UNIVERSITY OF VIRGINIA
BOARD OF VISITORS

Meeting of the Audit, Compliance, and Risk Committee

June 1, 2023

AUDIT, COMPLIANCE, AND RISK COMMITTEE

Thursday, June 1, 2023
1:30 – 2:30 p.m.
Board Room, The Rotunda

Committee Members:

Thomas A. DePasquale, Chair

Robert M. Blue

Mark T. Bowles

Carlos M. Brown

Louis S. Haddad

Babur B. Lateef, M.D

Stephen P. Long, M.D.

The Honorable L.F. Payne

Whittington W. Clement, Ex-officio

Adelaide Wilcox King, Faculty Consulting Member

<u>**AGENDA**</u>

UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: June 1, 2023

COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: I. Remarks by the Committee Chair

ACTION REQUIRED: None

BACKGROUND: Mr. Thomas DePasquale, the Committee Chair, will open the meeting, welcome guests, and provide an overview of the agenda.

UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: June 1, 2023

COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: II. Review and Approval of FY2024-FY2025 Audit Department
                                        Plan

BACKGROUND: The internal audit plan is discussed with and approved annually by the Audit, Compliance, and Risk Committee and the Board of Visitors. The audit plan is developed based on assessed risks to achievement of the University's objectives, stakeholder input, benchmarking with peers, macro-environmental factors, auditors' knowledge of UVA systems and processes, and resource availability. Timing of audits is influenced by institutional projects underway, available resources, and unforeseeable events.

Risk-Based Audit Planning

The Audit Department has developed a comprehensive register of risks relevant to UVA considering the University's education, patient care, and research missions. Weighted risk factors are used to score the risk register; available resources further refine the draft audit plan, which is discussed with key stakeholders and updated by their input. Ultimately, the proposed audit plan is shared with the Audit, Compliance, and Risk Committee and the Board of Visitors for their review and approval.

The two-year plan aligns to categories in the Enterprise Risk Management (ERM) programs of both the Academic Division and the UVA Health Division.

UVA Health Division Two Year Audit Plan

Primary ERM Risk Area	FY2024 UVA Health Audit Topic	Scope
Health Care Regulatory Compliance	Contract Management	Internal controls over contract development, approval, and management. (Deferred from FY2023)
	IRS 501(r) Compliance – UVA Community Health	Compliance with IRS 501(r) rules applicable to non-profit hospitals, such as community needs analyses and community benefit plans, financial assistance elements and publication. (Deferred from FY2023)
	Physician Transactions (Purchased Services) – UVA Community Health	Compliance with contract payment terms and UVACH policies for payments made to physicians or medical groups. (Deferred from FY2023--Audit to be conducted under the attorney client privilege)
	Medical Device Recalls and Credits	Policies and procedures for claims adjustments related to medical device recalls.
	Exclusion Screening for Vendors	Policies and procedures designed to ensure all on-site vendor representatives receive the required screening for potential exclusion from government payer programs.
	Trauma Activation Claims – Billing Compliance	Validate that Medicare claims for trauma services comply with Medicare billing guidelines.
Financial Sustainability	Late Charges – Professional Fee Billing	Level of compliance with Revenue Cycle standards for timely charge entry to patient accounts.
	Laboratory Outreach Billing (Non-patient receivables)	Billing and collection processes for the laboratory's outreach program (services provided to other organizations).
	Pharmacy 340B Program – UVA Community Health	Compliance to Pharmacy 340B regulatory requirements and assess practices for maximizing realized savings.
	Capital Asset Inventory Management – APA Audit Follow-up	Status of corrective action plans implemented in response to the internal control finding on capital asset inventory controls.

Primary ERM Risk Area	FY2024 UVA Health Audit Topic	Scope
	Warehouse Receiving Controls	The receiving processes at the new distribution warehouse – internal control design and effectiveness.
Workforce Management and Development	Incentive Compensation Plans – University Hospital	Internal controls around the University Hospital's incentive compensation plans.
IT Security and Governance	Ransomware Assessment Follow Up (IT Audit)	Determine if the recommendations outlined within the March 2022 Mandiant Purple Team Report have been addressed and closed by Management.
	Third Party Risk Management (IT Audit)	Identify and assess the controls supporting the third-party risk management program including governance & operating model, policies, and procedures, third party data management, risk models, assessment methodology, and tools and technology used to support reporting.
	Identity & Access Management (IT Audit)	Identify the methods, processes, and controls by which access is provisioned and deprovisioned both centrally and for selected applications that authorize access to end users.

