University of Colorado

Boulder | Colorado Springs | Denver | Anschutz Medical Campus

FOUR CAMPUSES UNITED
ALL FOUR:ONE

FISCAL YEAR 2023 INTERNAL AUDIT PLAN

June 15, 2022

CU Internal Audit: Mission and Vision

Mission Statement

The mission of the University of Colorado Department of Internal Audit is to enhance and protect organizational value by providing risk-based and objective assurance, advice and insight.

The Department's processes are designed to improve the university's operations and promote achievement of institutional objectives by utilizing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

Vision Statement

Insight with Impact

We are trusted partners.

We deliver timely and relevant perspective on risks and opportunities.

We are committed to our core values, intellectual curiosity, and alignment with our stakeholders.

CU Internal Audit: What We Do

Assurance: We focus on a broad set of governance, financial, operational and compliance risks, including IT systems and processes and information security, supporting CU's four strategic pillars: Affordability & Student Success; Discovery & Impact; Diversity, Inclusion, Equity & Access; and Fiscal Strength.

Advisory: We support our stakeholders in establishing best practices and internal controls, identifying and mitigating risks throughout the project lifecycle (e.g., participating in steering committees, reviewing process and control design, facilitating risk and opportunities conversations in system implementations, etc.), and provide perspective on sufficiency of policies for compliance with certain relevant regulations.

Investigations: We evaluate reports of employee fiscal misconduct received through various sources: CU EthicsLine, phone, email, or in-person. As needed, we provide support during litigation of related cases.

Education: We collaborate with our stakeholders and other university assurance and compliance functions to deliver insight on effective control environment, regulatory compliance, and fraud prevention and detection.

Core Principles and Standards

Internal Audit Core Principles require us to:

- Establish a risk-based plan to determine the priorities of the internal audit activity, consistent with the organization's strategies and goals
- Consider the input of senior management and the Board
- Communicate the internal audit activity plans and resource requirements, including significant interim changes and impact of resource limitations, to senior management and the Board for review and approval
- Be insightful, proactive, and future-focused

Assurance vs. Advisory Engagements

Assurance

- An objective examination of evidence for the purpose of providing an independent assessment on governance, risk management, and control processes for the organization. Examples may include financial, performance, compliance, system security, and due diligence engagements.
- The chief audit executive must establish a follow-up process to monitor and ensure that management actions have been effectively implemented or that senior management has accepted the risk of not taking action.
- Selected as an outcome of a risk assessment process.
- Results are typically communicated in a formal report format, including the engagement's objectives, scope and results.
- Backward-looking; insight through validation

