UNIVERSITY OF VIRGINIA
BOARD OF VISITORS

Meeting of the Audit, Compliance, and Risk Committee

September 14, 2023

AUDIT, COMPLIANCE, AND RISK COMMITTEE

Thursday, September 14, 2023
1:45 p.m. – 2:45 p.m.
Board Room, The Rotunda

Committee Members:

Thomas A. DePasquale, Chair
Rachel W. Sheridan, Vice Chair
Mark T. Bowles
Carlos M. Brown
The Honorable Paul C. Harris
Babur B. Lateef, M.D.
Stephen P. Long, M.D.
The Honorable L.F. Payne
Amanda L. Pillion
Douglas D. Wetmore
Robert D. Hardie, Ex-officio
Adelaide Wilcox King, Faculty Consulting Member

AGENDA

		PAGE
I.	**REMARKS BY THE COMMITTEE CHAIR** (Mr. DePasquale)	1
II.	**COMMITTEE DISCUSSION AND ACTION ITEMS**	
	A. UVA and UVA Health University Hospital Compliance and Privacy Programs, and Records and Information Management Program**:** Annual Program Reports (Mr. Gary Nimax, Ms. Annette Norton, Ms. Caroline Walters)	2
	• Action Item: Approval of Updated Compliance Charter (Mr. Nimax)	5
	B. FY2022-2023 Annual Financial Report Audit Progress (Mr. Augie Maurelli)	6
III.	**WRITTEN REPORTS**	
	A. UVA Audit Department Report: Audit Activities Fiscal Year 2024 Year to Date	7
	B. UVA Audit Department Report: Review of UVA Audit Activities for Fiscal Year 2023	14
	C. Institutional Compliance and Medical Center Compliance Goals for FY23-24	24
IV.	**ATTACHMENT: UPDATED COMPLIANCE CHARTER WITH EDITS**	
V.	**CLOSED SESSION**	
	• Discussion of (a) plans to protect public safety as it relates to specific cybersecurity threats or vulnerabilities and briefings by University staff members concerning actions taken to respond to such matters or a related threat to public safety; (b) the design, function, operation, or access control features of University IT security systems; (c) vulnerability assessments, information not lawfully available to the public regarding specific cybersecurity threats or vulnerabilities, and IT security systems, plans, and measures, where discussion in an open	

meeting would jeopardize personal and institutional safety; and (d) reports and plans related to University IT security. The relevant exemption authorizing the closed session discussion is Section 2.2-3711 A (19) of the Code of Virginia.

UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: September 14, 2023

COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: I. Remarks by the Committee Chair

ACTION REQUIRED: None

BACKGROUND: Mr. Thomas A. 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: September 14, 2023

COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: II.A. UVA and UVA Health University Hospital Compliance and Privacy Programs, and Records and Information Management Program: Annual Program Reports

ACTION REQUIRED: None

BACKGROUND: One of the institutional compliance goals shared with the Board of Visitors was to optimize the university's hotline management processes. Specifically, the compliance team reviewed the current reporting mechanisms in place institution-wide, considered alternatives to simplify and coordinate processes, and determined ways in which to compile and assess data to manage risks. They also identified the need to develop standard reporting and better monitor trends related to compliance concerns.

Leveraging the investment the board made in SafeGrounds, initially conceived to ensure the University's Title IX processes and workflow would ensure compliance with relevant state and federal laws and regulations, the university has moved other compliance areas into this incident management system.

The compliance function has evolved from a highly decentralized approach to one in which management and the board will have the appropriate visibility into compliance risk areas. This is a crucial part of demonstrating that the university has an effective compliance function.

Mr. Gary Nimax has served as the Assistant Vice President for Compliance at the University of Virginia since 2013. He started his career at the university in 1989 as a buyer in the medical center, before becoming the Assistant Director of Procurement Services for the academic division. He was later promoted to positions as a team lead on the university's Oracle software implementation, coordinator of process simplification, and the Assistant Vice President responsible for the administration of university-related foundations. Mr. Nimax also serves as president of the board of the Osher Lifelong Learning Institute (OLLI), a non-profit organization that is one of the university's related foundations. He earned his undergraduate degree from UVA and his Master of Business Administration from James Madison University. He obtained his professional certification as a Certified Compliance and Ethics Professional (CCEP) through the Society of Corporate Compliance and Ethics.

Effective September 18, Krista Barnes will be UVA Health's Chief Corporate Compliance and Privacy Officer, where she will oversee the strategic direction of UVA

Health's compliance and privacy programs. Ms. Barnes will lead UVA Health's work to protect patient privacy and comply with all federal and state laws.

An experienced leader, Ms. Barnes comes to UVA Health from the University of Texas MD Anderson Cancer Center in Houston, where she served as associate vice president and deputy chief compliance officer. In her role, she oversaw institutional compliance attorneys and teams responsible for compliance in billing and reimbursement, ethics research, data governance, conflicts of interest, and ethics. She also served as senior legal officer and director, overseeing MD Anderson's Privacy and Information Security Compliance and Institutional Compliance programs. Ms. Barnes has more than 20 years of experience in healthcare regulatory compliance, reimbursement litigation, HIPAA compliance, and Medicare and Medicaid reimbursement. She earned her bachelor's degree in psychology from Rice University, and her doctor of law degree from Duke University School of Law.

