

**UNIVERSITY OF VIRGINIA
BOARD OF VISITORS**

**Meeting of the Audit, Compliance,
and Risk Committee**

June 7, 2018

AUDIT, COMPLIANCE, AND RISK COMMITTEE

**Thursday, June 7, 2018
11:00 a.m. – 12:00 p.m.
Upper West Oval Room, The Rotunda**

Committee Members:

Babur B. Lateef, M.D., Chair
Robert M. Blue
Mark T. Bowles
L. D. Britt, M.D.
Frank M. Conner III, Ex-officio
Margaret F. Riley
Adelaide Wilcox King, Faculty Consulting Member

AGENDA

	<u>PAGE</u>
I. REMARKS BY THE COMMITTEE CHAIR (Dr. Lateef)	1
II. ACTION ITEMS	
A. Risk-Based Audit Plan for FY 2019 – FY 2020 (Ms. Saint)	2
B. Revised Audit and Compliance Charters (Ms. Saint and Mr. Nimax)	4
III. COMMITTEE DISCUSSION	
A. Auditor of Public Accounts (APA) Audit Entrance Meeting for Fiscal Year 2018 (Ms. Bianchetto to introduce Mr. Sandridge, who will report)	16
B. Enterprise Risk Management (ERM) Program: FY 2018 Report and FY 2019 Program Goals (Mr. Matteo)	17
IV. WRITTEN REPORTS	
A. Office of Audit and Compliance and UVA Health System Compliance FY 2018 Reports	23
B. FY 2018 Fourth Quarter Audit Follow Up Status Report	29
C. Ufirst Status Report	31

**UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY**

BOARD MEETING: June 7, 2018

COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: I. Remarks by the Committee Chair

ACTION REQUIRED: None

BACKGROUND: Dr. Babur Lateef, the Committee Chair, will open the meeting and provide an overview of the agenda.

**UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY**

BOARD MEETING: June 7, 2018

COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: II. A. Risk-Based Audit Plan for FY 2019 – FY 2020

BACKGROUND: UVA’s internal audit plan provides assurance on the effective functioning of the University’s significant risk mitigation activities, internal controls, and foundational processes. The plan is risk based, aligned with strategic initiatives, and focused on what matters most to the community of UVA stakeholders: the Board of Visitors, executive leaders, students, faculty, staff, regulators, award sponsors, patients, parents, and alumni.

To build the plan, the Audit Department relies on risk assessments and mitigating action plans provided by UVA’s Enterprise Risk Management program, Institutional Compliance, and Health System Compliance. Risk assessments are further informed by benchmarking with R1 and Ivy Plus institutions, input and requests from management and the Board of Visitors, and professional auditor judgment.

A dynamic approach to deploying the University’s internal audit resources allows the Audit Department to remain flexible and relevant to changing priorities and emerging risks. The Audit, Compliance, and Risk Committee will be briefed on changes to the approved plan as needed throughout the year.

UVA Audit Department FY2019-FY20 Proposed Two Year Plan:

Lead Audit Team	Risk Prioritized Audit Topics
<i>Audit Timing Determined by Assessment of Current Institutional Priorities; Detailed Scope Determined at Time of Audit</i>	
Audit Coverage: Pan- University	
IT & Health System	Ufirst Project Health Check: Provide feedback on project risk mitigation (through launch in January 2019)
Health System	Research Compliance Administration
Health System/Co-Sourced	Construction Contract Audits (Specific Capital Projects To Be Determined)
IT	Research Computing Security (Ivy Secure Computing Environment)
Academic & Health System	COSO Internal Controls Framework Pilots (Payroll and Financial Reporting Processes)
Academic	Financial and Budgetary Management Processes
Academic	Presidential Travel and Expenses (Conducted Annually)

Lead Audit Team	Risk Prioritized Audit Topics	
	<i>Audit Timing Determined by Assessment of Current Institutional Priorities; Detailed Scope Determined at Time of Audit</i>	
Audit Coverage: Academic Division		
Academic	International Student and Scholar Support	
Academic	Dining Services	
Academic	Student Health & Counseling	
Academic	Athletics Drug Testing Program (ACC Follow Up Request)	
IT	Security and Integrity of Key Instructional Systems	
IT	Network Infrastructure & Security: Vulnerability & Patch Management	
IT	Third Party IT Vendor Management; Cloud System Vendor Risks	
IT	Disaster Recovery & Business Continuity Planning	
Audit Coverage: Health System		
Health System	Revenue Cycle: Charge Capture (Procedures and Surgeries)	
Health System	Epic as a Platform: Managing Ongoing System Upgrades and New Functionality	
Health System	Outpatient Clinical Set Up	
Health System	Patient Friendly Access (PFA): Registration and Scheduling Processes	
Health System	Clinical Trials Billing (Epic)	
IT	Network Infrastructure & Security: Vulnerability & Patch Management	
IT	Disaster Recovery & Business Continuity Planning	
IT	Third Party IT Vendor Management; Cloud Vendor Risks	
IT	HIPAA Compliance – EPHI Security	
Audit Coverage: UVA’s College at Wise		
Academic	Comprehensive Risk Assessment with Specific Audits to Follow	
IT	General Computer Controls for Key Local UVA Wise Systems	

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

AUDIT DEPARTMENT FY 2019 – FY 2020 AUDIT PLAN

RESOLVED, the Audit Department FY 2019 - FY 2020 Audit Plan is approved as recommended by the Audit, Compliance, and Risk Committee.

**UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY**

BOARD MEETING: June 7, 2018

COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: II. B. Revised Audit and Compliance Charters

BACKGROUND: The internal audit department (Audit Department) and the institutional compliance function (Institutional Compliance) were combined in September, 2017 to form the Office of Audit and Compliance. The new structure is intended to enable greater collaboration and coordination of efforts related to compliance risks.

Prior to the combination, Institutional Compliance reported directly to the Executive Vice President and Chief Operating Officer. In the new structure, the AVP for Compliance reports directly to the Chief Audit Executive. These structural changes and administrative edits needed to align the documents necessitated revisions to both charters.

Marked-up versions of the current charters provided on the following pages show the proposed changes.

