AUDIT, COMPLIANCE, AND RISK COMMITTEE
(Open Session)

Thursday, February 18, 2016
2:15 – 3:15 p.m.
Auditorium of the Albert & Shirley Small
Special Collections Library, Harrison Institute

Committee Members:
Frank E. Genovese, Chair  John G. Macfarlane III
Mark T. Bowles       Jeffrey C. Walker
L.D. Britt, M.D.       William H. Goodwin Jr., Ex-officio
Frank M. Conner III  Adelaide Wilcox King, Faculty
               Consulting Member

AGENDA

I. REMARKS BY THE COMMITTEE CHAIR  1

II. ACTION ITEMS
A. Enterprise Risk Management Program Plan and Charter  2
B. Compliance Program Charter  6

III. COMMITTEE DISCUSSION
• Audit Department Two Year Plan  11

IV. WRITTEN REPORTS
• Compliance Program: Medical Center's Corporate
  Compliance and Privacy Office Status Report for
  Fiscal Year 2015 – 2016  16

V. CLOSED SESSION
• Evaluation of the performance of specific
  personnel, consultation with legal counsel, and
  discussion of security-related matters and Medical
  Center operations as provided for in Section 2.2-
  3711(A)(1), (7), (19) and (22) of the Code of
  Virginia.
UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: February 18, 2016

COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: I. Remarks by the Committee Chair

ACTION REQUIRED: None

BACKGROUND: The Committee Chair will provide an overview of the agenda.
BACKGROUND: Mr. James Matteo, Associate Vice President and Treasurer, assumed responsibility for the University’s Enterprise Risk Management program in November, 2015. Mr. Matteo will present a plan to reposition and enrich the University’s ERM effort.

DISCUSSION: The three-part plan includes refreshing the University’s ERM framework, enhancing Board and management reporting, and introducing and integrating ERM at the Health System and College at Wise. The plan will advance the ERM program by building upon work already done and by coordinating with audit and compliance efforts at the University.

At this meeting, Mr. Matteo will present an ERM charter to define the scope and responsibilities of key parties for the committees consideration and approval.

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

ENTERPRISE RISK MANAGEMENT CHARTER

RESOLVED, the Enterprise Risk Management Charter is approved as recommended by the Audit, Compliance, and Risk Committee.
Introduction

The University of Virginia's Enterprise Risk Management (ERM) program is designed to provide reasonable assurance that the University is managing risks that impact its ability to achieve its objectives. Risk encompasses both negative events and missed opportunities and includes inherent as well as emerging risks. An effective ERM program helps the University effectively deploy its resources in pursuit of its objectives.

It is the approach of the University to establish and support the ERM Program to assist the University in accomplishing its objectives by facilitating management's processes for identifying potential events and risks that could affect its strategic plans and to coordinate its responses to mitigate such risks.

Scope

The scope of the ERM program will include risk management activities at the Academic Division, Medical Center, and College at Wise. The ERM function will work closely with the Audit and Compliance functions. Efficiencies are gained through collaboration among the three functions, including:

- Linking work across the enterprise risk assessment, audit plan, and compliance plan.
- Sharing available resources
- Cross-leveraging each function's competencies

This collaboration is accomplished while recognizing the distinct roles played by each party. The ERM program is responsible for leading ERM within the organization. Compliance is responsible monitoring and promoting adherence to laws and regulations. Internal Audit is responsible, in part, for examining and evaluating the adequacy and effectiveness of the University's governance, risk management, and internal controls.
Objectives

The objective of the ERM program is to provide reasonable assurance that the University is managing risks that impact its ability to achieve its objectives. This includes:

- Creating a framework to effectively identify, assess, and manage risk.
- Promoting collaboration to manage cross-functional risks
- Assist in defining risk appetite and aligning that with strategy
- Enhancing risk response decisions
- Incorporating risk in the decision to allocate resources

Roles and Organization

The University’s Treasurer is responsible for administering the University’s ERM program. The Treasurer reports to the Executive Vice President and Chief Operating Officer. ERM is a collaborative effort that includes involvement at various levels of the organization, including:

Operating Units

ERM should be integrated into a unit’s planning process. ERM should be part of assessing and implementing strategies related to strategic and operating objectives. Those responsible for managing unit budgets and programs are in the best position to manage risk. Leaders of individual schools and units will provide a key role in the day-to-day management of such risks and the execution of related mitigation strategies.