Ms. Annette Norton has over 15 years of experience in healthcare compliance and privacy and is currently serving as the Interim Chief Compliance and Privacy Officer for UVA Health. The majority of her 15 years of experience has been at UVA Health in the Compliance and Privacy Office (Office), starting with the Office in 2005 as a project coordinator. Ms. Norton briefly left UVA in 2017 for a role as Privacy Officer and Research Compliance Officer at Piedmont Columbus Regional in Columbus, Georgia. She returned to UVA Health in 2020 as a Senior Analyst. She holds a Juris Master focused in Legal Studies/Healthcare from Florida State University College of Law, a Bachelor of Arts in Healthcare Administration from Mary Baldwin College, and is a Certified Professional Coder. She is also certified through the Health Care Compliance Association in compliance, privacy, and research.

Ms. Caroline Walters has served as University Records Officer at the University of Virginia since 2008. Prior to coming to UVA, she was the Records Manager at the University of North Carolina at Chapel Hill and a Records Analyst with the State of North Carolina. She achieved the Certified Records Manager designation in 2011 and is currently President of the Institute of Certified Records Managers (ICRM). She previously served as Regent for Exam Development and on the Exam Development Committee with the ICRM. She is a recipient of the Virginia Association of Government Archives and Records Administrators Outstanding Member (2016), and the Records and Information Management Office at UVA received the National Association of Government Archives and Records Administrators Program Excellence award in July 2023. Ms. Walters has a Bachelor of Arts in History (Phi Beta Kappa) and a Master of Arts in Public History from North Carolina State University, and a Master of Library Science from North Carolina Central University.

DISCUSSION: Mr. Gary Nimax, Assistant Vice President for Compliance, will review information about the institutional Compliance Helpline and other reporting mechanisms for which incidents are managed in SafeGrounds.

Ms. Annette Norton, Interim Chief Corporate Compliance and Privacy Officer for the Health System, will provide additional information about the compliance program managed by her office.

Ms. Caroline Walters, University Records Officer, will provide an overview of Records and Information Management and share information of which board members should be aware.

UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: September 14, 2023

COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: II.A.1. Approval of Updated Compliance Charter

BACKGROUND: The original Institutional Compliance Charter was approved by the board in February 2016 with a revised version approved by the board at its June 2018 meeting. Following a periodic review of the compliance charter, additional edits are now proposed.

The compliance charter summarizes the mission and purpose of the institutional compliance function. It also specifies the role of the Audit, Compliance, and Risk Committee, the professional standards and responsibilities related to the compliance program, and the interaction between the compliance, audit, and Enterprise Risk Management (ERM) functions. Additional proposed edits will summarize the purpose of the Compliance Network, describe the functional areas that report to the Assistant Vice President for Compliance, and include additional information about the need to report suspected wrongdoing and cooperate with investigations.

A red-lined version of the current charter is provided as an attachment to show the proposed changes.

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

INSTITUTIONAL COMPLIANCE CHARTER

RESOLVED, the updated Institutional Compliance Charter, dated September 14, 2023, is approved as recommended by the Audit, Compliance, and Risk Committee.

UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: September 14, 2023

COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: II.B. FY2022-2023 Annual Financial Report Audit Progress

ACTION REQUIRED: None

BACKGROUND: Mr. Augie Maurelli, Vice President and Chief Financial Officer, will provide a status report on the Fiscal Year 2022-2023 annual audit performed by the Auditor of Public Accounts.

UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: September 14, 2023

COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: III.A. UVA Audit Department Activities Fiscal Year 2024 Year to Date

BACKGROUND: To facilitate the Committee's oversight of internal controls, risk management, and compliance, the written report provides a report on current audit activities since the start of the new fiscal year and audit plan. In addition to audit status, a report on management's progress in completing action plans to remediate control deficiencies reported in prior audits is included.

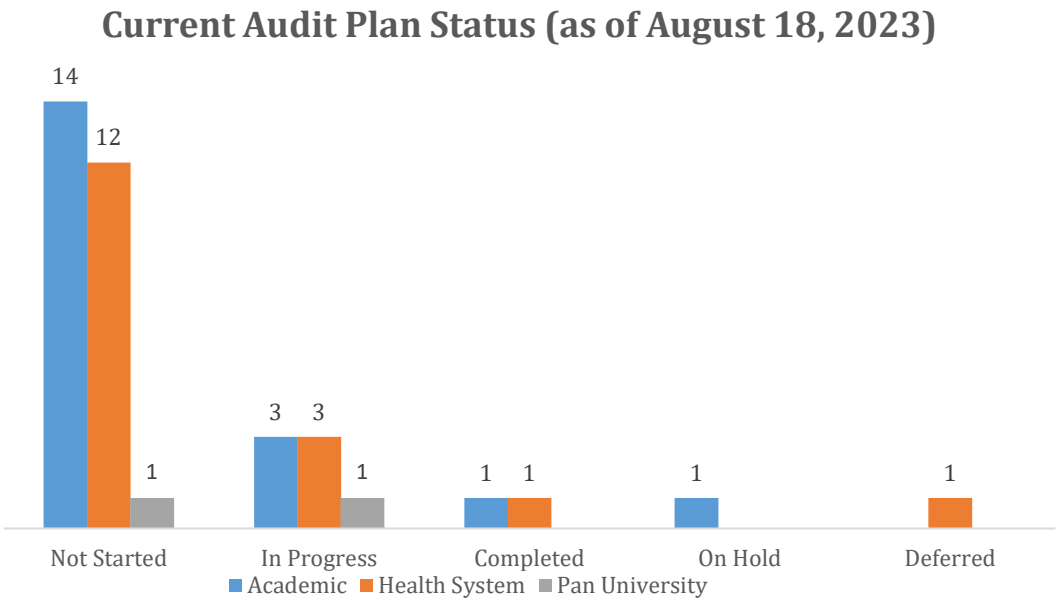
<table>
<tr><th colspan="2">First Quarter FY2024 Snapshot of Audit Activities</th></tr>
<tr><td colspan="2">• Two newly hired senior auditors joined the UVA Health audit team

