University of Colorado

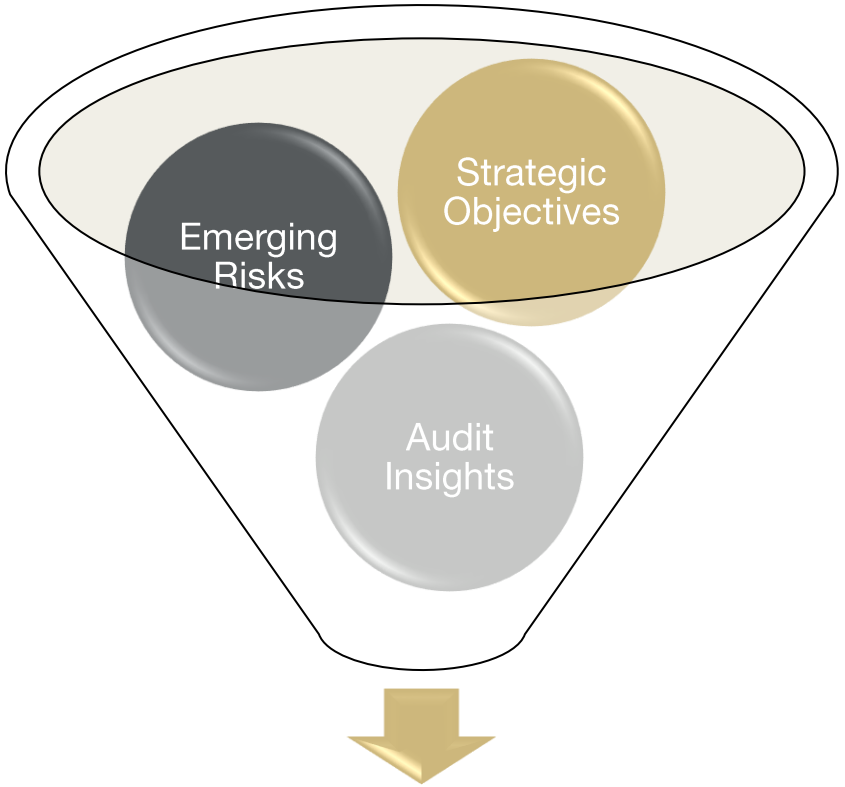
Boulder | Colorado Springs | Denver | Anschutz Medical Campus

FOUR CAMPUSES UNITED
ALL FOUR:ONE

FY22 Internal Audit Plan

June 9, 2021

Core Principles and Standards



Audit Plan

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

Source: The Institute of Internal Auditors

Responsive and Agile Audit Planning

Monitor key University initiatives and higher education emerging risks to identify potential projects, as well as evaluate whether the expected audit plan risk coverage has been achieved

Identify risk universe through system and campus leadership information (e.g., strategic plans and initiatives), evaluation of higher education emerging trends, as well as inherent process, fraud, and regulatory compliance risks