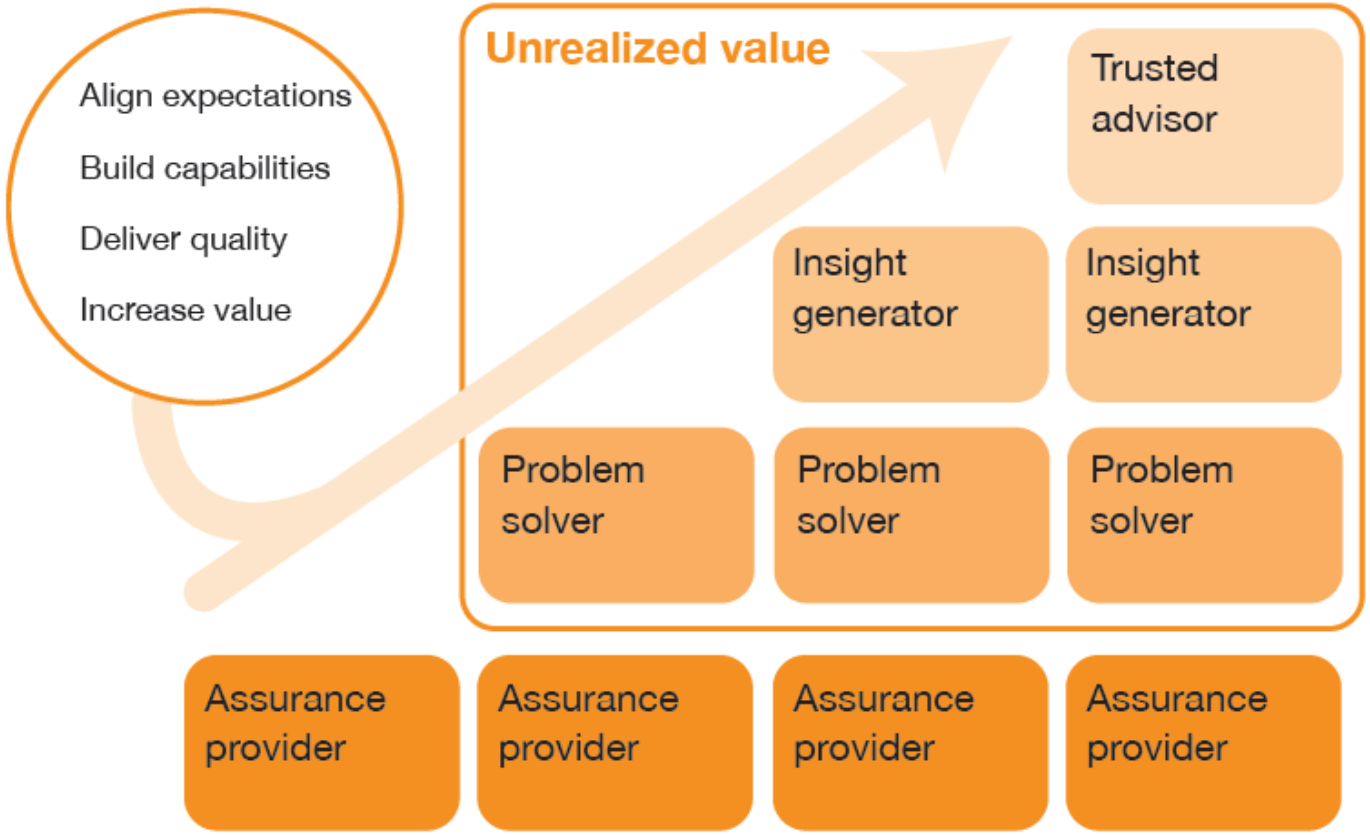
Advisory

- Advisory and related client service activities, the nature and scope of which are agreed with the client, are intended to add value and improve an organization's governance, risk management, and control processes without the internal auditor assuming management responsibility. Examples include counsel, advice, facilitation, and training.
- The internal audit activity must monitor the disposition of results of consulting engagements to the extent agreed upon with the client.
- Often identified through a management request.
- Results are typically communicated in the format agreed upon with the client (e.g., report, presentation, real-time advice).
- Forward-looking; insight through proactive advice

Source: The Institute of Internal Auditors

In Other Words…

Evolving Role of Internal Audit



Providing value-added services and proactive strategic advice to the business well beyond the effective and efficient execution of the audit plan

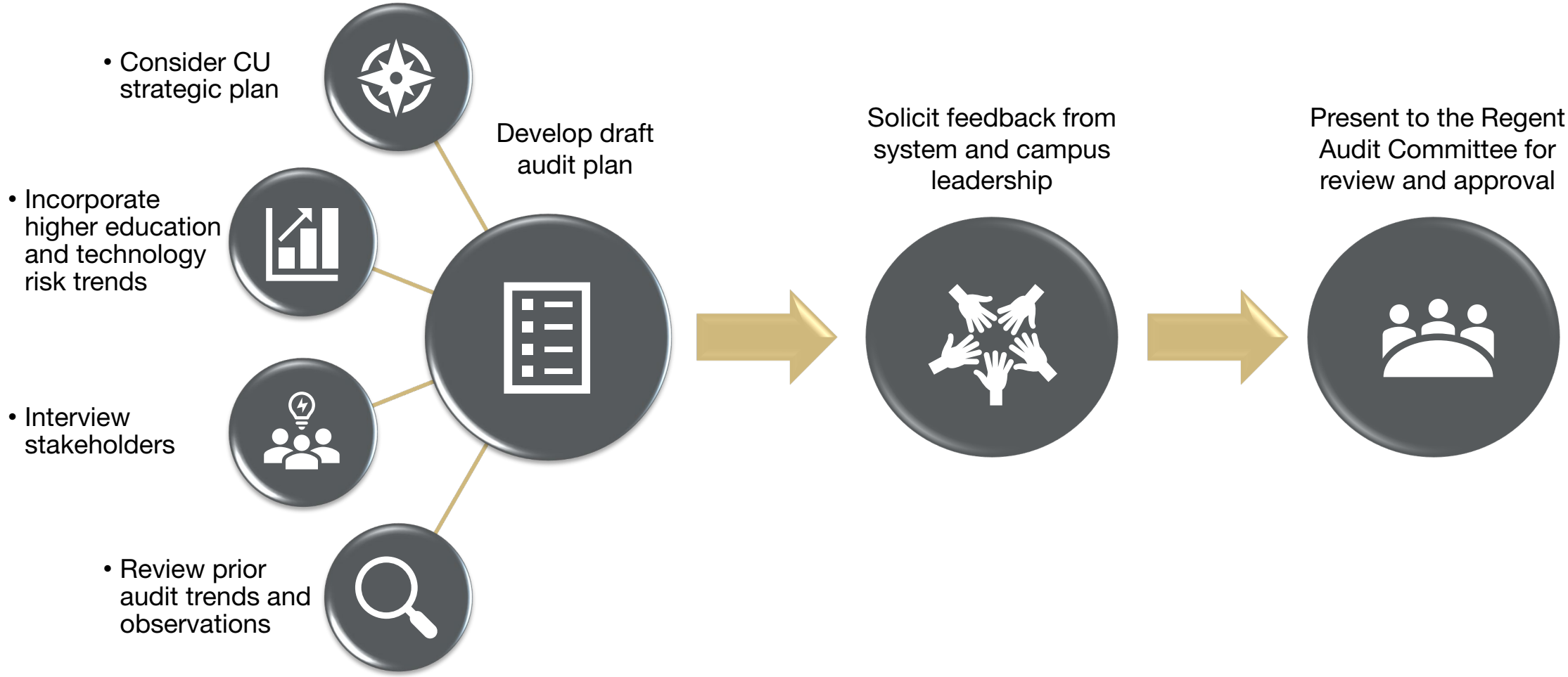
Taking a more proactive role in suggesting meaningful improvements and providing assurance around risk