2 Audits Completed:
• Contract Labor Controls (UVA Health)
• Salesforce Service and Marketing Cloud (Academic Division: UVA HR and Finance)

Support for University Initiatives:
• Ongoing participation in Policy Review Committee (Academic Division)</td></tr>
<tr><th>Key Issues Raised by UVA Audit</th><th>Regulatory Developments for Awareness</th></tr>
<tr><td>• Significant control breakdowns in UVA Health Accounts Payable and Procurement functions were observed in the audit of Contract Labor Controls. Additional procedures are being conducted as a follow-up. Changes to the approved FY24 UVA Health audit plan to pivot to areas of heightened risk are detailed below.

• Average length of time to remediate internal control gaps identified in audits is 8 months. 19 extensions to action plan completion dates established by management have been granted (From 11/10/2021 to 8/18/2023).</td><td>Federal initiatives to strengthen security over research data will require significant institutional resources to ensure compliance.
• NIH Data Management and Sharing Policy applies to all NIH research funded or conducted, in whole or in part, by NIH that results in the generation of scientific data. UVA guidance for researchers: Overview - NIH Data Management and Sharing Plan Guidance - HSL at University of Virginia-Claude Moore Health Sciences Library
• National Security Presidential Memorandum 33 (NSPM33): requires research institutions receiving Federal science and engineering support over $50 million dollars/year to certify the institution has established and operates a research security program.</td></tr>
</table>

Audit Activities Since June 2023 Audit Report



Summary of Findings Fiscal Year 2024 to Date	
Contract Labor Controls (UVA Health) 2 3 2 2 Priority 1 Findings; 3 Priority 2 Findings; 2 Working Control Findings	Audit testing revealed significant gaps in controls over labor expenses which taken together increase the risk of undiscovered errors or fraud. Issues were noted in the following areas: • Management override of accounts payable controls • Accounts payable segregation of duties violation, including violation of Medical Center policy on supervision of relatives • Lack of manager approval of contract worker time records • Agency contract maintenance
Salesforce Service Cloud Controls (HR, Academic Division Finance & Student Financial Services Unified Instance) 10	The objective of this audit was to assess the design and operating effectiveness of controls customers must implement as outlined in the 2022 Salesforce SOC 2 Type II report. Of the eleven (11) controls assessed, we considered ten (10) to be effective and one (1) to be not applicable.

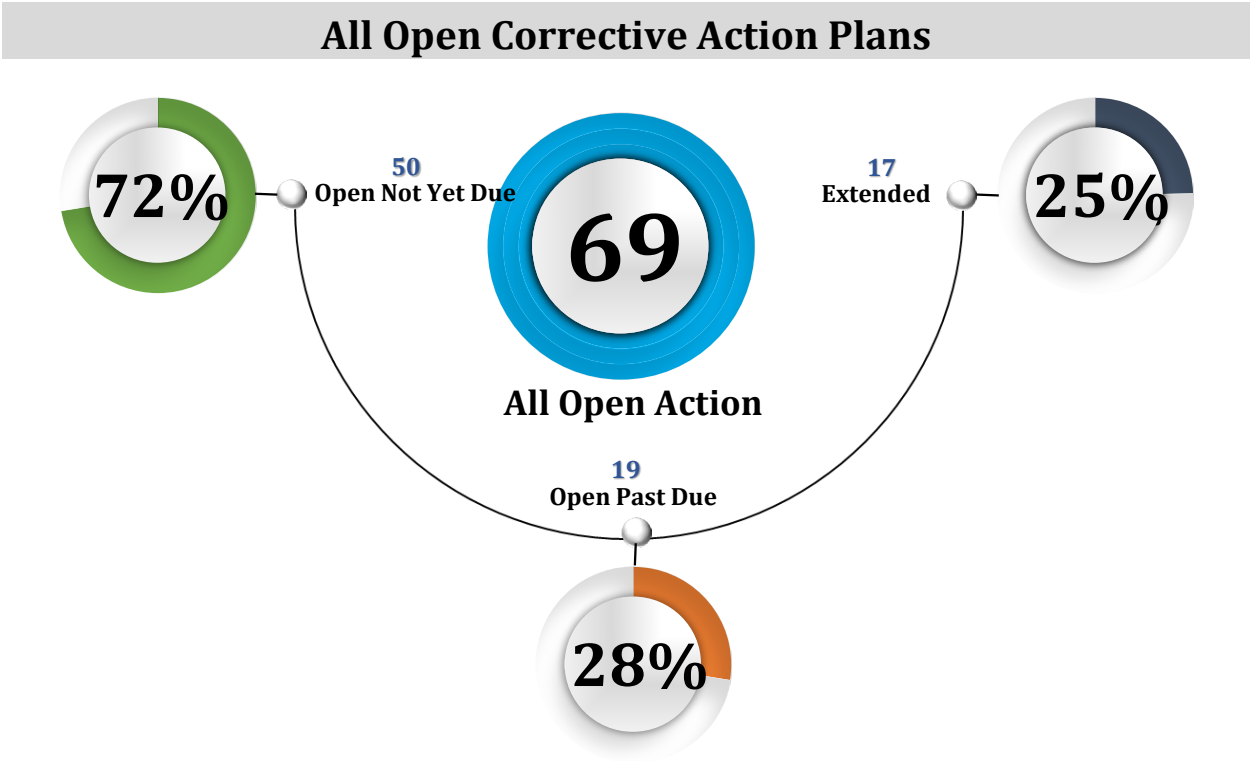
Audits in Progress (as of August 18, 2023)	
Project Title	Division
CARES Compliance - Higher Education Emergency Relief Fund (HEERF I, II, III) - Part 3 (FY24)	Academic
ESG - Sustainability Reporting	Academic and UVA Health
Physician Transactions (Purchased Services)	Health System
Presidential Travel and Expenses	Academic
School-Level Audits: Pilot Audit of McIntire School	Academic
Third Party Risk Management (IT Audit)	Health System
Trauma Activation Claims – Billing Compliance	Health System