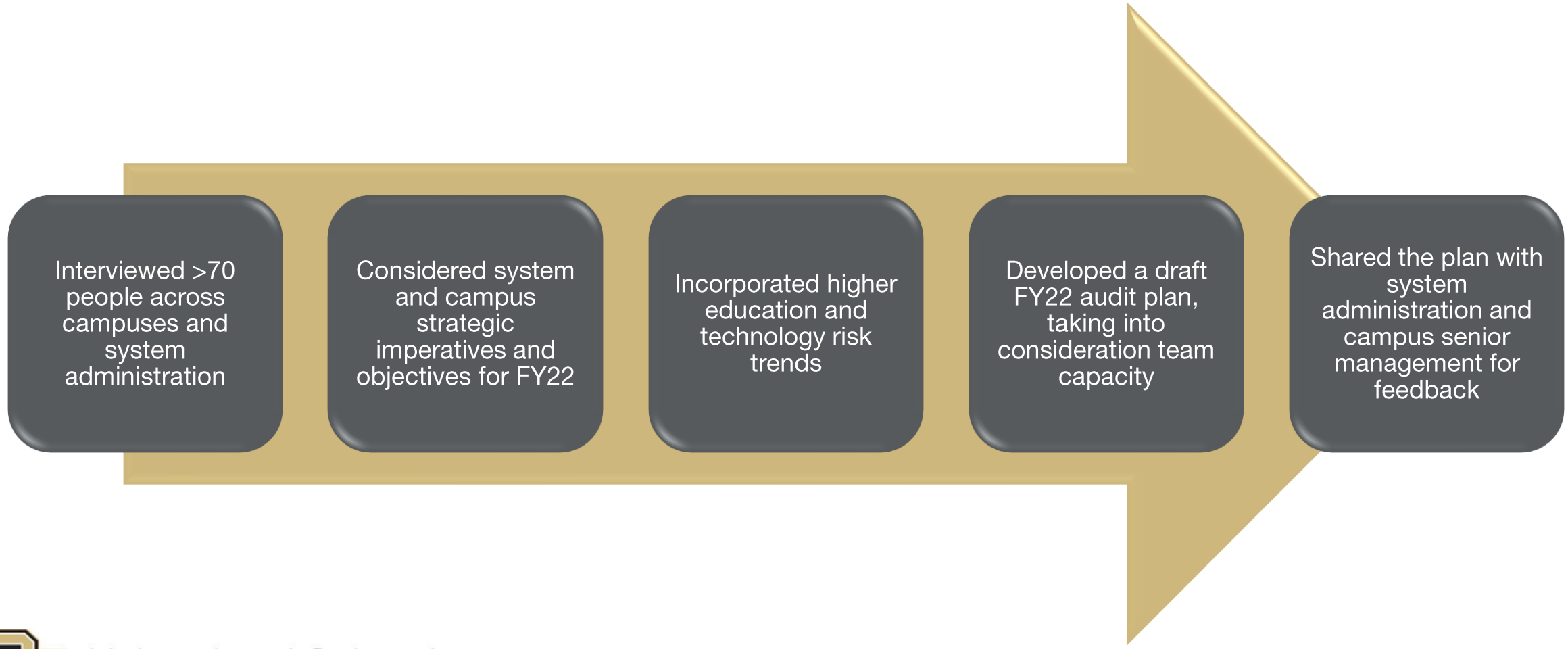
Assess inherent risk and the control environment of each key process, in the context of the University strategies, objectives and key initiatives

Align audit resources with initiatives of strategic and operational importance while considering existing processes, controls, and other mitigating factors, as well as prior audit history (including external reviews) and discussions with management.

Develop and ***execute*** the audit plan

University of Colorado
Boulder | Colorado Springs | Denver | Anschutz Medical Campus

FY22 Audit Plan Development



University of Colorado
Boulder | Colorado Springs | Denver | Anschutz Medical Campus

Higher Education Risk Themes and Audit Trends

Foreign Influence in Research

The federal government continues to investigate and prosecute cases of potential foreign influence, conflicts of interest, and theft of federally funded research by foreign nationals.

Data Privacy and Security

Universities continue to be in the spotlight over data breaches, including those associated with third parties. Additionally, we are seeing certain federal sponsors outline minimum data security requirements as a prerequisite for future federal funding.

System Implementations

Significant system implementations are being planned for or actively implemented. Institutions need to make sure that their substantial investments in these systems achieve their planned outcome from a functionality, timing, and budget perspective.

Compliance

Recent high profile compliance issues, including Section 117 reporting, conflict of interest and commitment issues, and Section 508 Digital Accessibility have highlighted enhancement opportunities in central compliance functions.

Procurement fraud / Remote work risks

Universities have been increasingly the target of procurement fraud. Additionally there has been concern that lack of defined policies and procedures around use of procurement cards for home office expenditures could lead to improper use of University funds.