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

AUDIT DEPARTMENT CHARTER

RESOLVED, the updated Audit Department Charter, dated June 7, 2018, is approved as recommended by the Audit, Compliance, and Risk Committee.

INSTITUTIONAL COMPLIANCE CHARTER

RESOLVED, the updated Institutional Compliance Charter, dated June 7, 2018, is approved as recommended by the Audit, Compliance, and Risk Committee.

UNIVERSITY OF VIRGINIA INTERNAL AUDIT ~~DEPARTMENT~~ CHARTER

Purpose:

Internal Auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes. The UVA Office of Audit and Compliance Department assists UVA's Board of Visitors and University management in the discharge of their oversight, management, and operating responsibilities by providing independent assurance and consulting services to the University community. Our services add value by improving the control, risk management and governance processes to help the University achieve its business objectives.

Internal Auditing Policy:

It is the policy of the of the University to establish and support the Office of Audit and Compliance Department to assist the University in accomplishing its objectives by bringing a systematic and disciplined approach to evaluate and improve the effectiveness of the University's governance , risk management, and internal controls. The internal audit activity's responsibilities are defined by the Audit, Compliance, and Risk Committee (ACR Committee) of the Board of Visitors (Board) as part of its oversight role.

Authority:

The internal auditor, with strict accountability for confidentiality and safeguarding 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 an engagement.

All employees are requested to assist the Audit Department in fulfilling its roles and responsibilities. The internal audit activity will also have free and unrestricted access to the ACR Committee and its chairman.

Organization:

The Chief Audit Executive will report functionally to the ACR Committee chairman, and administratively to the President of the University.

The ACR Committee will:

- Approve the Audit Department charter.
- Approve the risk based audit plan.
- Approve the internal audit budget and resource plan.
- Receive communications from the Chief Audit Executive on the Audit Department's performance relative to its plan and other matters.
- Approve decisions regarding the performance evaluation, appointment, or removal of the Chief Audit Executive
- Approve the remuneration of the Chief Audit Executive
- Make appropriate inquiries of management and the Chief Audit Executive to determine whether there is inappropriate scope or resource limitations.

The Chief Audit Executive will communicate and interact directly with the ACR Committee, including in executive sessions and between ACR Committee meetings as appropriate.

Professional Standards

UVA's Office of Audit and Compliance Department will govern itself by adherence to The Institute of Internal Auditors' Mandatory Guidance, which includes the Core Principles for the Professional Practice of Internal Auditing, the Code of Ethics, the International Standards for the Professional Practice of Internal Auditing, and the Definition of Internal Auditing.

The Office of Audit and Compliance Department will adhere to the University's relevant policies and procedures as well as the *Generally Accepted Governmental Auditing Standards* of the Government Accountability Office.

Core Principles for the Professional Practice of Internal Auditing:

The Office of Audit and Compliance Department will continuously strive to be effective by operating in a manner consistent with the IIA's Core Principles:

- Demonstrates integrity.
- Demonstrates competence and due professional care.
- Is objective and free from undue influence (independent).
- Aligns with the strategies, objectives, and risks of the organization.
- Is appropriately positioned and adequately resourced.
- Demonstrates quality and continuous improvement.
- Communicates effectively.

- Provides risk-based assurance.
- Is insightful, proactive, and future-focused.
- Promotes organizational improvement.

Independence and Objectivity:

The internal audit activity will remain free from interference by any element in the University, including matters of audit selection, scope, procedures, frequency, timing, or report content to permit maintenance of a necessary independent and objective function. The Chief Audit Executive must disclose such interference to the ACR Committee and discuss the implications.

Internal auditors will have no direct operational responsibility or authority over any of the activities audited. Accordingly, they will not implement internal controls, develop procedures, install systems, prepare records, or engage in any other activity that may impair internal auditors' independence or judgment.

Internal auditors may provide assurance services for areas previously consulted, provided the consulting services did not impair objectivity.

Internal auditors will exhibit the highest level of professional objectivity in gathering, evaluating, and communicating information about the activity or process being examined. Internal auditors will make a balanced assessment of all the relevant circumstances and not be unduly influenced by their own interests or by others in forming judgments.

The Chief Audit Executive will annually evaluate reporting lines and responsibilities and confirm to the ACR Committee annually the organizational independence of the Office of Audit and Compliance Department.

Responsibility:

The scope of internal auditing encompasses, but is not limited to, the examination and evaluation of the adequacy and effectiveness of the University's governance, risk management, and internal controls as well as the quality of performance in carrying out assigned responsibilities to achieve the University's stated goals and objectives. This includes:

- Evaluating the design, implementation, and effectiveness of the organization's ethics-related objectives, programs, and activities.
- Evaluating risk exposure relating to achievement of the University's strategic objectives.
- Assessing whether the information technology governance of the organization supports the organization's strategies and

objectives.

- Evaluating the reliability and integrity of information and the means used to identify, measure, classify, and report such information.
 - In order to enable this responsibility, the Office of Audit and Compliance Department will participate in the planning, development, implementation, and modification of major computer- based and manual systems to ensure that:
 - (a) adequate controls are incorporated into the system;
 - (b) thorough system testing is performed at appropriate stages;
 - (c) system documentation is complete and accurate; and
 - (d) the resultant system is a complete and accurate implementation of the system specifications.
- Evaluating the systems established to ensure compliance with those policies, plans, procedures, laws, and regulations which could have a significant impact on the University.
- Evaluating the means of safeguarding assets and, as appropriate, verifying the existence of such assets.
- Evaluating the effectiveness and efficiency of resource utilization.
- Evaluating operations or programs to ascertain whether results are consistent with established objectives and goals and whether the operations or programs are being carried out as planned.
- Assessing and making appropriate recommendations for improving the governance process in its accomplishment of the following objectives:
 - Promoting appropriate ethics and values within the organization
 - Ensuring effective organizational performance management and accountability
 - Communicating risk and control information to appropriate areas of the organization
 - Coordinating the activities of and communicating information among the board, external and internal auditors, and management.
- Monitoring and evaluating the effectiveness of the organization's risk management processes.
- Performing consulting services related to governance, risk management, and control.
- Reporting significant risk exposures and control issues, including

fraud risks, governance issues, and other matters needed or requested by the ACR Committee or management.

