UNIVERSITY OF VIRGINIA
BOARD OF VISITORS
MEETING OF THE
AUDIT AND COMPLIANCE
COMMITTEE

November 15, 2013
AUDIT AND COMPLIANCE COMMITTEE

Friday, November 15, 2013
9:45 a.m. – 10:45 a.m.
President’s Reception Room, The Rotunda

Committee Members:
Hunter E. Craig, Chair
Frank B. Atkinson    John L. Nau III
Kevin J. Fay    Linwood H. Rose
Frank E. Genovese    George Keith Martin, Ex-officio
Victoria D. Harker    Adelaide Wilcox King, Faculty
Bobbie G. Kilberg    Consulting Member

AGENDA

I.  ACTION ITEM (Ms. Barbara J. Deily)
   • Audit Charter  1

II. INFORMATION ITEMS
   A. Auditor of Public Accounts (APA) Audit and    2
      Management Report (Ms. Deily to introduce
      Ms. Karen Helderman, Ms. Helderman to report)
   B. Report from the Assistant Vice President    3
      for Compliance and Enterprise Risk Management
      (Ms. Deily to introduce Mr. Gary Nimax, Mr.
      Nimax to report)
   C. Summary of Audit Findings  5

III. EXECUTIVE SESSION – LIST OF ITEMS

IV.  ACTION ITEM
   • Approval of the Summary of Audit Findings  12

V.  Attachment
   • Audit Charter
UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: November 15, 2013

COMMITTEE: Audit and Compliance

AGENDA ITEM: I. Audit Charter

BACKGROUND: Ms. Barbara J. Deily, Chief Audit Executive, will present the Audit Charter for approval. As a result of a Quality Assessment Review in 2004, it was agreed that, at a minimum, the Board would review and approve the Audit Charter every time there was a change in the Audit and Compliance committee chair. Given the frequency of change in committee chair assignments, we now have defaulted to an annual review.

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

APPROVAL OF THE AUDIT CHARTER

RESOLVED, the attached Audit Charter, updated on November 15, 2013, is approved as recommended by the Audit and Compliance Committee.
UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: November 15, 2013

COMMITTEE: Audit and Compliance

AGENDA ITEM: II.A. Auditor of Public Accounts (APA)
Audit and Management Report

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 to the Board on her findings. Ms. Deily will introduce Ms. Karen Helderman, who will report. This will be a high level report with preliminary findings. The APA will make a full report of all their work in February 2014 as usual.

Karen Helderman is an audit director with the Office of the Auditor of Public Accounts and has more than 27 years of audit experience. She specializes in managing audits that are highly automated and also serves as a systems development audit director. Since 2003, much of her work has involved following Virginia’s activities to consolidate the IT infrastructure, develop project management standards, and replace existing central administrative systems. Karen and her team have made recommendations on these activities and other major systems development initiatives in numerous audit reports.

Ms. Helderman graduated with a bachelor’s degree in accounting from Christopher Newport University and is currently enrolled in Virginia Tech’s MBA program. She is a certified public accountant, a certified information systems auditor, and a project management professional. She currently serves as vice-chair of the National State Auditor’s Association E-Government Committee.
BACKGROUND: Beginning in 2008, the University worked with KPMG to conduct an initial assessment of the University's current framework for assessing and managing the University's strategic and high-level operational risks. There were two phases to the ERM project. In Phase I, the University explored the feasibility and desirability of developing a framework that could link the different risk management programs which are already in place. As part of Phase II, KPMG conducted interviews with selected University officials and members of the Board of Visitors to begin developing the University's portfolio of top risks.

At the November 15, 2010 meeting of the Finance Committee, President Sullivan reported that the consolidated risk register had been reviewed by the vice presidents, who identified the most significant risks in their areas. From that list the vice presidents identified the top five institutional risks.

The top risks identified at that time included a lack of resources to maintain core programs and pursue strategic objectives, a process for allocating financial resources that may not be consistent with the University's strategic initiatives, the utilization of funding to promote individual school/department goals rather than institutional goals, investments in academic programs that may not yield the desired returns, and incidents related to safety in general.

The University will be updating its risk register given the turnover in senior administration and board members, the new strategic plan and internal financial model, and changes in the higher education landscape.
DISCUSSION: In April 2013, Pat Hogan named Gary Nimax as the Assistant Vice President for Compliance and Enterprise Risk Management. Mr. Nimax will review the University’s ERM program with the committee and discuss related goals for fiscal year 2013-14:

1. Reenergize ERM efforts, started in 2008 with KPMG, in which we assessed strategic and high-level operational risks.
2. Review institutional risks identified in the initial risk register to identify the university’s current top risks and document mitigation efforts.
3. Develop tools to assist the university in discussing and evaluating risks associated with major University initiatives.
4. Seek ways to incorporate ERM principles into our strategic plan to document how we will identify and mitigate related risks.