Source: PwC 2021 Higher Ed Risk Trends

FY22 Audit Plan

University-Wide	CU System	CU Boulder	CU Anschutz	CU Denver	UCCS
Higher Education Emergency Relief Funds (HEERF) Allocation Review*	Voluntary Self-Disclosure and External Reviews Follow Up	Policy Governance*			
Post COVID-19 Return to Work Policies and Practices	Procurement: System-Wide Contracts	Subrecipient Monitoring	Conflict of Interest (COI) Governance		National Cybersecurity Building
Post-Retirement Hiring Process	Business Continuity and Disaster Recovery Processes	Athletics: PointsBet Process	Self-Insurance and Risk Management Trust	College of Architecture & Planning: Research Compliance	Human Resources – Pay Equity Implementation and Compliance*
Foreign Gifts and Contracts*		International Students and Faculty Visa Sponsorship and Compliance	Cost Transfers		Human Resources – Effort Reporting Process*
Employee Security Awareness		NIST SP800-171/CMMC Audit Readiness	Donor Stewardship		
Incident Response Management		Vulnerability and Patch Management			
Salesforce Platform					
Data Lakes					

University of Colorado
Boulder | Colorado Springs | Denver | Anschutz Medical Campus

*** Consultation/Advisory**

University of Colorado

Boulder | Colorado Springs | Denver | Anschutz Medical Campus

FOUR CAMPUSES UNITED
ALL FOUR:ONE

Appendix

FY2022 Audit Plan

Campus	Engagement	Source
System-Wide	**Higher Education Emergency Relief Fund (HEERF) Allocation Review*** *Review the allocation of Coronavirus emergency relief funding administered by the Department of Education for compliance with relevant published guidelines, including accuracy of calculations, reporting presentation and disclosure, fund disbursement governance, and implementation of fraud, waste and abuse controls.* ***Proposed timing:*** *June – September 2021*	Risk Assessment
System-Wide	**Post COVID-19 Return to Work Policies and Practices** *Review practices for compliance with established policies, particularly in the areas of accommodations, remote work, inventory tracking, and documentation retention.* ***Proposed Timing:*** *March – May 2022*	Risk Assessment
System-Wide	**Post-Retirement Hiring Process** *Evaluate the extent to which the university utilizes retiree employment and assess current practices for compliance with applicable laws, Administrative Policy Statement (APS) 5054, as well as potential impact on succession planning, talent retention, and reputational risk.*	Audit Insight
System-Wide	**Foreign Gifts and Contracts*** *Under Section 117 of the Higher Education Act of 1965 (HEA), most institutions of higher education (IHEs) are required to report, twice each year, foreign gifts and contracts of $250,000 or more (considered alone or in combination with other gifts or contracts with a foreign source) and to disclose any foreign ownership or control to the Secretary of Education. Beginning in 2019, the Department of Education (ED) has sought to expand these disclosure requirements and has begun an aggressive enforcement effort to address what it alleges is "pervasive noncompliance" by IHEs with these reporting requirements. This advisory will assess the effectiveness of systems and processes implemented at the university to ensure complete, accurate, and timely reporting of foreign gifts and contracts to ED in compliance with Section 117 of the HEA.*	Management Request

FY2022 Audit Plan (continued)

Campus	Engagement	Source
System-Wide	**Employee Security Awareness** *Given the overwhelming trend of targeting information systems through personnel email, social engineering, and online channels, this audit will assess personnel awareness, readiness, and contribution to cybersecurity defense. IA will test and evaluate training programs, phishing tests and remedial training, enterprise record keeping, marketing, and other mechanisms associated with employee security awareness and behavior. Alignment and breadth/depth of impact will be considered.*	Risk Assessment
System-Wide	**Incident Response Management** *The widely diverse, distributed, and decentralized nature of university IT systems and the collaborative and personnel-dependent nature of university services create a heightened risk for security incidents and breaches. Practiced maturity in incident response lowers the cost/impact of an incident to those affected, and ensures consistent messaging, timely actions, and compliance to diverse international, federal, state, and local reporting authorities, reducing reputational impact. The audit will assess process design and controls against leading standards and evaluate university readiness for timely, compliant, consistent, and predictable response to IT security breaches and events.*	Risk Assessment
System-Wide	**Salesforce Platform** *The Salesforce platform is a key component of some of the highest-profile IT projects and objectives at the university, including the unified customer relationship management (CRM) and student success programs. The audit will focus on leveraging information from these major program areas to evaluate data integration, protection, and governance standards supporting effective reliance on this third-party service platform as a university resource. Roles and responsibilities, identity integration, project/proposal and customization management, and the management of data according to classification and security risk will be considered.*	Risk Assessment
System-Wide	**Data Lakes** *Evaluate new data integration and availability platforms, programming interfaces, and cloud-based solutions for delivering enterprise data in a highly available manner. Governance, roles, control responsibilities, and participation guidance will be assessed with a focus on data governance and management principles for all participants. The audit will evaluate architectural alignment between various projects or sources for adherence to aligning policies, principles and standards.*	Risk Assessment