- Evaluating specific operations at the request of the ACR Committee or management, as appropriate.
- Reporting periodically on the ~~Audit Department's~~ purpose, authority, and responsibility of the Office of Audit and Compliance and performance relative to its plan.

Internal Audit Plan:

At least annually, the Chief Audit Executive will submit to senior management and the ACR an internal audit plan for review and approval. The internal audit plan will consist of a work schedule as well as budget and resource requirements for the next year. The Chief Audit Executive will communicate the impact of resource limitations and significant interim changes to senior management and the Board.

The internal audit plan will be developed based on a prioritization of the audit universe using a risk-based methodology, including input of senior management, the ACR, and Board.

The Chief Audit Executive will review and adjust the plan, as necessary, in response to changes in the organization's business, risks, operations, programs, systems, and controls. Any significant deviation from the approved internal audit plan will be communicated to senior management and the ACR through periodic activity reports.

Audit Department Services:

The Chief Audit Executive is empowered to conduct assurance services, special audit projects, reviews, or investigations at the request of the Board, ACR Committee, President, General Counsel, EVP Provost, EVP Chief Operating Officer, EVP Health Affairs, or their designee, to assist management in meeting its objectives, promoting economy and efficiency in the administration of, or preventing and detecting fraud and abuse in its programs and operations. The Office of Audit and Compliance ~~Department~~ may also provide consulting services, beyond ~~the Audit Department's~~ assurance services, to assist management in meeting its objectives. Examples may include facilitation, process design, training, and advisory services.

Coordination with External Auditing Agencies:

The Chief Audit Executive, with the goal of avoiding duplication of work, will

coordinate the ~~department~~office's audit efforts with those of the Commonwealth of Virginia's Auditor of Public Accounts, or other external auditing agencies as applicable, by participating in the planning and definition of the scope of proposed audits so the work of all auditing groups is complementary and their combined efforts provide comprehensive, cost-effective audit coverage for the University.

Reporting and Monitoring:

A written report will be prepared and issued by the Chief Audit Executive or designee following the conclusion of each internal audit engagement and will be distributed as appropriate. Internal audit results will be available for review by the ACR and Board of Visitors.

The internal audit report will include management's response and corrective action taken or to be taken in regard to the specific findings and recommendations. Management's response to audit findings and recommendations should include a timetable for anticipated completion of action to be taken and an explanation for any corrective action that will not be implemented.

The ~~Office of Audit and Compliance Department~~ will be responsible for appropriate follow-up on its engagement findings and recommendations. All significant findings will remain in an open issues file until cleared. The ACR will receive periodic reporting from the Chief Audit Executive on the status of management's action plan implementation.

The Chief Audit Executive will periodically report to senior management and the ACR on the internal audit activity's purpose, authority, and responsibility, as well as performance relative to its plan. Reporting will also include significant risk exposures and control issues, including fraud risks, governance issues, and other matters needed or requested by senior management, ACR, or the Board.

Quality Assurance and Improvement Program:

The Chief Audit Executive must develop and maintain a quality assurance and improvement program that covers all aspects of the internal audit activity. The program must include both internal and external assessments to evaluate the internal audit activity's conformance with the Standards and an evaluation of whether internal auditors abide by the Code of Ethics.

External assessments must be conducted at least once every five years by a qualified independent assessor or assessment team from outside the organization.

The Chief Audit Executive must discuss with the ACR Committee:

- The form and frequency of external assessment;
- The qualifications and independence of the external assessor or assessment team, including any potential conflict of interest.

The program will also assess the efficiency and effectiveness of the internal audit activity and identify opportunities for improvement.

The Chief Audit Executive must communicate results of the quality assurance and improvement program to senior management and the ACR Committee.

Updated on June ~~8X~~, 20178

UNIVERSITY OF VIRGINIA COMPLIANCE CHARTER

Mission and 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 Assistant Vice President for Compliance reports to the [Chief Audit Executive Executive Vice President and Chief Operating Officer](#). [The Chief Audit Executive reports functionally to the ACR Committee chairman, and administratively to the President of the University.](#)

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 having responsibility for a specific area of compliance must ensure the following:

- Oversight of compliance in their specific functional areas;
- Adherence to the University's compliance policies;
- Implementation of corrective action as necessary, arising from compliance reviews and/or investigations.

The role of the Assistant Vice President for Compliance is to remain well-informed on the content and operation of the University's 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 Internal Audit Department](#) 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 [typecategory](#) 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](#)

**UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY**

BOARD MEETING: June 7, 2018

COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: III. A. Auditor of Public Accounts (APA) Audit Entrance Meeting for Fiscal Year 2018

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. Ms. Bianchetto, Vice President for Finance, will introduce Mr. Eric M. Sandridge, who will discuss with the committee the fiscal year 2017-2018 audit.

Eric M. Sandridge 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 member of the National State Auditors Association (NSAA) Audit Standards and Reporting committee and NSAA Single Audit committee. He is a graduate of the College of William and Mary and is a CPA, CISA, and CGFM.

**UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY**

BOARD MEETING: June 7, 2018

COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: III. B. Enterprise Risk Management (ERM) Program: FY 2018 Report and FY 2019 Program Goals