Based on a reassessment of risks following the UVA Health Contract Labor Controls audit, we highlight below the changes to the plan approved by the Committee in the June 2023 meeting.

UVA Health Audit Plan Changes	
June 2023 Audit Plan Topic	Change
Capital Asset Inventory Management – APA Follow-up	Replaced by Provider Based Billing Compliance
Procure-to-Pay Process Controls	Added
Provider Based Billing Compliance	Advanced from FY2025 plan to FY2024 plan

Status of Management's Action Plans to Remediate Control Deficiencies

The Institute of Internal Auditor's *Standard 2500: Monitoring Progress* requires the chief audit executive to establish and maintain a system to monitor the disposition of results communicated to management. The table below shows the number of action plans to correct control deficiencies that have not been implemented by the due dates *established by management*. (Reflects status as of August 18, 2023 for action plans due by 6/30/2023.)



Notes: Nine (9) action plan due dates were extended before they were overdue. Eight (8) action plans were extended once the due date for completion had passed. Total extended plans: 17.

Average duration of open action plans: 248 days (calculated from close of audit to August 18, 2023).

Audit	Action Item	Priority Rating	Action Plan Owner
2019 Fixed Fee Monitoring and Management	Two action items from this audit remain past due. These issues address the implementation of a residual balances policy and the associated monitoring metrics. As of July 2023, a policy was under development to bring before the policy committee. **Originally due: 6/30/2020 Extended to 1/14/2022**	2 Priority 2 (P2) control gaps	Stewart Craig, Executive Director, Office of Sponsored Programs

Audit	Action Item	Priority Rating	Action Plan Owner
2020 Accounts Payable	Two action items from this audit remain outstanding. These issues concern monitoring for potential employee/vendor conflicts of interest, and post transaction monitoring in Workday. Management anticipates resolution of both items by November 2023. **Originally due: 6/30/2022** **First extension Granted additional 16 months to 10/31/2022** **Second extension granted. New due date: 11/2023**	2 Priority 2 (P2) control gaps	Mark Cartwright, Senior Director of Procurement & Supplier Diversity Services (original Action Plan Owners were predecessors in equivalent position)
2021 Research Conflict of Interest *	Three action plans from this audit remain outstanding. The issues include developing roles and responsibilities, implementing monitoring procedures, and updating policies (PROV-009) and SOPs of a comprehensive COI program. Management anticipates resolution of these action items by February 2024 as part of the implementation of the Huron Compliance Suite. The roll out of the COI module has been delayed while the Office of Sponsored Programs has been working with Huron on integration issues related to the Huron Grants and Agreements module. **Originally due: 12/31/2021** **First extension: Granted additional 18 months to 6/30/2023** **Second extension granted. New due date: 2/2024**	3 Priority 2 (P2) control gaps	Margaret Harden, Associate Provost for Academic Administration; Rob Merhige, Assistant VP for Commercializati on Compliance; Kelly Hochstetler, Interim Assistant VP for Operations, Policy, and Compliance
2021 – DISM Computer Science – SEAS	Two action items from this audit remain past due. These issues concern network monitoring (e.g., non-compliance of policy required vulnerability scans and installation of anti-malware on network-connected devices) and moving administrative workstations to the Academic Protected Network. Network Monitoring	2 Partially Meets Policy (ISO 27002) control gaps	Paul Henderson, Computer Systems Senior Engineer – SEAS

Audit	Action Item	Priority Rating	Action Plan Owner
	Originally due: 6/30/2021 **First extended 5 months to 11/10/2021** **Second extension: granted an additional 7 months to 5/31/2022** Admin Workstations **Originally due: 5/31/2021** **Extended to 5/31/2022**		
2021 University Advancement Service's Third-Party Payment Processing	One action item from this audit remains past due. This issue concerns the receipt of a contractually required SOC 2 Type II operating control effectiveness review from the payment process vendor, CDS Global. Management anticipates receipt of a current SOC 2 Type II report in late August 2023. **Originally due: 10/31/2022**	1 Priority 2 (P2) control gap	David Pinker, IT Director Advancement Services
2022 Safety & Security Program Assessment - Follow Up	Three action items from this audit are past due. 1) The consolidation of the Medical Center workplace violence coordinator position into the Department of Safety and Security Division of Threat Assessment . Current plan: An assessment of university and Medical Center committees that support threat assessments, workplace violence, etc. will be completed, resulting in a gap analysis and definition of role and scope of the Workplace Violence coordinator position and an MOU between . 2) the consolidation of the Fire Safety Program under the AVP for Safety and Security, and 3) the housing of all safety and security functions in a dedicated command center. Current plan for #2 and #3: Organizational discussions have been initiated concerning the consolidation of the Fire Safety Program and space planning for the dedicated command center.	3 Priority 2 (P2) control gaps	Timothy Longo, Associate Vice President for Safety and Security / Chief of Police