FY2022 Audit Plan (continued)

Campus	Engagement	Source
System Administration	**Voluntary Self-Disclosure and External Reviews Follow Up** *Voluntary Self Disclosures (VSDs) by parties who believe they may have violated applicable export control regulations indicate a party's intent to comply with U.S. export control requirements. The audit will review VSDs by the university, and the steps the university stated would take place to mitigate the violation from occurring again in the future. The mitigation steps will also be reviewed to ensure the university implemented them.*	Audit Insight
System Administration	**Procurement: System-Wide Contracts** *Vendor agreements are a business contract between the university and the vendor agreeing to exchange goods and services for compensation for specific amounts and prices. The audit will review contracts with vendors used across all campuses to determine if contracts can be combined to obtain better pricing.*	Audit Insight
System Administration	**Business Continuity and Disaster Recovery Processes** *Disaster recovery and business continuity practices are a wide variety of activities designed to ensure recovery from external forces or interrupting events and the continuity of business during that recovery effort. For a selected critical IT service(s), the audit will evaluate service support to ensure key recovery and continuity milestones are deliverable, tested and communicated with accountable parties. The audit will focus on the identification and prioritization of data (criticality and classification) to ensure higher value assets are protected from system, storage, natural, and service-oriented failures including the ever-prevalent ransomware and data extortion threats of the digital transformation era.*	Risk Assessment
CU Boulder CU Anschutz CU Denver UCCS	**Policy Governance*** *An effective compliance program is built on a foundation of policies and procedures that give both content and effect to ethical norms and are intended to reduce risks identified by the organization as part of its risk assessment process. Implementation of a policy governance framework provides the structure for development, approval, implementation, review, and distribution of policy and related procedures, standards, and guidelines. This advisory will assess the reliability, efficiency, and effectiveness of the policy governance framework at each campus and System Administration, and will identify opportunities to improve policy management, awareness, and training.*	Risk Assessment

FY2022 Audit Plan (continued)

Campus	Engagement	Source
CU Boulder	**Subrecipient Monitoring** *In managing federal grants and contracts awarded to the University of Colorado Boulder, the university bears a responsibility to ensure proper use and oversight of funds allocated to subcontractors and research partners. While these subrecipient agreements are designed to benefit the research, they also represent additional risk to the university if not managed properly. This audit will review the design and implementation of monitoring practices and controls to comply with sponsoring agency requirements and ensure funds are used in accordance with applicable rules, regulations, and contractual agreements.*	Risk Assessment
CU Boulder	**Athletics: PointsBet Process** *In November 2019, Colorado voters passed Proposition DD, which legalized physical and online sports betting in the state of Colorado. In September 2020, PointsBet, an online gaming operator headquartered in Denver, and Learfield IMG College, the media rights holder for University of Colorado Boulder Athletics, completed a corporate sponsorship agreement making PointsBet a partner with the University of Colorado. The objective of this audit will be to assess the partnership agreement, controls to prevent improper influence of athletes or access to proprietary information, and assess policies regarding wagering on University of Colorado athletic events by students, faculty and staff.*	Risk Assessment
CU Boulder	**International Students and Faculty Visa Sponsorship and Compliance** *At the University of Colorado Boulder, demonstrating compliance with federal regulations and completeness of documentation authorizing international student and faculty participation requires coordination between various entities across the campus. This audit will assess campus policies, procedures, and effectiveness of controls designed to ensure sufficient communication between participating campus entities.*	Risk Assessment

FY2022 Audit Plan (continued)