ACTION REQUIRED: None

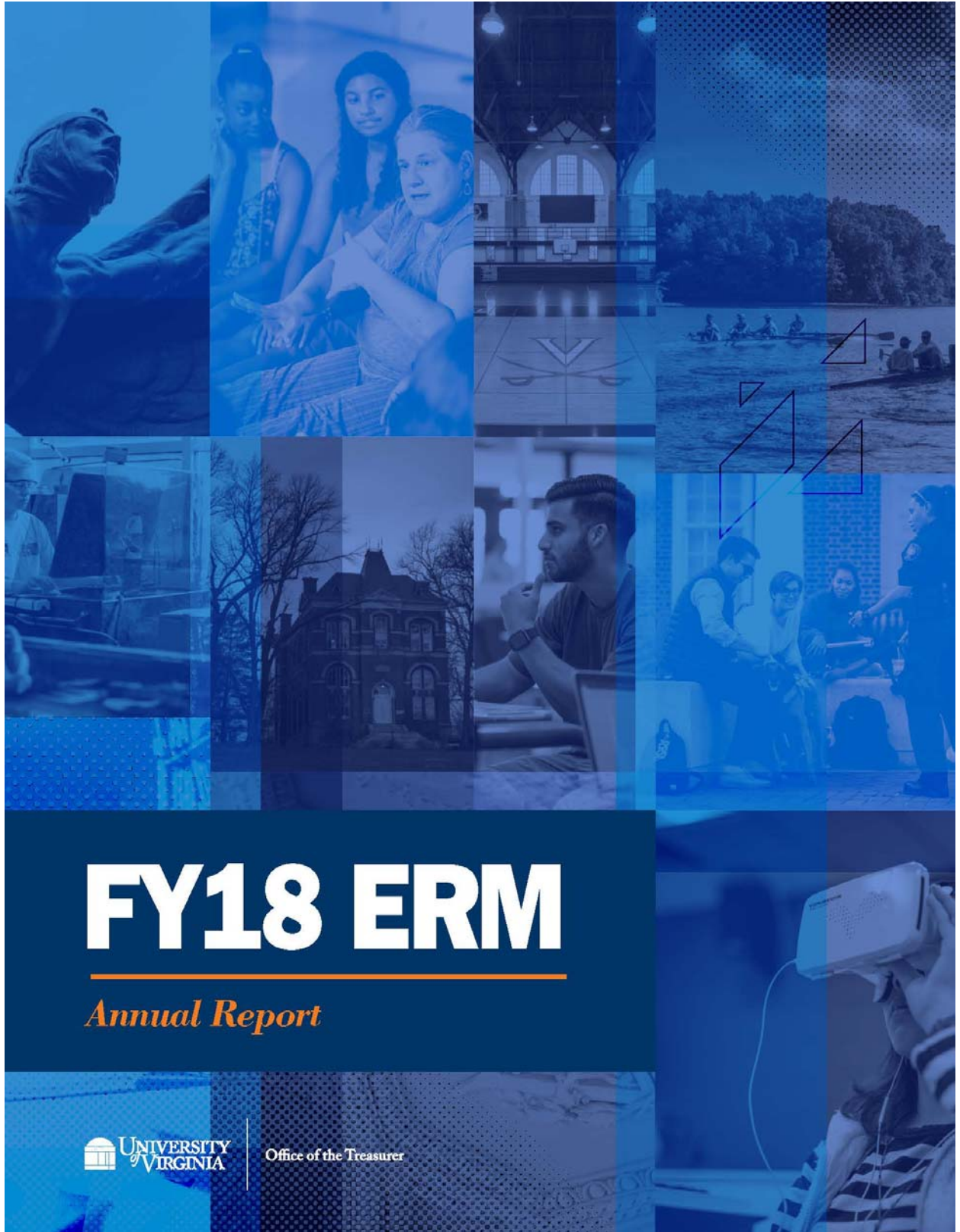
BACKGROUND AND DISCUSSION: Mr. James Matteo, Associate Vice President and Treasurer, will report on the ERM program and will review the attainment of the FY 2018 goals, discuss program goals for FY 2019, and share the FY 2018 ERM Annual Report. The ERM Goals for FY 2018 included:

1. **Enhancing communication and discussion among executives and board members related to key risk management** - Over the past year, BOV committee chairs were introduced into ERM risk mitigation discussions. ERM key risks were assigned to appropriate BOV committees and committee chairs were engaged in discussions with risk leads and executive owners. This effort engaged BOV members in the risk management process and helped the University gain additional perspectives on mitigation plans and mitigation confidence.
2. **Strengthening risk management efforts through better understanding and use of risk appetite and key risk indicators** - This past year, the University held the first meeting of risk leads from the Academic Division and Health System. The goal of the meeting was to strengthen and standardize risk ledgers, provide a forum to share experience, and introduce risk appetites into the risk management discussion.
3. **Updating the ERM charter** - The ERM charter was updated in September 2017, primarily to make the following changes:
 - Redefining the mission of the ERM effort
 - Clarifying the objectives of the program
 - More clearly defining the roles supporting the program
 - Recognizing the creation of Risk Management Networks at the Academic Division and Health System
4. **Better aligning and integrating ERM efforts with University planning and audit cycles** - The timing of the ERM cycle has been realigned to coincide with the University's annual goal setting and audit planning processes. As ERM is informed by the University goals and helps inform the audit plan, this realignment has helped the program find its fit within existing planning activities.

The ERM Goals for FY 2019 include:

- **Fully onboarding the College at Wise** – While the College at Wise has been included in the Academic Division’s ERM effort, the University would like to expand the program to specifically address Wise’s unique environment and risks.
- **Building a risk interaction map** – Many of the key risks of the Academic Division and Health System overlap (e.g., research, IT). Many risks and their mitigation plans affect departments across the University. The goal is to build a map that captures these interactions and identifies risks that may fall between or span organizational areas.
- **Migrating ERM data into a new Governance, Risk, and Compliance (“GRC”) system** – The Office of Audit and Compliance is planning to implement a new GRC system. We are planning at this time to migrate ERM data into this system.

The second annual ERM executive report follows. It includes the key risks of the Academic Division and Health System, a heat map of the key risks, and a brief synopsis of the past and future years’ activities.