Primary ERM Risk Area	FY2025 UVA Health Audit Topic	Scope
Health Care Regulatory Compliance	Clinical Trials Billing Compliance	Policies, procedures, and internal controls for compliant billing of clinical research
	Provider Based Billing Compliance – UVA Culpeper Medical Center	Compliance with Medicare billing rules for provider-based clinics.
	Balance Billing (No Surprises Act)	Compliance with regulatory requirement around billing specific services provided to patients with out-of-network coverage.
	Price Transparency	Compliance with the regulatory requirement to publish standard fees and provide estimates to patients.
	Information Blocking Rule	Compliance around the HHS rule prohibiting any practice likely to interfere with, prevent, or discourage access, exchange, or use of electronic health information (EHI).

Primary ERM Risk Area	FY2025 UVA Health Audit Topic	Scope
	Hospice Program	Management controls for the Hospice Program, including third-party management and processes to ensure compliance with the unique regulatory requirements for hospice programs.
Financial Sustainability	Financial Assistance and Financial Counseling	Processes for helping uninsured patients find resources to help pay medical costs.
	Insurance Verification and Validation	Procedures and controls for gathering and validating patient insurance coverage prior to providing services.
	Ambulatory Scheduling – Follow-up Audit	Follow-up to FY2021 audit focused on procedures for monitoring and improving patient access in ambulatory clinics.
Quality and Patient Safety	Provider Credentialing	Compliance with provider credentialing policies and procedures.
	Opioid Stewardship Program	Assess maturity of the Opioid Stewardship Program at the University Hospital.
	Practitioner Peer Review	Assess whether peer review process conforms to UVA Health policy and procedures.
	Event Reporting (Be Safe program)	Processes and controls in place for event reporting, analysis, and response (adverse events, near misses and unsafe conditions).
IT Security and Governance	Threat and Vulnerability Management (IT Audit)	Identify and assess the controls supporting the threat and vulnerability management processes used for identifying, classifying, prioritizing, remediating, and mitigating software and firmware vulnerabilities.
	HIPAA Security Compliance (IT Audit)	Evaluate if adequate security procedures are in place at the Health Systems to protect the privacy of individually identifiable health information, called protected health information
	Incident Response (IT Audit)	Identify and assess the formal incident response capabilities including incident response policies, procedures, and playbooks, incident response governance, ownership and oversight, incident review metrics and reporting, prevention and

Primary ERM Risk Area	FY2025 UVA Health Audit Topic	Scope
		detection mechanisms, and training and awareness.

UVA Academic Division Two Year Audit Plan

Primary ERM Risk Area	FY2024 Academic Division Audit Topic	Scope
Community	ESG - Sustainability Reporting (In Progress from FY23 plan)	Assess controls ensuring relevant, quality information is captured through the reporting process, culminating in the preparation of reliable sustainability reports.
Learning & Knowledge Creation	UVA Wise Academic Records - Degree Related Data (Jenzabar)	Evaluate design and effectiveness of controls over the maintenance of degree-related data, including grade submissions and changes, course substitutions and/or degree requirement exceptions, and incoming transcripts.
Compliance	NCAA Compliance: Financial Aid for Student-Athletes	Assess UVA Athletic Department Compliance Office's oversight of student-athletes Financial Aid considering anticipated impacts of the NCAA Name, Image, and Likeness (NIL) policy.
	CARES Compliance - Higher Education Emergency Relief Fund (HEERF I, II, III) - Part 3 (FY24)	Evaluate design and effectiveness of controls and processes related to HEERF funds data collection, use, accounting, and reporting.
	Presidential Travel and Expense	Annual audit of the President's Travel and Entertainment expenses. Audits were paused during pandemic-impacted years. Audit will cover FY23 expenses.
Operations	Benefits Administration	Follow-up on KPMG recommendations for the UVA Health Plan.
	School-Level Audits: Pilot Audit of McIntire School (In Progress from FY23 plan)	Complete pilot of school level audit program as a prelude to annual school level audits.
	School-Level Audits (3)	Assess effectiveness of risk-relevant school level controls and processes at 3 UVA schools.

Primary ERM Risk Area	FY2024 Academic Division Audit Topic	Scope
Fiscal Sustainability	Workday Financials Controls Validation: Grants and Contracts	Assess the effectiveness of key financial business process controls related to expenditures of sponsored funding.
	Workday Financials Controls Validation: Gifts	Assess the effectiveness of key financial business process controls related to the acceptance, receipt, recording, and processing of gifts to the University.
	Student Financial Services	Evaluate design and effectiveness of controls over accuracy and timeliness of student billing and accounts receivable.
	Payroll	Evaluate controls over payroll processes including Workday user access, identification of employees working out-of-state/country, and untimely terminations resulting in overpayments.
	Football Operations Building Construction Audit	Audit initiated in FY23 continues through the construction life cycle.
	Hotel and Conference Center Construction Audit	Audit initiated in FY23 continues through the construction life cycle.
Technology Risks	Ransomware Assessment Follow Up (IT Audit)	Determine if the recommendations outlined within the December 2021 Mandiant Purple Team Report for the Academic Division have been addressed and closed by Management.
	Third Party Risk Management (IT Audit)	Identify and assess the controls supporting the third-party risk management program such as: governance & operating model, policies, and procedures, third party data management, risk models, assessment methodology, and tools and technology used to support reporting.
	IT Disaster Recovery (IT Audit)	Determine and evaluate if adequate processes are in place for recovering critical systems and data in the event a service disruption or breach occurs.

