UNIVERSITY OF VIRGINIA
BOARD OF VISITORS
MEETING OF THE
AUDIT AND COMPLIANCE
COMMITTEE
NOVEMBER 14, 2014
AUDIT AND COMPLIANCE COMMITTEE

Friday, November 14, 2014
8:30 – 9:30 a.m.
Auditorium of the Albert and Shirley Small
Special Collections Library, Harrison Institute

Committee Members:
Frank E. Genovese, Chair
L.D. Britt, M.D.
Allison Cryor DiNardo
Barbara J. Fried
William H. Goodwin Jr.
George Keith Martin, Ex-officio
Adelaide Wilcox King, Faculty Consulting Member

AGENDA

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

II. INFORMATION ITEMS
A. Auditor of Public Accounts (APA) Audit and Management Report (Ms. Deily to introduce Ms. Karen Helderman; Ms. Helderman to report) 2
B. Discussion on the Expanded Role of the Audit and Compliance Committee (Mr. Genovese) 3
C. Compliance Report on Revised Project Schedule (Written Report) 4
D. Summary of Audit Findings 6

III. EXECUTIVE SESSION – LIST OF ITEMS

IV. ACTION ITEM
   • Approval of the Summary by the Auditor of Public Accounts and the Summary of Internal Audit Findings 11

V. ATTACHMENTS
   1. Audit Charter
   2. Enterprise Risk Management Slides, June 5, 2014
UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: November 14, 2014

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 an annual review.

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

AUDIT CHARTER

RESOLVED, the attached Audit Charter, updated on November 14, 2014, is approved as recommended by the Audit and Compliance Committee.
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 on findings for the fiscal year 2013-2014 audit.

Karen Helderman is an audit director with the Office of the Auditor of Public Accounts and has more than 28 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.
UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: November 14, 2014

COMMITTEE: Audit and Compliance

AGENDA ITEM: II.B. Discussion on the Expanded Role of the Audit and Compliance Committee

ACTION REQUIRED: None

BACKGROUND: With the appointment of the Assistant Vice President for Compliance and Enterprise Risk Management in 2013, the Audit and Compliance Committee began receiving reports covering Enterprise Risk Management (ERM). Consequently, the Committee’s role has expanded beyond audit and compliance matters to include the overall risk management program at the University. ERM background slides from the June 2014 Board meeting are included as an attachment to the Committee booklet.

DISCUSSION: Given the expanded role of the Committee in overseeing ERM efforts, a suggestion has been made to revise the charge of the Committee to encompass other risk-related activities. This discussion provides an opportunity for recommendations from the Committee.

The discussion should include:

1) whether the role of the committee should be formally expanded,
2) how to best report on key institutional risks in the future,
3) what criteria should be used in bringing risk areas to the Board (for ERM, Audit & Compliance),
4) whether a change in the name of the committee would be warranted, e.g. "Audit and Risk Committee", and
5) how the scope of the committee would be described to encompass the change.
UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: November 14, 2014

COMMITTEE: Audit and Compliance

AGENDA ITEM: II.C. Compliance Report on Revised Project Schedule (Written Report)

ACTION REQUIRED: None

BACKGROUND: Each year the Board approves the project schedule for the Office of Corporate Compliance at the Health System. Significant revisions to the schedule are presented to the Board. This report does not require formal action, but is information of which it should be made aware.

DISCUSSION: As the result of an extended vacancy, the original project schedule has been revised. The revised schedule is presented below.

Corporate Compliance and Privacy Office
Determination of Hours Available for 2014-2015
Corporate Compliance and Privacy Projects
REVISED PROJECT SCHEDULE NOVEMBER 2014

<table>
<thead>
<tr>
<th>Fiscal Year 2014-2015</th>
<th>TOTAL</th>
<th>REVISED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Hours Available</td>
<td>8,320</td>
<td>8,320</td>
</tr>
<tr>
<td>Less: Vacancies</td>
<td>-0-</td>
<td>1,560</td>
</tr>
<tr>
<td>Sub-Total</td>
<td>8,320</td>
<td>6,760</td>
</tr>
<tr>
<td>Professional Development</td>
<td>320</td>
<td>260</td>
</tr>
<tr>
<td>Leave and Holidays</td>
<td>1,160</td>
<td>940</td>
</tr>
<tr>
<td>Other Activities: Office and Personnel Administration</td>
<td>320</td>
<td>260</td>
</tr>
<tr>
<td>Hours Available for Compliance &amp; Privacy Projects</td>
<td>6,520</td>
<td>5,300</td>
</tr>
</tbody>
</table>
### Allocation of Hours Available for Corporate Compliance & Privacy Projects

