UNIVERSITY OF VIRGINIA
BOARD OF VISITORS

Meeting of the Audit, Compliance, and Risk Committee

June 8, 2017

AUDIT, COMPLIANCE, AND RISK COMMITTEE
Thursday, June 8, 2017
1:45 – 2:30 p.m.
Board Room, The Rotunda

Committee Members:

Frank E. Genovese, Chair
Mark T. Bowles
L. D. Britt, M.D.
Frank M. Conner III
Babur B. Lateef, M.D.
James B. Murray Jr.
William H. Goodwin Jr., Ex-officio
Adelaide Wilcox King, Faculty Consulting Member

AGENDA

UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: June 8, 2017

COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: I. Remarks by the Committee Chair

ACTION REQUIRED: None

BACKGROUND: Mr. Frank Genovese, 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 8, 2017

COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: II.A. Audit Department Accomplishments and Scorecard for FY 2017 (Written Report)

ACTION REQUIRED: None

BACKGROUND: The report summarizes the accomplishments of the UVA Audit Department for FY17. The report is for informational purposes only; it does not require formal action.

FY 2017 Year in Review

Audit Department Accomplishments

Highlights of significant projects and insights delivered to the University of Virginia by the Audit Department throughout FY 2017

FY 2017 Year in Review

Audit Department Accomplishments

Our unit's goals are somewhat evergreen. Cover risks at the Health System and Academic Division and get better internally. Here's how we performed against those simple but powerful goals in FY2017.

Goal 1: Health System Risk Coverage

Goal Description: Engage with Health System leaders to ensure optimal coverage of strategic, operational, compliance, and enterprise risk mitigation for all elements of the University of Virginia's Health System. Ensure audit resources are appropriately balanced to address health system higher priority risks and significant projects.

The department made important inroads into the UVA Health System during FY2017. In prior years, our connection to the Health System was suboptimal; relationships and the positioning of the Department continue to be repaired and reinvented.

Our signature project in the Health System in FY2017 was (and remains) the Epic Phase 2 Project Health Check. The team's collaborative, in-depth assessment of risks to the project's successful implementation was a catalyst to improving communication with Epic's executive sponsors. **Our objective reporting and continuous interactions with the Epic project management team are helping to mitigate risks associated with go-live of this $120 million system implementation.**

Given the size and scope of the Epic implementation, our project health check alone could have provided ample value to the health system, but we also completed reviews of IT controls for Pyxis, the automated medication dispensing system, and Unix servers deployed at the UVA Medical Center.

Goal 2: Academic Division Risk Coverage

Goal Description: Engage with relevant leaders to ensure optimal coverage of strategic, operational, compliance, and enterprise risk mitigation for all elements of the University of Virginia's Academic Division. Ensure audit resources are appropriately balanced to address higher priority risks and significant projects.

Continuing the transformation of internal auditing at UVA

- Hired and on-boarded Director of Health System Audits
- Hired Director of IT Audits (June 2017)
- Audit Department Process Improvements:
  - Standardized and documented Audit Methodology
  - Developed and documented Integrated Assurance Methodology for assessing the effective functioning of 2nd line of defense units
  - Implemented Audit Department scorecard to report to Audit, Compliance, and Risk Committee
  - Implemented timekeeping system to track staff utilization on value added work

Our risk coverage of the Academic Division included a number of audits and projects:

- **Compliance Risk Assessment**: We were instrumental in ensuring UVA had a documented compliance risk assessment in place (a necessary component of an effective compliance function according to the US Federal Sentencing Guidelines) and performed project management in support of AVP Compliance. The team led the creation of the compliance risk framework, facilitated meetings among compliance, legal, and other subject matter experts, and documented risks.

- **Integrated Assurance**: We created a methodology to evaluate the effective functioning of the University's 2nd Line of Defense functions (management assurance functions that perform ongoing controls monitoring, create policy guidance, and provide training). This tool can be used to evaluate the processes and controls employed by 2nd Line units to ensure complianc with laws and regulations. Given the University's substantial investment in compliance oversight, this methodology provides feedback to leadership on opportunities for maximizing compliance effectiveness.

