior administration, and other departments.

02

Cybersecurity in higher education: security awareness and training

Cybersecurity in higher education: security awareness and training

On October 30, 2023, EDUCAUSE released a report entitled *Growing Needs and Opportunities for Security Awareness* resulting from a recent survey of college and university respondents. The report highlights the criticality of the design and effectiveness of security awareness programs in managing cybersecurity threats and notes that the goal of security awareness training is to "provide people with knowledge that will enable them to protect the sensitive data of individuals and the institution." The report concludes that while security awareness training is pervasive in the industry, training programs should cover more stakeholders, be expanded to cover institutional privacy and data governance policies, and be better monitored to ensure effectiveness and appropriate reporting. Following are key takeaways from the report.

Management and effectiveness

- Although most institutions mandate security awareness training, the design and frequency of such programs vary.
- Indeed, 94% of respondent institutions have a security awareness training program. About half of those (49%) exclusively use third-party services to create content, and only 14% exclusively develop content in-house.
- Most respondents (90%) indicated that such training is mandatory for employees, although required frequency is inconsistent. Still, a majority (65%) said such training is required annually, and 71% include such training in new-employee training programs.
- Only 38% of respondents reported that such training is "effective or very effective", whereas 61% said it is "somewhat effective."
- While the vast majority run security awareness programs for staff (99%) and faculty (97%), only 36% said it is available for students.

Recording and reporting

- The report notes that most institutions record some information on training completion but that such data is not widely shared within the institution.
- Nearly all respondents (97%) indicated their institution records training completion rates. Nearly two-thirds (66%) record phishing test failure rates; however, of those, only 50% said that individuals who fail phishing tests must undergo additional training.
- Interestingly, only 16% of respondents indicated that their institution records the cybersecurity policy acceptance rate.
- Respondents said that recorded information on security awareness training is most often reported to the IT office (60%) and institutional leadership (56%). Far fewer respondents indicated reporting to other groups, such as individual departments (26%) or human resources (only 17%).

Cybersecurity in higher education: security awareness and training (cont'd)

Security awareness training focus areas

- EDUCAUSE notes that training is largely focused on federal regulations and institutional security policies, whereas institutional privacy and data governance policies are often excluded.
- A majority of respondents (69%) said their institution's training covers federal regulations, such as the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act (HIPAA), as well as institutional security policies (67%).
- Among the topics least likely to be included in security awareness training programs were other types of regulations (e.g., the Gramm-Leach-Bliley Act (GLBA), at 7%), state and regional regulations (12%), and international regulations (17%).
- Only 35% of respondents noted that training includes institutional privacy policies, and just 23% said training covers institutional data governance policies (if they exist).

Risks and rewards

- Based on several open-ended comments received in the survey, EDUCAUSE noted that inadequate training introduces immeasurable risks, with one respondent commenting that the "human factor is the biggest risk/weakest link."
- The report also notes that respondents indicated that effective security awareness training has observable positive impacts, such as reduced reputational risk, improved financial outcomes, and lower insurance rates.

Promising practices

- Similar to law enforcement campaigns that stress "if you see something, say something," the report concludes that "building a culture of cybersecurity means students, faculty, and staff can act as an early warning system."
- Trainings should be required, more frequent, and more targeted. Given the rapidly evolving cybersecurity environment, mandatory training that is provided more often, in shorter but more effective formats, and tailored to more stakeholders (especially students) based on the types of data available to those groups, should improve cybersecurity.

03

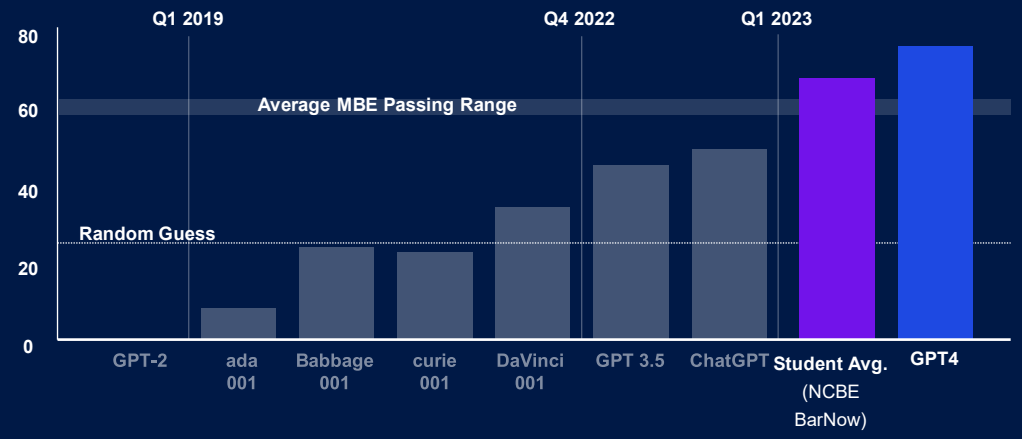
Artificial intelligence (AI) in higher education and in the audit

GenAI is moving quickly from media buzz to business value

In the last year, GPT4 has passed

- The Uniform Bar Exam
- US medical licensing exam
- Law School Exams
- Stanford Medical School clinical reasoning final
- The SAT
- The GRE
- USA Biology Olympiad Semifinal
- AP Exams
- AMC 10 / 12
- Sommelier Exams (written portion, not taste)

Gen AI performance on multistate bar exam*



*Source: https://www.iit.edu/news/gpt-4-passes-bar-exam

Business leaders are taking notice

76%

"Expect Generative AI to have the **largest impact on broader society** out of all emerging technologies"

66%

"Predict Generative AI to have a **high/very high impact on their firm in the next 3-5 years**"

60%

"Expect to adopt Generative AI **within 6-12 months**"

Source: KPMG Generative AI Survey of 300 executives; March 2023

AI in higher education

In the news…

> Risks and Rewards as Higher Ed Invests in an AI Future.” **Inside Higher Ed, September 5, 2023**

> How Will Artificial Intelligence Change Higher Ed?” **The Chronicle of Higher Ed, May 23, 2023**

> Integrating Generative AI into Higher Education: Considerations” **EDUCAUSE, August 30, 2023**

Administration

Student services

Admissions

Supply chain

Research

Marketing

Use cases for AI

While generative AI in higher education is often considered in an academic context—where it remains both a threat (e.g., academic dishonesty) and opportunity (e.g., online education)—it also has tremendous potential to transform finance and other administrative processes at colleges and universities.

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

- Filtering and combining data sets to identify trends.
- Further automating core business processes and user-support systems.
- Combing through public data to 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.

Industry perspectives on AI

2023 EDUCAUSE survey, August 2023

83% of college and university respondents believe "generative AI will profoundly change higher education in the next three to five years," and 65% believe its use has "more benefits than drawbacks."

Inside Higher Ed, September 2023

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.

Chronicle of Higher Education, May 2023

"AI will help control costs … admissions and student services will be first … While much of the discussion has focused on what generative AI means for teaching, learning, and research, its immediate impact will likely be felt on functions outside of the academic core."

AI adoption and governance

At this time, AI's emergence in higher education remains nascent. While other industries are exploring the capabilities that AI—and generative AI in particular—can bring to their organizations, many are taking a slow and steady approach to adoption. In fact, according to a KPMG survey, 37% of finance leaders are still in the planning stages of their generative AI journeys. Any number of issues can result in the technology making mistakes that can affect an entity's forecasts and reputation. But for leaders who make the effort to put the right controls in place around AI, the benefits can outweigh the risks.

Questions the institution should ask include:

- How will the institution maintain compliance with the patchwork of differing laws and regulations currently governing generative AI?
- 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 should we use?
- 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 our 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?
- How will the board oversee the institution's AI programs?

AI in the audit: our vision and focus

A glimpse of where we're headed …

AI-augmented audit

Through substantial investments in AI capabilities, we are delivering relevant, high-impact intelligent automation to drive audit quality and efficiency.

Robust data extraction

Automated data extraction and transformation capabilities of general ledger and subledger data will provide relevant audit data while alleviating the burden on you.

World-class data infrastructure and capabilities

Connected, unified, and transparent data infrastructure will enable efficiencies through the use of your relevant data across the audit lifecycle.

Next-generation KPMG Clara platform

Expanding on our world-class audit platform powered by a real-time and integrated AI eco-system, enhancing our robust continued risk assessment processes, generating relevant insights to you.

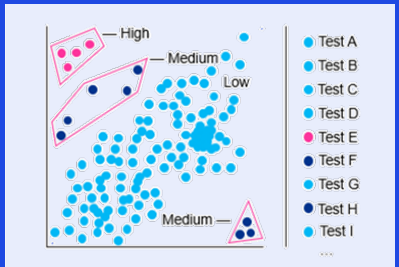
At KPMG, we believe intelligent automation will enable a faster, more agile audit, increasing quality while reshaping the nature of auditing itself. AI helps us focus on where risk truly lies, delivering a better audit across the board.

KPMG works with the world's leading technology companies to develop unique-to-KPMG, AI-based audit tools.

This approach ensures we are on the cutting-edge of what's now – and what's next.

We have a concerted and accelerated effort underway to test new AI use cases, including the security and legal risks associated with these tools.

Our approach



Currently deployed: Risk scoring with machine learning

Transactions are processed through a series of automated concurrent tests to develop a risk score – by transaction and account. No more random sampling.

2023 Pilot efforts: Generative AI

> Clara, please analyze the client control document for completeness of data elements."

> I have evaluated the document for completeness of data elements. Would you like to see a full listing?"

Benefits

Increased quality. Heightened efficiency. Less disruption. Deeper insights. A better audit experience.
Our vision is to embed AI into every aspect of the audit as we develop the next generation of KPMG Clara.

Microsoft MindBridge

The way forward

As a multidisciplinary firm, KPMG brings a holistic approach to using AI in the audit – leveraging advances across the organization to deliver a better audit experience.

GenAI

Deploying the power of AI to our people in a responsible way

Workflow

AI embedded at every stage of the audit effort

Cognitive search

Knowledge management as a force multiplier

Advanced analytics and intelligent agents

Connecting insights across the audit

Copilot

Embedded in key audit programs to supercharge impact

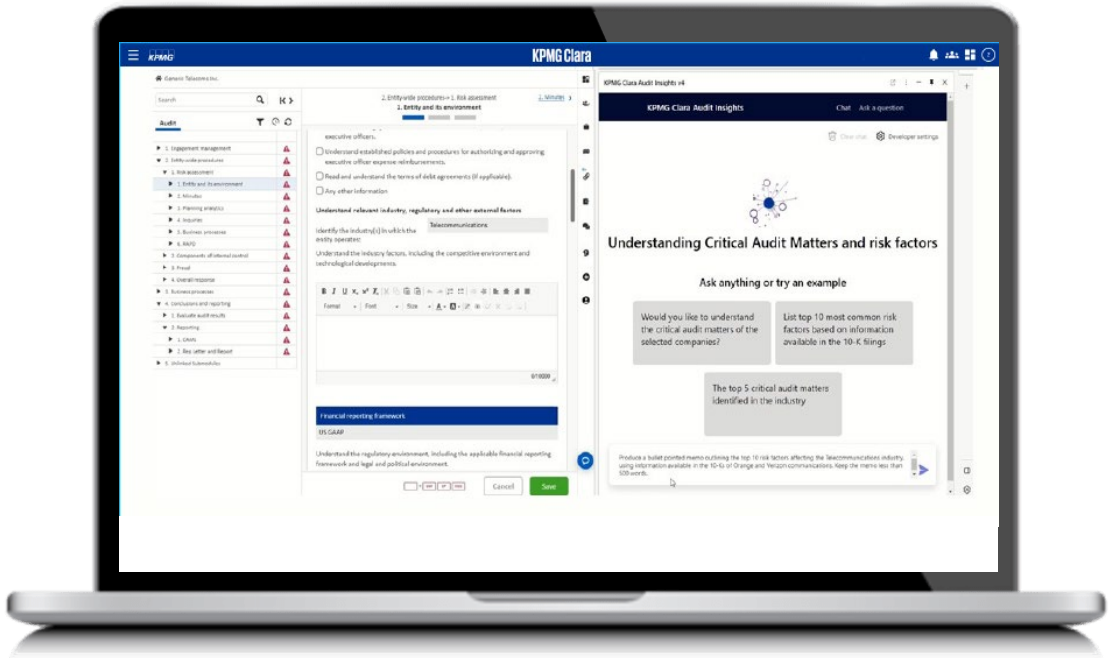
Data-driven audit

Using data to quickly zoom in on the right transactions

There will always be a need for human judgment, but as AI becomes more sophisticated, so will its use in the audit, which means increased benefits to our clients.