Primary ERM Risk Area	FY2025 Academic Division Audit Topic	Scope
Community	ESG Reporting	Evaluate current ESG reporting, metrics, and data analytics distributed across the University.

Primary ERM Risk Area	FY2025 Academic Division Audit Topic	Scope
Safety	Child Development Center	Identify and assess oversight controls for contracted child day care services that ensure regulatory compliance and promote safety and security.
Compliance	Animal Care & Use Program	Evaluate the effectiveness of controls that support regulatory compliance over animal care and use, and promote safety, appropriate care, and security for individuals, animals, and facilities.
	Presidential Travel and Expenses	Annual audit of the President's Travel and Entertainment expenses. Audits were paused during pandemic-impacted years. Audit will cover FY24 expenses.
	Research - Post Award Administration (Pan-University)	Assess effectiveness of post-award controls for selected sponsored awards to ensure compliance with sponsor requirements, applicable regulations, and University policy. (Deferred from FY2023)
Fiscal Sustainability	UVA Wise Student Financial Services	Evaluate design and effectiveness of controls over accuracy and timeliness of student billing and accounts receivable.
	Workday Financials Controls (3 business cycles)	Assess the ongoing effectiveness of key financial business process controls and managerial reporting capabilities to support operational decisions.
	Football Operations Building Construction Audit	Audit initiated in FY23 continues through the construction life cycle
	Hotel and Conference Center Construction Audit	Audit initiated in FY23 continues through the construction life cycle
Operations	School-Level Audits (3)	Assess effectiveness of risk-relevant school level controls and processes at 3 UVA schools.
Technology Risks	Incident Response (IT Audit)	Identify and assess the formal incident response capabilities including incident response policies, procedures, and playbooks, incident response governance, ownership and oversight, incident review metrics and reporting, prevention and detection mechanisms, and training and awareness.
	Identity & Access Management (IT Audit)	Identify the methods, processes, and controls by which access is provisioned and deprovisioned both centrally and for a

Primary ERM Risk Area	FY2025 Academic Division Audit Topic	Scope
		particular application that authorizes access to end users.
	Data Integrity (IT Audit)	Determine and assess the design and operating effectiveness of the controls in place for financially relevant systems (ERP, GL, payroll systems) to ensure the data associated with the financial transactions within the system are processed completely and accurately.

ACTION REQUIRED: Approval by the Audit, Compliance, and Risk Committee and by the Board of Visitors

---

AUDIT DEPARTMENT FY2024-FY2025 AUDIT PLAN

       RESOLVED, the Audit Department FY 2024-FY 2025 Audit Plan is approved as recommended by the Audit, Compliance, and Risk Committee.

UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGEND7A ITEM SUMMARY

BOARD MEETING: June 1, 2023

COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: III. Auditor of Public Accounts FY2022-2023 Audit Entrance
                                      Meeting

ACTION REQUIRED: None

BACKGROUND: The Auditor of Public Accounts of the Commonwealth conducts an annual audit of the University and the Medical Center and reports findings to the Board of Visitors. Mr. Augie Maurelli, Associate Vice President for Financial Operations, will introduce Mr. David Rasnic and Mr. Scott Booker, who will discuss with the committee the FY 2022-2023 external audit.

David Rasnic is the Director of Higher Education Programs for the Virginia Auditor of Public Accounts. His current responsibilities include management of the office's Higher Education Programs Specialty Team and project management oversight for various agencies and institutions of the Commonwealth. He also coordinates required federal audits at the Commonwealth's institutions of higher education and NCAA Agreed Upon Procedures engagements. He is a graduate of Virginia Tech and is a CPA and CISA.

Scott Booker is Audit Director of Process Innovation on the Higher Education Programs team at the Virginia Auditor of Public Accounts. Scott earned his Bachelor of Science degree in Accounting and Finance from Virginia Tech and is a Certified Information Systems Auditor (CISA).