Audit	Action Item	Priority Rating	Action Plan Owner
	Originally due: 6/30/2023		
2023 Workday Financial Controls: Expense Reimbursements	One action plan from this audit is past due concerning T&E card transactions that remained unprocessed after 60 days in Workday. Since April 2023, progress to date includes a >50% decrease in T&E card transactions that remain unprocessed after 60 days. Management anticipates full resolution by March 2024 to allow for testing of a new data monitoring process using Card Integrity. **Originally due: 6/30/2023 Extended to 3/24/2024**	1 Priority 2 (P2) control gap	Raegan Harouff Gaye, Travel and Business Operations Manager, PSDS
ICD/ECG Coding Compliance	One action plan from this audit is past due. Revenue Cycle was to change the coding practices for certain types of claims for implantable cardiac devices. **Originally due: 6/30/2023**	1 Priority 2 (P2) Issue	Sarah Hetmanski, Director of Revenue Integrity
HIPAA Security Risk Assessment Follow-up	Two action plans were granted extensions. Both action plans related to evaluating the feasibility of implementing Data Loss Prevention (DLP) tools on workstations and endpoints. **Originally due: 6/30/2023 Extended to: 8/31/2023**	2 Does Not Meet (DNM) Issues	Phil Napier, Information Security Officer, UVA Health
IT Disaster Recovery Audit	**Two action plans were granted extensions**. One related to establishing a link between Recovery Point Objectives (RPO) and Disaster Recovery (DR) tiers. The other was to update the Security Awareness program to include Disaster Recovery. **Originally due: 6/30/2023 Extended to: 11/30/2023**	2 Partially Meets (PM) Issues	Phil Napier, Information Security Officer, UVA Health
Graduate Medical Education Program	One action plan is past due, to update the IT security risk assessment for the New Innovations system and re-evaluate the feasibility of establishing single sign-on and/or multi-factor authentication. **This action plan is in progress, with an extension granted. Originally due: 4/30/2023 Extended to: 10/31/2023**	1 Priority 2 (P2) Issue	Diane Farineau, Director, Graduate Medical Education Office

*Audit performed under engagement of University Counsel

UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

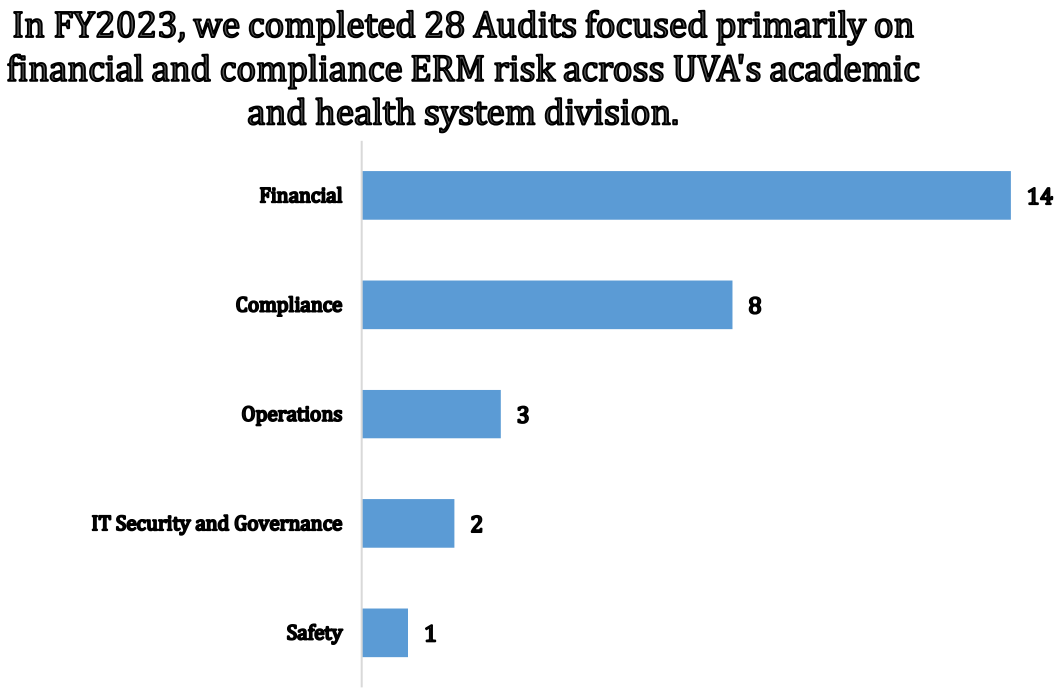
BOARD MEETING: September 14, 2023

COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: III.B. UVA Audit Department Report: Review of UVA Audit Activities for Fiscal Year 2023

BACKGROUND: The report summarizes UVA Audit activities for the completed fiscal year 2023.