KPMG Clara generative AI

With our global alliance partner Microsoft, we have embarked on a journey to embed Generative AI into our smart audit platform – KPMG Clara. This will make our auditors more productive and give them the tools to provide quicker feedback, make more insightful connections, and deliver a better audit experience.



AI done right

Although early adoption is key, we are focused on avoiding reliance on a 'black box' so we're building 'explainability' and 'traceability' at the core.

Bolstered productivity

Focused on removing time-consuming low value tasks, we'll apply our skills in other, more judgmental areas or in order to give insights to you.

Quality embedded

We are teaching our model with our knowledge databases to capture our vast experience. This means quality information accessible in seconds.

Secure integration

KPMG Clara has been built on a solid and secure Azure Cloud backbone, allowing us to easily integrate Generative AI in partnership with Microsoft.

04

ESG in higher education

ESG overview

ESG refers to strategic and operational environmental, social, and governance (ESG) risks and opportunities with the potential to have a material impact on long-term financial sustainability and value creation. For higher education and other not-for-profit entities, ESG goals may align inherently with an organization's charitable mission and programs.

ESG overview

Environmental criteria consider how an entity acts in its role as a steward of nature, such as energy use, recycling practices, pollution, and natural resource conservation.

Social criteria examine how well an entity manages relationships with employees, suppliers, customers, and the community, including diversity and inclusion metrics.

Governance criteria are concerned with quality of entity leadership, internal controls, executive compensation process, audits, and other oversight responsibilities. An example is board-level diversity.

Boards and executives increasingly see ESG topics as important to long-term value creation, and are identifying the need to meet stakeholder demand for ESG information in a way that drives value for the organization.

ESG in higher education

Colleges and universities face increasing stakeholder demands for ESG data, particularly around DEI, climate impacts, and governance of key risks such as cybersecurity. The activities affected and stakeholders involved are perhaps more numerous than in any other industry.

Institutional activities

- Admissions & enrollment
- Student health & safety
- Faculty/staff recruitment & retention
- Endowment management
- Fundraising & sponsored programs
- Cyber & data privacy
- Facilities & dining
- International & affiliate activities
- Supply chain
- Patient care

Stakeholders

- Students & parents
- Grantors & donors
- Faculty & staff
- Board of Trustees
- Bondholders
- Regulators
- Communities & patients

Recent ESG-related developments

The ESG landscape potentially affecting colleges and universities is fast-evolving and merits continuous monitoring.

U.S. Supreme Court

— Two June 2023 rulings end race-conscious affirmative action in college admissions and reverse the Biden administration's plan to forgive up to $400 billion in federal student loans.

— Reversal of *Roe v. Wade* in 2022 results in changes to state laws, impacting not only abortion rights and employee health coverage, but also stem cell research at academic medical centers.

Other federal activity

— Congressional hearings in December 2023 spur allegations that antisemitism is tolerated on college campuses while differing ideological perspectives are not.

— In December 2023, the U.S. Department of Education releases data showing how many colleges and universities consider an applicant's legacy status in their admissions processes, renewing debates on legacy preferences.

— The proposed *Endowment Transparency Act of 2022* would require colleges and universities to disclose investments and bond underwriting managed by women- and minority-owned firms.

— The SEC's new cybersecurity risk and governance disclosure rules take effect in December 2023, and final climate disclosure requirements are expected to be issued in March 2024.

States

— A backlash against DEI results in a ban on diversity programs at public institutions in several states, including Florida, Texas, Oklahoma, and others.

— October 2023, the California Governor signs three disclosure laws that will shape climate reporting for entities with activities in California far beyond the state's borders.

International

— The European Union's (EU's) Corporate Sustainability Reporting Directive amends and significantly expands existing EU requirements for sustainability reporting, including for U.S. based entities with activities in the EU.

ESG backdrop – SEC regulatory agenda

ENVIRONMENT: CLIMATE

- Final rule expected in March 2024
- KPMG analysis (150 responses)
- **79%** supported standard-setting in general (not necessarily the SEC's specific proposal)
- SEC staff continues to question climate disclosures under existing guidance

SOCIAL

- Human capital
  - Proposal expected April 2024
  - SEC strategic plan: People are a company's "most important asset"
- Corporate board diversity
  - Proposal expected October 2024

GOVERNANCE

- Cybersecurity risk governance
  - Final rule became effective in December 2023
  - Builds on existing guidance

Two of the California Bills signed into law

	SB-253	SB-261
Title	Climate Corporate Data Accountability Act	Greenhouse gases: climate-related financial risk
Scope	US companies > $1B annual revenue doing business in California	US companies > $500M annual revenue doing business in California
Reporting	Annual: Scopes 1, 2, 3 GHG emissions	Biennial: Report with climate-related financial risk and measures adopted to reduce and adapt to climate-related financial risk
Status	First reports in 2026 (2025 data)	First reports due by Jan 1, 2026
Assurance	• Scopes 1, 2: limited (2026); reasonable (2030) • Scope 3: TBD	None proposed
Next steps	California Air Resources Board to work out operational details	

Laws are based on whether an organization does business or operates in California, not whether the entity has a physical presence. To date, colleges, universities, and other not-for-profit organizations meeting the thresholds above have not been specifically scoped out of these requirements, and it remains unclear how or whether they may be subject to such requirements.

California carbon offsets disclosure law: AB-1305

Effective January 1, 2024

To date, colleges, universities, and other not-for-profit organizations meeting the scoping criteria below have not been specifically scoped out of this requirement, and it remains unclear how or whether they may be subject to the requirement.

	Scoping	Disclosures
Group 1	Business entities **marketing or selling voluntary carbon offsets** in California.	Details of the carbon offset project, accountability measures if the project is not completed or does not meet projections, relevant data and calculation methods to independently reproduce and verify the emissions reduction credits.
Group 2	Entities operating in California that **make claims** within the state regarding any of the following: • achievement of net-zero emissions; • the entity (or related entity or product) is carbon neutral; • implying the entity (or related entity or product) does not add GHG emissions to the atmosphere; or • the entity (or related entity or product) has made significant reductions to GHG emissions.	Information about the GHG emissions associated with the claims – e.g. how the claim was determined to be accurate, how interim progress is measured, whether there is independent third-party verification.
Group 3	Entities operating in California that make any of the claims outlined in Group 2 above and that also **purchase or use voluntary carbon offsets** sold within the state.	Information about each project or program – e.g. name of business entity selling the offset, offset project type, whether there is independent third-party verification.

Federal suppliers proposal

	Federal suppliers
Title	**Proposed:** Federal Supplier Climate Risks and Resilience Rule
Scope	• Major contractors: > $50M, Significant contractors: > $7.5M - $50M
Reporting	• All: Scopes 1, 2 GHG emissions; complete the CDP Climate Change Questionnaire • Major: Scope 3, climate risks, science-based targets (SBTi) **Exceptions:** A new FAR section at 23.XX04 outlines certain exceptions. Per FAR 23.XX04(a), a significant or major contractor is not required to inventory its Scope 1 or Scope 2 emissions and a major contractor is not required to complete an annual climate disclosure or set science-based targets, as described in section II.B. of this preamble, if it is— • An Alaska Native Corporation, a Community Development Corporation, an Indian tribe, a Native Hawaiian Organization, or a Tribally owned concern, as those terms are defined at 13 CFR 124.3; • A higher education institution (defined as institutions of higher education in the OMB Uniform Guidance at 2 CFR part 200, subpart A, and 20 U.S.C. 1001); • A nonprofit research entity; a state or local government; or an entity deriving 80% or more of its annual revenue from Federal management and operating (M&O) contracts that are subject to agency annual site sustainability reporting requirements. * The exception for institutions of higher education or nonprofit research entities is provided because a large majority of such entities that are significant or major contractors either already set GHG reduction targets and make sustainability disclosures but are likely doing so (in accordance with current commercial norms for sustainability reporting) with standards and systems other than those specified in this rule, or are pass-through entities with minimal Scope 1 and 2 emissions and little capacity to manage Scope 3 emissions and climate risks.
Status and Assurance	• Pending report following public consultation. Could be finalized by the end of 2024. • No assurance on such information has been proposed.

The EU's Corporate Sustainability Reporting Directive (CSRD)

The European Union's (EU's) 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 may be in the scope of the CSRD is complex, as each EU member state defines, in the transposition of the CSRD into local law, the legal forms of entities that are subject to the requirements.

Scoping requirements	The provisional CSRD includes different scoping requirements for EU-based vs. non-EU based companies – referred to as 'general' vs 'non-EU parent' scoping. Whereas general scoping depends on listing status or size, non-EU scoping is based on a combination of physical presence in the EU and net turnover (revenue) generated in the EU.	
Scoping for EU-based and non-EU based entities	**General scoping**	**Non-EU parent scoping**
	The CSRD would apply to all companies operating in the EU and their subsidiaries (EU-based companies) that meet the following general scoping requirements: • Large companies or large groups (i.e., a company including all its subsidiaries on a consolidated level) that meet at least two of the following: > 250 employees; > €40M net turnover (revenue); > €20M total assets. • Companies with listed securities in the EU other than 'micro-companies'. A micro-company meets at least two of the following: < 10 employees; ≤ €2M net turnover; ≤ €2M total assets.	Irrespective of the general scoping described above, an ultimate non-EU parent company would be subject to the CSRD if it has: • substantial activity in the EU – i.e. it generated net turnover greater than €150M in the EU for each of the last two consecutive years; and • at least: − one subsidiary that meets the general scoping of the CSRD; or − one branch (in general, a physical presence) that generated net turnover greater than €40M in the preceding year.
Status	There is much to resolve in terms of how these laws will be implemented, including how colleges, universities, and other not-for-profits with activities in the EU could be impacted.	

ESG considerations – bond rating agencies

S&P and Moody's

have both reaffirmed that they will continue to incorporate ESG scoring in their methodologies and explicitly include ESG considerations in ratings reports. Here are some other key takeaways from what ratings agencies are saying around ESG:

Municipal Securities Rulemaking Board (MSRB) RFI

MSRB in December 2021 solicitated information from various industries to better understand ESG practices; however, no requirements have been proposed.

Moody's

November 2020 research announcement, "ESG factors material in 50% of public-sector rating actions in 2019 and Q1 2020."

S&P and Moody's

ESG factors will continue to influence credit quality pertaining to municipal securities, including those issued by higher education and other not-for-profit entities.

Emergence of data requested or required to be submitted to banks or other creditors with respect to ESG (including DEI) could evolve over time.

ESG ratings considerations – Moody's

Risks and challenges identified

Environmental

- Climate management
- Extreme weather

Social

- Access, affordability
- Student support services (i.e. mental health)
- Changing consumer preferences

Governance

- High leadership turnover
- Increased politicization of higher education
- Cybersecurity
- International campus and student risks from geopolitical realignments

These considerations result in "Issuer Profile Scores" (IPSs)

- Carbon transition
- Physical climate risks
- Water management
- Waste and pollution
- Natural capital

- Customer relations
- Human capital
- Demographic and societal trends
- Health and safety
- Responsible production

- Financial strategy and risk management
- Management credibility and track record
- Organizational structure
- Compliance and reporting
- Board structure and policies.