FY18 ERM

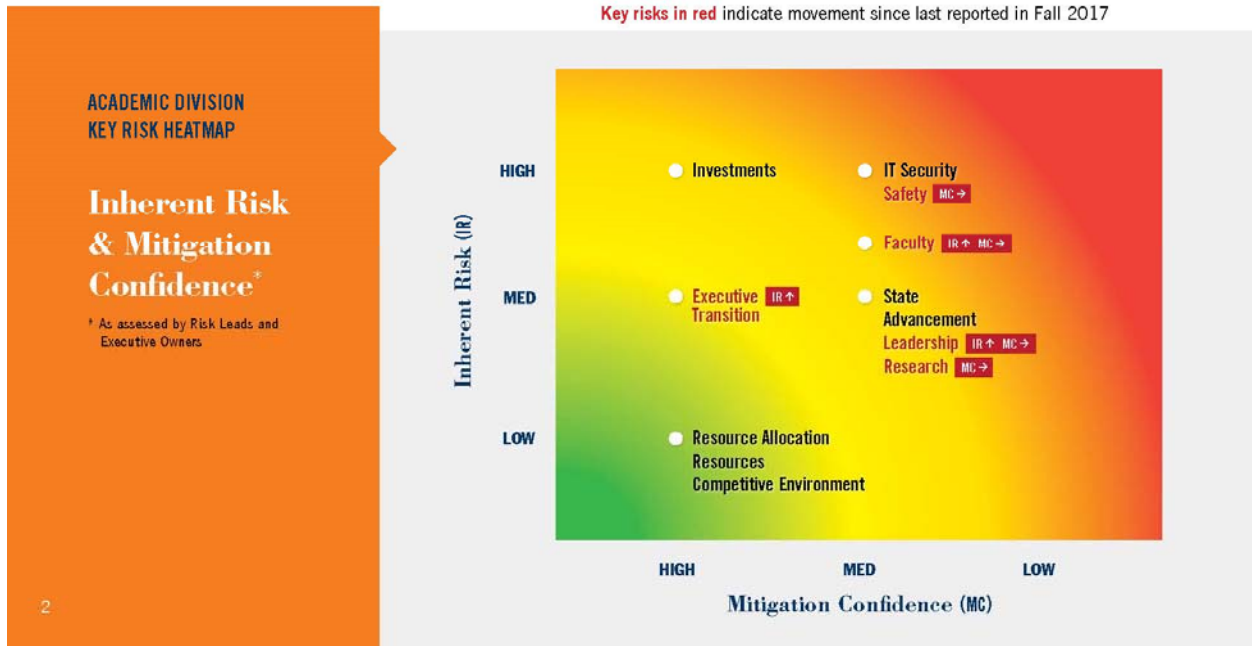
Annual Report



Office of the Treasurer

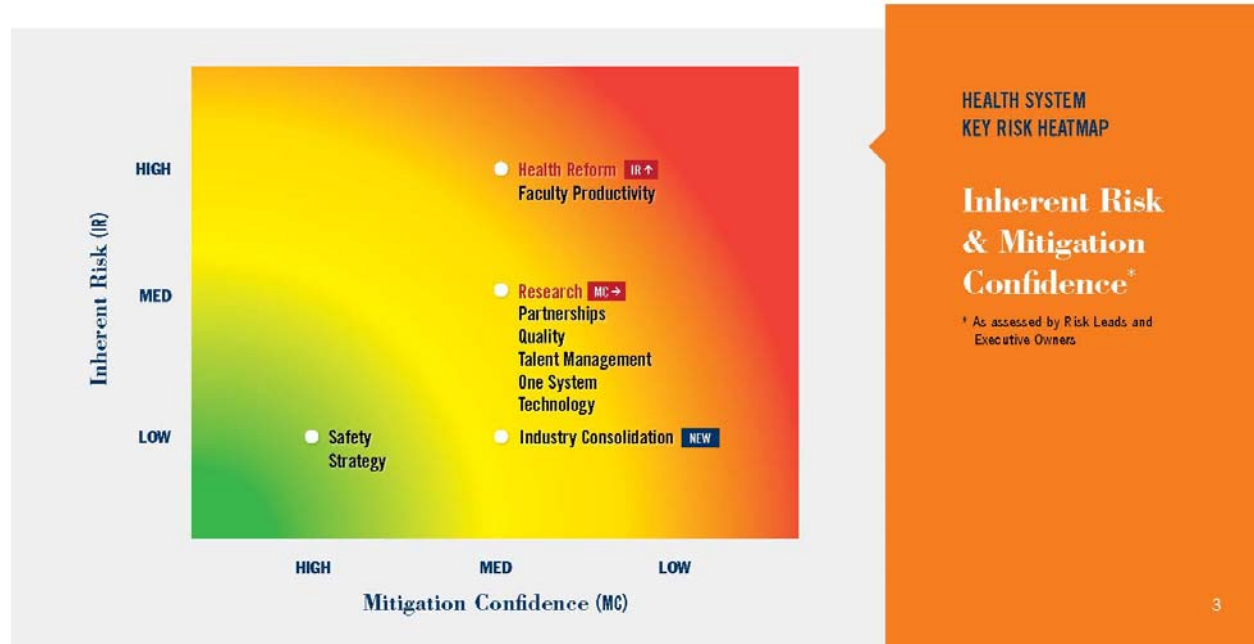
ERM Key Risks – Academic Division

ACADEMIC DIVISION RISK	RISK LEAD(S)	EXEC. OWNER
ADVANCEMENT - Developing and implementing a campaign strategy that adequately addresses philanthropic investment and fundraising strategies	VP for Advancement	President
COMPETITIVE ENVIRONMENT - Assessing the University's competitive space in undergraduate, graduate, and professional programs	Vice Provost for Academic Affairs	EVP-Provost
EXECUTIVE TRANSITION - Preparing for an executive leadership transition and a potential change in the University's strategic direction	Chief of Staff for the President	BOV, President
FACULTY - Attracting, retaining, and developing a distinguished faculty	Vice Provost for Faculty Affairs	EVP-Provost
INVESTMENTS - Stewarding assets particularly related to investable assets	AVP & Treasurer	EVP-COO
IT SECURITY - Enhancing cybersecurity in an era of increasing threats	Chief Information Officer	EVP-COO
LEADERSHIP - Maintaining and renewing a highly skilled and cooperative executive team given the attractive alternatives for the best executives	President	President
RESEARCH - Research leadership, infrastructure, and funding to adequately support the accomplishment of our research objectives	VP for Research	EVP-Provost
RESOURCE ALLOCATION - Developing an optimal process for allocating resources in meeting strategic objectives	VP for Finance	EVP-COO
RESOURCES - Diminished, or loss of, financial resources from major funding sources (e.g., State, Advancement, Research, Endowment)	VP for Finance	EVP-COO
SAFETY - Maintaining a safe environment for the University community	Chief of Police Dir of Emergency Preparedness	EVP-COO, VP for Student Affairs
STATE - Concern about whether public policy in the State will continue to be supportive of quality public higher education	Senior VP for Operations	President