Bringing analysis and perspective on root causes of issues identified in audit findings, to help business units take corrective action

Delivering objective assurance on the effectiveness of an organization's internal controls

Source: PwC: *2014 state of the internal audit profession study*

Internal Audit Plan Development Process



Top 12 Risks Affecting Organizations in 2022

1. **Cybersecurity** – The growing sophistication and variety of cyberattacks continue to wreak havoc on organizations' brands and reputations, often resulting in disastrous financial impacts.
2. **Talent Management** – The increased need for and acceptance of remote operations, including working from home, as well as continued dynamic labor conditions, are redefining how work gets done.
3. **Organizational Governance** – Governance encompasses all aspects of how an organization is directed and managed – the system of rules, practices, processes, and controls by which it operates.
4. **Data Privacy** – The growing list of regulations from jurisdictions around the world is making data privacy increasingly complex and dynamic.
5. **Culture** – With an increasing percentage of professional employees working remotely full or part time, organizations are challenged to maintain, enhance, or control their organizational culture.
6. **Economic & Political Volatility** – The ongoing impacts of the pandemic combined with the normal dynamics of macroeconomic cycles have the potential to create volatility in the markets in which organizations operate.
7. **Change in Regulatory Environment** – Fundamental changes in government appetites for regulation can have a significant impact on organizations.
8. **Supplier & Vendor Management** – For an organization to be successful, it has to maintain healthy and fruitful relationships with its external business partners and vendors.
9. **Disruptive Innovation** – We are in an era of innovative business models, fueled by disruptive technologies.
10. **Social Sustainability** – Increasingly, there is a recognition that organizations have significant influence on individuals who they employ, who work in their value chain, who consume their products and services, and who live in their communities.
11. **Supply Chain Disruption** – The disruption to business-as-usual operations globally, rooted in the global pandemic, has highlighted the need for resilience in supply chains in support of organizations' achievement of strategic objectives.
12. **Environmental Sustainability** – Organizations are facing increased pressure from stakeholders, including shareholders, regulators, customers, and employees, to evaluate and disclose how they are impacting the environment in which they operate.

Source: The IIA OnRisk 2022

Risk Themes in Higher Education

Cybersecurity Threats

With the conflicts abroad between Ukraine and Russia, Universities are focusing on cybersecurity and what steps can be taken to help prepare themselves to respond to a potential attack or disruption such as a ransomware attack.

Decentralized Operating Environment

Universities continue to focus on the risks that result from their decentralized operating environments, evaluating their internal control environments, and determining the appropriate risk appetite between unit autonomy and centralized business processes.

Future of Remote Work

With changing worker preferences re: remote work, Universities need to think through their remote work policies to continue to be an employer of choice; there are also ongoing considerations as they relate to taxes and information technology.

Foreign Influence in Research

There continues to be a focus on foreign influence within both Universities and the federal government. Even with the Justice Department ending the "China Initiative", we expect ongoing sponsor requirements as they relate to foreign national reporting and completeness in other support disclosures, as well as the Department of Education's Section 117 reporting requirement.

Gramm-Leach-Bliley Act (GLBA)

As Universities are subject to the GLBA, they must follow the updated FTC Safeguards Rule which mandates new requirements to be in place by December 9, 2022; there are significant updates, including additional specificity of security requirements.