In addition, Moody's may establish a CIS to explain the impact of ESG considerations on the rating of the issuer or transaction. The CIS is based on a qualitative assessment of the impact of ESG considerations in the context of the issuer's other credit drivers that are material to a given rating. The scale ranges from CIS-1 ("Positive") to CIS-5 ("Very Highly Negative").

Regulatory key takeaways

Regulations in the corporate sector, both in the United States and abroad (and in the EU in particular) are fluid and quickly evolving.

- Some of these regulations have the potential to apply to colleges, universities, and other not-for-profit entities.
- Organizations must maintain awareness of the changing landscape.

Other stakeholders and standard setters have heightened the focus on ESG directives and reporting:

- AICPA – issued *Attestation Engagements on Sustainability Information*, authoritative guide.
- FASB & GASB – while neither has established requirements to date, each have acknowledged and deliberated the intersection of ESG matters with financial reporting standards.
- Rating agencies continue to acknowledge and assess ESG factors in their methodologies.

ESG frameworks and reporting – higher education

Public and private colleges and universities

- College and university climate action plans
- Office of Sustainability websites and annual reports
- Office of Diversity, Equity and Inclusion websites and reports
- Sustainability Tracking, Assessment & Rating System

The Princeton Review

- Guide to Green Colleges
- Sustainability-focused
- Ranks Top 50 Green institutions
- Provides sustainability information from 400+ institutions deemed “green” by meeting certain criteria

Sustainability Tracking, Assessment & Rating System (STARS)

- **Reporter** – provides information, but does not elect to receive a rating
- **Bronze** – minimum overall score of 25
- **Silver** – minimum overall score of 45
- **Gold** – minimum overall score of 65
- **Platinum** – minimum overall score of 85

Total points = overall institution score
Bonus category – Innovation & Leadership

Academic:
Curriculum, Research

58
available points

Engagement:
Engagement, Public Engagement

41
available points

Operations:
Air & Climate, Buildings, Energy, Food & Dining, Grounds, Purchasing, Transportation, Waste, Water

72
available points

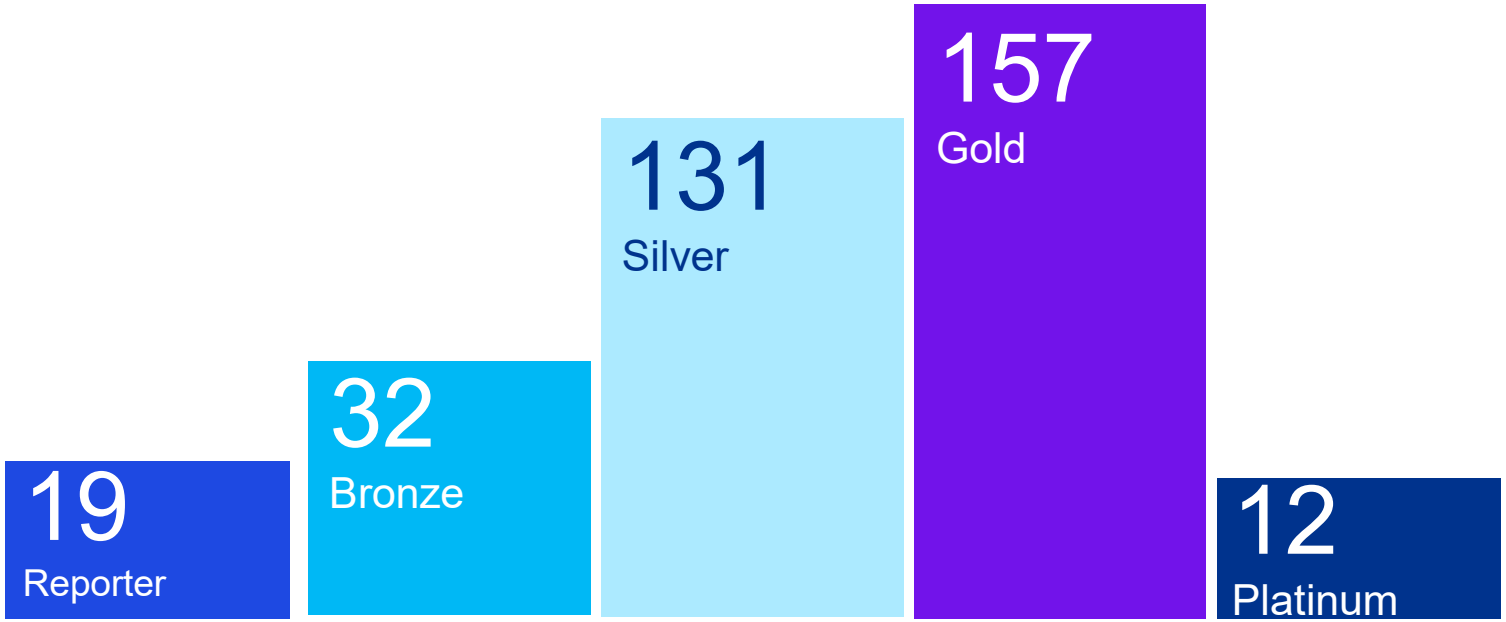
Planning & Admin:
Coordination & Planning, Diversity & Affordability, Investment & Finance, Wellbeing & Work

34
available points

STARS – overall scores

1,184 institutions have registered to use the STARS Reporting Tool, of which 582 have earned a STARS score. Of the 606 institutions with at least one published STARS report, 351 are active designations, while the remainder have expired (due to lack of refreshed reporting by an institution).

Number of institutions by score category (active only)

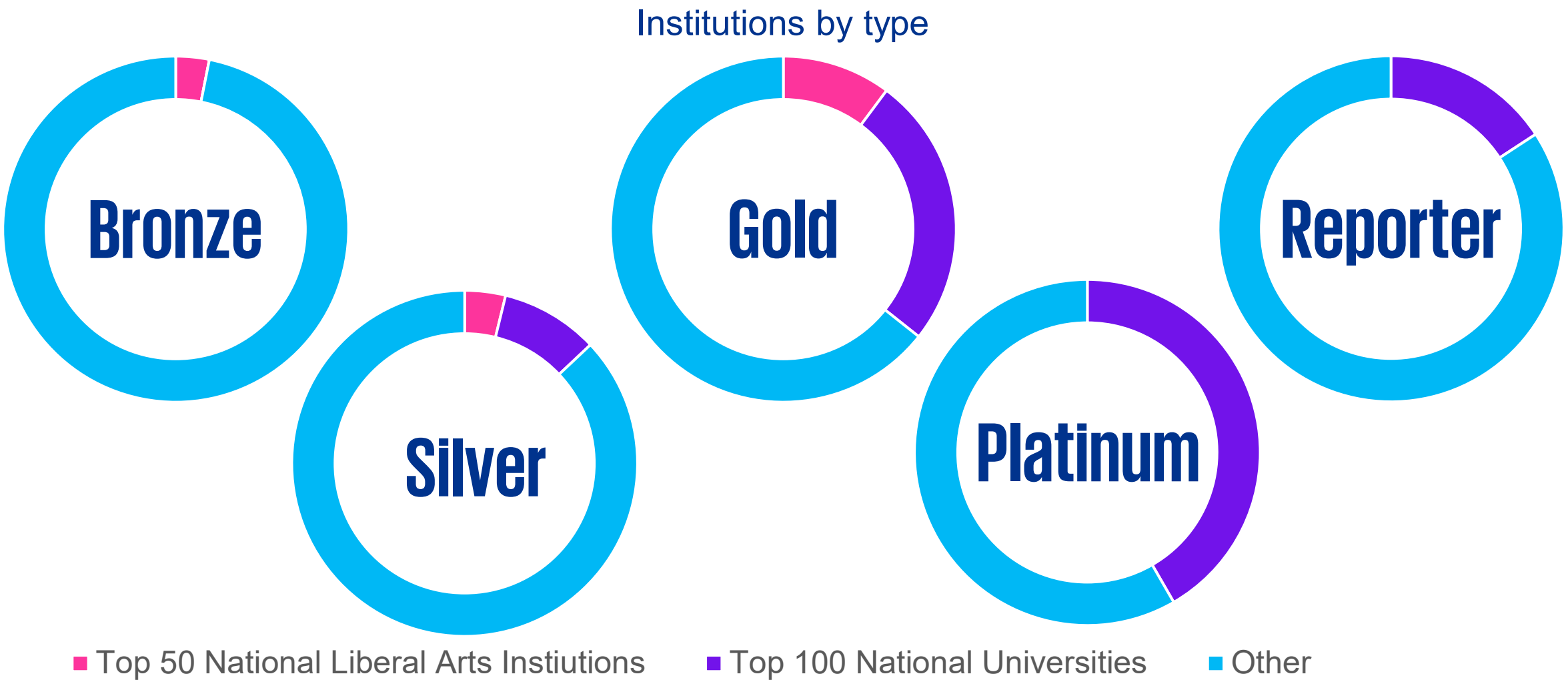


Minimum overall scores

Bronze	25
Silver	45
Gold	65
Platinum	85

Source: STARS, Sustainability Tracking Assessment & Rating System (aashe.org), February 2024

STARS – overall scores (cont'd)



Source: STARS, Sustainability Tracking Assessment & Rating System (aashe.org), February 2024

Top 5 for higher education

What are the 5 things your institution should consider now for ESG?

01

Does my institution have an ESG strategy? Who is responsible?

02

How and by whom are material ESG risks identified?

03

Have key metrics been defined, and is a reporting framework in place?

04

What processes and controls exist over data being collected and reported?

05

Do we (or should we) obtain assurance about the integrity of ESG data and processes?

05

2023 *NACUBO-Commonfund Study of Endowments*

2023 *NACUBO-Commonfund Study of Endowments*

Released in February 2024

Respondents

- A total of 688 institutions–aggregating $839.1 billion of total endowment value–took part in the Study, which covered the fiscal year ended June 30, 2023 and included private and public institutions and institutionally related entities (such as foundations).
- Study data were arranged in seven cohorts based on size, which ranged from endowments with assets under $50 million to those with assets over $5 billion. The median endowment size was $209.1 million, whereas the average was $1.2 billion.
- Once again, the Study showed that endowment wealth in the sector remains heavily concentrated, with 58% of total market value held by endowments with more than $5 billion in assets.

Returns

- The Study showed an overall return for FY23 of 7.7%, net of fees, in contrast to the -8.0% return reported for FY22. Trailing 10-year returns averaged 7.2%.
- Institutions with endowments over $5 billion had an average return of 2.8%, whereas those in the three smallest size cohorts were the only ones with average returns of 8.0% or more.
- While returns of institutions with larger allocations to alternative strategies lagged in FY23, over the longer term they have generated higher returns. For example, institutions with assets over $5 billion reported 10-year average annual returns of 9.1% vs. institutions in the other six size categories, which reported 10-year average annual returns of 6.5% to 8.0%.

Asset allocation

- Asset allocation was a primary factor creating return differences among the seven cohorts in the Study in FY23, as it has been in the past. While smaller institutions' larger allocations to publicly traded securities resulted in the highest returns in FY23, alternative investment strategies remained the largest allocation among Study participants overall.
- Significant alternative strategies included private equity (17.1%), marketable alternatives (15.9%), and venture capital (11.9%). In addition, real assets represented 11.2% of allocations. Taken together, over half of the average portfolio value is comprised of alternative and real asset strategies, with much higher allocations of these assets in larger endowments driving the average.

2023 *NACUBO-Commonfund Study of Endowments* (cont'd)

Released in February 2024

Spending

- Distributions from endowments in FY23 increased 8.4% over FY22. Endowments funded an average 10.9% of annual operating budgets, with endowments over $5 billion and $1 billion leading the way in funding 17.7% and 17.1%, respectively, of their annual operating budgets. The average effective spending rate increased to 4.7% in FY23 (from 4.0% in FY22), with private institutions reporting a 5.0% average rate (vs. public institutions at 4.1%).
- Consistent with prior years, the largest share of spending distributions was for student aid (47.7%). This was followed by research (17.5%), endowed faculty positions (11.1%), operations and maintenance (7.4%), and all other purposes (16.4%).