Gary Nimax serves as the Assistant Vice President for Compliance and Enterprise Risk Management. His responsibilities include the creation of a new compliance and enterprise risk management office, as well as the supervision of the Director of Property and Liability Risk Management and the Medical Center’s Chief Corporate Compliance and Privacy Officer.

Mr. Nimax has worked at the University since 1989 in a variety of administrative roles, including positions as a buyer in the medical center, as Assistant Director of Procurement Services for the Academic Division, as team lead for the Integrated Systems Project, as Assistant to the Vice President for Management and Budget, and most recently as the Assistant Vice President and Director of University-Related Foundation Administration.

Mr. Nimax earned his undergraduate degree from UVA and his Master of Business Administration from James Madison University. He obtained his professional certification as a Certified Compliance and Ethics Professional (CCEP) through the Society of Corporate Compliance and Ethics.
UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: November 15, 2013

COMMITTEE: Audit and Compliance

AGENDA ITEM: II.C. Summary of Audit Findings

ACTION REQUIRED: None

BACKGROUND: Ms. Deily will present a summary of audit findings on the following audit reports: Health System Sensitive Information Management and Control, University Sensitive Information Management and Control, and Office of Sponsored Programs (OSP) Pre-Award Services.
BACKGROUND

The University of Virginia Health System (HS) managed sensitive data based on the assumption that all HS computers and networks contain sensitive information. Therefore, the HS encrypted all local workstation (desktop) computers to protect the information. To the extent possible, HS encrypted information stored on the network as well. This audit did not review encryption of mobile devices. HS recently purchased a Symantec Data Loss Prevention (DLP) product to monitor data transmissions leaving the Health System’s network and to identify if these transmissions contain any sensitive information. Future plans were to extend use of the DLP product to restrict unencrypted sensitive information from being sent out of the network and to scan network servers and workstations for unnecessary sensitive information. HS has also purchased ZixMail, an encrypted email solution, for emailing sensitive information. Sensitive information has numerous inherent risks. Unidentified sensitive information may be inadequately protected and vulnerable to theft or loss. Inadequate physical and logical protection over sensitive information may also lead to theft or loss. Finally, lack of management oversight may lead to unenforced policies and standards.

AUDIT OBJECTIVES

Audit objectives included a review of sensitive information strategic planning and management; policy, standards and procedures; HS management and control processes; local workstations protection; and network server protection.

OPINION ON AUDIT OBJECTIVES

Overall, it appeared that management and security in place for the HS sensitive information were fairly stringent. HS management was receptive to our verbal comments regarding extending the use of the DLP product to network servers and local workstations.

MANAGEMENT’S RESPONSE

Management concurs and has agreed to consider our verbal recommendations.
IMPACT TO THE UNIVERSITY

The impact of proper security surrounding sensitive information management and control is always important in the Health System environment because of the following concerns:

- Public relations issues,
- HIPAA/FERPA/PCI non-compliance, and
- Monetary loss as a result of lawsuits related to the disclosure of sensitive information.
BACKGROUND

The Information Security Policy and Records Office (ISPRO) facilitated the 2008 University Social Security Number Remediation Initiative (Initiative) directing departments and schools to discontinue collecting social security numbers (SSN) unless needed to conduct business or required by law. The University assigned departments and schools responsibility for identifying where sensitive information was stored and for removing or protecting the sensitive information as appropriate. Additionally, the University issued the Electronic Storage of Highly Sensitive Data Policy and Institutional Data Protection Standards. The Electronic Storage of Highly Sensitive Data Policy defined sensitive information and provided high level guidance on periodically scanning workstations for sensitive information, remediating exceptions, and obtaining approval when sensitive information needed to be maintained. The Institutional Data Protection Standards identified general controls for storing sensitive information.

AUDIT OBJECTIVES

Audit objectives included a review of sensitive information strategic planning and management; policy, standards and procedures; University department and school management and control processes; and higher level reviews of local workstations protection and network server protection.

OPINION ON AUDIT OBJECTIVES

The University policy, standards, and procedures related to sensitive information management and control required improvement to ensure proper management oversight and control practices.

AREA NOTED FOR IMPROVEMENT

University policy, standards, and procedures related to sensitive information required improvement to properly address sensitive information scanning and management oversight.