UNIVERSITY OF VIRGINIA
7BOARD OF VISITORS AGEND7A ITEM SUMMARY

BOARD MEETING: June 1, 2023

COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: IV.A. Office of Audit and Compliance Audit Department Report (Written Report)
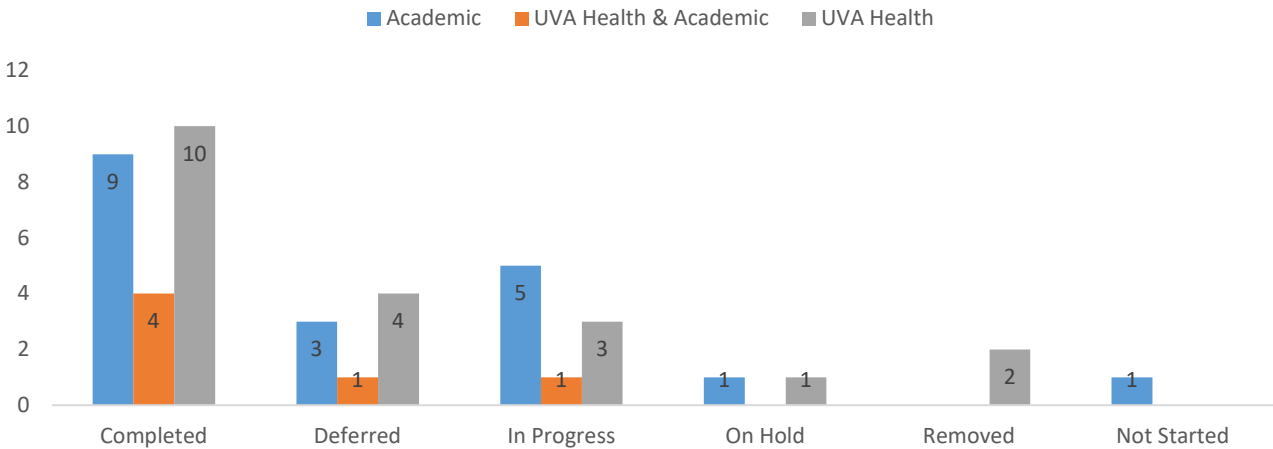
BACKGROUND: To facilitate the Committee's oversight of internal controls, risk management, and compliance, the written report summarizes UVA Audit's work performed during the period February 7, 2023- May 5, 2023:

1) Executive summary of audit activities
2) BOV approved audit plan status reports
3) Summary of audit findings for the period

1. UVA Audit Activities for the Period[1]: Executive Summary

BOV Approved Audit Plan Status: as of May 5, 2023: 23 audits have been completed; 9 are in progress. We deferred 7 audits to accommodate management's schedule/capacity and removed 2 to shift resources to other engagements. Final disposition of the FY2023 plan will be reported in September 2023.

Audit Plan Status by Division

■ Academic   ■ UVA Health & Academic   ■ UVA Health

Status	Academic	UVA Health & Academic	UVA Health
Completed	9	4	10
Deferred	3	1	4
In Progress	5	1	3
On Hold	1		1
Removed			2
Not Started	1		

---

[1] Board material due dates necessitate reporting only the data available to meet those deadlines (i.e., data is not a complete Fiscal Year quarter)

2. Completed Audits FY2023 Year to Date (July 1, 2022-May 5, 2023):

Division	Audit Plan Year	Audit Topic
UVA Health	2022	Ambulatory Medication Charge Capture
	2023	Capture of CC/MCC
	2023	Charge Capture – Interventional Radiology
	2023	Charge Capture – Renal Services
	2023	Graduate Medical Education (GME) Program
	2023	HIPAA Security Risk Assessment Follow-up (IT Audit)
	2023	IT Disaster Recovery (IT Audit)
	2023	Joint Commission (JC) Readiness: Performance Improvement Chapter Updates – Gap Analysis
	2023	Timekeeping and Payroll
	2023	Coding Compliance: ICD Procedure with Separately Billed ECG
Academic & UVA Health	2023	Main Heat Plant Coal Operations (Replaced University Police Department)
	2022	Research Data Security
	2022	Safety and Security
	2023	UVA Health Plan Pharmacy Benefits Rates (Added to Plan)
Academic	2023	CARES Compliance – Higher Education Emergency Relief Fund (HEERF I, II, III) – Part 2 (FY23)
	2023	Football Operations Building: Construction Risk Assessment (Replaced Physics Building Renovation construction audit)
	2023	Housing Division Financial Review (Added to Plan)
	2023	Institutional Data
	2023	International Operations
	2023	Student Financial Aid: UVA Wise
	2023	Student Information System (SIS) IT Controls
	2023	Workday Finance IT General Controls (ITGCs) (Replaced Ransomware Assessment Follow Up Audit)
	2023	Workday Financial Controls Validation: Treasury Pilot

3. BOV Approved Audit Plan Status Report (Changes to Plan and Progress on Audits)

Because the plan is intentionally dynamic to maintain its relevance, a status report on the department's activities is provided at each Committee meeting.