Look Back on Fiscal Year 2023



Final Disposition of FY2023 Audit Plan[1]

	Division	Audit Topic	Audit Scope	Status as of August 18, 2023
1	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**
2	UVA Health	Capture of CC/MCC	Evaluate capture of CC/MCC, identify root causes of any gaps, and assess financial impact	**Completed**
3	UVA Health	Case Management	Case management processes focused on inpatient throughput and preventing excess length of stay	**Completed**
4	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**
5	UVA Health	Charge Capture – Interventional Radiology	Same as above for Interventional Radiology	**Completed**
6	UVA Health	Coding Compliance: ICD Procedure with Separately Billed ECG	Review medical record documentation for cardiac pacemaker or ICD procedure to validate support for appending modifier 59 to the ECG	**Completed**

[1] The FY2022-2023 audit plan was approved by the Board of Visitors, as recommended by the Audit, Compliance, and Risk Committee, at its June 2022 meeting. The table shows the disposition of the approved audit topics for FY2023.

	Division	Audit Topic	Audit Scope	Status as of August 18, 2023
7	UVA Health	Contract Labor Controls (Addition to Plan)	Design and effectiveness of the internal controls associated with contract labor expenses, including timekeeping and accounts payable controls.	**Completed**
8	UVA Health	Contract Management	Controls over contract development, approval, and management	**Deferred to FY2024**
9	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**
10	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 Reports, validation of rotation schedules, and time and effort reports	**Completed**
11	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**
12	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**
13	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**

	Division	Audit Topic	Audit Scope	Status as of August 18, 2023
14	UVA Health	Physician Transactions (Purchased Services)	Compliance with contract terms and UVA policies, such as contract reviews/ approvals	**In Progress-Deferred to FY2024**
15	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 to FY2024**
16	UVA Health	SaaS Governance (Salesforce Focus) (IT Audit)	Controls around the onboarding, setup, and establishment of key configurations for Cloud and SaaS based vendors	**Removed**
17	UVA Health	Timekeeping/Payroll	Controls over timekeeping and payroll accuracy. Potential focus on high-risk areas such as premium pay, traveler payroll	**Completed**
18	UVA Health	UVA Orthopedic Center Ivy Road	Closeout procedures for construction of UVA Ortho Center	**Completed**
19	UVA Health	UVACH: Controlled Substances Compliance	Compliance with controlled substances DEA regulations at UVA Prince William Medical Center	**Completed**
20	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 to FY2024**
1	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	**Completed**

	Division	Audit Topic	Audit Scope	Status as of August 18, 2023
			exceptions, and incoming transcripts.	
2	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**
3	Academic	Construction Projects: • Hotel and Conference Center • Football Operations Building	Using an outside expert in construction project management accounting, perform procedures relevant to phases of specified construction projects.	**Hotel and Conference Center Audit On Hold** **FOB Phase 1 Risk Assessment Completed**
4	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 (Added to the Plan)**
5	Academic	Institutional Data (FY22 Audit Plan)	Ensure data used in external reporting conveys quality information (complete, accurate, timely, available) for ratings and rankings. (COSO Principle 13)	**Completed**
6	Academic	International Operations Phase 2 (FY22 Audit Plan)	Phase 1: Develop inventory of international activities to determine eventual audit scope. Phase 2: Assess higher priority activities identified in Phase 1.	**Completed**

	Division	Audit Topic	Audit Scope	Status as of August 18, 2023
7	Academic & UVA Health	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**
8	Academic	Salesforce Service Cloud Controls (IT Audit)	Assess the design and operating effectiveness of controls Salesforce customers must implement as outlined in the 2022 Salesforce SOC 2 Type II report.	**Completed**
9	Academic	School-Level Audit (Pilot)	Develop and pilot an audit program to assess effectiveness of key unit/school level controls and processes	**In Progress**
10	Academic	Student Financial Aid: UVA Wise	Follow-up on APA findings at UVA Wise	**Completed**
11	Academic	Student Information System (SIS) IT Controls	Evaluate design and effectiveness of IT controls over the Student Information System	**Completed**
12	Academic	Workday Benefits Administration	Follow-up on KPMG recommendations for the UVA Health Plan	**Deferred to FY2024**
13	Academic	Workday Financials Control Validation: Accounting and Financial Reporting Cycle	Scope covers the design and operation of internal controls in the accounting cycle.	**Completed**
14	Academic	Workday Financials Control Validation: 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	**Completed**

	Division	Audit Topic	Audit Scope	Status as of August 18, 2023
			processing, and financial reporting.	
15	Academic	Workday Financials Control Validation: Expense Reimbursements	Scope covers the design and operation of internal controls in the expense and T&E reimbursement process.	**Completed**
16	Academic	Workday Financials Control Validation: 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)**
17	Academic	Workday Financials Control Validation: Treasury Pilot	Assess the effectiveness of key financial business process controls.	**Completed**
1	Academic & UVA Health	ESG - Sustainability 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**
2	Academic & UVA Health	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)**
3	Academic & UVA Health	UVA Health Plan Pharmacy Benefit Rates	A special project to evaluate the processes around an unexpected increase in pharmacy claims expenses in the UVA Health Plan.	**Completed (Added to the Plan)**

2. Summary of Audit Findings by Priority Rating in Reports Issued in FY 2023 (July 1, 2022, through June 30, 2023)

The table below shows the distribution of rated findings across Academic and UVA Health divisions (note: certain audits span both divisions and are labeled "Academic & UVA Health.") See page 22 for the Rating Scale.