Fundraising

- New gifts to endowments totaled $13.3 billion among all Study participants (down more than 10% from the $14.9 billion raised in FY22). The average new gift in FY23 for all Study participants was $20.4 million, while the median new gift was $4.7 million.
- As previously noted, endowment growth at larger institutions in FY23 was constrained by more muted investment returns. In addition, less robust endowment giving in FY23 – likely due in part to negative public market indices at the end of calendar 2022 – contributed to endowments growing only 4% at institutions in the two largest size cohorts. By contrast, endowments at institutions in the two cohorts with smaller endowments grew by 6%.

ESG considerations

- The Study reported that although adoption of responsible investing practices has grown over the years, 65.4% of respondents in the FY23 Study had not adopted such practices. For those who have, 51.0% factored responsible investing into investment manager due diligence in FY23 (down slightly from the 52.3% that did so in FY22).
- Various barriers to implementation were cited by respondents who have not pursued ESG practices in their portfolios. Among those are potential adverse impacts on investment performance and conflicts with mission/fiduciary duty; difficulty assessing the extent to which ESG mandates in the portfolio have been achieved; lack of enough quality managers; and higher investment fees.

06

Related party disclosures required by U.S. Department of Education (ED)

Background

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.

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.

Excerpt from ED regulation 34 C.F.R 668(d)(1) :

As part of these financial statements, the institution must include a detailed description of related entities based on the definition of a related entity as set forth in the Accounting Standards Codification (ASC 850). The disclosure requirements under this paragraph (d)(1) extend beyond those of ASC 850 to include all related parties and a level of detail that would enable the Department to readily identify the related party. Such information ~~may~~ must include, but is not limited to, the name, location and a description of the related entity including the nature and amount of any transactions between the related party and the institution, financial or otherwise, regardless of when they occurred. If there are no related party transactions during the audited fiscal year or related party outstanding balances reported in the financial statements, then management must add a note to the financial statements to disclose this fact.

External reporting considerations

	General Purpose	Federal Audit Clearinghouse (FAC)	eZ-Audit Submission to ED
Financial statement audit performed in accordance with…	Generally accepted auditing standards (GAAS)	GAAS *Government Auditing Standards* (GAGAS)	GAAS GAGAS
Financial Responsibility Standards: (a) incremental note disclosure;(b) Supplementary Schedule of Financial Responsibility Data	Does not include	Does not include	Includes
Related party note	Include in accordance with ASC 850	Include in accordance with ASC 850	Include in accordance with ASC 850 **and ED regulations**
Purpose and use	General use and submission to EMMA	Submission to FAC	Submission to ED

FASB ASC 850 Master Glossary defines related parties as:

a. Affiliates of the entity (An *affiliate* is a party that, directly or indirectly through one or more intermediaries, controls, is controlled by, or is under common control with an entity.)
b. Entities for which investments in their equity securities would be required, absent the election of the fair value option under the "Fair Value Option" subsection of FASB ASC 825-10-15, to be accounted for by the equity method by the investing entity
c. Trusts for the benefit of employees, such as pension and profit-sharing trusts that are managed by or under the trusteeship of management
d. Principal owners of the entity and members of their immediate families
e. Management of the entity and members of their immediate families
f. Other parties with which the entity may deal if one party controls or can significantly influence the management or operating policies of the other to an extent that one of the transacting parties might be prevented from fully pursuing its own separate interests
g. Other parties that can significantly influence the management or operating policies of the transacting parties or that have an ownership interest in one of the transacting parties and can significantly influence the other to an extent that one or more of the transacting parties might be prevented from fully pursuing its own separate interests

Other ASC 850 related party considerations:

- Material related party transactions, other than compensation arrangements, expense allowances, and other similar items in the ordinary course of business (FASB ASC 850-10-50-1)
- If the reporting entity and one or more other entities are under common ownership or management control and the existence of that control could result in operating results or financial position of the reporting entity that are significantly different from those that would have been obtained if the entities were autonomous, the nature of the control relationship should be disclosed even though there are no transactions between the entities (FASB ASC 850-10-50-6)

Paragraph 3.193 of the AICPA Not-for-Profit (NFP) Auditing and Accounting Guide:

Related parties of NFPs might include, but are not limited to, the following:

- Officers, board members, founders, substantial contributors, and their immediate family members
- Members of any related party's immediate family
- Parties providing concentrations in revenues and receivables
- Supporting organizations (such as 509(a)(3) organizations)
- Financially interrelated entities
- Certain national and local affiliates that don't necessarily meet the definition of affiliate in FASB ASC
- Other entities whose officers, governing board members, owners, or employees are members of the NFP's governing board or senior management, if those individuals have significant influence to an extent that one or more of the transacting parties might be prevented from fully pursuing its own separate interests

Examples of related party transactions per the NFP Guide:

- Material contributions from related parties (FASB ASC 850-10-50-1)
  - FinREC believes the NFP need not identify by name the party making the contribution
- Significant concentrations of revenues and receivables from related parties
- Office space lease from a governing board member (FASB ASC 850-10-50-1)
- Legal services provided by a firm in which an officer's immediate family member is a person of influence, such as a partner (FASB ASC 850-10-50-1)
- Printing services from a printing shop owned by a governing board member of the NFP (FASB ASC 850-10-50-1)
- Supplies from a company for which one of the NFP's governing board members is a governing board member (FASB ASC 850-10-50-1)
- Loans to a founder or significant donor or immediate family member (FASB ASC 850-10-50-1)

Key takeaways

- Reconsider the term “related party” in the context of ED’s requirement and GAAP.
- Re-evaluate the institution’s systems, processes, and internal controls necessary to capture and evaluate information needed to comply.
- The implications of personally identifiable information associated with certain disclosures may be complicated, should be carefully assessed, and may merit discussions with the parties affected.
- Understand how a rejected filing could impact the institution.
- Work closely with legal counsel and auditors to navigate the process and any issues identified.
- Continue to monitor and consider AICPA guidance, as well as future clarifying guidance provided by ED (if any).

07

Other developments affecting federal grants and contracts

Proposed revisions to Uniform Guidance (2 CFR Part 200)

Background

In September 2023, the Office of Management and Budget (OMB) issued proposed updates to revise portions of its Guidance for Grants and Agreements, including 2 CFR Part 200. OMB notes that the proposal is intended to clarify existing regulations, reduce agency and recipient burden, and incorporate revisions using plain language. As proposed, the revisions would impact auditees and auditors. Currently, there is no timeline for when or if each proposed change will become effective.

Among the proposed changes are provisions that would:

- Raise the Single Audit threshold from $750,000 to $1,000,000.
- Revise certain areas of cost principles, including clarification of pension costs.
- Remove prior written approval for certain items of cost.
- Raise the de minimis indirect cost rate from 10% to 15%.
- Remove a requirement that indirect cost rates be publicly available on a government-wide website.
- Amend the definition of “modified total direct costs” to exclude subaward costs above $50,000 (up from the current level of $25,000) in the application of indirect cost recoveries.
- Raise the threshold for items defined as capital expenditures (e.g., equipment) from $5,000 to $10,000.
- Use the terms “recipient” and “subrecipient” instead of “non-federal entity,” except where a specific provision applies.
- Modify and expand many other definitions.
- Potentially expand the definition of “questioned costs” to provide greater understanding of the term.
-

Changes to the Federal Audit Clearinghouse (FAC)

1

The FAC provider changed from Census to GSA and went live on October 2, 2023

https://www.fac.gov/

2

Single audits for fiscal periods ending in 2023 and thereafter are submitted to the new GSA FAC

3

The 30-day submission requirement was waived for 2023 submissions with fiscal periods ending between January 1, 2023 and September 30, 2023

4

The GSA continues to make improvements to the FAC site and respond to questions submitted by users

08

Update to *Government Auditing Standards*

Update to *Government Auditing Standards*

What's new?

The Government Accountability Office (GAO) has updated *Government Auditing Standards* (GAGAS, commonly known as the Yellow Book) to reflect new developments related to audit organizations' systems of quality management. These standards are intended to help ensure that an audit organization produces reliable, objective, and high-quality engagements for use in holding management and officials entrusted with public resources accountable for carrying out their duties.

When is this effective?

Government Auditing Standards 2024 Revision is effective for financial audits, attestation engagements, and reviews of financial statements for periods beginning on or after December 15, 2025, and for performance audits beginning on or after December 15, 2025, with early implementation permitted.

What are the major revisions?

- Emphasizes the responsibility of an audit organization's leadership for proactively managing quality on its engagements.
- Promotes scalability of the system of quality management used by audit organizations of differing size and complexity.
- Establishes a risk-based process for achieving quality management objectives. This stems from a change in approach to quality, under which *quality management* replace the former term, *quality control*.
- Flexibility for audit organizations subject to other quality management standards to avoid the burden of designing, implementing, and operating separate systems of quality management.
- Promotes proactive and effective monitoring activities and increased emphasis on tailoring monitoring activities.
- Provisions for optional engagement quality reviews of GAGAS engagements.
- Includes application guidance on key audit matters for when they may apply to financial audits of government entities and entities that receive government financial assistance.

09

Presentation of discounts to student services revenues (GASB institutions)

Presentation of discounts to student services revenues – accounting evolution

- GASB 34:
  - Paragraph 100, Fn 41:

    Revenues should be reported net of discounts and allowances with the discount or allowance amount parenthetically disclosed on the face of the statement or in a note to the financial statements. Alternatively, revenues may be reported gross with the related discounts and allowances reported directly beneath the revenue amount
- GASB 35:
  - Colleges and universities: tuition, fees, and auxiliaries
- NACUBO:
  - AR 2000-05, *Scholarship Discounts and Allowances*
  - Non-authoritative guidance for GASB reporters
  - Public not-for-profit colleges and universities reporting under GASB
  - Specific identification and “alternate method”
    - Alternative method results in proportional estimation of scholarship allowances

Presentation of discounts to student services revenues – where we are today

- Current thinking:
  - Actual determination of discount (i.e., student by student) is optimal
  - Alternate method is outdated, requires significant estimation and management judgment, and tends to understate the tuition discount and overstate financial aid expense
  - Two decades later, college and university accounting systems are more robust
  - GASB re-evaluating revenue presentation more generally
- NACUBO proposal:
  - *Accounting for and Reporting Financial Aid as a Discount to Tuition and Other Fee Revenues -Public Institutions* would supersede AR 2000-05
  - Conceptual framework outlined
  - Example calculation methods provided
  - More precise and accurate presentation
  - Suggested implementation: fiscal 2025 or sooner

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**

AUDIT COMMITTEE

April 11, 2024

Resolution authorizing retention of external audit firm for the fiscal year (FY) 2024 mandatory annual audits

WHEREAS, on April 11, 2022 the Audit Committee recommended, and the Board of Trustees approved, authorizing the Vice President for Finance and Administration to enter into a contract with KPMG, LLP to obtain external audit services to conduct the annual financial statement audit and other related audits of the university for five consecutive years during the period April 1, 2022, through March 31, 2027, at a total contract price not to exceed $2,160,000, with continuation of said contract subject to an annual performance review by the Audit Committee; and