Division	Audit Topic	Scope	Status as of May 5, 2023
UVA Health	Ambulatory Medication Charge Capture	An evaluation of the medication use process, including drug ordering, dispensing, administration, and waste capture; and charging and billing processes at seven clinics. Testing whether charges were accurately captured and billed for drugs administered and wasted using data analytics.	**Completed**
UVA Health	Capture of CC/MCC	Evaluate capture of Complications and Comorbidities (CC) and Major Complications and Comorbidities (MCC), identify root causes of any gaps, and assess financial impact	**Completed**
UVA Health	Joint Commission (JC) Readiness: Performance Improvement Chapter Updates – Gap Analysis	Quality program activities specific to the revised Performance Improvement Chapter in the JC Survey Manual. Identify gaps for action to support JC Survey readiness	**Completed**
UVA Health	Charge Capture – Renal Services	Internal controls over capture of charges for renal services, including interface controls between clinical system and Epic hospital billing	**Completed**
UVA Health	Charge Capture – Interventional Radiology	Same as above-for Interventional Radiology	**Completed**
UVA Health	Coding Compliance: ICD Procedure with Separately Billed ECG	Review medical record documentation for Implantable Cardiac Device (ICD) Procedure with Separately Billed Electrocardiogram (ECG) to validate support for appending modifier 59 to the ECG	**Completed**
UVA Health	Graduate Medical Education (GME) Program	Internal controls over the key processes for GME programs, such as accuracy of GME data reported on Medicare Cost	**Completed**

Division	Audit Topic	Scope	Status as of May 5, 2023
		Reports, validation of rotation schedules, and time and effort reports	
UVA Health	HIPAA Security Risk Assessment Follow-up (IT Audit)	Review results of periodic HIPAA security risk assessment and determine if any identified gaps were sufficiently addressed	**Completed**
UVA Health	IT Disaster Recovery (IT Audit)	The design and operating effectiveness of the controls established for recovering data and systems during and after an event	**Completed**
UVA Health	Timekeeping and Payroll	Controls over timekeeping and payroll accuracy. Potential focus on high-risk areas such as premium pay, traveler payroll	**Completed**
UVA Health	UVACH: Controlled Substances Compliance	Compliance with controlled substances DEA regulations at UVA Prince William Medical Center.	**In Progress**
UVA Health	Case Management	Case management processes focused on inpatient throughput and preventing excess length of stay	**In Progress**
UVA Health	Contract Labor Controls	To assess the design and effectiveness of the internal controls associated with payments for Traveler Nurses and to prevent fraud.	**In Progress**
UVA Health	UVA Orthopedic Center Ivy Road Construction Audit Closeout	Closeout procedures for construction of UVA Ortho Center	**On Hold**
UVA Health	UVACH: IRS 501(r) Compliance	Compliance with IRS 501(r) rules applicable to non-profit hospitals, such as community needs analyses and plans, financial assistance program elements, publication and required signage, etc.	**Deferred**
UVA Health	Contract Management	Controls over contract development, approval, and management	**Deferred**
UVA Health	Physician Transactions (Purchased Services)	Compliance with contract terms and UVA policies, such as contract reviews/ approvals	**Deferred**
UVA Health	Ransomware Assessment Follow Up (IT Audit)	Determine if the recommendations of the 2022 Mandiant Purple Team ransomware report for the Health System division have been implemented	**Deferred**

Division	Audit Topic	Scope	Status as of May 5, 2023
UVA Health	Epic User Role Change Review (IT Audit)	Processes and controls followed when a user changes roles within the UVA Medical Center and determine how that user's access gets updated/ changed or revoked accordingly	**Removed**
UVA Health	SaaS Governance (Salesforce Focus) (IT Audit)	Evaluate controls over the Salesforce deployments across UVA to evaluate governance over Software as a Service (SaaS)	**Removed**
UVA Health & Academic	Main Heat Plant Coal Operations	Assess risks and evaluate operating controls related to the usage and disposal of coal at UVA's Main Heat Plant.	**Completed (Replaced University Police Department)**
UVA Health & Academic	Research Data Security	Security over IT systems and applications in selected labs	**Completed**
UVA Health & Academic	Safety and Security	Follow up on implementation status of consultant's safety recommendations	**Completed**
UVA Health & Academic	UVA Health Plan Pharmacy Benefits Rates	Evaluated the processes surrounding an unexpected increase in pharmacy claims expenses in the UVA Health Plan.	**Completed**
UVA Health & Academic	UVA Sustainability Program and Reporting	Assess controls ensuring sustainability reporting captures relevant information and maintains quality through the process, culminating in the preparation of reliable sustainability reports.	**In Progress**
UVA Health & Academic	Research - Post Award Administration	Assess effectiveness of post-award controls for selected sponsored awards to ensure compliance with sponsor requirements, regulations, and University policy.	**Deferred to FY2025**
Academic	Institutional Data	Ensure data used in external reporting conveys quality information (complete, accurate, timely, available) for ratings and rankings. (COSO Principle 13)	**Completed**
Academic	CARES Compliance – Higher Education Emergency Relief Fund (HEERF I, II, III) – Part 2 (FY23)	Evaluate design and effectiveness of controls and processes related to HEERF funds data collection, use, accounting, and reporting.	**Completed**