Fiscal Year 2023 Rated Findings at a Glance

The table below summarizes the number of findings by priority rating for audits performed during the prior fiscal year (FY2022-2023).

Project Name	Division	Priority Rating for Findings (See Ratings Scale for Definitions)					
		P1	P2	OP	W	DNM	PM
Joint Commission Performance Improvement Chapter	UVA Health		3	3	4		
Pharmacy Benefit Rates (5 unrated findings)	Academic & UVA Health						
HIPAA Security Risk Assessment Follow-Up	UVA Health				14	4	1
Vascular and Interventional Radiology Charge Capture	UVA Health		2		1		
UVA Health IT Disaster Recovery	UVA Health				12	1	2
Graduate Medical Education	UVA Health		2	1	2		
Capture of Complication or Comorbidity	UVA Health						
UVA Medical Center Timekeeping and Payroll	UVA Health	1	1		4		
UVA Medical Center Implantable Cardiac Device with Separately Billed Electrocardiogram	UVA Health		1				
Case Management	UVA Health	1	3		4		
UVA Prince William Medical Center Controlled Substances	UVA Health	2	9		13		
Contract Labor Controls	UVA Health	2	3		2		
Student Information System	Academic			2	21		
Housing Division Financial Review (no findings)	Academic						

Project Name	Division	Priority Rating for Findings (See Ratings Scale for Definitions)					
		P1	P2	OP	W	DNM	PM
College at Wise Financial Aid Follow-Up (2 unrated findings)	Academic						
International Operations Phase 2	Academic		2		3		
Institutional Data	Academic			1	5		
Football Operations Building - Construction	Academic						
Workday Finance IT General Controls	Academic			4	7	6	4
Workday Financial Controls – Treasury	Academic		2		9		
Workday Financial Controls – Accounts Payable	Academic	5	1		14		
Workday Financial Controls – Expense Reimbursement	Academic		3	2	4		
Workday Financial Controls – Accounting and Financial Reporting	Academic	1	5	1	3		
Academic Records Degree-Related Data	Academic		2	1	4		
Salesforce Service Cloud Controls (HR, Academic Division Finance & Student Financial Services Unified Instance)	Academic				10		
Safety and Security Program Assessment	Academic & UVA Health		4		10		
FY22 Covid-Related Relief Funds	Academic & UVA Health		1		4		
Main Heat Plant Coal Operations	Academic & UVA Health		1		6		
Ivy Musculoskeletal Center Construction Closeout	UVA Health						
Total (7 unrated findings)		12	45	15	156	11	7

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: September 14, 2023

COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: III.C. Institutional Compliance and Medical Center Compliance Goals for FY23-24 (Written Report)

ACTION REQUIRED: None

DISCUSSION:

Institutional Compliance Goals
Fiscal Year 2023-2024

1. **SafeGrounds Reporting**: Enhance institutional reporting dashboard for data in SafeGrounds to create more effective reporting and monitoring of compliance concerns. Information Technology Services (ITS) plans to build reporting capabilities directly into the SafeGrounds system, as opposed to using Qlik for reporting purposes, which should provide new opportunities for institution-wide reporting.

2. **Director of Privacy Programs** – conduct a national search to hire a Director of Privacy Programs to focus on information privacy for the academic division and manage the university's response to ever increasing compliance requirements related to privacy. Onboard the successful candidate to develop more robust and aligned privacy protocols throughout the university.

3. **Conflict of Interest**: convene key stakeholders across Grounds to identify current gaps in the University's current portfolio of COI programs; explore possible strategies and systems for developing a future comprehensive COI program.

Medical Center Compliance Goals
Fiscal Year 2023-2024

1. **Compliance Program Assessment:** We will evaluate the UVA Health Compliance Program through an assessment that will help answer whether the program adequately covers the seven elements of an effective healthcare compliance program and identify the strengths and weaknesses of the current program.

2. **Expand Coding Audit Function:** Expand the coding audit function with the addition of a dedicated Auditor to examine compliance with regulatory requirements for documentation of medical necessity, accurate coding, billing and reimbursement from Medicare for specific services, and to assess compliance in high-risk areas as identified

by the Office of Inspector General/Health & Human Services Work Plan.

3. **Compliance and Privacy Office Staffing:** Onboard Ms. Krista Barnes, UVA Health Chief Compliance and Privacy Officer. Review staffing model to ensure adequate staffing to support the UVA Health Compliance Program.

ATTACHMENT

See attached file for Compliance Charter with edits shown.

DRAFT 8/11/23

University of Virginia Compliance Charter

Purpose:

The University of Virginia's compliance function supports the University's fundamental commitment to the highest standards of ethics, integrity, and lawful conduct by promoting adherence to all applicable federal, state, and local laws, regulations, as well as standards and internal policies and protocols.

Institutional compliance promotes greater coordination of and consistency among individual University compliance programs, covering a wide variety of requirements related to academics, athletics, human resources, research, health care, information technology, and numerous administrative functions. The University established a compliance program to prevent, detect, and respond appropriately to potential violations of law and to foster a corporate culture that promotes integrity and ethical behaviors in all matters relating to compliance.

Authority:

The Assistant Vice President for Compliance, with strict accountability for confidentiality and safeguarding of records and information, is authorized to have full, free, and unrestricted access to any and all of the University's records, physical properties, and personnel pertinent to carrying out compliance investigations, and to review and monitor compliance issues. All employees are requested to assist the compliance function in fulfilling its roles and responsibilities.