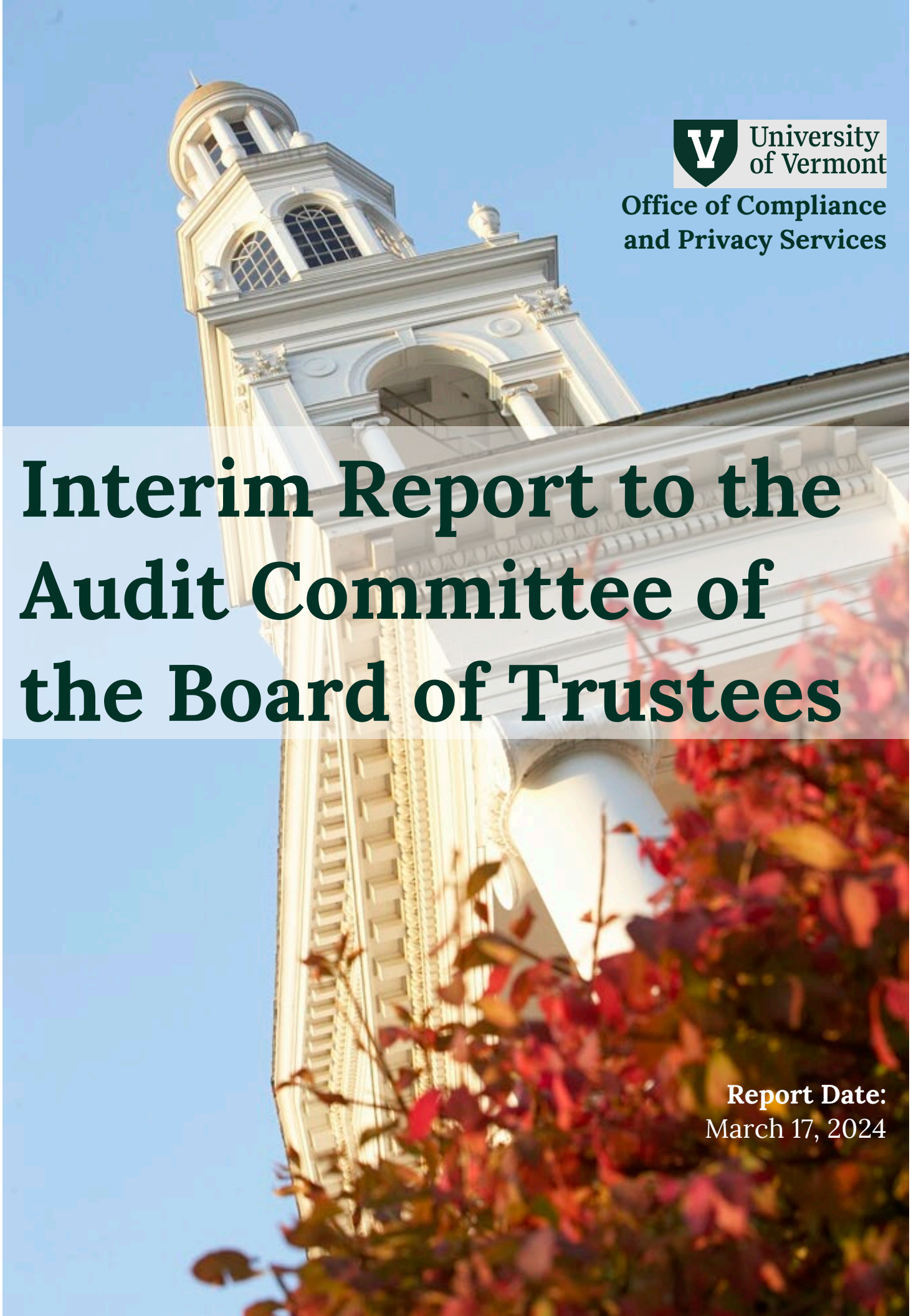
WHEREAS, the Audit Committee recommends retention of KPMG, LLP for the FY 2024 mandatory audits;

BE IT RESOLVED, that the annual audit shall be conducted in compliance with the requirements of the University Bylaws and state and federal law.

Office of Compliance and Privacy Services

Board of Trustees - Audit Committee
April 11, 2024

Prepared By
Tessa Lucey, Director of Compliance Services
and Chief Privacy Officer



University of Vermont

Office of Compliance and Privacy Services

Interim Report to the Audit Committee of the Board of Trustees

Report Date:
March 17, 2024

Office of Compliance & Privacy Services

Michael Schirling
Chief Safety and Compliance Officer

Tessa Lucey
Director of Compliance and Chief Privacy Officer

Maureen Jennings
Records Custodian and Compliance Coordinator

Danielle Slauzis
Institutional Policy Manager and Compliance Coordinator

Amy Vile
Administrative Assistant

Table of Contents

Introduction

This interim report details the activities conducted by the Office of Compliance and Privacy Services ("the Office") that have occurred since the last report was presented to the Audit Committee on November 6, 2023. The Office is responsible for administering the University of Vermont's Compliance[1], Privacy[2], and Enterprise Risk Management (ERM) programs.

The Compliance Program enhances coordination, consistency, and efficiency by providing an institutional perspective of the University's compliance assurance activities. The Compliance Program is designed to reduce the risk of noncompliance and, as a result, reduce potential fines, penalties, and sanctions and improve and enhance the University's culture of compliance. The Compliance Program achieves this by meeting Section 8 of the Federal Sentencing Guidelines which outlines the seven steps of an effective compliance program.

The University is required to comply with state, federal, and international privacy laws. The Privacy Program champions privacy across the University and promotes UVM's commitment to safeguarding the personal, protected, sensitive and confidential data that we hold, access and use. The Privacy Program protects non-public protected data ("NPPD") by embedding privacy protections into operations and by promoting the importance of safeguarding the private, confidential, sensitive, and proprietary information that the University has been entrusted with.

The purpose of UVM's ERM program is to enhance the University's ability to achieve its mission, vision, and strategic objectives and strengthen its competitive position by fostering an institution-wide culture of risk and opportunity awareness and providing a structured, consistent, and continuous process for the early and proactive identification and reporting of material risks and opportunities to senior management and trustees.

These programs provide ongoing assessment, monitoring, resources, and assistance with an emphasis on continuous improvement, risk reduction, and culture of compliance enhancement. These programs further provide a single, central contact for compliance, privacy, and enterprise risk information and guidance for the entire University of Vermont community.

Section I: Compliance Work Plan Efforts

Institutional Policies – Policy Process Improvement

UVM's new "Institutional Policy Manager and Compliance Coordinator" position was filled as of October 30, 2023. The new internally developed policy management software application was launched in December 2023. An institutional policy program improvement project plan has been developed and is scheduled to be presented to key stakeholders in April. The goal of this project is to improve policy compliance through development of a program to increase understanding and remove barriers to access. This workplan item also directly impacts the ERM register risk entitled "Insufficient Knowledge/ Understanding of Policy Expectations".

[1] UVM's Compliance Program includes the policy, conflict of interest, and public records programs.
[2] UVM's Privacy Program includes the records retention program.

Research: Foreign Influence, Subcategory – Visiting Scholars/Scientist Process Improvement

Status: In Process.

After identifying some operational inefficiencies, the Office re-engaged key stakeholders and the responsible official on the visiting scholar/scientist process. The Office is providing guidance to those units operationally responsible for improving the efficiency and effectiveness of this regulated process.

Research – Foreign Influence: Sanction Check Process Improvement

Status: In Process.

Recently, UVM began performing background checks on all newly hired staff. Background checks run through UVM's vendor include a check against the federal sanction and exclusion lists. The process for visiting scholars and scientists also includes a background check requirement. Newly hired faculty are expected to be added to this background check process. The staff and faculty group make up the largest population that, had we implemented a separate sanction check process, would have required separate sanction checks. The discussion is ongoing to determine whether the University needs to begin performing sanction checks on foreign vendors/third parties and international students participating in research.

Compliance Program – Virtual Education Program

Status: Closed.

The Office launched "Policy Fridays" and the first session was held via Teams on March 15th. Initial feedback has been positive. Policy Fridays will continue as scheduled.

Compliance Program – Compliance Training

Status: In-Process.

The Office was able to add both Compliance/Code of Conduct and Privacy awareness training into onboarding for new staff. Compliance/Code of Conduct was added to orientation in January and Privacy was added in February. The Office is working with UVM's Information Security Officer and the Director of Environmental Health & Safety to develop similar awareness training video shorts for both cybersecurity and campus health and safety. The Office continues to provide compliance and privacy training upon request and when a compliance risk has been identified.

Health & Safety – Protection of Minors: UVM Youth Programs (UVMYP) Policy & Process Improvement

Status: In-Process.

The Office worked with the Department of Risk Management to finalize updates to UVM's Protection of Minors Policy. These updates were posted to the institutional policy website in November 2023. Through the Division, the Office is working with the State of Vermont and with key internal stakeholders to formulate a process for obtaining fingerprint supported background checks for those working in UVM Youth Programs.

Compliance Program – Contingent: HelpLine Oversight

Status: Continuous.

The Office continues to track HelpLine reports. Since the last report to this Committee, the Office received 18 reports through the HelpLine. The total number of reports in CY 2023 was 29, and the cumulative total since inception is 238 reports.

Privacy Program – Data Risk Classification

Status: In Process.

The Office worked with key stakeholders across campus to develop a date risk classification matrix which is expected to be posted online by April 15, 2024.

Contingent: Consults, New Compliance Issues, Data Incidents, Government Reviews

Status: Continuous.

For Calendar Year (CY) 2023, the office received 75 consults in 9 different categories. Unlike recent years where information security/privacy represented most of the consult requests, CY23 saw Conflict of Interest/Conflict of Commitment consults and Information Security/Privacy consults both at 23% of the annual total. We are still seeing a large percentage (80%) of consults directly linked to the ERM Heat Map.

Observations: As a matter of routine operations, the Office continues to follow up on outstanding compliance observations and recommendations from prior years. The Office provides a detailed status report in the Annual Report presented to the Audit Committee in November.

Government Reviews: Also included in its Annual Report, the Office summarizes those government reviews that have been reported to the Office. According to the Audit Committee Charter, in addition to the annual reporting of government reviews, the Director reports findings of government agency audits, investigations, reviews and monitoring activities that the Director considers significant, that are initiated by a government agency as a result of a whistleblower report or on a for-cause basis, or that result in a fine, penalty, refund, disallowance or questioned cost in excess of $10,000. As of the last report to the Audit Committee, there have been no such government reviews reported to the Office that meet this reporting criteria.

Data Incidents: The Office separately tracks data incidents. Since the last report to this Committee, the Office has not received any data incident reports. There were three reports received in 2023; 2 were inadvertent disclosures (internal incidents) and 1 was a phishing incident (external incident). All three of these incidents resulted in notification to the affected individuals, one of which was required and two were at UVM's discretion. UVM was also required to report the phishing incident to the Vermont Attorney General. UVM also used its discretion and reported it to the FBI.

Section II: Compliance Program Effectiveness Activities

The framework for UVM's compliance program is based on, and follows closely the structure of, the U.S. Department of Justice's most recent guidance outlining the components ("the seven elements") of an effective corporate compliance program.

Element I: Standards & Procedures

The Office continues to administer and maintain UVM's Institutional Policies website.

New and substantially updated Policies & University Operating Procedures (UOPs) since the November 2023 report to the Audit Committee:

- Free Expression; Campus Speakers; Response to Disruption Policy (Replaces the Free Expression and Campus Disruption Policy, and Campus Speakers Policy)
- Protection of Minors (Revised)
- Domestic Travel Involving Students (New)

Policies and UOPs retired since the November 2023 report to the Audit Committee include:

- Mandatory Covid-19 Vaccine Policy for Employees (retired)

Element II: Oversight

The Director continues to serve as the individual assigned with day-to-day responsibility of the Program. The Director reports to the Chief Safety and Compliance Officer. In addition, the Director meets regularly and routinely with the Chief Internal Auditor and the Office of General Counsel. Through these channels, the Director would be able to report suspected systemic non-compliance to the Chair of the Audit Committee should such a report be necessary.

Element III: Avoid Delegation of Authority to Unethical Individuals

UVM performs background checks as required by law and for many new hires depending on the nature of the position. Sanction checks were historically only performed by the Office of the Vice President for Research (OVPR) for subrecipients of sponsored awards and those named in sponsored awards and agreements that meet certain criteria. As reported in the Foreign Influence work plan item summary included in Section I of this report, sanction and exclusion checks are included in background checks and are now also being run by Human Resources for all new staff hires.