| Division	Audit Topic	Scope	Status as of May 5, 2023
Academic	Housing Division Financial Review	Validate the type of expenditures recorded in the University's financial system was appropriate for the Housing Division and determine the Housing Division's compliance with UVA's reserve policies.	**Completed**
Academic	International Operations	Identify the activities of university-owned entities in China, France, and Italy; understand the management controls associated with the operation of those entities and evaluate the effectiveness of the controls.	**Completed**
Academic	Student Financial Aid: UVA Wise	Follow-up on APA findings at UVA Wise.	**Completed**
Academic	Student Information System (SIS) IT Controls	Evaluate design and effectiveness of IT controls over the Student Information System	**Completed**
Academic	Workday Financial Controls Validation: Treasury Pilot	Assess the effectiveness of key financial business process controls	**Completed**
Academic	Workday Finance IT General Controls (ITGCs)	Our review focused on controls fifteen (15) relevant IT general controls responsible for ensuring a secure, controlled, and well managed Workday Finance environment.	**Completed (Replaced Ransomware Assessment Follow Up)**
Academic	Football Operations Building	Using an outside expert in construction project management accounting, perform procedures relevant to phases of specified construction projects.	**Risk Assessment Completed (Replaced Physics Building renovation)**
Academic	Academic Records - Degree Related Data	Evaluate design and effectiveness of controls over the maintenance of degree-related data, including grade submissions and changes, course substitutions and/or degree requirement exceptions, and incoming transcripts.	**In Progress**

Division	Audit Topic	Scope	Status as of May 5, 2023
Academic	School-Level Audit (Pilot)	Develop and pilot an audit program to assess effectiveness of key unit/school level controls and processes.	**In Progress**
Academic	Workday Finance: Accounts Payable	Evaluate relevant Accounts Payable controls in Workday. The controls are responsible for the integrity of financial reporting and regulatory compliance of vendor management, invoice processing, payment processing, and financial reporting.	**In Progress**
Academic	Workday Financial Controls Validation: Accounting and Financial Reporting Cycle	Scope covers the design and operation of internal controls in the accounting cycle.	**In Progress**
Academic	Workday Financial Controls Validation: Expense Reimbursements	Scope covers the design and operation of internal controls in the expense and T&E reimbursement process.	**In Progress**
Academic	SaaS Governance (Salesforce Focus) (IT Audit)	Evaluate controls over the Salesforce deployments across UVA to evaluate governance over Software as a Service (SaaS)	**Not Started**
Academic	Hotel and Conference Center	Using an outside expert in construction project management accounting, perform procedures relevant to phases of specified construction projects	**On Hold**
Academic	University Police Department	Scope to be refined based on results of 2021 CALEA accreditation report.	**Deferred**
Academic	Workday Benefits Administration	Follow-up on KPMG recommendations for the UVA Health Plan.	**Deferred**
Academic	Ransomware Assessment Follow Up (IT Audit)	Determine if the recommendations of the 2022 Mandiant Purple Team ransomware report for the Health System division have been implemented	**Deferred**

3. Special Projects

Division	Topic	Scope	Status as of May 5, 2023
UVA Health	UVA Hotline Investigation	Allegations of financial mismanagement and concerns about duplicate vendor payments: Unsubstantiated	**Completed**
UVA Health & Academic	State Hotline Investigation	Allegations of Time Abuse: Unsubstantiated	**Completed**

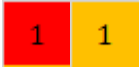## 4. Summary of Audit Findings for the Period February 7-May 5, 2023