Source: PwC 2022 Higher Ed Risk Trends

Risk Themes in Higher Education (cont.)

Stay focused on cybersecurity.

Higher education continues to be the most affected sector for malware attacks. While tools and techniques to thwart attacks continue to emerge, shifts to hybrid work and learning amid traditionally more open and decentralized IT environments have exacerbated the vulnerability to cyber threats.

Monitor other emerging risks and industry matters.

Evolving workforce expectations and continued disruptions due to the "great resignation" and competition for talent in many finance, accounting, internal audit, and IT roles has prompted unprecedented personnel turnover and staffing shortfalls in critical compliance, operational, and student-facing functions.

Intensifying wage and price inflation, coupled with continued supply chain shortages and disruptions

Integrity and consistency of reporting beyond the financial statements and ESG is critical.

Understand how the institution is managing and reporting on ESG.

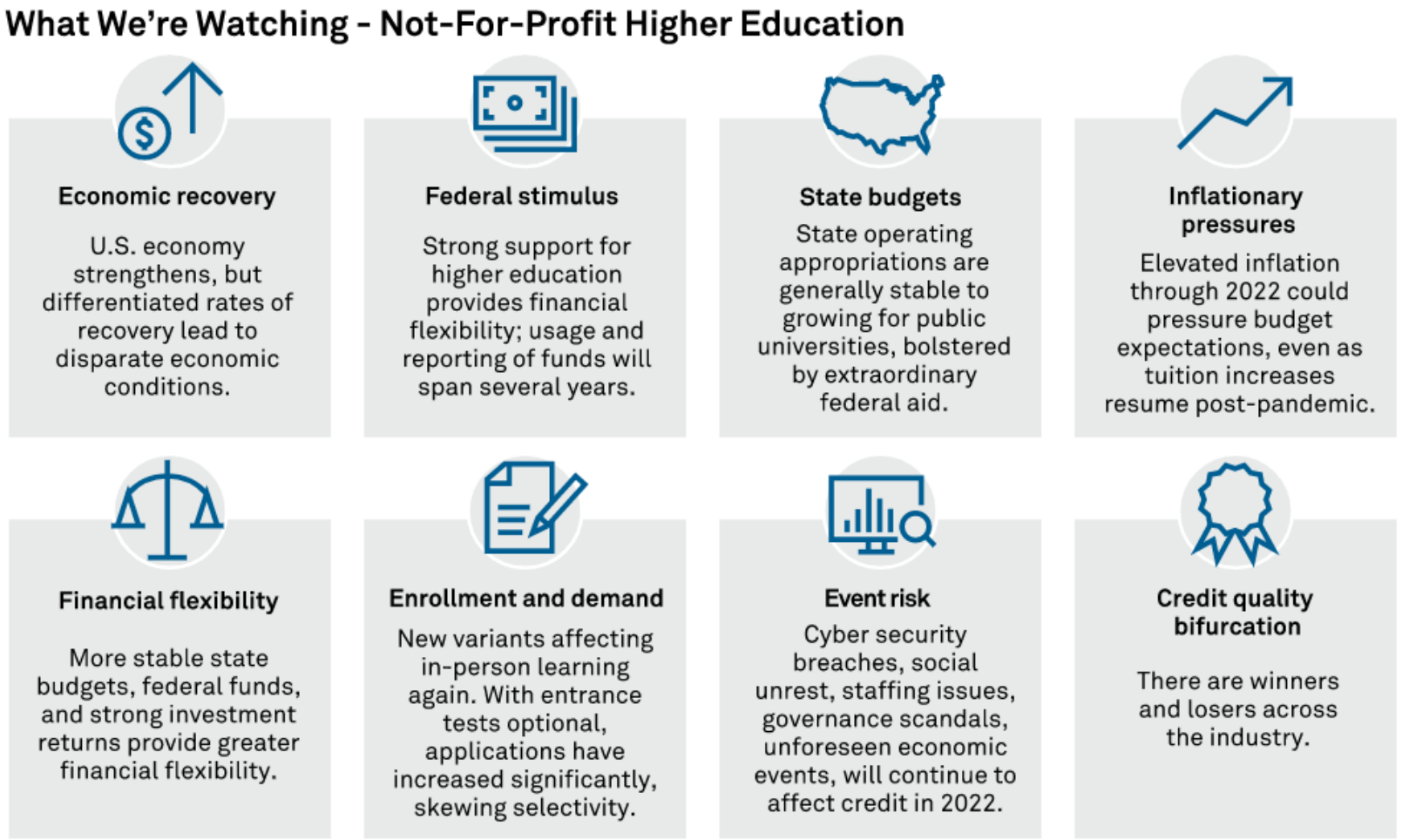
Higher education institutions are facing increasing stakeholder demands – from board members, bond markets, and local communities to students, faculty, and donors – for more visible and higher-quality information about environmental, social, and governance risks and opportunities.