Risk Management Council

The Risk Management Council (“RMC”) is comprised of representatives from the major functional areas of the University, including the Health System. The RMC’s objectives are to provide a comprehensive assessment of risk at the University and provide reasonable assurance that the University is managing risks that impact its ability to achieve its objectives. This group would focus on both inherent risks and emerging risks, both of which are critically important. The RMC assesses risks and discusses risk mitigations approaches. The RMC will share these insights with the University’s executive leadership for discussion.
University Executive Leadership

The RMC will review key risks and mitigation strategies with the University's executive leadership. Executive leadership will help set the University's risk appetite, contribute to the assessment of risks, and provide guidance on how to report key risks to the ACR.

The Board of Visitor's Audit Compliance and Risk ("ACR") Committee

The ACR Committee will:

- Approve the Enterprise Risk Management Charter.
- Receive communications from the Treasurer on the University's Enterprise Risk Management assessment and mitigation efforts.
- Review, at least annually, the institutions risk governance framework including the risk assessment and mitigation strategies.
- Make appropriate inquiries of management and the Treasurer to determine whether all ERM efforts have the necessary resources and direction to be as effective as possible.

The Treasurer will communicate and interact directly with the Chair of the ACR committee, including in executive sessions and between ACR committee meetings as appropriate.
UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: February 18, 2016

COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: II.B. Compliance Program Charter

BACKGROUND: At its June 2015 meeting, the Board received information about the external assessment of the University’s internal audit program. The Quality Assurance Review (QAR) report recommended that there "...needs to be a charter for Compliance and the Enterprise Risk Management areas that clearly defines what the objectives are for these functions and how the Board expects them to interact with each other". The Audit Charter was approved by the Board at its September 2015 meeting.

DISCUSSION: Mr. Gary Nimax, Assistant Vice President for Compliance, will review the Compliance Charter for the Committee’s consideration and approval. The charter summarizes the mission and purpose of the compliance function for the University, including its Medical Center. 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 ERM functions.

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

COMPLIANCE CHARTER

RESOLVED, the Compliance Charter is approved as recommended by the Audit, Compliance, and Risk Committee.
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.

Organization

The Assistant Vice President for Compliance oversees institutional compliance activities and programs to confirm they are reasonably designed, implemented, communicated, and enforced.

The Assistant Vice President for Compliance reports to the Executive Vice President and Chief Operating Officer. The Assistant Vice President for Compliance coordinates the University-wide network of functional compliance officers.

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 Document 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 Internal Audit 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 complete self-assessments to 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 category 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.

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.
UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: February 18, 2016

COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: III. Audit Department Two Year Plan

ACTION REQUIRED: None

BACKGROUND: For purposes of supporting the Committee’s oversight of the Audit Department, Ms. Carolyn Saint, Chief Audit Executive, will discuss the Audit Department’s planned activities for FY 2016-FY 2017.
## People: Goals
- Develop and retain top talent
- Build risk and controls expertise, business acumen, leadership
- Create partnership with external firm for access to deep subject matter expertise as needed (co-source)

<table>
<thead>
<tr>
<th>Milestone Due Dates</th>
<th>FY 2016</th>
<th>FY 2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rebuild the team</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Hire Director Health System Audits</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>2. Select co-sourcing partner(s)</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>3. Recruit for vacant staff positions</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Increase proficiency</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Incorporate learning goals and annual training requirements into individuals’ annual performance goals</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>2. Develop training curriculum encompassing audit specific competencies, University-relevant business acumen, and leadership skills</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