MANAGEMENT'S RESPONSE

Management concurs and has agreed to correct the identified condition.
IMPACT TO THE UNIVERSITY

The impact of proper security surrounding sensitive information management and control is always important in the University environment because of the following concerns:

- Public relations issues,
- HIPAA/FERPA/PCI non-compliance, and
- Monetary loss as a result of lawsuits related to the disclosure of sensitive information.
BACKGROUND

The pre-award function within the Office of Sponsored Programs (OSP) and their designee, School Of Medicine Grants and Contracts Office, facilitates the performance of research and management of proposal preparation and submission to numerous sponsors on behalf of the University. Grant administrators assist faculty and research administrators with proposal preparation, proposal review, proposal submission, award management, sub-awards, and negotiation of terms and conditions. The negotiation of terms and conditions include: sponsored research agreements, clinical trial agreements, material transfer agreements, and confidentiality agreements. Another essential responsibility of the pre-award function is to ensure regulatory compliance through the proposal review prior to the acceptance of the award and during the negotiation of terms and conditions.

AUDIT OBJECTIVES

The objectives of this audit were to determine whether: 1) the pre-award process for submitting grant proposals to sponsors on behalf of the University was efficient and effective; and 2) compliance with University policies and procedures, and where applicable, Federal regulations, was maintained in preparing and submitting the grant proposals.

OPINION ON AUDIT OBJECTIVES

The operational efficiency of the OSP’s pre-award function could be improved by implementing an electronic research administration system in order to maximize the ability of the University to submit proposals in a timely manner. Except for one issue where an internal document was missing the signature of the Principal Investigator, the pre-award function was in compliance with University policies and procedures, as well as with Federal regulations.

AREAS NOTED FOR IMPROVEMENT

1) The University should consider implementing an electronic research administration system that would enhance the efficiency of the current manual, paper-laden, pre-award, grant proposal process.
2) University policy should be followed in regard to ensuring that all signatures are obtained prior to submission to the sponsors.

MANAGEMENT’S RESPONSE

Management concurs and has agreed to correct the identified conditions.

FINANCIAL IMPACT

In fiscal year 2011-12, OSP processed approximately $300 million in grant awards. In an environment that is increasingly competitive to obtain grant awards, an integrated electronic research administration system could better position the University for receiving grants.
BOARD MEETING: November 15, 2013

COMMITTEE: Audit and Compliance

AGENDA ITEM: IV. Approval of the Summary of Audit Findings

BACKGROUND: This resolution reflects discussion by the Committee, in Executive Session, of a summary of recent audits conducted by the Audit Department.

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


RESOLVED, the Summary of Audit Findings for the period August 15, 2013 through September 30, 2013, as presented by the Chief Audit Executive, is approved as recommended by the Audit and
AUDIT CHARTER

It is the policy of the University to establish and support the Audit Department for the purpose of assisting management in the effective discharge of its responsibilities for the control of University resources.

The mission and objectives of the Audit Department are to add value to the organization and improve institutional operations through a variety of methods including:

Evaluating and advising on improving the effectiveness of institutional processes and programs for governance, control and enterprise risk management.

Performing financial audits for the purpose of ensuring that:

(a) Cash, accounts receivable, and other assets of the University are promptly and completely recorded, accounted for, authorized, and adequately safeguarded against losses and misappropriation.

(b) Liabilities of the University have been properly incurred and are properly recorded and discharged. Audits directed to financial accountability will include a review of records, source data, fiscal procedures, and internal controls.

Performing operational audits for the purpose of ensuring that University operations are conducted efficiently, effectively, and in accordance with appropriate and adequately documented policies, plans, and procedures. Operational audits will encompass a review of the policies, plans, procedures, organizational structure, staffing, and output of the audited unit. These audits also will include evaluating the accomplishment of established objectives and goals for operations and programs.
Providing the Board of Visitors and senior management with an independent, fair, and objective appraisal of the effectiveness of the University's financial accountability systems and operational performance in accordance with the priorities established by the Chief Audit Executive in coordination with the Board of Visitors, the President, and the Executive Vice Presidents and approved by the President and the Board of Visitors.

Providing management with constructive criticism and positive recommendations designed to strengthen and improve performance results and cost effectiveness of their operations.

Informing the Board of Visitors and Senior University management of any financial irregularities, investigations, or other risks to the institution that the auditors discover during the course of their work.