- **Curry School of Education:** We had several recommendations with University-level applicability, including the need for the Registrar to improve the accuracy of information in official published materials. Our recommendations were well received and actions have been taken to correct control gaps identified.
- **Distributed IT Systems Management**: Our project explored risks inherent in a decentralized environment: if IT systems that are connected, directly or indirectly, to University infrastructure are not properly managed and secured, the security of core systems or infrastructure could be undermined or circumvented. Our work is being used to facilitate dialog and greater cooperation between central IT and the schools and departments that are outside it. ***That's a win!***
- **Security Enhancement Plan Project Health Check:** the IT Audit team did work to confirm the projects in the SEP Program, now known as Secure UVA, are on track as reported to the ACR Committee of the BOV.
- **Ufirst Project Health Check:** The first installment of results and insights on risks to achieving the Ufirst project's objectives were delivered to the project team in March 2017. Work on Ufirst risks will continue in FY18.
- **Ivy Cloud Project Health Check**: Our preliminary work on Program Governance and Project Management sparked many conversations about governance and ownership of the high performance computing environment known as Ivy Cloud. These conversations have stimulated action and enhanced ownership of this important capability. This will help ensure the value in the investment in the Ivy Cloud environment delivers the envisioned ROI for researchers and the University. We'll evaluate Ivy Cloud security and controls in FY2018.

Goal 3: Optimize Audit Department Operations

Goal Description:

1. Identify, prioritize, and execute Audit Department Value Charter elements and related scorecard metrics.
2. Engage in Fundamentals of Transaction 3 month course to enhance Leadership and Relationship Acumen (12/31/2016)
3. Define, document, communicate, and train department on Audit Methodology (9/30/2016)
4. Update audit risk universe and plan; obtain BOV Audit Committee approval at June 2017 meeting
5. Define, document, communicate, and begin execution of Audit Training Curriculum.

We completed bullets 1 through 4 and are in progress on 5. Our staffing, resources, and higher priority commitments in 2016 delayed us in fully executing a formal training curriculum (though we do require auditors to obtain a minimum 40 hours in continuing education each year). We'll make defining the competencies and training for auditors at each level a focus area for FY2018.

UVA Audit Department Value Scorecard

[Data as of April 30, 2017]

Measures	Year to Date Metric Achievement Status	Previous Reporting Mar 2017
People: Leadership & Relationship Acumen		
Internal Team		
Team Participation in Introduction to Transactional Competence (ITC) Program *Target: 100% participation*		
Training hours per audit in non-technical "differentiator" competencies *Target: 20 Hours*		
External Stakeholders		
Audit Satisfaction Scores *Target: Above Average*	Completed Survey Tool	
Collaboration on Cross Functional Projects and Committees *Target: 3/year*		
People: Industry & Technical Competence		
Training Hours Earned on Priority Skills *Target: 20 Hours*		
Average Certifications Held by Each Auditor Target: 1/auditor		
Active Participation in Professional Associations Target: 1/auditor		
Audit Process: Efficient & Effective Audit Process		
Staff Utilization *Target: 80%*	85%	84%
Individual audit project actual to budget hours variance *Target: 10% or less*		
Completion of Lean Project on Audit Processes *Target: 1/year*		
Costs contained/recovered/revenue enhancements identified ($); *Target: **Establish baseline in 2016/17***		
Plan: Relevance to Risks that Matter Most		
Audit resources dedicated to higher or emerging risk areas *Target: 75% Actual: 82.4%*		
Recommendations Made *Target: **Establish baseline in 2016/2017***	66	59

UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: June 8, 2017

COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: II.B. University Compliance Goals for Academic Division for FY 2018 (Written Report)

ACTION REQUIRED: None

BACKGROUND: Below are the institutional compliance goals identified by Gary Nimax, Assistant Vice President for Compliance, for fiscal year 2018.

Compliance Goals - Fiscal Year 2017-18
1. Review and update the university's Code of Ethics for approval by the Board of Visitors.
2. Complete the onboarding of the medical center's new Compliance and Privacy Officer, Regina Verde, including the operational changes necessary since that role was converted from an academic division position to a medical center position.
3. Review improvements to be made regarding the university's compliance with digital accessibility, background check policies, and UFirst project compliance requirements.
4. Use the results of 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 (legal, operational, and reputational), levels of effort necessary to address regulatory changes, regulatory scrutiny, and cross-functional coordination.
5. Expand marketing and use of the university's anonymous helpline in order to more effectively monitor compliance reporting.

UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: June 8, 2017

COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: II.C. Medical Center Compliance Program Goals for FY 2018 (Written Report)

ACTION REQUIRED: None

DISCUSSION: Below are the Medical Center compliance goals identified by Regina Verde, Corporate Compliance & Privacy Officer, for fiscal year 2018.