## Audit Operations: Goals
- Accelerate organizational speed of execution
- Build quality and standards into audit methodologies and processes
- Expand use of data analytics in all aspects of audit cycle
- Define, track, and report audit value indicators

<table>
<thead>
<tr>
<th>Milestone Due Dates</th>
<th>FY 2016</th>
<th>FY 2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Productivity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Implement timekeeping system, define staff utilization goals</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>2. Begin tracking and reporting utilization metrics</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>3. Implement audit project portfolio management process</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Quality and standards</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Define and document audit methodologies for consistent project execution</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>2. Formalize internal quality assurance program</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>3. Standardize management action plan follow up process</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>4. Develop and implement ‘after-action’ process to embed continuous learning and improvement into the department</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
### Audit Operations: Goals (continued)
- Accelerate organizational clock speed
- Build quality and standards into audit methodologies and processes
- Expand use of data analytics in all aspects of audit cycle
- Define, track, and report audit value indicators

| Data analytics | 1. Execute data analytics strategy across training, audit methodology, and tool selection | X | X |
| 3. Identify audit value drivers. Define relevant data points for reporting metrics. | X |

| Technology: Goals | 1. Assess full capabilities of AutoAudit and align audit processes to capture technology’s value (scheduling, risk assessment, work flow, management action plan follow up, etc.) | X | X | X |
| Data analytics | 2. Based on data analytics strategy recommendations, implement/support selected data mining and visualization tools | X | X |

### Milestone Due Dates

<table>
<thead>
<tr>
<th></th>
<th>FY 2016</th>
<th>FY 2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feb-Jun '16</td>
<td>Jul-Dec '16</td>
<td>Jan-Jun '17</td>
</tr>
</tbody>
</table>

### Optimize Audit Workpaper system (AutoAudit)

- Employ technology to enable greater efficiency and effectiveness of Audit department
- Enable greater use of data analytics in audit processes as defined in the data analytics strategy

| 1. Assess full capabilities of AutoAudit and align audit processes to capture technology’s value (scheduling, risk assessment, work flow, management action plan follow up, etc.) | X | X | X |
| Data analytics | 2. Based on data analytics strategy recommendations, implement/support selected data mining and visualization tools | X | X |
## Risk Topic
<table>
<thead>
<tr>
<th>Audit Department Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk Topic</strong></td>
</tr>
<tr>
<td>Cybersecurity</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>IT Asset Management and System Security</td>
</tr>
<tr>
<td>IT Change Control and Configuration</td>
</tr>
<tr>
<td>Research Data and IT System Security</td>
</tr>
<tr>
<td>Research Grant Compliance</td>
</tr>
<tr>
<td>Fiscal Stewardship and Internal Controls</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Risk Topic</td>
</tr>
<tr>
<td>----------------------------------</td>
</tr>
<tr>
<td>Travel and Expense Management</td>
</tr>
<tr>
<td>Donor Gift Restrictions</td>
</tr>
<tr>
<td>Inventory Management</td>
</tr>
<tr>
<td>Business Continuity</td>
</tr>
<tr>
<td>Large Scale Program Risk</td>
</tr>
<tr>
<td>Healthcare Industry Consolidation</td>
</tr>
<tr>
<td>Patient Care and Safety</td>
</tr>
<tr>
<td>Legal and Regulatory Compliance</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>ERM Program Enhancements</td>
</tr>
</tbody>
</table>

The Audit Department Plan is continuously evaluated for relevance. Projects may be reprioritized to respond to emerging risks, changes in business strategies or plans, or business readiness for the audit.
BACKGROUND: Ms. Lori Strauss, the Chief Corporate Compliance and Privacy Officer for the Medical Center, prepared this written status report of her office’s activities for fiscal year 2015-2016. The report will inform the Board of compliance and privacy projects for the first six months of the fiscal year (FY). The report does not require formal action, but is information of which the Board should be made aware.