Reinforce the institution's focus on ethics and compliance.

Reputational costs of an ethics or compliance failure are higher than ever, particularly given the increased fraud risk due to employee financial hardship, pressures on management to meet enrollment or other budgetary goals, and increased vulnerability to cyberattacks.

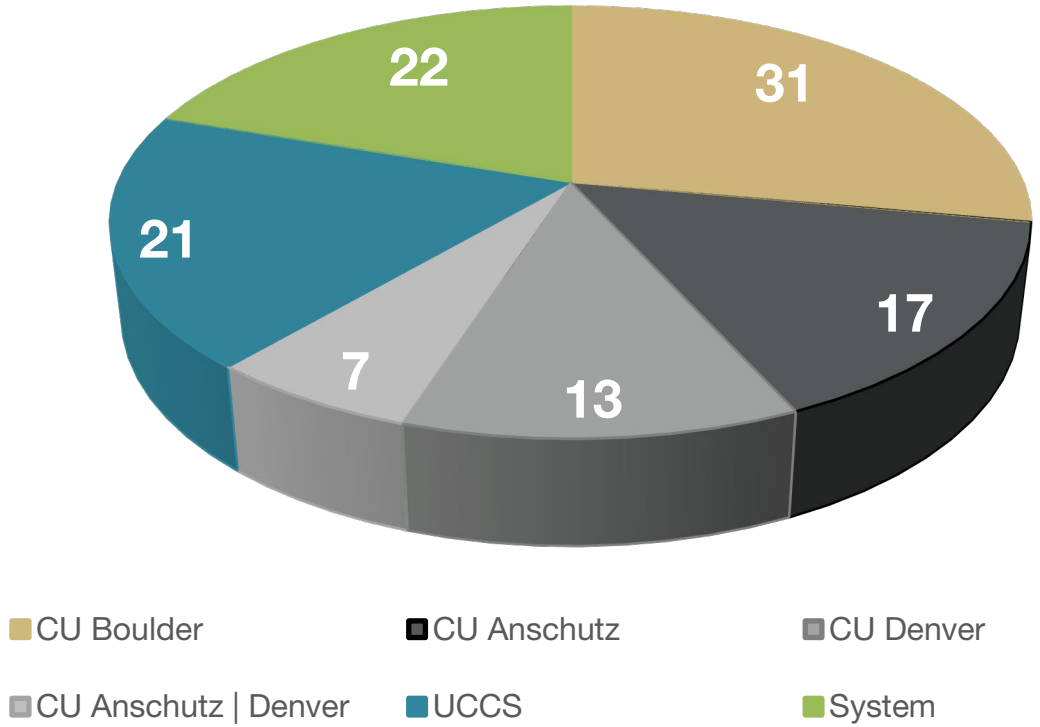
Source: KPMG Insight "On the 2022 Higher Education Audit Committee Agenda"

Risk Themes in Higher Education (cont.)



Source: S&P Global "Outlook for Global Not-For-Profit Higher Education: Out of the Woods, but not Yet in the Clear"

Campus & System Administration Interviews



- 111 individuals interviewed with varied levels of responsibility and oversight
- Intentionally included a cross-section of representatives with accountability for student success; research; compliance; risk management; finance; legal; diversity, inclusion, equity and access; operations; athletics; staff and faculty affairs
- Discussed FY23 priorities, challenges, success indicators and enablers, data needs and quality, ways Internal Audit can support

Key Risk Areas Addressed in FY23 Audit Plan

FY23 Audit Plan

CU System	CU Boulder	CU Anschutz	CU Denver	UCCS
Code of Conduct *	Asset Management – Inventory and Equipment	Financial Aid		Conflicts of Interest
Executive Expenses	Conflicts of Interest	H-1B Visa Program		Cybersecurity Event Detection
Information Technology Equipment Decommissioning	Export Control	Access Control – Service Accounts	Student Data Management	Donor Stewardship
Non-Retaliation Program Assessment *	Hiring of Non-Tenure Track Faculty	Effort Reporting Process		Effort Reporting Process ^
PeopleSoft Time & Labor *	Information Technology Asset Management (Software)	"Grateful Patient" Data Transfer		Minors on Campus
Virtual Private Networks	International Students and Faculty Visa Sponsorship and Compliance ^	HIPAA Security Compliance in Remote and Hybrid Work Arrangements		
Wire Transfers	Minors on Campus			
	Research Data Security			
	Subrecipient Post-Award Monitoring Practices			