The work of the Audit Department will be conducted in accordance with the International Standards for the Professional Practice of Internal Auditing as promulgated by the Institute of Internal Auditors. Other professional standards, such as the Government Accounting Office "Yellow Book," shall be utilized when appropriate.

The following policies identify the responsibilities of the Audit Department and provide guidelines for its interaction with all University departments and activities.

Organizational Responsibilities

The Chief Audit Executive shall be responsible to the Board of Visitors but shall maintain a dual reporting relationship to both the Board and the President. The Chief Audit Executive will seek input on the department's activities from the Board of Visitors, the President, and the Executive Vice Presidents. The Chief Audit Executive will have unrestricted access to the President and the Board of Visitors. The Chief Audit Executive is responsible for the direction of the audit function and for seeing that the results of examinations
and actions taken are communicated to appropriate levels of University management and, as appropriate, the President and the Board of Visitors.

The Chief Audit Executive will draft an annual audit plan and will solicit input on this plan from the Board of Visitors, the President, the Executive Vice Presidents, and other senior management of the institution. The plan will be submitted to the Board of Visitors for approval.

Nothing herein shall be construed as preventing the Chief Audit Executive from consulting with the President and the Executive Vice Presidents on activities of the department, its findings, or significant issues. Nor shall the President and the Executive Vice Presidents be prevented from consulting with the Chief Audit Executive as may be necessary to the execution of their duties.

The Audit Department will give full consideration to scheduling special audit requests made by any department or activity. All requests should be in writing to the Chief Audit Executive and state the purpose and scope of the audit.

Independence

The Audit Department will be organizationally and functionally independent from all University operations and will have no responsibility for the departments and activities being audited while being responsive to their needs and requirements. Because the Audit Department must be independent in carrying out its responsibility to monitor and evaluate control procedures instituted by management, the extent of audit work to be performed with respect to those procedures is limited to the assessment of such procedures.

The Audit Department normally performs tests of underlying records and documentary support for transactions. Accordingly, objectivity would be lost if the Audit Department routinely participated in accumulating data or reconstructing records.
Authorities and Limitations

The Audit Department personnel will have complete, free, and unrestricted access to all University departments, activities, records, properties, and personnel, and is not to be restricted in their activities. Where appropriate, special arrangements will be made for the examination of confidential information.

Systems Planning and Development

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 in 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.

The Audit Department will conduct post-installation evaluations of major information technology systems to ensure that these systems meet their intended purpose and objectives. The department will also review computer operations supporting such systems to ensure that generally accepted standards for systems integrity and security, as well as system-specific controls, are being observed.

Security Investigations

The Audit, Risk Management and University Police Departments are to be notified if assets have been lost through defalcation or other security breaches. The Audit Department will perform sufficient tests and investigations to identify the weaknesses in procedures, which permitted the defalcation to occur. However, the investigation of the specific event with the objective of recovery and/or prosecution is the responsibility of
the University Police Department, with the decision to prosecute being the responsibility of the appropriate Commonwealth’s Attorney.

Coordination with External Auditing Agencies

The Chief Audit Executive will coordinate the department’s audit efforts with those of the University’s independent public accountants or other external auditing agencies 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. Duplication of work will be avoided as much as possible.

Reporting

Prior to the completion of a formal report, an exit conference will be conducted with the department or activity head. The conference will be a review of all findings, conclusions, and recommendations. A formal report will be issued at the conclusion of every audit, which will present a concise, clear and factual review of the conditions found, together with recommendations for improvement. A formal written response shall be issued to the Chief Audit Executive, or the Audit Director issuing the report, within 30 days addressing each finding, recommendation, and exception included in the audit report. This response will include the department’s or activity’s plan for implementing the recommendations or a presentation of significant disagreement with the findings and/or recommendations.

A follow-up review of significant audit recommendations will be made by the Audit Department to establish that agreed-to recommendations have been adopted. A memorandum will be issued on the follow-up review to the President, the Executive Vice President and Chief Operating Officer, the Executive Vice President and Provost, and the Executive Vice President for Health Affairs as appropriate.
Distribution of Reports

Audit reports will be issued to the Executive Vice President or Vice President most directly responsible for the department or activity involved. In addition, copies of all such reports will be distributed to the President, the Executive Vice President and Chief Operating Officer, and the senior fiscal administrator having a functional interest in the subject matter.

All audit reports will be available for review by the Board of Visitors.

A summary of significant audit findings will be prepared for each Board meeting and submitted to the Board of Visitors, the President, the Executive Vice President and Chief Operating Officer, the Executive Vice President and Provost, and the Executive Vice President for Health Affairs as appropriate.