Element IV: Education & Training

The Office continues to provide opportunities for education and training related to compliance, ethics, and privacy. The Office was successful in getting compliance and privacy awareness training into new employee orientation and has posted awareness video shorts on its compliance training website. When appropriate, the Office also works with the Division's training coordinator to improve the efficiency and effectiveness, as well as increase availability, of identified compliance training topics.

Element V: Reporting, Monitoring & Auditing

The Office continues to monitor the status of corrective actions and observations and continues to monitor the HelpLine. The Office also works with the Office of Audit Services on audit findings related to compliance concerns. Refer to the Work Plan item "Compliance Program Operational Activities" for additional information. In addition to the HelpLine, the Office also has a robust system of reporting options that include policy review, existing chains of command, or to the Office via email, phone/Teams, website and in-person reporting options.

Element VI: Enforcement & Discipline

Many University Policies and UOPs contain language addressing disciplinary action for violations. In most cases, disciplinary action follows the University's progressive discipline process. For represented staff, the disciplinary action follows that which is outlined in the collective bargaining agreements. For non-represented staff, the Office is notified of all terminations, both voluntary and involuntary, on a regular basis. If an individual who had filed a compliance report was involuntarily terminated, the Office would initiate a review of the circumstances surrounding the termination. There have been no such terminations since the last report to the Audit Committee.

Element VII: Response & Prevention

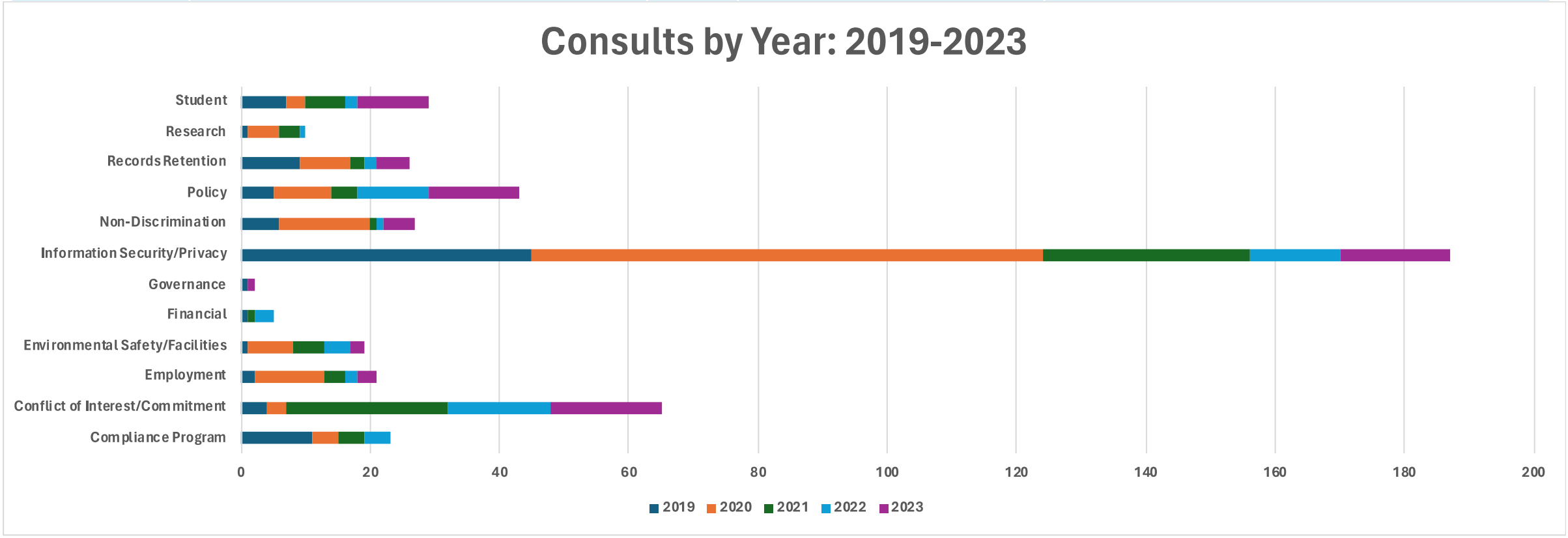
The Office tackles both response and prevention by providing awareness training to staff upon hire and proactively providing more in-depth training to faculty and staff when compliance risks are identified. By providing this awareness, the likelihood of incidents is reduced. By providing open chains of communication and multiple reporting mechanisms, the Office is able to work with key stakeholders to address allegations of non-compliance promptly and thoroughly. By combining prevention and response and continually increasing communication and education, the program fosters a culture of ethical conduct and minimizes regulatory risk for the University.

Section III: Enterprise Risk Management (ERM)

The 2023 Enterprise Risk Management survey results were reported to this committee and a copy provided to all trustees in February 2024. Board reports for portfolio level risks and opportunities are currently being scheduled and will continue through 2024. The next assessment cycle began this year and will be reported to the Board of Trustees in early 2025.

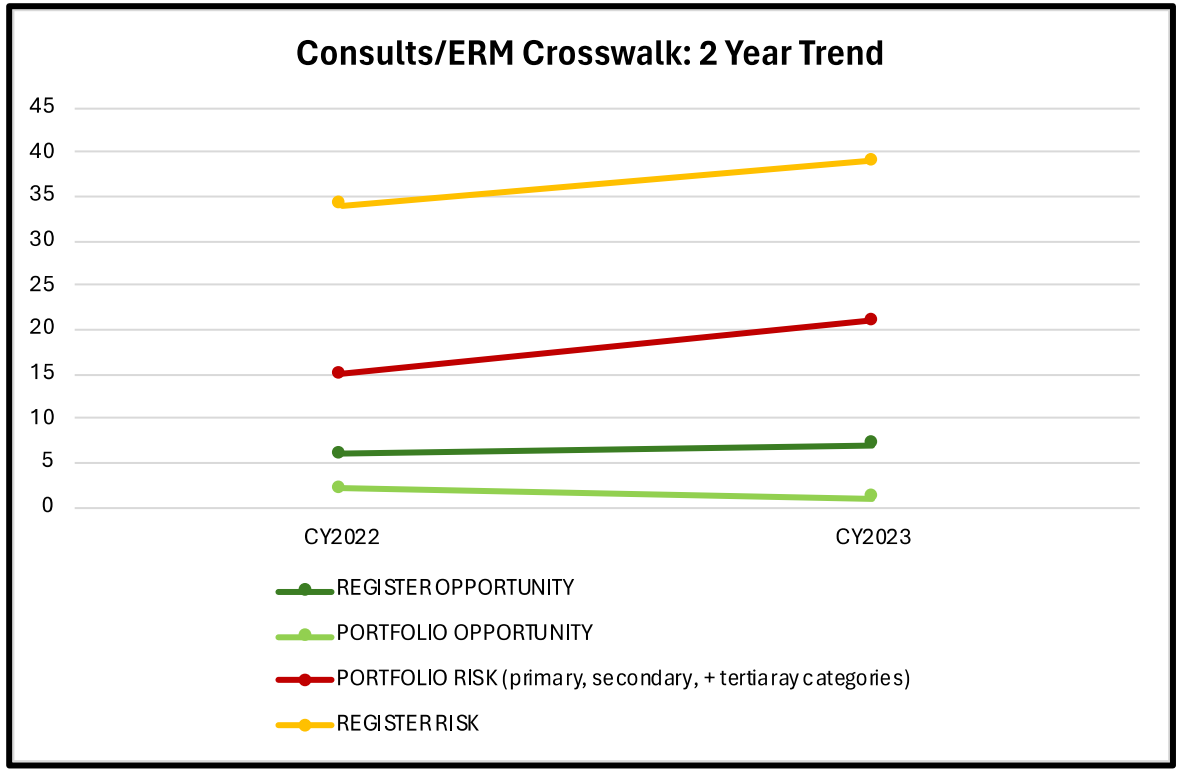
COMPLIANCE WORK PLAN DASHBOARD: contingent

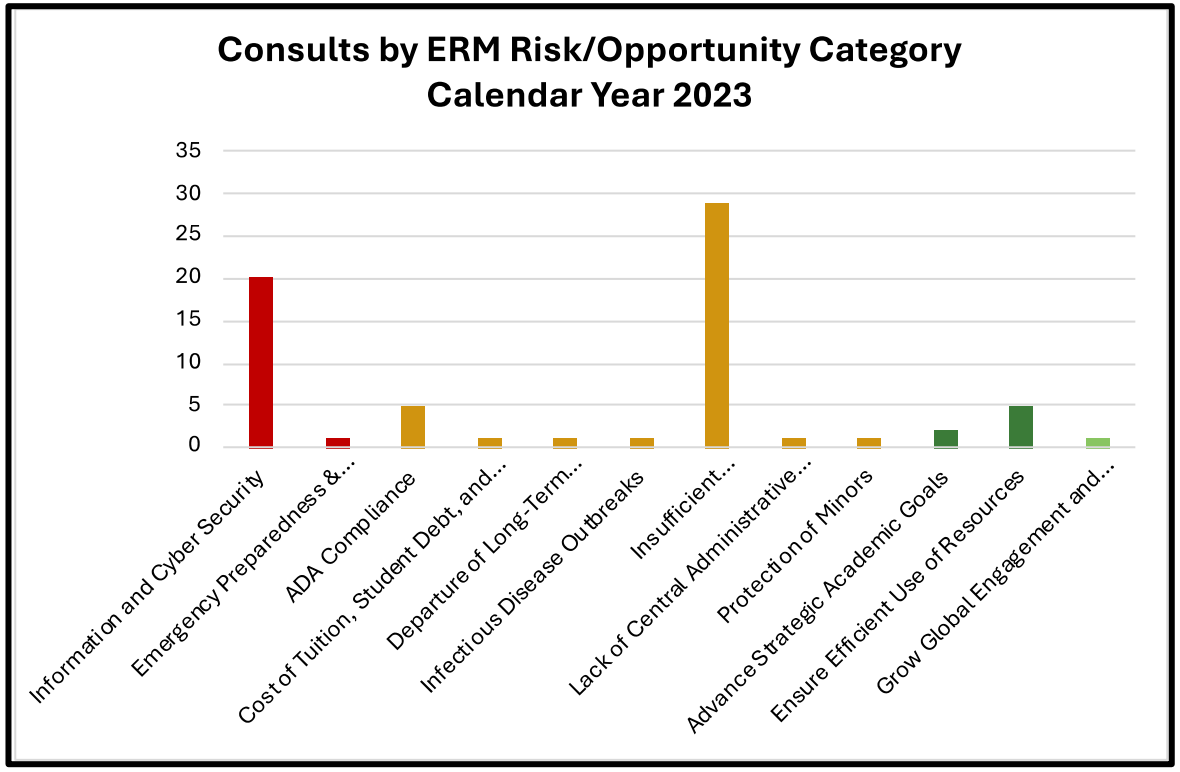
PROGRAM ELEMENT	STATUS	TOTAL	TIMEFRAME	COMMENTS/PLAN
CONTINGENT: CONSULTS, NEW COMPLIANCE ISSUES & COMPLIANCE PROGRAM OPERATIONAL ACTIVITIES				
CONSULTS	Total Calendar Year (CY) 2023	75	1/01/2023 – 12/31/2023	
	Total CY 2024 To Date	21	1/01/2024 – 3/17/2024	
GOVERNMENT REVIEWS	Government reviews initiated since last report	2	07/01/2023 – 3/17/2024	