*** Advisory Project**

^ Rollforward from FY22 Audit Plan

Other IA Initiatives for FY23

- Support the revision of APS 7003 *Collection of Personal Data from Students and Customers*
- Principles of Ethical Behavior website update
- CU Compliance Community (“CUC2”)
- CU EthicsLine – branding, marketing, capabilities refresh
- Advance Internal Audit’s use of technology, data analytics

University of Colorado
Boulder | Colorado Springs | Denver | Anschutz Medical Campus
FOUR CAMPUSES UNITED
ALL FOUR:ONE
APPENDIX
FY23 PROJECT DESCRIPTIONS

Please Note…

The following descriptions are intended to provide a high-level, preliminary sense of planned projects. They are not meant to definitively represent the nature, extent, and timing of the procedures to be performed.

For **audit/assurance engagements**, objectives and scope of each project will be refined during planning procedures and presented to the stakeholders at the entrance meeting.

For **advisory/consulting engagements**, objectives, scope, and deliverables will be agreed-upon with the clients and documented in an engagement letter.

FY23 Audit Plan

Campus	Engagement	Source
System Administration	**Code of Conduct *** *The Code of Conduct states the university's commitment to upholding the highest ethical, professional, and legal standards. Furthermore, it serves as a conduit to implement and operationalize several Regent Laws and Policies. The Code of Conduct is subject to periodic review for continued applicability and alignment with accepted practices. Internal Audit will work closely with the group appointed to perform the review and provide perspective regarding the existing content, proposed changes, and the process to disseminate the changes to the university community.* ***Proposed timing:*** *To be aligned with working group*	Audit Insight
System Administration	**Executive Expenses** *On an annual basis, Internal Audit reviews expenses submitted by the CU President, Chancellors, and Vice Presidents. The scope will include transactions for FY22.* ***Proposed timing:*** *August-September 2022*	Cadence
System Administration	**Information Technology Equipment Decommissioning** *The speed of technology continues to increase at an unprecedented rate. Product lifecycles grow shorter and the need for innovation is now a necessity. Organizations upgrading their IT equipment must also consider a thorough decommissioning strategy for outdated IT equipment, particularly taking into consideration possibilities of new malicious cyber-attacks and data theft. This audit will review the process for decommissioning and disposal of IT equipment at CU System, with focus on critical backups of data, asset safeguarding, removal of access, data erasure, and compliance with regulations such as PCI DSS, HIPAA, FERPA, FISMA and NIST.*	Risk Assessment

Pillar 1: Affordability & Student Success
Pillar 2: Discovery & Impact
Pillar 3: Diversity, Inclusion, Equity & Access
Pillar 4: Fiscal Strength

FY23 Audit Plan

Campus	Engagement	Source
System Administration	**Non-Retaliation Program Assessment *** *Under Regent Laws and Policies and the university's Code of Conduct, members of the university community are expected to report known and suspected violations of university policy or applicable law to appropriate university authorities. Faculty, staff, and students should feel safe to engage in frank, honest communication – raising questions or concerns without fear of retaliation. Such a non-retaliation program also reflects the university's commitment to compliance with applicable state and federal non-retaliation laws. Internal Audit will evaluate the effectiveness of non-retaliation policy and related enforcement, training, and awareness efforts essential to support an environment that encourages good faith reporting of known or suspected violations and participation in any investigation of alleged violations.*	Audit Insight
System Administration	**PeopleSoft Time & Labor *** *CU is in the process of replacing MyLeave with PeopleSoft Human Capital Management's Time and Labor module. The new module will be compatible with the existing payroll system and eliminate potential errors created by miscommunications between the disparate platforms. This advisory project will provide support to the implementation group by participating in risk and control discussions, as well as a review of policies, procedures, project stage gates and user acceptance testing process to the extent applicable. Insights will be shared real-time to contribute to the project's success.* ***Proposed timing:** To be aligned with working group*	Audit Insight
System Administration	**Virtual Private Networks (VPNs)** *VPNs create a tunnel, barrier, or boundary to maintain information flow of data by university constituents to internal networks designed with security outcomes in mind. Access security risks are accentuated if VPNs are improperly deployed, ineffectively managed or monitored. The objective of the audit will be to provide assurance of effectiveness of implemented VPN access and security controls.*	Risk Assessment
System Administration	**Wire Transfers** *Internal Audit will review the existing controls over wire transfers for design sufficiency and operating effectiveness.*	Risk Assessment