The table below summarizes audit control findings by priority rating for audits performed since the last report to the Committee.
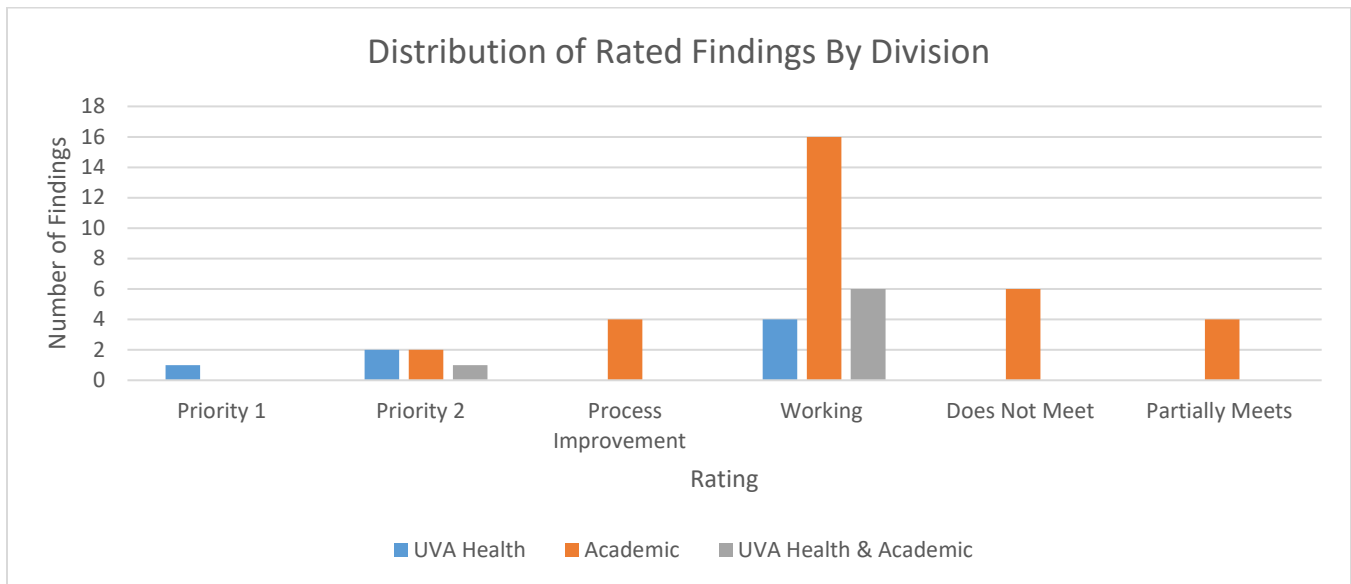
Distribution of Rated Findings By Division

Project Name	Division	Priority Rating for Findings (See Ratings Scale for Definitions)					
		P1	P2	OP	W	DNM	PM
UVA Medical Center Timekeeping and Payroll	UVA Health	1	1		4		
UVA Medical Center Implantable Cardiac Device with Separately Billed Electrocardiogram	UVA Health		1				
Workday Finance IT General Controls	Academic			4	7	6	4
Workday Financial Controls – Treasury	Academic		2		9		

Project Name	Division	Priority Rating for Findings (See Ratings Scale for Definitions)					
		P1	P2	OP	W	DNM	PM
Main Heat Plant Coal Operations	UVA Health & Academic		1		6		
Total		1	5	4	26	6	4

The following summarizes findings from reports issued this period.

Audit	Summary of Findings
Timekeeping and Payroll – UVA Medical Center **1** **1** 1 Priority 1 and 1 Priority 2 rated findings	The lack of a formal timekeeping policy and monitoring controls has resulted in a control breakdown over timekeeping review and approval. For the six pay periods in scope, only about half (52%-58%) of the timecards supporting the payroll expenses received supervisory approval. These gaps in control design and effectiveness combine to increase the Medical Center's vulnerability to payroll abuse or potential fraud. Because the Kronos system is a key subsidiary system to Workday Payroll, the timecard approvals represent a fundamental fiscal control to demonstrate that financial transactions are properly authorized and legitimate organizational expenses.
Implantable Cardiac Device with Separately Billed Electrocardiogram - UVA Medical Center **1** 1 Priority 2 rated finding	The auditors found insufficient documentation of medical necessity in 21 (84%) of the 25 cases reviewed. None of the separately billed ECGs was reimbursed by Medicare, resulting in no inappropriate claim payments. The estimated annual revenue opportunity to improve clinical documentation and appeal the 21 claims to Medicare is $1,202. Given a low volume of this type of charge representing limited revenue opportunity, Revenue Cycle will modify their procedures to remove these types of charges from future claims to improve revenue integrity and reduce the risk of external audit issues.
Workday Finance IT General Controls **6** **4** 6 Does Not Meet and 4 Partially Meets IT control-related findings	The review focused on eighteen (18) relevant IT general controls, which is supported by the ISO/IEC27002:2013 Information Technology – Security Techniques – Code of Practice for Information Security Controls (ISO) framework. Significant control weaknesses were identified in the areas of Managing Access and Managing Change. These weaknesses represent a risk to the objectives of a secure, controlled, and well-managed Workday operating environment.

