TO: The Audit, Compliance, and Risk Committee:

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

and

The Remaining Members of the Board:

Frank B. Atkinson Victoria D. Harker
Whittington W. Clement Bobbie G. Kilberg
Helen E. Dragas Tammy S. Murphy
Kevin J. Fay James V. Reyes
Barbara J. Fried Joe Garofalo, Faculty Member
John A. Griffin Daniel T. Judge, Student Member

FROM: Susan G. Harris

SUBJECT: Minutes of the Meeting of the Audit, Compliance, and Risk Committee on February 18, 2016

The Audit, Compliance, and Risk Committee of the Board of Visitors of the University of Virginia met, in Open Session, at 2:15 p.m., on Thursday, February 18, 2016, in the Auditorium of the Albert and Shirley Small Special Collections Library of the Harrison Institute. Frank E. Genovese, Chair, presided.

Present were William H. Goodwin Jr., Mark T. Bowles, L.D. Britt, M.D., Frank M. Conner III, John G. Macfarlane III, Jeffrey C. Walker, and Adelaide Wilcox King.

Frank B. Atkinson, Whittington W. Clement, Kevin J. Fay, Barbara J. Fried, and James V. Reyes were also present.
Present as well were Teresa A. Sullivan, Patrick D. Hogan, Thomas C. Katsouleas, Melody S. Bianchetto, Susan G. Harris, Donna P. Henry, W. Thomas Leback, David W. Martel, Debra D. Rinker, Nancy A. Rivers, Colette Sheehy, and Farnaz F. Thompson.

Presenters were James S. Matteo, Gary S. Nimax, Carolyn D. Saint, and Lori J. Strauss.

Mr. Genovese opened the meeting. After reviewing the agenda, he reported that the University separated the administrative responsibilities for compliance and enterprise risk management programs to increase the attention devoted to these two areas.

Action Item: Enterprise Risk Management Program Plan and Charter

Mr. James Matteo, Associate Vice President and Treasurer, reviewed the plan for the Enterprise Risk Management (ERM) program and the amended ERM charter. The plan has three priorities and three objectives. The first priority is to reposition and enrich the program by introducing a Risk Management Council, aligning the framework with best industry practices, and positioning the program so that ownership of the risk lies with the operating units. The second priority is to enhance and streamline Board reporting. The third is to integrate risk management at the Health System with the University’s program. The objectives are to synchronize University-wide risk management efforts, integrate the program with strategic planning and budgeting, and develop a proactive approach to identify, assess, and monitor key risks.

The amended charter clarifies the program’s objectives; establishes its scope; outlines the relationship with the audit and compliance functions; and clarifies the roles of the University’s executive leadership, the Risk Management Council, and the operating units. The Enterprise Risk Management Charter is attached to these Minutes.

On motion, the following resolution was approved by the committee.

ENTERPRISE RISK MANAGEMENT CHARTER

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

Action Item: Compliance Program Charter

Mr. Gary Nimax, Assistant Vice President for Compliance, reviewed the seven elements from the Federal Sentencing Guidelines that compliance professionals consider to be the components of an effective compliance program.
Mr. Nimax explained that the compliance network at the University is comprised of individuals responsible for compliance in their respective areas. While these individuals report to their vice presidents or managers, they are also responsible to Mr. Hogan and Mr. Nimax. They meet regularly with Mr. Hogan and Mr. Nimax to review compliance initiatives, share best practices, discuss changes in the compliance field, and identify projects of mutual interest.

The Compliance Charter summarizes the compliance mission; describes the operation of the compliance network; outlines the process for meeting the seven compliance program elements; specifies professional standards and responsibilities; outlines the interaction between the compliance, internal audit, and ERM functions; and addresses the role of the Audit, Compliance, and Risk Committee. The Charter incorporates best practices from the compliance charters of other institutions of higher education. The Compliance Charter is attached to these Minutes.

On motion, the following resolution was approved by the committee.

COMPLIANCE CHARTER

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

Audit Department Two Year Plan

Ms. Carolyn Saint, Chief Audit Executive, provided an overview of the goals and audits in the work plan for the 2016 and 2017 fiscal years. Goals focus on personnel, operations, and technology. Personnel goals include rebuilding the audit team. In lieu of immediately hiring new auditors, the department will consider hiring firms to provide services in areas where they have expertise and where it would be too difficult or too expensive to build in-house expertise. Operational goals include accelerating the execution of audits, building quality standards into audit methodologies, and expanding the use of data analytics. Technology goals include optimizing technology to improve efficiency.

Proposed audits include research grant compliance, legal and regulatory compliance, assessment of enterprise wide risk management, and an evaluation of the effectiveness of the University’s decentralized compliance function.

Medical Center’s Corporate Compliance and Privacy Office Status Report for Fiscal Year 2015-2016

Committee members did not question or comment on the written report in the committee materials.
Executive Session

The following motion was read and approved, and the committee continued in closed session at approximately 2:55 p.m.:

I move that the committee go into closed session to evaluate the performance of specific personnel; to consult with legal counsel; and to discuss Medical Center operations, as provided for in Sections 2.2-3711(A)(1), (7), and (22) of the Code of Virginia.

At 3:00 p.m. the committee concluded closed session and approved the following motion:

I move that we vote on and record our certification that, to the best of each member’s knowledge, only public business matters lawfully exempted from open meeting requirements and which were identified in the motion authorizing the closed session, were heard, discussed or considered in closed session.

On motion, the committee adjourned at 3:00 p.m.

SGH:wtl
These minutes have been posted to the University of Virginia’s Board of Visitors website:  http://www.virginia.edu/bov/auditminutes.html
ATTACHMENTS
UNIVERSITY OF VIRGINIA
ENTERPRISE RISK MANAGEMENT CHARTER

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. Leaders of individual schools and units play a unique and essential role with regard to ERM. Within their units, they are in the best position to ensure a pervasive ERM culture, and to develop processes, that can be vital in identifying and assessing exposure to critical risks. These leaders also play 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 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.

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 wrongdoing 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.