**Fiscal Year 2014-2015**

<table>
<thead>
<tr>
<th>Description</th>
<th>Total</th>
<th>REVISED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hours Available for Compliance &amp; Privacy Projects</td>
<td>6,520</td>
<td>5,300</td>
</tr>
<tr>
<td>Consulting: Policy and Procedure Reviews, Guidance</td>
<td>420</td>
<td>420</td>
</tr>
<tr>
<td>Developing and Conducting Training: Department-Specific Training, Website Content, Communications</td>
<td>300</td>
<td>300</td>
</tr>
<tr>
<td>Unscheduled Compliance Projects: Investigations, Industry Alerts, Management Requests</td>
<td>1,500</td>
<td>1,500</td>
</tr>
<tr>
<td>Unscheduled Privacy Projects: Investigations, Notice Revisions, Risk Assessments, Breach Notifications</td>
<td>1,500</td>
<td>1,500</td>
</tr>
<tr>
<td>Hours Available for Compliance &amp; Privacy Scheduled Projects</td>
<td>2,800</td>
<td>1,580</td>
</tr>
</tbody>
</table>

### Corporate Compliance & Privacy Projects
**Fiscal Year 2014-2015**

<table>
<thead>
<tr>
<th>Scheduled Projects</th>
<th>HOURS</th>
<th>REVISED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outpatient &amp; Procedure Coding, Billing, &amp; Documentation</td>
<td>800</td>
<td>250</td>
</tr>
<tr>
<td>Privacy Auditing and Monitoring: Monthly Site Visits</td>
<td>400</td>
<td>400</td>
</tr>
<tr>
<td>Inpatient Medicare Severity Diagnosis Related Groups: Correct Coding and Medical Necessity</td>
<td>1,200</td>
<td>530</td>
</tr>
<tr>
<td>Compliance and Privacy Training: Annual, New Hire, Hybrid</td>
<td>400</td>
<td>400</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>2,800</td>
<td>1,580</td>
</tr>
</tbody>
</table>
BOARD MEETING: November 14, 2014

COMMITTEE: Audit and Compliance

AGENDA ITEM: II.D. Summary of Audit Findings

ACTION REQUIRED: None

BACKGROUND: Ms. Deily will present a summary of audit findings on the following audit reports: University Accounting and Finance; and Medical Center Employee Access Management.
BACKGROUND

The mission of the Office of the University Comptroller (Comptroller’s Office) is to provide financial and administrative leadership and services of the highest quality to the University community. The Comptroller’s Office currently has a staff of thirty employees and is divided into four major units: Financial Analysis; Financial Operations and University Reporting; Training and Outreach; and Tax Compliance and Operational Contracts. Current responsibilities include: (1) recording and reporting the movement of monies through the University’s accounts; (2) negotiating, approving, and administering certain contracts made between the University and external entities; (3) preparing official institutional financial, tax compliance, and other regulatory reports and statements; (4) conducting financial studies and analyses, and preparing executive and departmental management information; (5) ensuring compliance with Federal, State, and University fiduciary rules and regulations; and (6) distributing financial policies and procedures to guide the day-to-day financial activities of the institution.

AUDIT OBJECTIVES

The objectives of the audit were to determine whether: 1) revenue generating activities/centers were established and monitored in accordance with University policies and procedures; and 2) opportunities were present to enhance efficiency and effectiveness within selected operations of the Comptroller’s Office. This audit did not focus on the accuracy of the financial transactions as part of the review work.

OPINION ON AUDIT OBJECTIVES

Audit could not make a determination as to whether all revenue generating activities (RGAs) were established in accordance with University policies and procedures because the policies were established at different times, and it was not clear how, or if, these policies and procedures applied to older RGAs. Opportunities to enhance effectiveness over the monitoring of RGAs were noted. In addition, opportunities were identified, in centralized and decentralized departments, to enhance the efficiency of cost transfer processing, as well as, the effectiveness of Internal Control Questionnaire (ICQ) response monitoring and oversight.
AREAS NOTED FOR IMPROVEMENT

1) Opportunities were identified to enhance the efficiency of the cost transfer process, particularly in the areas of automation and levels of authority.

2) Existing policies and procedures related to RGAs should be reviewed with the intent of developing one comprehensive policy that could be used for establishing and monitoring RGAs.

3) Central guidance should be enhanced to ensure monitoring efforts of annual ICQ responses are being performed to a defined standard.

MANAGEMENT’S RESPONSE

Management concurs and has agreed to address the identified conditions.

FINANCIAL IMPACT

Cost savings could be achieved via the automation of select cost transfer processes, as well as possible policy changes. If RGAs are not administered in accordance with federal requirements, funding to the institution could be affected.
BACKGROUND

In many large entities, human resource departments play an integral part along with information technology (IT) departments in securing information technology. The University of Virginia Medical Center operates a Human Resources department and a Technology Services department. Under the guidance of University and Health System (HS) policies, standards, and procedures, these HS departments perform human resources and employee access management processes.

Proper management of employee and third-party access and related human resources processes is essential throughout the employee life cycle including the stages of pre-employment, onboarding, employment, and off-boarding. Consistently managed employee and third-party access provides a foundation for securing sensitive data, networks, systems, and applications.

AUDIT OBJECTIVES

Audit objectives included a review of the Medical Center’s management of employee access life cycle and related human resources processes.

OPINION ON AUDIT OBJECTIVES

Opportunities were noted to improve the Medical Center’s management of employee and third-party access and related human resources processes.