COMPLIANCE WORK PLAN DASHBOARD: contingent

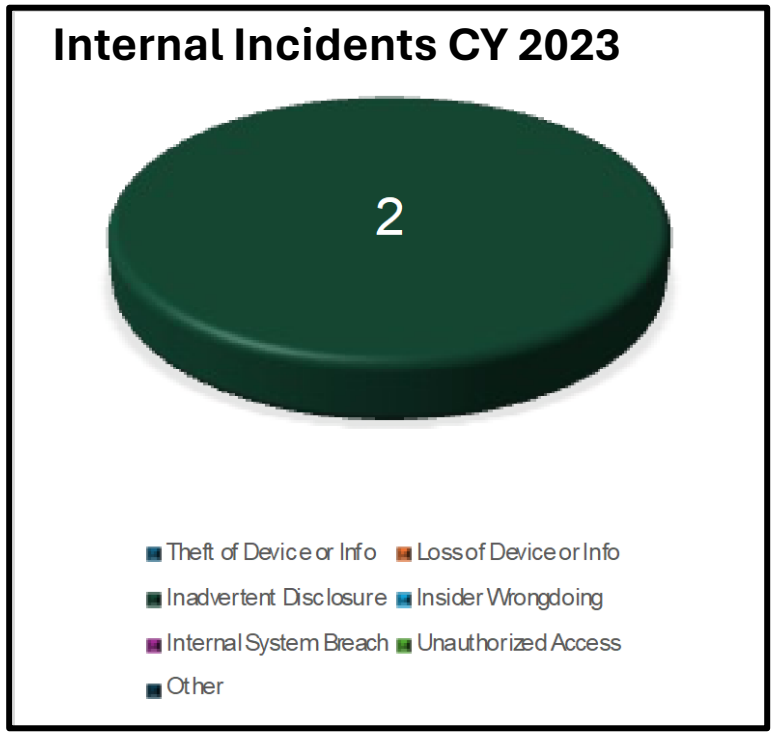
PROGRAM ELEMENT	STATUS	TOTAL	TIMEFRAME	COMMENTS/PLAN
CONTINGENT: CONSULTS, NEW COMPLIANCE ISSUES & COMPLIANCE PROGRAM OPERATIONAL ACTIVITIES				
CONSULTS CY 2023	Related to Enterprise Risk Management (ERM) Risks	60	1/01/2023 – 12/31/2023	
	Related to ERM Opportunities	8	1/01/2023 – 12/31/2023	
CONSULTS YTD 2024	Related to ERM Risks	1	1/01/2024 – 3/17/2024	
	Related to ERM Opportunities	22	1/01/2024 – 3/17/2024	

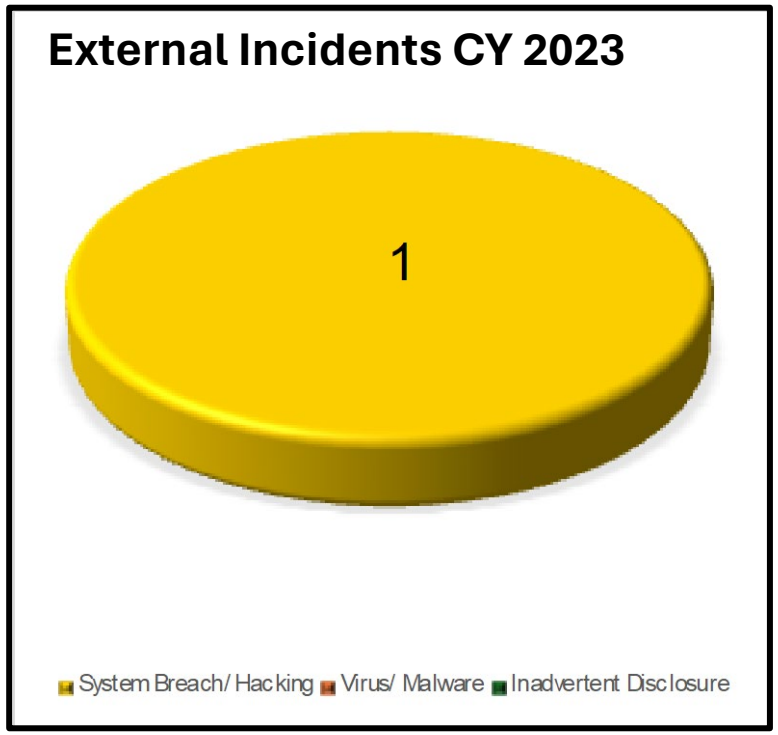


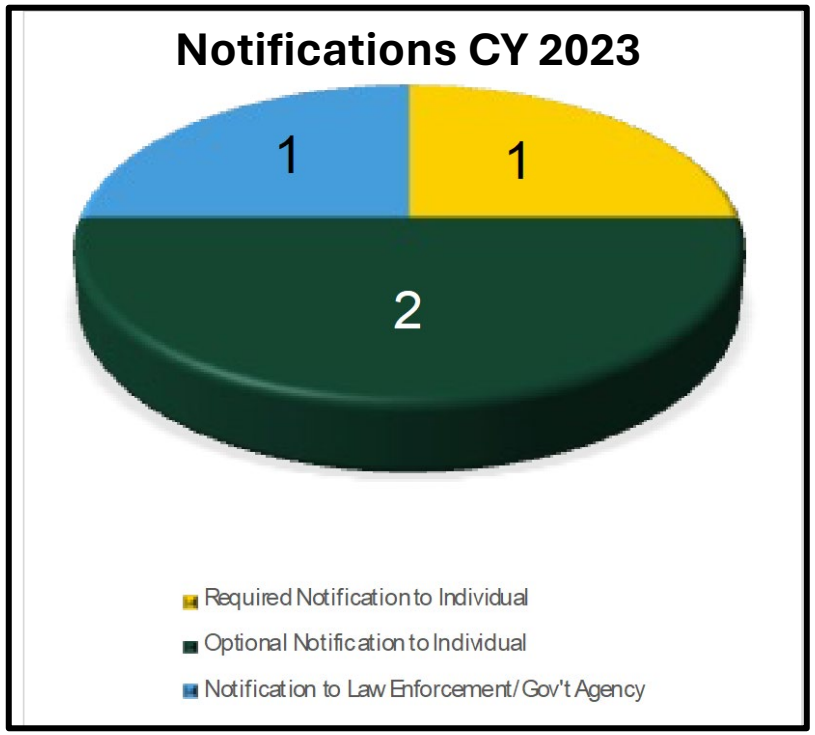


COMPLIANCE WORK PLAN DASHBOARD: PRIVACY

PROGRAM ELEMENT	STATUS	TOTAL	TIMEFRAME	COMMENTS/PLAN
CONTINGENT: CONSULTS, NEW COMPLIANCE ISSUES & COMPLIANCE PROGRAM OPERATIONAL ACTIVITIES				
DATA INCIDENTS	Total CY 2023	3	1/01/2023 – 12/31/2023	
	Total Year-To-Date 2024	0	1/01/2023 – 3/17/2023	