The Corporate Compliance and Privacy Office ("Office") is on target to complete 100% of the FY 2016 scheduled projects that were approved by the Audit, Compliance, and Risk Committee at its June 2015 meeting. Scheduled projects include hospital coding, billing, and documentation audits of inpatient, outpatient, and procedure area claims; privacy site audits of inpatient, outpatient, and procedure areas; and preparing and presenting compliance and privacy training. The project schedule is developed by incorporating risk areas identified in the Department of Health and Human Services Office of the Inspector General (DHHS-OIG) Work Plan, regulatory risk topics, industry publications, recent settlements and corporate integrity agreements of other organizations, federal and state agency compliance and privacy reviews, management’s feedback, and internal requests.

The OIG Work Plan provides valuable insights for the UVA Medical Center by providing the OIG’s planned areas of focus for investigation and enforcement activities. The Office uses the Work Plan as a tool to assess if areas are risks for the Medical Center, suggesting that the Office should audit Medical Center processes to ensure they are working as expected.
The Office provides department-specific compliance and privacy training as requested; performs hospital documentation, coding, billing, and privacy auditing and monitoring as identified; conducts compliance reviews of Medical Center and Health System policies and procedures; and provides guidance on regulations, rules and laws.

Office staff serve on several committees to provide compliance and privacy guidance. The committees include Grievance, Quality, Health Information Management, Laboratory Compliance, Clinical Information and Technology Oversight, and Ethics, among others. Office staff are sought to review and provide feedback on compliance and privacy policies and procedures, including Compliance Code of Conduct, Documentation of Patient Care, Requests for Restriction of Patient Information, Access to Electronic Medical Records and Institutional Computer Systems, Clinical Staff Code of Conduct, and Violations of Confidentiality.

Office staff are consulted regularly by staff, management, clinicians, and others to locate regulations, provide input on Medical Center policy and procedure revisions, assess clinical areas and new locations for privacy safeguards, and provide guidance on compliance and privacy inquiries.

The Office provides ongoing education and training using various delivery methods. The privacy and compliance web-based training modules for newly hired employees were reviewed and revised to incorporate changes to policies and procedures regarding accessing one’s own medical record. All Medical Center employees as well as any individual that works in or on behalf of the Medical Center must complete these modules as a new hire. Office staff communicate with area managers of 14 departments regarding their new employees and assign the new hire privacy module for the Health Insurance Portability and Accountability Act hybrid areas identified as part of the Medical Center’s covered entity. Monthly privacy or compliance reminders are provided for the Medical Center’s Management Group to share with employees, highlighting topics from the Department of Health and Human Services Office for Civil Rights, audit trends, and policy changes. The topics during the first six months of the fiscal year included the policy change on accessing one’s own record; internet and intranet access and usage specifying encryption and appropriate cloud usage; violations of confidentiality and notification of Human Resources; incidental uses and disclosures of protected health information and safeguards; and identity theft red flags and
notification. Three department-specific privacy training sessions were provided for the Graduate Medical Education orientations and for the Ophthalmology Department.

The Office had a vacant Compliance and Privacy Specialist position for approximately 2 months in the beginning of the fiscal year. The staff prioritized projects and shared duties to meet the needs of the Medical Center during the vacancy. The Office’s employees have completed training and demonstrated proficiency by obtaining certification in ICD-10 coding as required to perform their work duties. ICD-10 coding was implemented on October 1, 2015 as scheduled with no unforeseen consequences thus far. EPIC, the electronic medical record, Phase II is to be implemented on July 1, 2017 and will include registration, scheduling, and hospital and professional billing; therefore, Office staff participated in the EPIC Phase II Development and Adoption sessions to learn of the anticipated system operations and to offer guidance as needed for the system builders.