AREAS NOTED FOR IMPROVEMENT

1) Health System Medical Center’s processes related to pre-defining financial and administrative system’s roles and responsibilities and managing accounts with privileged access required improvement.

2) Onboarding and off-boarding processes and procedures required improvement.

3) Comparative review of HSMC’s Conditions of Employment with the International Organization for Standardization (ISO) 27002 identified missing content for inclusion.
MANAGEMENT'S RESPONSE

Management concurs and has agreed to correct the identified conditions.

IMPACT TO THE UNIVERSITY

The impact of employee access management and related HR processes are always important because of the following concerns:

- Availability of mission critical systems, operations and services.
- Public relations issues.
- Monetary loss as a result of server down time and hours spent in repair or recovery as a result of damage done by employees having improper access.
UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: November 14, 2014

COMMITTEE: Audit and Compliance

AGENDA ITEM: IV. Approval of the Summary by the Auditor of Public Accounts and the Summary of Internal Audit Findings

BACKGROUND: This resolution reflects discussion by the Committee, in Executive Session, of the findings of the Auditor of Public Accounts and a summary of recent audits conducted by the Internal Audit Department.

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

AUDITOR OF PUBLIC ACCOUNTS’ FINDINGS AND THE SUMMARY OF INTERNAL AUDIT FINDINGS

RESOLVED, the Auditor of Public Accounts’ Findings for fiscal year 2013-2014, and the Summary of Audit Findings for the period August 16, 2014 through October 15, 2014, as presented by the Chief Audit Executive, are approved as recommended by the Audit and Compliance Committee.
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.

November 2014
Academic Division
Enterprise Risk Management (ERM)

Audit and Compliance Committee
June 5, 2014
Executive Summary

- Risk Assessment process executed with input from Deans and Vice Presidents.

- Primary risks refined to top nine – focused on most important to institutional continuity.
Top Institutional Risks

1. Sufficient funding/resources to achieve goals
   - Maintain core programs and pursue strategic objectives
   - Align fundraising with strategic priorities
   - Maintain historical Grounds, infrastructure and address needed capital projects
   - Maintain State appropriations at a level necessary to accommodate enrollment growth and inflation
   - Sustain and grow research mission
   - Sustain AccessUVA
   - Continue top decile performance of endowment

2. Management of human capital
   - Achieve competitive compensation
   - Manage generational turnover in faculty
   - Effective succession planning
Top Institutional Risks

3. **Legal compliance risks (state/federal/other)**
   - Comply with federal, state, or other established regulatory requirements (e.g. NCAA, SACS)

4. **Keeping pace with changes in higher education**
   - Effectively implement strategic plan
   - Ensuring adequate learning spaces to offer competitive graduate and undergraduate curricula

5. **Failure to maintain reputation with key stakeholders**
   - Maintain/improve higher education rankings
   - Maintain key accreditations
Top Institutional Risks

6. **Failure to manage geo-political and economic risks**
   - Manage risks of increasing international experiences of faculty and students
   - Effectively manage changing economic circumstances (e.g. growth/hyperinflation)

7. **Safety/security of student, faculty and staff**
   - Effectively mitigate and respond to incidents on Grounds or at University-affiliated programs (e.g. racial incidents, harassment, pandemic risk, sexual assault, or other violence)
   - Manage risks of increasing international experiences of faculty and students
Top Institutional Risks

8. **Cybersecurity/leveraging IT**
   - Protect sensitive data and information
   - Effectively leverage technology in the residential educational experience

9. **Capitalize on organizational/operational efficiencies**
   - Effectively pursue organizational excellence
   - Manage risk of differing priorities, inefficiencies, and complexity in decentralized operations and authority
## Sample Mitigation Strategy

### Faculty Compensation

<table>
<thead>
<tr>
<th>Key Risk</th>
<th>Management of human capital</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sub Risk</td>
<td>The University’s faculty compensation may not be competitive with peers</td>
</tr>
<tr>
<td>Risk Owner</td>
<td>Executive Vice President &amp; Provost</td>
</tr>
<tr>
<td>Key Stakeholders</td>
<td>Board, Senior Management, Faculty</td>
</tr>
</tbody>
</table>

### Current Mitigation Activities

- At its February 2013 meeting, the Board of Visitors approved a resolution supporting the goal of raising average faculty salaries into the Top 20 among U.Va.’s Association of American University (AAU) peers. The University’s current average faculty salary is ranked No.26 in the AAU.

- The resolution sets a goal of reaching the Top 20 within a four-year period ending in June 2017, with the understanding that it will be addressed in the University’s annual operating budget.

### Mitigation Effectiveness

<table>
<thead>
<tr>
<th>Effectiveness</th>
<th>Action Plans</th>
<th>Responsible Person</th>
<th>Due Date</th>
</tr>
</thead>
</table>
| 1- Effective  | • Continue to assess recruiting and retention metrics  
• Monitor university’s position in AAU rankings | Executive Vice President & Provost | Ongoing |