Compliance Goals Fiscal Year 2017-18
1. Rebuild the Medical Center Compliance & Privacy Office to create a complete team; continue to develop team members and Office function into an interactive and facilitative resource for the Health System, providing routine interaction and support to managers and their teams, scheduled and episodic compliance training, interactive assistance in issue resolution, as well as the standard functions of auditing and compliance investigation and documentation.
2. Evaluate the results of the compliance risk assessment conducted by former Medical Center compliance leaders in partnership with University Compliance, Internal Audit and General Counsel to ascertain risk levels to the Medical Center Compliance Program. Use this assessment to reexamine 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. Perform and oversee audits to assess compliance in high risk areas as identified by the FY 2017 Office of Inspector General/Health & Human Services Work Plan; audits will examine compliance with regulatory requirements for documentation of medical necessity for appropriate admissions, accurate coding, billing and reimbursement from Medicare for specific services, etc. The Office will work in conjunction with other functional areas in conducting these reviews.

UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: June 8, 2017

COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: III.A. Proposed FY 2018 – FY 2019 Audit Plan

BACKGROUND: The Audit, Compliance, and Risk Committee (the Committee) has oversight responsibility for UVA's internal audit program. The Committee assesses and approves the scope of audit activities outlined in the UVA Audit Department's annual plan.

UVA Audit's planning process filters risk inputs down to auditable risks, then considers them by degree of assurance required, risk impact, and available hours and resources. The result is a strategically relevant, risk-based, and dynamic plan that focuses on what needs to go right to achieve UVA's mission and objectives.

The chart that follows represents our current view of the topics and timing most relevant for audit attention. Because our plan is dynamic, we will adjust it as needed, in consultation with UVA leadership and the Audit, Compliance, and Risk Committee, to align with changes in risks and priorities.

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

AUDIT DEPARTMENT FY 2018-FY 2019 AUDIT PLAN

RESOLVED, the Audit Department FY 2018-FY 2019 Audit Plan is approved as recommended by the Audit, Compliance, and Risk Committee.

UVA Audit Department FY 2018-FY 2019+ Proposed Plan:

Education (Student Experience and Safety)			
Audit Topic	FY18	FY19+	ERM Risk Alignment
Admission Communications	X		Competitive Environment
Lab Safety (Undergrad)	X		Safety
Environmental Health & Safety	X		Safety
Student Health & Counseling		X	Safety
Dining and Residence Life Safety		X	Safety
Security and Integrity of Key Instructional Systems		X	IT Security
International Programs		X	Safety, IT Security
Clinical Care			
Legacy System Revenue Cycle	X		Technology
Epic Phase 2 Post-Implementation Revenue Cycle	X	X	Technology
Procurement Cycle Processes: Medical Devices		X	
Business Processes: • Financial Budgeting • Forecasting and Reserves • Clinical Trials Revenue		 X X X	
Research			
Pre-Award Processes	X	X	Research
Award Set Up Processes	X	X	Research
Award Management Procesess	X	X	Research
Closeout Processes	X	X	Research
Fundamental Business and IT Processes			
Ufirst HR Transformation Project Health Check	X	X	Resource Allocation
IT Security across UVA (includes SecureUVA, Medical Devices, Key IT Systems, Key Database Access	X	X	IT Security
Presidential and Executive Travel and Expenses	X	X	Leadership
UVA Travel and Expense Systems (New)	X		Resource Allocation
PCI Compliance	X	X	IT Security
Annual Inventories	X	X	
Construction Project Audits (co-sourced)	X	X	Resource Allocation
Strategic Investment Fund Reporting	X	X	Resources
Facilities Contract Management		X	Resource Allocation
Donor Gift Processing		X	Resources

UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: June 8, 2017

COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: III.B. Proposed Changes to Audit Department Charter to Conform to New IIA Standards

BACKGROUND: The UVA Audit Department follows the Institute of Internal Auditors' (The IIA) International Standards for the Professional Practice of Internal Auditing (Standards). An update to the Standards is effective beginning January 1, 2017.

We propose the following changes to the current Audit Department Charter:

1. The IIA's Mandatory Guidance must be recognized in the Charter. Mandatory Guidance includes the Core Principles for the Professional Practice of Internal Auditing; the Code of Ethics; the Standards; and the Definition of Internal Auditing. These are reflected in the updated Charter.
2. Core Principles for the Professional Practice of Internal Auditing must be referenced in the Charter. The Core Principles are used to evaluate the effectiveness of the internal audit function. We have added these to the Charter following Professional Standards.
3. Updates to the Chief Audit Executive's mandatory disclosure requirements related to the department's Quality Assurance and Improvement Program were made.
4. Clarification of the Chief Audit Executive's organizational reporting was made.