Organization:

The Assistant Vice President for Compliance oversees institutional compliance activities and programs to confirm they are reasonably designed, implemented, communicated, and enforced. To facilitate effective oversight, the Assistant Vice President for Compliance coordinates and chairs the Compliance Network, a University-wide network of functional compliance officers. The Compliance Network is responsible for developing appropriate compliance policies and procedures, providing education on compliance risks, maintaining related documentation, recommending corrective actions, submitting required reports, keeping the appropriate University constituencies informed of compliance issues,

and updating senior management and the University community on recent developments.

The Assistant Vice President for Compliance works closely with the compliance managers at UVA Health and the University's College at Wise to determine which compliance requirements will be handled jointly and which will be managed separately.

Functional areas reporting to the Assistant Vice President include:

- Records and Information Management – leads the University's effort to manage, retain, and dispose of university records in compliance with all regulations and policies; delivers training and guidance on responsible records management including the disposal of records eligible for destruction.

- Privacy - leads the University's effort to safeguard all personally identifiable information (PII) collected, used, disseminated, and stored by the University; develops and maintains privacy policies and procedures, and provides training and consultation on requirements.

The Assistant Vice President for Compliance reports to the Chief Audit Executive. The Chief Audit Executive reports functionally to the ACR Committee chairman, and administratively (day-to-day operations) to the ~~President of the University~~ Executive Vice President and Chief Operating Officer.

The Audit, Compliance, and Risk (ACR) Committee will:

- Approve the Compliance Charter and periodically reassess it for continued relevance.
- Receive communications from the Assistant Vice President for Compliance regarding compliance strategies, plans, and other relevant matters.
- Make appropriate inquiries of management and the Assistant Vice President for Compliance to determine whether all compliance efforts have the necessary resources and scope.
- Support leadership for the compliance program by promoting and supporting a University-wide culture of ethical and lawful conduct.

The Assistant Vice President for Compliance will communicate and interact directly with the Chair of the ACR Committee, including in executive sessions and between committee meetings as appropriate to ensure direct access to the board.

Professional Standards

The compliance function's objective is to establish and promote standards that meet the U.S. Federal Sentencing Guidelines' criteria for an effective compliance program.

1. Compliance standards and procedures to prevent and detect criminal activity;
2. Oversight by high-level personnel, with periodic reporting to the board from individuals with operational responsibility;
3. Due care in delegating substantial discretionary authority;
4. Effective communication and training to all levels of employees;
5. Systems for monitoring, auditing and reporting suspected wrong-doing without fear of reprisal and for periodically evaluating the effectiveness of the compliance and ethics programs;
6. Consistent enforcement of compliance standards including disciplinary mechanisms and appropriate incentives to perform in accordance with the compliance and ethics program; and
7. Reasonable steps to respond to and prevent further similar offenses upon detection of a violation.

In addition, the Medical Center's compliance program also follows the program elements defined in the Department of Health and Human Services' Office of the Inspector General's "Compliance Program Guidance for Hospitals".

Responsibilities:

Members of the University community will: ~~having responsibility for a specific area of compliance must ensure the following:~~

- ~~Oversight of~~ Monitor compliance in their specific functional areas;
- Adhere~~nce~~ to the University's ~~compliance~~ policies;
- Implement~~ation of~~ corrective action as necessary, arising from compliance reviews and/or investigations.
- Report all violations of law or University policy, without fear of retaliation for reports made in good faith.
- Cooperate with all investigations into suspected wrongdoing.

The role of the Assistant Vice President for Compliance is to remain well-informed on the content and operation of the ~~University's~~ institutional compliance and ethics program in order to exercise reasonable oversight of the effectiveness of the program, including:

1. *Standards of Conduct/Policies and Procedures:* confirming that the University implements policies, procedures, training programs, and internal control systems that are reasonably capable of reducing misconduct and that comply with relevant regulatory requirements.
2. *Compliance Roles and Responsibilities*: establishing clear roles and responsibilities across the University.
3. *Compliance Oversight:* exercising reasonable oversight over compliance activities by requesting and receiving updates from compliance officers.
4. *Reporting and Investigative Mechanisms*: confirming that the University maintains an effective mechanism for stakeholders to report or seek guidance regarding potential or actual wrongdoing.
5. *Correction and Prevention*: working with the University's senior leadership to promote and enforce compliance through appropriate incentives and disciplinary measures.
6. *Culture of Integrity and Compliance*: promoting the University's culture of integrity and compliance, through communication of compliance standards and policies.

Interaction with Audit and Enterprise Risk Management:

The Assistant Vice President for Compliance will work closely with colleagues in the Office of Audit and Compliance to assess and prioritize which compliance areas present the greatest risk and need for attention, based on regulatory environment and complexity, overlap with University strategic plans, and consequences of non-compliance. Managers with responsibility for specific areas of compliance will evaluate their individual compliance efforts against a list of criteria necessary to have an effective compliance program.

The Enterprise Risk Management (ERM) program is designed to identify and mitigate key institutional risks. For example, one type of risk to be considered is legal and regulatory compliance risk. The regular review of compliance requirements may highlight an emerging institutional risk. Conversely, the

identification of key institutional risks may guide the work of the compliance function and initiate a mitigation strategy that the University may use to address a given risk.

Updated on ~~June 7, 2018~~ September 15, 2023