FY23 Audit Plan

Campus	Engagement	Source
Boulder	**Asset Management – Inventory and Equipment** *With the shift to approved remote and hybrid work environments, certain university-owned property and resources are now maintained outside the boundaries of the campus. This audit will review processes implemented by the campus to track inventory and equipment used by university personnel and assess practices for ensuring compliance with established policies.*	Risk Assessment
Boulder	**Conflicts of Interest (COI)** *The university's reputation of high-quality education, research, and service depends on the integrity of the personnel who perform these duties. A COI exists when a university representative has or is perceived to have a significant financial, personal, or professional interest that is directly or indirectly at odds or inconsistent with the university's interests. Internal Audit will review campus processes for disclosing, assessing, and managing potential conflicts of interest, including the development, communication, and monitoring of COI management plans.*	Management Request
Boulder	**Export Control** *Federal export control laws and regulations have been established to protect and restrict access to information and technology developed within the United States. The Office of Export Control (OEC) at CU Boulder has primary responsibility for ensuring compliance with these export control regulations. This audit will evaluate the sufficiency and effectiveness of controls within OEC and the programs OEC is responsible for managing.*	Audit Insight
Boulder	**Hiring of Non-Tenure Track Faculty** *Responsibility for determining the need for, marketing and recruitment of, and hiring of non-tenure-track faculty is distributed to each school and college on the CU Boulder campus to facilitate flexibility in meeting their unique objectives. This audit will review processes for hiring individuals into these non-tenure-track faculty positions, evaluate controls and opportunities to enhance the efficiency and effectiveness of procedures, and assess compliance with federal and state regulations and campus guidance.*	Risk Assessment

FY23 Audit Plan

Campus	Engagement	Source
Boulder	**Information Technology Asset Management (Software)** *Actively managing (maintaining inventory, tracking, and correcting) all software (operating systems and applications) on the network to ensure only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution is a critical security control. The objective of this audit is to evaluate the existence of software inventory procedures, processes and tools utilized at the campus level to identify, manage and monitor software purchasing and deployment in order to comply with university and campus policies, and software licensing agreements.*	Risk Assessment
Boulder	**International Students and Faculty Visa Sponsorship and Compliance (Rollover from FY22 Audit Plan)** *At CU Boulder, demonstrating compliance with federal regulations authorizing international student and faculty presence and participation requires coordination between various entities across the campus. This audit will assess campus policies, procedures, and effectiveness of controls designed to ensure that both the university and its guests on J-1 visas are in compliance with federal regulations and guidance.*	Risk Assessment
Boulder	**Minors on Campus** *In addition to the opportunities provided to matriculated students, the university offers various educational, cultural, and athletic opportunities to school students in and around the university community. These programs require additional resources and increased responsibility to ensure the health and safety of these valued participants. This audit will evaluate the application of controls designed to protect minors participating in campus-sponsored programs and test adherence to established university policies and procedures.*	Risk Assessment

FY23 Audit Plan

Campus	Engagement	Source
Boulder	**Research Data Security** *Throughout their research activities, principal investigators are often in possession of sensitive data that should be appropriately safeguarded in order to comply with grant provisions, and federal, state and local regulations. Therefore, it is critical to develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data. Internal Audit will evaluate governance, policy, controls, procedures and processes to detect, manage and monitor duplication and copying of confidential and highly confidential research information by internal employees to comply with university, campus, department, and regulatory requirements for research data security.*	Risk Assessment
Boulder	**Subrecipient Post-Award Monitoring Practices** *In managing federal grants and contracts awarded to the University of Colorado Boulder, the university is responsible for the proper use and oversight of funds allocated to subcontractors and research partners. In 2022, an audit of pre- and post-award monitoring practices within the Office of Contracts and Grants at CU Boulder was completed. This audit will review the design and implementation of monitoring practices and controls for ensuring funds are used in accordance with applicable rules, regulations, and contractual agreements, which is the responsibility of each award's primary investigator with assistance from financial administrators across the campus.*	Risk Assessment
Denver | Anschutz	**Financial Aid** *Title IV of the Higher Education Act ("Student Assistance") authorizes programs that provide financial assistance to students pursuing post-secondary education. This audit will review the rules and regulations governing program integrity and eligibility under Title IV to ensure CU Denver | CU Anschutz meets relevant federal requirements.* ***Proposed timing:** Q3 – Q4 FY23*	Risk Assessment
Denver | Anschutz	**H-1B Visa Program** *The H-1B visa program allows the university to temporarily employ foreign workers in positions requiring the theoretical and practical application of highly specialized knowledge and a bachelor's degree or higher in a specific specialty or equivalent. This audit will review the established H-1B process for consistency and compliance with federal regulations.*	Risk Assessment