Campus	Engagement	Source
CU Boulder	**NIST SP800-171/CMMC Audit Readiness** *Starting in 2021, federal contracts involving controlled unclassified information will be held accountable to National Institute of Standards and Technology (NIST) performance standards embodied through capability maturity evaluations (Cybersecurity Maturity Model Certification (CMMS) Audits) and against national standards. The audit will evaluate readiness to engage external auditors, achieve sufficient maturity ratings, and incorporate NIST standards into affected university policies, procedures, and operations.*	Risk Assessment
CU Boulder	**Vulnerability Management** *Vulnerability management encompasses the processes that identify IT assets, discover security vulnerabilities of those assets, risk-prioritize treatment of those vulnerabilities, ensure patching and updating, and manage remediation and exception tracking and reporting. The audit will assess the practice at the Boulder campus against the CIS Top 20 control guidelines and other IT security framework sources to ensure the practice is effective.*	Management Request
CU Anschutz CU Denver	**Conflict of Interest (COI) Governance** *This audit will review the process for collecting and validating COI information, including ensuring accuracy of the information, appropriate follow up on identified COI, periodic update, and evaluation of compliance with the "1/6 Rule."*	Risk Assessment
CU Anschutz	**Cost Transfers** *Grant funds are expected to be used to further the research the sponsor elected to support when awarding the funds to the university. However, transferring funds from one grant to another may represent a potentially unallowable expenditure. Therefore, additional requirements have been put in place by the campus to ensure these types of transactions are properly documented and authorized. The audit will review cost transfers to assess compliance with university and campus policies, and ensure controls are sufficiently designed to effectively support and monitor the increased risk posed by these types of transactions.*	Risk Assessment

FY2022 Audit Plan (continued)

Campus	Engagement	Source
CU Anschutz	**Self-Insurance and Risk Management Trust** *The University of Colorado Self-Insurance and Risk Management Trust (the Trust) provides professional liability insurance coverage (also referred to as malpractice insurance coverage) to faculty, staff, students, and health care practitioners-in-training across each of the university's four campuses. The audit will include a review of processes affecting the financial statements of the Trust to ensure appropriate controls are in place to mitigate risks that could lead to losses and/or a misstatement of the financial statements.*	Cadence
CU Anschutz	**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. The audit will review donor gifts provided to the campus to assess whether they are used timely and as the donor intended within university policy guidelines.*	Risk Assessment
CU Denver	**College of Architecture & Planning** *Research funding is a significant source of revenue for the University of Colorado Denver. To ensure sponsored funds are used appropriately and efficiently, and to help secure continued support and enhance future growth, the campus must implement appropriate preventive and detective controls. This audit will assess effectiveness of policies, procedures, and operational controls designed to manage and ensure compliance of college research activities, including effort certification, procurement processes, expense allocation, monitoring, and document retention.*	Risk Assessment

FY2022 Audit Plan (continued)

Campus	Engagement	Source
UCCS	**National Cybersecurity Building** *UCCS has received a $2.75 million federal grant to expand and renovate the National Cybersecurity Center located on North Nevada Avenue. The grant is matched by awards from the El Pomar Foundation, the Anschutz Foundation, and the John Lane Foundation. The Cybersecurity Center is in a federal opportunity zone, meaning that any entity making investments in the project is eligible for federal tax benefits. The audit will review the project and lease accounting, contract compliance with partners, and compliance with state and federal funding requirements.*	Risk Assessment
UCCS	**Human Resources – Pay Equity Implementation and Compliance*** *Achieving and maintaining pay equity represents a significant risk to the university. The federal Equal Pay Act holds employers strictly liable for unequal pay between members of the opposite sex for substantially equal work. The Colorado Equal Pay for Equal Work Act (CEPEWA), effective January 1, 2021, greatly expands the definition of wage discrimination, changes the process for handling wage discrimination claims, and imposes a variety of other obligations on employers. This advisory will support the campus' effort to effectively implement appropriate policies and controls to ensure compliance with CEPEWA and related regulations.*	Management Request
UCCS	**Human Resources – Effort Reporting Process*** *This advisory project 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.*	Management Request