ERM Key Risks – Health System

HEALTH SYSTEM RISK	RISK LEAD(S)	EXEC. OWNER
HEALTH REFORM - Reduced Medical Center revenues as a result of government payment reform	CEO, Medical Center	EVP-Health Affairs
STRATEGY - Strategic direction in a changing competitive environment (flexibility around change)	EVP-Health Affairs	EVP-Health Affairs
TALENT MANAGEMENT - Recruitment and retention of key personnel (patient care services positions, research, and leadership)	CEO, Medical Center Dean, School of Medicine	EVP-Health Affairs
ONE SYSTEM - Alignment of health system entities towards a single system of operation	EVP-Health Affairs	EVP-Health Affairs
QUALITY - Maintaining Joint Commission accreditation	Chief of Quality & Performance Improvement, MC	EVP-Health Affairs
RESEARCH - Research leadership, infrastructure and funding to adequately support the accomplishment of our research objectives	Dean, School of Medicine	EVP-Health Affairs
TECHNOLOGY - Investment and enablement	Chief Information & Technology Officer, MC	EVP-Health Affairs
SAFETY - A major quality or safety event	Chief of Quality & Performance Improvement, MC	EVP-Health Affairs
PARTNERSHIPS - Maximize the benefits of off-grounds partnerships	EVP-Health Affairs	EVP-Health Affairs
INDUSTRY CONSOLIDATION – Commercial payer industry changes (industry consolidation and changes in contracting)	EVP-Health Affairs	EVP-Health Affairs
FACULTY PRODUCTIVITY - Managing faculty productivity (clinical and research)	Chief Medical Officer, MC Dean, School of Medicine	EVP-Health Affairs



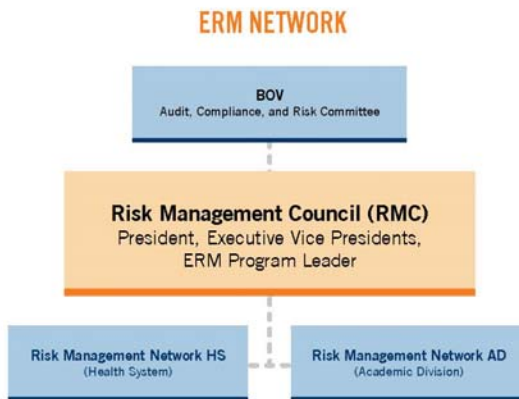
FY18 ERM WRAP-UP

The ERM Program made significant strides in FY18. As the ERM process matures we continue to focus our efforts on expanding the dialogue around key risks, strengthening risk mitigation plans, and further developing a network of people supporting the effort. In higher education, ERM has been quickly adopted, but slow in being fully actualized. The University's ERM program is among the leading ERM programs in the industry. We find ourselves becoming a resource for other schools, presenting our approach to colleagues, and assuming leadership roles among ERM professional organizations.

In FY18, we witnessed significant advancements in our ERM efforts.

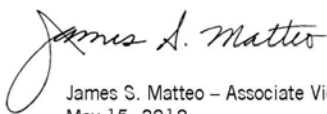
Key accomplishments included:

- Engaging Board of Visitors committee chairs in the ERM effort – this year we began connecting risk leads, executive owners, and BOV committee chairs to discuss key risk management efforts and to gain consensus on risk management activities.
- Reforming the Risk Management Council (RMC) – the council has been elevated to include the President and senior executives, with the current structure looking like the chart to the right. We further expanded the network to include update meetings with the President's Cabinet and Deans.
- Conducting the first pan-University meeting of risk leads – to strengthen and standardize risk mitigation plans. The meeting helped to create common expectations regarding risk ledgers and helped us begin to identify the interaction between risks.



Goals for FY19

- Further onboard UVA Wise – The College at Wise has previously been included in ERM as an operating unit of UVA. We feel a dedicated ERM effort similar to that of the Academic Division and Health System will add value to UVA-Wise operations.
- Building a risk interaction map – Many key risks of the Academic Division and Health System overlap (e.g., research, IT). Many risks and their mitigation plans impact departments across the University. Our goal is to build a map that captures these interactions and, hopefully, identifies risks that may fall between organizational areas.
- Migrate ERM data into a new Governance, Risk, and Compliance (“GRC”) system being implemented by Internal Audit.



James S. Matteo – Associate Vice President and Treasurer
May 15, 2018

**UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY**

BOARD MEETING: June 7, 2018

COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: IV.A. Office of Audit and Compliance and UVA Health System
Compliance FY 2018 Reports (Written Reports)

ACTION REQUIRED: None

BACKGROUND: The Office of Audit and Compliance and the UVA Health System
Compliance Office's reports summarizing FY 2018 accomplishments follow.



FY 2018 Audit Department Year in Review

Highlights of Work Performed, Insights Delivered, and Continuous Improvements Made

Throughout the year, the Audit Department worked alongside management to provide real-time assurance on controls and risk mitigation effectiveness for the University's most important initiatives. Signature projects for the year included:

Minors Protections and Title IX Complaint Management

- ✓ Assembled a team of experts to evaluate UVA's policies and procedures for ensuring the safety of minors in programs across Grounds and at the College at Wise. Work wrapping up at the time of this report.

UVA Archives and Special Collections

- ✓ Audit report equipped Dean of Libraries and UVA leadership with detailed recommendations for security improvements to safeguard UVA's priceless treasures for future generations of scholars.

Undergraduate Safety in Labs, Shops, and Studios

- ✓ The audit undertook a comprehensive analysis of the Environmental Health & Safety Department's processes for ensuring UVA students have a safe environment in which to learn.
- ✓ Outside consultants were able to rely on the audit report to partially reduce their project scope, avoiding associated costs.