A marked up version of the current charter is provided to 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 University of Virginia Audit Department's charter, reflecting changes to conform to The IIA's recently updated professional standards, is approved as recommended by the Audit, Compliance, and Risk Committee.

UNIVERSITY OF VIRGINIA AUDIT DEPARTMENT CHARTER

~~Introduction~~**Purpose**:

Internal a~~A~~uditing is an independent, ~~and~~ 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 Audit 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. ~~that is guided by a philosophy of adding value to improve the operations of the University of Virginia and the University of Virginia Health System (the University). Its mission is to enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight.~~

~~Role~~**Internal Auditing Policy**:

It is the policy of the of the University to establish and support the Audit 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 ~~(i.e. day to day operations)~~ to the President of the University. ~~through her delegate, the Executive Vice President and Chief Operating Officer.~~

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 Audit 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 Audit 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 Audit 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 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 confirm to the ACR Committee annually the organizational independence of the Audit 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 Audit 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, responsibility 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: ~~Special Projects:~~

The Chief Audit Executive is empowered to conduct assurance services, special audit projects, reviews, ~~advisory services,~~ 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 Audit 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'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 Audit 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 ~~internal audit activity~~Chief Audit Executive must develop and ~~will~~ 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 ~~will include an evaluation~~ evaluate ~~of~~ the internal audit activity's conformance with the ~~Definition of Internal Auditing and 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 ~~will communicate to senior management and the ACR on the internal audit activity's quality assurance and improvement program, including results of ongoing internal assessments and external assessments conducted at least every five years~~must communicate results of the quality assurance and improvement program to senior management and the ACR Committee.

Updated on ~~September 18, 2015~~June 8, 2017

UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: June 8, 2017

COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: IV.A.1. Cost of Compliance

ACTION REQUIRED: None

DISCUSSION: Mr. Gary Nimax, Assistant Vice President for Compliance, will report to the board on the University's expenditures to comply with federal requirements. He will describe the estimate the University prepared of the overall cost to comply with various federal, state, and other regulatory requirements, and how the cost of compliance has changed over the last 10 years.

UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: June 8, 2017

COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: IV.A.2. Medical Center Compliance and Privacy Office Year-To-Date Perspectives

ACTION REQUIRED: None

DISCUSSION: Ms. Regina Verde, Corporate Compliance & Privacy Officer for the Medical Center, will report to the board, offering her perspective on the state of the Medical Center Compliance Program based on five months of experience. Points will be made that tie to the Medical Center Compliance Program Goals for FY 2018.

UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: June 8, 2017

COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: IV.B. Enterprise Risk Management (ERM) Report

ACTION REQUIRED: None

BACKGROUND AND DISCUSSION: Mr. James Matteo, Associate Vice President and Treasurer, will report on the ERM program and discuss the achievement of the FY 2017 priorities for the program. The priorities included repositioning the program, building a network of individuals to support the ERM effort, and, most importantly, onboarding the Health System into the ERM program.

The ERM program was repositioned to (1) shift the focus of the program toward enabling strategic goals through the identification of strategic risks and opportunities, and (2) align the annual ERM cycle with the planning and audit cycles.

Over the past 15 months, significant steps have been taken to develop a framework and governance model to support a robust ERM program. At its February 2016 meeting, the Board approved a new ERM charter that defines scope and responsibilities under the program. In the last quarter of FY 2016, we established a network of individuals to advance risk management efforts at the Academic Division and Health System, including:

- Risk Management Council - formed to provide guidance in support of the global ERM effort

- Risk Management Networks - in the Academic Division and Health System, comprised of representatives from major business units to help identify risks, including emerging risks, and serve as a connection between executive-level and department risk management activities.

Beginning in the first quarter of FY 2017, we undertook an effort to renew the Academic Division's risk register. We also began the process of onboarding the Health System and developed its inaugural risk register. With work for the Academic Division and Health System on parallel tracks, we presented the Academic Division's updated key risk list at the December 2016 BOV meeting. At the March 2017 BOV meeting we presented the Health System's key risk list. In addition to containing key risks, both lists established executive owners and risk leads, the individuals who have responsibility for developing risk management plans for the key risks.

Over the past three months, we have worked with the risk leads and executive owners to develop risk management plans for each of the key risks of the Academic Division and the Health System. As of the June 2017 BOV meeting, risk management plans have been completed for each key risk across both divisions.

The completion of the FY 2017 priorities ushers in the next generation of ERM at the University. The ERM program has been repositioned to better engage management in taking an active role in the process and providing them with the tools and language necessary to better manage institutional risks.