Audit	Summary of Findings
Workday Financial Controls – Treasury **2** 2 Priority 2 rated findings	The project covered 12 key controls identified by management for which Treasury is responsible. We tested all these controls and identified two areas needing improvement. First, the annual review of segregation of duties performed by Treasury staff was not documented. Second, the settings for some ACH debit limits for some entities were inconsistent with the limits for similar entities. These settings could potentially allow excessive withdrawals from university bank accounts.
Main Heat Plant Coal Operations **1** 1 Priority 2 rated finding	We determined that no security threat assessment had been conducted for university utilities, including the Main Heat Plant facility/operations. Accordingly, we recommended a physical security risk and threat assessment of UVA's Main Heat Plant as this is an essential element of the university's infrastructure.

Rating Scale		
P1	**Priority 1**	A Priority 1 item signifies a control and/or process deficiency of sufficiently high risk that it provides minimal or no assurance that institutional objectives will be achieved. Management must take immediate corrective action to mitigate Priority 1 deficiencies.
DNM	**Does Not Meet**	An IT control that is not in place or is ineffective to achieve the relevant IT controls framework (e.g., ISO-27002-2013) requirement
P2	**Priority 2**	A Priority 2 item signifies a control and/or process deficiency that hinders the effectiveness and efficiency of unit level operations, potentially impeding the attainment of institutional objectives. Management must take timely corrective action to mitigate Priority 2 deficiencies.
PM	**Partially Meets**	An IT control that meets some, but not all, of the relevant IT controls framework (e.g., ISO-27002-2013) requirement
OP	**Process Improvement**	A process improvement item signifies an opportunity to achieve additional control and/or process efficiencies.
W	**Working**	Control tested or process evaluated is working as designed

UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: June 1, 2023

COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: IV.B. Institutional Compliance and Medical Center Compliance
Goals for FY22-23: Year-End Status Report

ACTION REQUIRED: None

DISCUSSION:

Institutional Compliance Goals
Fiscal Year 2022-2023
Year-End Status Report

1. **Helpline Optimization:** Continued to coordinate institution-wide reporting mechanisms and manage compliance-related incidents in a single platform: we expanded marketing of the compliance helpline and web intake form through a series of presentations to Fiscal Administrators, Research Administrators, and the Clinical Staff Executive Committee. We published articles in two different employee newsletters to provide internal communications to staff. In SafeGrounds, we implemented new functionality to provide a way to follow-up with anonymous reporters on cases and an enhanced institutional reporting dashboard to create more effective reporting and monitoring of compliance concerns.

2. **Compliance Risk Assessment:** Completed preliminary work to update the integrated assurance risk assessment, based on the items listed on the compliance matrix, to identify which items represent the highest institutional risks. Items were scored, in consultation with compliance subject matter experts, based on legal risk, operational risk, reputational risk, mitigation efforts, regulatory scrutiny, and cross functionality.

3. **Conflict of Interest**: We convened key stakeholders across Grounds to identify current gaps in the University's current portfolio of COI programs and explored possible strategies for developing a future comprehensive COI program. We have implemented enhancements and provided guidance to new staff managing the Statement of Economic Interests process, reviewed the research COI process in more depth, and will participate in the evaluation of the potential uses of a new Huron module for COI.

Medical Center Compliance Goals
Fiscal Year 2022-2023
Year-End Status Report

1. **Compliance Risk Assessment:** Performed a biannual comprehensive Compliance Risk Assessment to evaluate potential risk areas with operational, financial, reputational and/or stakeholder impact using the framework of the Office of Inspector General (OIG) elements of an effective compliance program. We used a five-stage process of evaluating the potential risks to include: risk identification; risk ranking; risk prioritization; work plans; and results and action plans. Two departments were selected for evaluation of potential risk areas. Risks in each area were analyzed, and the strengths and areas for improvement identified; follow-up corrective action plans are in progress.

2. **End of the Public Health Emergency:** Continue to evaluate and mitigate compliance risks stemming from the end of the Public Health Emergency (PHE), which was declared by the Secretary of the Department of Health and Human Services (HHS) in January 2020 and expired on May 11, 2023. During the PHE, flexibilities and waivers issued gave the federal government flexibilities to temporarily waive or modify certain requirements in a range of areas, including the Medicare, and Medicaid programs in responding to COVID-19. A particular area of focus was on Medicare telehealth services. We continue to assess the status of each waiver, and are collaborating with Telemedicine, University Counsel, and clinical leaders to provide guidance and communication plans to assure compliance after May 11.

3. **Compliance and Privacy Office Staffing:** The role of Chief Compliance and Privacy Officer (Officer) is currently vacant as Regina Verde retired from this position on July 8, 2022. The role is currently being filled in an interim role by another staff member. A national search is ongoing. The Office continues to prioritize projects due to reduced staffing, as the Officer role continues to be filled by another staff member.