Pillar 1: Affordability & Student Success
Pillar 2: Discovery & Impact
Pillar 3: Diversity, Inclusion, Equity & Access
Pillar 4: Fiscal Strength

FY23 Audit Plan

Campus	Engagement	Source
Anschutz	**Access Control – Service Accounts** *Information Technology (IT) service accounts are created to support the integration and management of IT applications and services, testing, or other service capabilities that are critical to university data and services. These accounts are similar to user accounts, and typically have high level access rights and privileges. The audit will review the processes and practices of service account management and monitoring to meet compliance with university and campus policies.*	Risk Assessment
Anschutz	**Effort Reporting** *Internal Audit will assess the practices around effort reporting for Principal Investigators with the intent to evaluate the design and effectiveness of the current control environment and help identify potential gaps that may lead to inaccurate reporting of time worked and allocated.*	Risk Assessment
Anschutz	**“Grateful Patient” Data Transfer** *The “Grateful Patient” program is a way for patients to make a gift of gratitude for the care experienced at University Hospital. Patient data is transferred from UCHealth University Hospital to University Advancement. Internal Audit will review the integrity and security of the data transfer.*	Risk Assessment
Anschutz	**HIPAA Security Compliance in Remote and Hybrid Work Arrangements** *The university has an ethical and legal obligation to safeguard the security and privacy of personal health information it collects or maintains in carrying out its mission of advancing research and knowledge and providing state-of-the-art health care. In the context of emerging hybrid and remote work arrangements, Internal Audit will identify areas where protected health information is generated and stored, and assess access and data security procedures, practices and effectiveness of controls for compliance with university policy and applicable data security regulations.*	Risk Assessment

FY23 Audit Plan

Campus	Engagement	Source
Denver	**Student Data Management** *University Information Services (UIS) offers a wide range of enterprise data services to support the university's academic mission and the strategic vision of each campus. These services encompass many functions that provide data to the campus directly related to student administration and student success. The objective of the audit is to assess procedures, processes and practices by the campus to secure access and data management of enterprise data instances in compliance of university policies.*	**Risk Assessment**
Colorado Springs	**Conflicts of Interest (COI)** *The university's reputation of high-quality education, research, and service depends on the integrity of the personnel who perform these duties. A COI exists when a university representative has or is perceived to have a significant financial, personal, or professional interest that is directly or indirectly at odds or inconsistent with the university's interests. Internal Audit will review campus processes for disclosing, assessing, and managing potential conflicts of interest, including the development, communication, and monitoring of COI management plans.*	**Risk Assessment**
Colorado Springs	**Cybersecurity Event Detection** *Threats of and attempted of cyber attacks on university IT services and data are sophisticated, widespread, and continuous. Detection of such events is critical to minimizing and mitigating harm and unauthorized access by bad actors or hackers. The objective of the audit is to assess processes, practices, and methodologies employed to detect, monitor, and manage cybersecurity events against university and campus electronic resources.*	**Risk Assessment**
Colorado Springs	**Donor Stewardship** *Donor stewardship involves managing gifts as donors intended, updating donors on the progress and impact of the gifts, and cultivating donors to keep them interested in giving to the university. Donor intent is the purpose for which a donor intends a charitable gift or bequest. This audit will examine the use of current and endowment funds at UCCS to ensure the gifts are spent in accordance with the donor's intent and the monies are spent in a timely manner.*	**Risk Assessment**

Pillar 1: Affordability & Student Success

Pillar 2: Discovery & Impact

Pillar 3: Diversity, Inclusion, Equity & Access

Pillar 4: Fiscal Strength

FY23 Audit Plan

Campus	Engagement	Source
Colorado Springs	**Effort Reporting** *Internal Audit will assess the practices around recording percent effort for academic colleges' full-time employees who have "add on" appointments. The intent is to evaluate the design and effectiveness of the current control environment and help identify potential gaps that lead to greater than 100% reporting of time worked.*	Risk Assessment
Colorado Springs	**Minors on Campus** *In addition to the opportunities provided to matriculated students, the university offers various educational, cultural, and athletic opportunities to school students in and around the university community. These programs require additional resources and increased responsibility to ensure the health and safety of these valued participants. This audit will evaluate the application of controls designed to protect minors participating in campus-sponsored programs and test adherence to established university policies and procedures.*	Risk Assessment

Pillar 1: Affordability & Student Success

Pillar 2: Discovery & Impact

Pillar 3: Diversity, Inclusion, Equity & Access

Pillar 4: Fiscal Strength