Safety and Security Review: Margolis Healy

- ✓ The Audit Department, together with the AVP for Clery Compliance, provided program management to coordinate and track the efforts of outside consultants

Introducing the Office of Audit and Compliance



In September, 2017, Institutional Compliance joined the Audit Department to create the Office of Audit and Compliance.

This new organizational assurance model puts key elements of corporate governance—assurance and institutional compliance—under one umbrella.

In FY2019, we will continue to leverage the benefits of the combination:

- Improved communication and coordination
- Alignment of priorities
- Joint participation on relevant projects
- Reduced complexity for stakeholders
- Effective sharing of information and data for improved risk

Margolis and Healy to assess safety and security policies and procedures following the events of August 11 and 12.

Travel and Expense Management

- ✓ Following the University's implementation of new policies and systems for travel (TravelUVA) and expense management (ExpenseUVA) in 2017, the audit highlighted the need to improve controls and oversight for \$70 million in annual expenditures.

Other Projects Delivered

- ✓ **Ufirst HR Transformation Project**—project health checks communicated lessons learned from transition between project's phases and emphasized the need to improve alignment on objectives between Academic Division, Health System, and UPG.
- ✓ **Institutional Base Salary**—in depth analysis of UVA's institutional base salary computations—the foundation of costing for sponsored research—resulting in recommendations for Workday implementation.
- ✓ **Medical Center Procurement**—confirmed effective functioning of controls over purchases of goods and services at the Medical Center.
- ✓ **Medical Device Procurement and Security**—collaborated with Health System IT and Clinical Engineering to establish a baseline for security of networks running sensitive medical devices in the Medical Center.
- ✓ **Strategic Investment Fund**—recommendations for continued strengthening of procedures and controls over SIF were presented to the BOV's SIF Administrative Committee.
- ✓ **Presidential Travel and Carr's Hill Expenses**—performed annually at President Sullivan's request.
- ✓ **NCAA Football Attendance**—annual analysis performed as NCAA FBS requirement.
- ✓ **Foundation Relationship Assessment**—provided advice and assistance to Treasury's risk assessment.

Support Provided to University Initiatives

The Audit Department participated in a variety of steering committees and work groups across FY2018. In addition to ongoing roles on the Finance Projects Advisory Council, ERM Risk Network, Policy Review Committee, and the IT Security Advisory Committee, we helped UVA tackle specific projects including:

- ✓ **NIST 800-171 Controlled Unclassified Information (CUI) Compliance**—participated on a cross-functional team to define controls over UVA's CUI-designated secure IT environment for researchers. We also participated on the **CUI for Student Financial Data** work group.

- ✓ **Advisory Committee on the Future of the Historic Landscape**—provided administrative support to this Dean’s Working Group subcommittee.
- ✓ **Finance Transformation**— helped evaluate RFPs received from potential Finance Transformation consulting partners.

University and UVA Health System Compliance: Accomplishments FY 2018

University Compliance Goals - Fiscal Year 2017-18

1. Reviewed and updated the university's Code of Ethics for review with new senior leaders in FY18-19, prior to seeking approval by the Board of Visitors.
2. Completed the onboarding of the medical center's new Compliance and Privacy Officer, including the operational changes necessary to convert to a medical center position.
3. Completed compliance reviews related to digital accessibility project on a multi-year project plan. New policy was completed and posted regarding background checks and on-going responsibility for employees to disclose criminal convictions. Continued to review UFirst compliance, including a discussion of related compliance concerns and a demonstration of the new learning management system with the Compliance Network.
4. Reviewed and updated the compliance risk assessment conducted in partnership with Internal Audit and General Counsel to confirm the strength of the university's compliance efforts. This assessment evaluated which compliance areas present the greatest risks, based on the consequences of non-compliance, levels of effort necessary to address regulatory changes, regulatory scrutiny, and cross-functional coordination.
5. Obtained additional software licenses of our incident management system and completed training for staff to expand the marketing and use of the helpline.

UVA Health System Compliance FY 2018 Summary Report

1. Restructured the Medical Center Compliance & Privacy Office to create a complete team; established developmental goals and actively mentored team members in accomplishing; created awareness within the health system through targeted compliance and privacy communication and training; provided routine interaction and support to managers and their teams in issue resolution, as well as the standard functions of auditing and compliance investigation and documentation.

2. Reviewed the findings of the prior compliance risk assessment conducted by former Medical Center compliance leaders in partnership with University Compliance, Internal Audit and General Counsel; updated the tool in preparation for redeployment to examine the compliance areas of greatest risk based on the consequences of non-compliance (legal, operational, and reputational), levels of effort necessary to address regulatory changes, regulatory scrutiny, and cross-functional effort.
3. Performed a series of coding audits to examine compliance with regulatory requirements for documentation of medical necessity for appropriate admissions, accurate coding, billing and reimbursement from Medicare for specific services; also in support of Revenue Cycle processes and data integrity post-Epic Phase II.

**UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY**

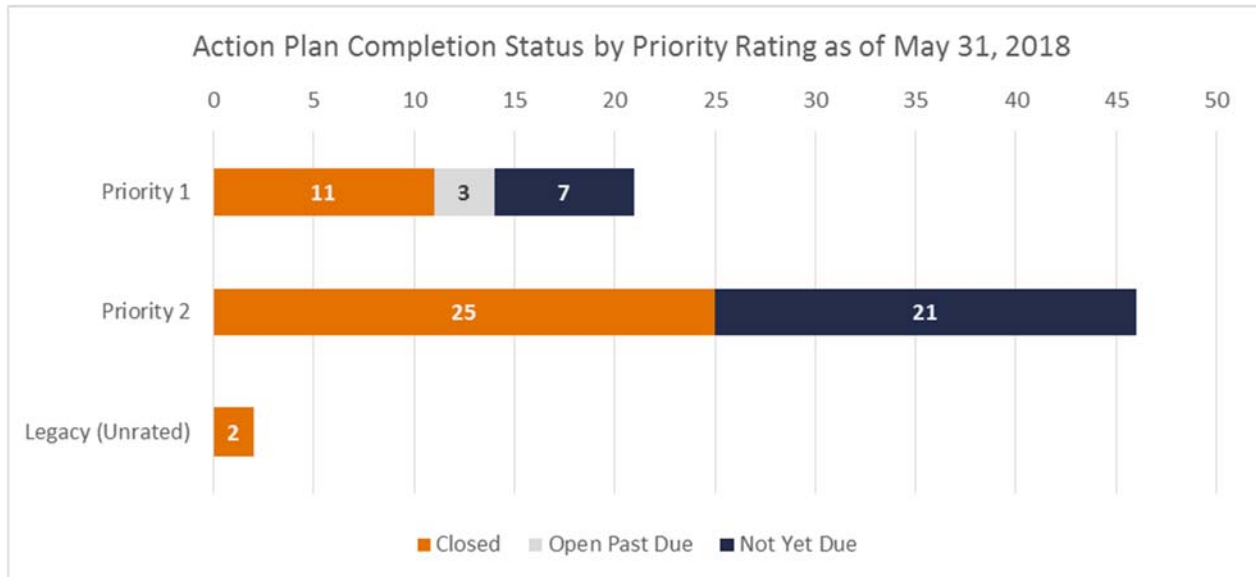
BOARD MEETING: June 7, 2018

COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: IV.B. FY 2018 Fourth Quarter Audit Follow Up Status Report

ACTION REQUIRED: None

BACKGROUND: IIA 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 chart below displays the status of management’s action plans through May 31, 2018.



Details of Open Past Due Action Plans:

Audit	Past Due Action Item	Priority Rating	Action Plan Owner
Archives and Special Collections	Security System Administration: General system policies and procedures under development in tandem with security system upgrade – project completion expected August 2018 (Due 1/1/18)	P1	Guy Mengel, Director Library Facilities and Security

Audit	Past Due Action Item	Priority Rating	Action Plan Owner
Archives and Special Collections	Security System Administration: Routine maintenance plans and regular testing schedule also being developed in tandem with security system upgrade (Due 1/1/18)	P1	Guy Mengel, Director Library Facilities and Security
Archives and Special Collections	Training: Establish and implement formal training programs (security and fraud awareness) for ASC staff (Due 2/1/18)	P1	Heather Riser, Harrison-Small Director of Operations, and ASC Standing Security Committee

Archives and Special Collections (ASC) continues to pursue solutions and funding for the following past due action plans, which were all classified with Priority 2 ratings.

Environmental Conditions: The fire suppression system in Harrison-Small still has the potential to damage the collection if used (initial discharge of discolored water). While a Novec 1230 or Inergen system could be installed to limit damage to collection materials, a study would need to be completed to determine costs to supplement or replace the current water-based system. The library will continue to pursue ways to mitigate risk, including identifying funding for system supplementation/replacement. (Due 9/1/17)

Security Cameras: Installation of cameras in the processing room were not part of the current security and camera upgrades. While some risk is accepted as a result of that decision, ASC will pursue a design for the installation and implementation of processing room cameras in the future. (Due 9/1/17)

Theft Risk – Internal: Consistent with the decision to not check belongings of employees when exiting areas where collections items are stored, a policy requiring inspections was not developed. Though personal items are prohibited from storage/stack areas, collection items are temporarily stored in staff areas while being processed and consulted. At this time, ASC will not check personal belongings of employees when exiting staff areas, and will pursue ways to restructure staff space to accommodate lockers and to identify funding for this type of renovation. (Due 3/1/18)

**UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY**

BOARD MEETING: June 7, 2018

COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: IV.C. Ufirst Status Report

ACTION REQUIRED: None

BACKGROUND: Ms. Kelley Stuck, Vice President and Chief Human Resources Officer, prepared the following report on the status of the HR transformation project called Ufirst.



Decision to Reschedule Software Launch

In late March, the University announced the decision to reschedule the launch of the supporting technology for the HR Transformation, Workday, from July 2018 to January 2019. This decision was recommended by Vice President for Human Resources Kelley Stuck and Ufirst Project Executive Director Sean Jackson, and was supported by the organization.

We have emphasized from the beginning of this project that service and quality are our most important objectives. We knew this would be a particularly challenging project, given our aggressive timeline and the complexities of integrating data and functionality across the Academic Division and Health System.

The rescheduled launch date of January 2019 will allow the team to finalize the necessary changes, complete testing, and be confident in the accuracy of the payroll and benefits deductions, the two most critical areas from our customer's point of view.

Since the Decision

The Ufirst project team has updated the published communications and training schedules for Workday and will continue to engage and educate University faculty, staff, and team members throughout the coming months. Other important elements of the HR and Payroll transformation will continue to move forward as planned.

Operating under the new organizational model without the benefit of the Workday software is challenging and will likely be frustrating at times for both HR and their customers. However, the longer transition period will also allow for further alignment and cleanup of processes and practices across Grounds.

The Ufirst Project teams have created a series of seven quality gates from now through November that must be met to achieve our goal of a successful January Workday launch. Each of the Quality Gates is supported by a detailed project plan. To ensure that we remain aware of and respondent to the numerous risks that confront a project of this magnitude and complexity, we will continue to take advantage of third-party guidance through the Gartner's Independent Verification and Validation and UVA Internal Audit's Project Health Check processes.

Progress to Date

Our progress to date has been substantial:

- The new HR Organization (UVA HR) is staffed and continuing to transition work from the Schools/Units and deliver services both in the new model during this period of transition.
- HR Business Partners have been selected, trained and have transitioned to schools and units, supporting human resource priorities and ensuring that HR service expectations are being met.
- The HR Solution Center, launched in December 2017, is achieving and maintaining extraordinarily high satisfaction ratings (4.5+ out of 5).
- The Payroll transformation is proceeding with new streamlined processes designed and configured in Workday to support the new Payroll organization.
- We have built over 300 HR and Payroll processes and a new HR service delivery structure to which resources are now aligned.
- Employee data has been integrated into a single data source to support the new service delivery model.
- We have successfully tested the processes for recruitment, hiring, set up of compensation, and learning program enrollment in the Workday environment.

The Ufirst project represents a significant step forward for the University and plays a critical role in our ability to attract and retain exceptional faculty, staff, and team members committed to teaching, research, and patient care. We are confident that the revised schedule provides us with the time necessary to deliver on this promise.