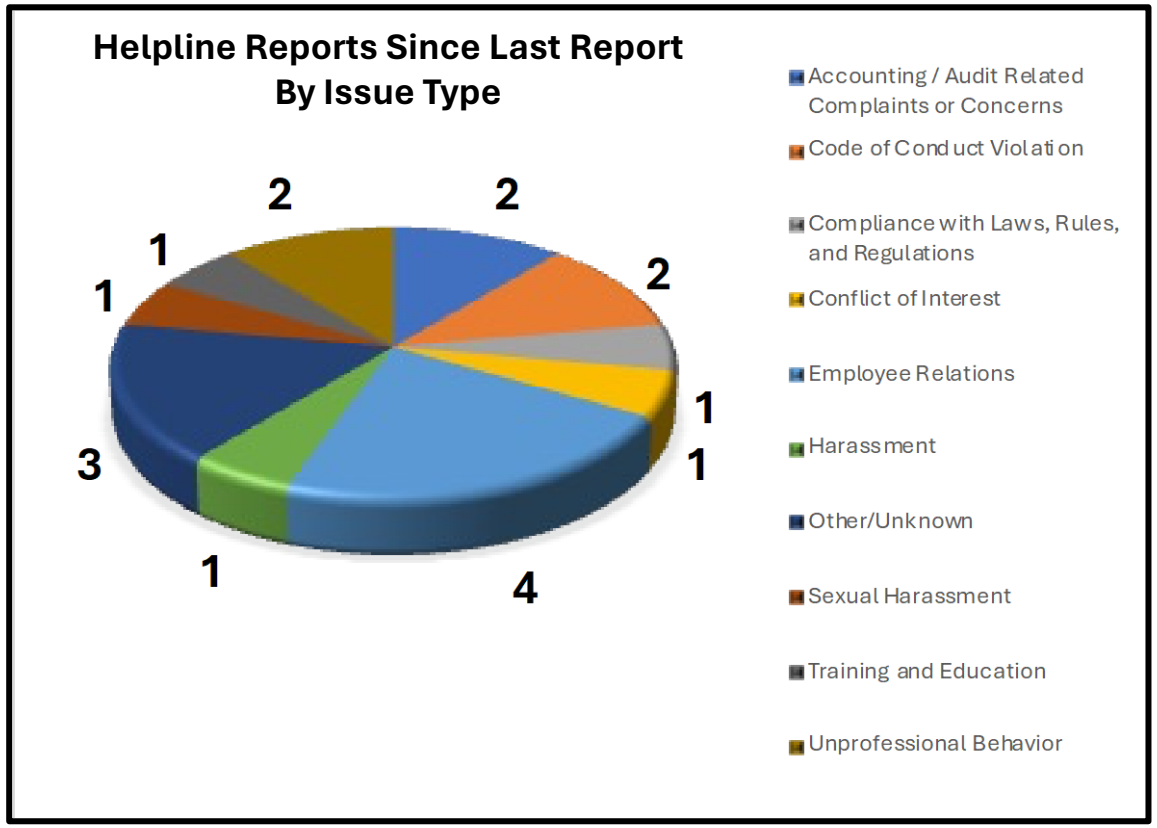


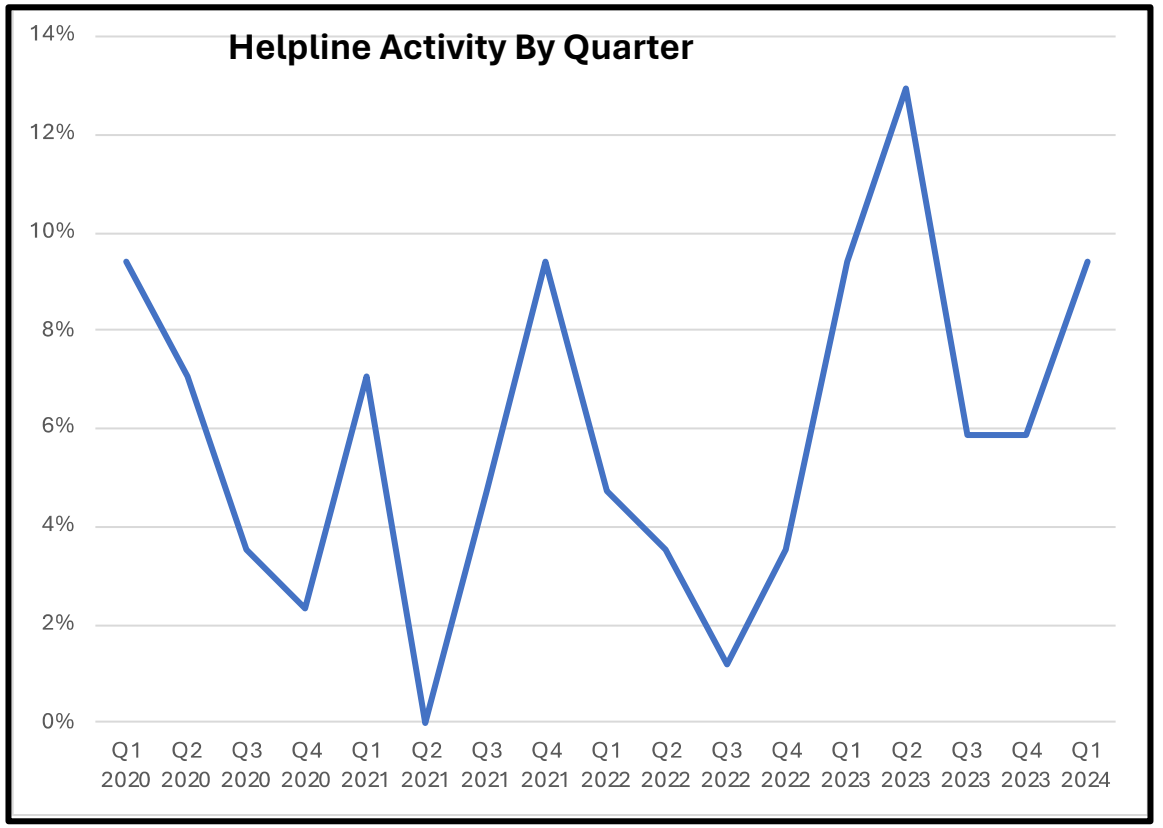




COMPLIANCE WORK PLAN DASHBOARD: HELPLINE

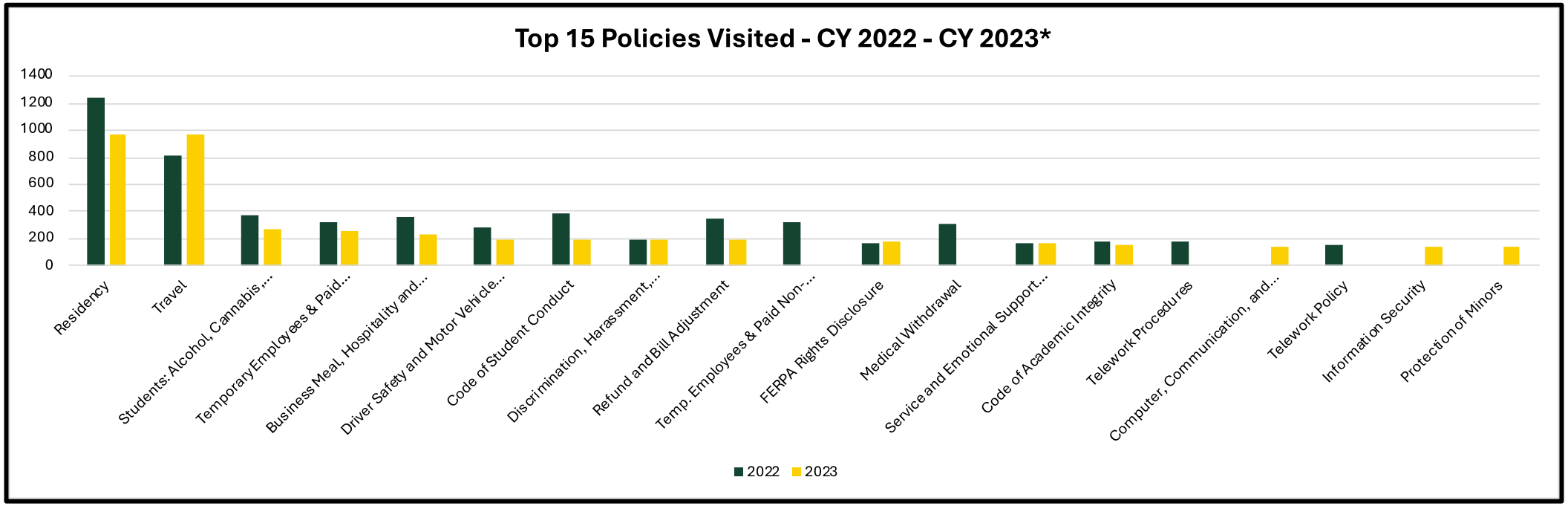
PROGRAM ELEMENT	STATUS	TOTAL	TIMEFRAME	COMMENTS/PLAN
CONTINGENT: CONSULTS, NEW COMPLIANCE ISSUES & COMPLIANCE PROGRAM OPERATIONAL ACTIVITIES				
HELPLINE	Reports Received Since Last Report	18	7/01/2023 – 3/17/2024	
	Cumulative Since Inception	238	2/01/2010 - 3/17/2024	





COMPLIANCE WORK PLAN DASHBOARD: POLICIES

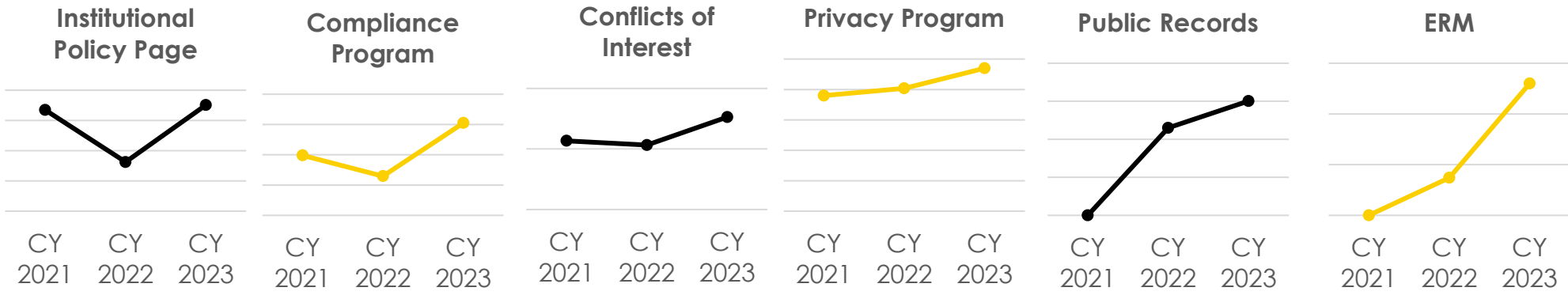
PROGRAM ELEMENT	STATUS	TOTAL	TIMEFRAME	COMMENTS/PLAN
CONTINGENT: CONSULTS, NEW COMPLIANCE ISSUES & COMPLIANCE PROGRAM OPERATIONAL ACTIVITIES				
POLICIES/UOPs	Total Policies	96	As of 12/31/2023	
	Total UOPs	65	As of 12/31/2023	
	Total Visits to Individual Policies/UOPs	14,672	1/01/2023 – 12/31/2023	
New/Revised, CY 2023	New Policies/UOPs	3	1/01/2023 – 12/31/2023	
	Revised Policies/UOPs	19	1/01/2023 – 12/31/2023	



*Missing annual figures does not mean 0 visits to the page. It means that it did not break the top 15 for that year.

COMPLIANCE WORK PLAN DASHBOARD: PROGRAMMATIC

PROGRAM ELEMENT	STATUS	CY 2022	CY 2023	COMMENTS/PLAN
CONTINGENT: CONSULTS, NEW COMPLIANCE ISSUES & COMPLIANCE PROGRAM OPERATIONAL ACTIVITIES				
PROGRAM WEB SITES	Institutional Policy Page	4725	5102	
	Compliance Program Main Page	1294	3051	
	Conflicts of Interest	532	763	
	Privacy Program Main Page	202	235	
	Public Records	460	601	Page went live 3/31/2022
	Enterprise Risk Management	148	520	Statistics available beginning in May 2022
OFFICE OVERSIGHT PROGRAMS WEB VISITS: TRENDING				



Attachment 6

OFFICE OF COMPLIANCE AND PRIVACY SERVICES
www.uvm.edu/erm
B159, Billings Library, 48 University Place, Burlington, VT 05405
P: (802) 656-3086 E: erm@uvm.edu

Enterprise Risk Management

Enterprise Risk Management Update

Board of Trustees – Audit Committee
April 11, 2024

Prepared By
Tessa Lucey, Director of Compliance and Chief Privacy Officer

---

In February 2023, the Board of Trustees received a biennial report on Enterprise Risk Management assessment results. Throughout the year, committees will receive status updates on risks and opportunities that fall under their purview. Included in this report is the update on the following:

- Emergency Preparedness and Institutional Continuity
- Campus Threats and Mass Casualty

Risk – Emergency Preparedness and Institutional Continuity

National events continue to paint a vivid picture of the challenges facing campuses. Coupled with the recent experience of the Covid-19 pandemic and the need for formal emergency preparedness policies, plans, and protocols, the likelihood score increased resulting in this risk moving up from the inventory (2018, 2019) to the portfolio (2022).

The University's operations are like those of a small city. Events and emergencies of varying sizes can and do occur. Planning for, mitigating the risks and impact of, and responding to those emergencies is a core competency for an institution the size of UVM. Human-caused or natural hazard events could (i) impair our general ability to operate, (ii) impair institutional and/or unit continuity through a variety of means including loss of access to key leaders, and/or (iii) damage or destroy infrastructure, facilities, or technologies. Emergency management, led by a director, together with partners throughout the institution (including an established emergency operations group), work with federal, state, and local emergency management teams and responders to identify risks, plan for responses, employ mitigation strategies, and ensure plans exist for swift recovery if necessary. A few areas of recent emphasis include:

(1) minimize risk of damage or loss of research and/or research interruption;
(2) emergency communications;
(3) ensure preparedness through regular drills and exercises with the emergency operations group.

UVM's All Hazards approach has been beneficial for managing higher frequency, low and moderate impact events. Our focused efforts to respond to and recover from a larger scale event are on-going. Actions and controls implemented to date include:

(1) The Emergency Management & Institutional Continuity (EM_IC) policy rewritten, adds an emergency response team for administrative divisions/colleges/schools;
(2) An EM_IC plan to implement National Fire Protection Association (NFPA) 1600 was developed and is being implemented;
(3) Various hazard-specific response plans have been updated; and
(4) FM digital radios were purchased and are being used to enhance communication with first responders.

Going forward, we will continue our work in policing, fire safety, environmental safety, and risk management together with our efforts to increase capacity in emergency preparedness and operations through ongoing training and drills for our emergency operations group, awareness and response training for affiliates, and future education and training for campus leaders on institutional continuity planning.

Opportunity – Campus Threats and Mass Casualty

Nationwide, the trend of increasing active threats in workplaces, on campuses, in schools, and in other locations such as supermarkets and malls continues. Additionally, global and national events and related demonstrations, rhetoric and political divisiveness have sometimes put the focus on college campuses. These trends create risks of violent/disruptive behavior. College campuses generally provide a "soft target" impacting the risk profile. Given these trends, the risk increased from a risk score of 6 (2018, 2019) to a risk score of 12 (2022).

Events of this nature are high-impact and would have a long-lived reputational impact, but are a low probability. Similar to other physical and natural risks, the risk is best addressed using an all-hazards approach.

Management actions and controls implemented to date include:

1. Regular active threat training for UVM Police Services;
2. Emergency Operations Group practice managing both an active threat and mass casualty incidents (bomb, etc.);
3. Faculty, staff and students are offered active threat response training (optional) on an ongoing basis. Without a mandate, the entire campus community is not routinely and regularly trained in these situations, though almost all college-aged students have received regular active threat training during the K-12 education and we are working to incorporate it into new student training/orientation.

In addition, UVM Police takes special precautions, with assistance from the State Police explosive detection unit, in checking the main commencement venue and other high-profile or highly charged events on campus for explosives. UVM Police have a protocol in place, last exercised in 2007. EOG and mutual aid partners conducted active shooter table-top exercise in 2019 and again with on-campus partners in 2023. The University has obtained a DHS grant for road barriers to enhance large venue safety. Those units are in service. In April 2023 a large-scale active threat tabletop exercise with campus, local, State, and federal partners will be conducted by the

Department of Homeland Security. In August 2023 we held a threat exercise with senor leadership, and we obtained $203K in grants over two years to increase closed circuit television (CCTV) coverage.

Of note, mitigation plans for both of these risks (Emergency Preparedness and Institutional Continuity and Campus Threats, Mass Casualty) are closely interwoven. While they are listed as separate risks in the portfolio and will, therefore, be reported separately, the mitigation plans and the steps that we take as an institution to reduce the risk for one cannot be done without also addressing the other.