UNIVERSITY OF VIRGINIA
BOARD OF VISITORS
MEETING OF THE
AUDIT, COMPLIANCE, AND
RISK COMMITTEE
NOVEMBER 12, 2015
AUDIT, COMPLIANCE, AND RISK COMMITTEE
(Open Session)

Thursday, November 12, 2015
3:00 – 4:00 p.m.
Auditorium of the Albert & Shirley Small
Special Collections Library, Harrison Institute

Committee Members:
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

AGENDA

I. REMARKS BY THE COMMITTEE CHAIR 1

II. INFORMATION ITEMS
A. Audit Department Quarterly Report (Written Report) 2
B. Report on Enterprise Risk Management (Written Report) 4
C. Auditor of Public Accounts (APA) Audit and Management Report (Ms. Melody Bianchetto, AVP for Finance, to introduce Mr. Eric Sandridge, Director of Higher Education Programs, Auditor of Public Accounts; Mr. Sandridge to report) 8

III. 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.
• Exclusions of records relating to public safety as provided for in Section 2.2-3705.2(3) of the Code of Virginia.

IV. ACTION ITEM
• Auditor of Public Accounts’ Findings 9
UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: November 12, 2015

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.
UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: November 12, 2015

COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: II.A. Audit Department Quarterly Report (Written Report)

ACTION REQUIRED: None

BACKGROUND: For purposes of supporting the Committee's oversight of the Audit Department, Ms. Carolyn Saint, Chief Audit Executive, prepared a summary of key activities in progress and reports issued during the first quarter of FY 2016.
# Audit Department Update Q1 FY2016

## Audit Projects In-Flight
- Foundations: Advisory report in draft
- UNIX Security Audits (Health System and Univ.): reports in draft
- Curry School of Education: Fieldwork underway
- IT Asset Management: Planning phase
- Pyxis Access (medication mgmt. system): Report in draft
- EPIC Implementation: Project Health Check in progress
- In partnership with IT Security, consulted with UVIMCO to strengthen access controls.
- Ivy Cloud Computing: consultation
- Preparing frameworks for auditing Financial Stewardship, Integrated Assurance

## Observations, Headlines, and Challenges
- Global risk themes* are relevant to UVA and our audit plan addresses them:
  - The increased interconnectedness of modern organizations
  - Digitalization and the strategic importance of data
  - The relentless pace of regulation
  - The increasing speed of business

*CEB’s 2016 Audit Plan Hot Spots

Of note for the Health System:
- DHHS’ OCR is moving forward with a permanent HIPAA Privacy audit program in early 2016. This is in response to OIG’s unfavorable report on OCR’s oversight.

## Audit Reports Issued
- Presidential Travel & Entertainment Expenditures FY2015: controls working effectively—no issues to report
- General Ledger Transfers: Controls for maintaining original donor restrictions on University funds when transferred are operating effectively—no issues to report

## Upgrading Audit’s Skills & Acumen
- Standardizing, documenting, and training on Audit’s methodologies related to:
  - Process Audits
  - Project Health Checks
  - Integrated Assurance
  - Financial Stewardship
  - Advisory Projects
  - Investigations
- Assessing Audit team skills/competencies against standard competency model. Customized training and development plan to follow.
- Director of Audit: offer extended to experienced health care audit leader. Expect an answer by Oct. 30.
- Senior IT Auditor: interviewing solid pool of candidates
UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: November 12, 2015

COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: II.B. Report on Enterprise Risk Management (ERM) (Written Report)

ACTION REQUIRED: None

BACKGROUND: At its June 2014 meeting, Mr. Gary Nimax, who is the Assistant Vice President for Compliance and Enterprise Risk Management, reviewed the University’s ERM program with the Board. The Board discussed nine institutional risk categories, along with more specific subcategories, that represent the key institutional risks for the academic division. The Board requested regular reports on the various institutional risks and related risk mitigation efforts with associated metrics.

Shown on pages 5-7 is the documentation developed to outline the mitigation strategies identified to manage the following key institutional risks:

- Cybersecurity
- International and Geo-Political Risks
# Cybersecurity

**Risk Description**  
The University must protect sensitive data and information.

**Risk Owners**  
EVP/Chief Operating Officer

## Mitigation Strategies Currently in Place

- Information Security, Policy & Records Office: dedicated team focused on IT security across the University
  - Develops and publishes security policies.
  - Currently performs limited assessments, scans, investigation, remediation.
- Secure Highly-Sensitive Data in Central Administrative Systems:
  - Strong security controls for systems containing highly sensitive data (SSNs, bank account information, passport numbers, etc. housed in HR, Finance, and Student ERP systems: controls include firewalls, two-factor authentication, regular vulnerability scans, network encryption, intrusion protection). Moderate security controls for systems that do not contain highly sensitive data: controls include anti-virus, ad hoc vulnerability scanning, limited malware detection at network level.
  - Strong perimeter controls for all medical systems that could house patient records and data. These controls include network/system controls and encrypted e-mail/devices, as well as firewalls, two-factor authentication, regular vulnerability scans, network encryption, and intrusion protection.
- External Assessments:
  - Penetration testing recently completed; maturity assessments and recommendations; enhancements completed on a regular basis.
- Cyber Risk Insurance:
  - Coverage for liability from theft, loss, or unauthorized disclosure.

<table>
<thead>
<tr>
<th>Due Date</th>
<th>Action Plans</th>
<th>Responsible Person</th>
</tr>
</thead>
<tbody>
<tr>
<td>FY2018-19</td>
<td>• Implement 3-year Security Enhancement Program</td>
<td>Chief Information Officer</td>
</tr>
</tbody>
</table>

**Key Performance Indicators**

- Being developed in connection with the Security Enhancement Program

  - TBD
International and Geopolitical Risks

<table>
<thead>
<tr>
<th>Risk Description</th>
<th>Effectively manage the risks of increasing international experiences of faculty and students.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Owners</td>
<td>Provost, Chief Operating Officer</td>
</tr>
</tbody>
</table>

**Mitigation Strategies Currently in Place**

- The International Studies Office (ISO) establishes policies and guidelines for student travel programs with regards to health, safety and security planning, and approves destinations and itineraries in collaboration with the school and relevant service units. ISO also maintains the Crisis Management Plan for Education Abroad protocol as well as the student travel registry. ISO works with the Education Abroad Risk Management Committee regarding petitions to travel to countries with travel warnings or restrictions. Final authority rests with the Vice Provost for Global Affairs.

- Policies – Institutional, State, & Federal: include the Policy on Student International Travel, Procurement policies, Export Controls, the Standards of Conduct, Honor, and all other relevant UVA academic and non-academic policies and procedures. Additionally, Clery, VAWA, and Title IX reporting requirements are followed. Local law, e.g., customs and immigration regulations, and partner organization policies and procedures are also respected.

- Education abroad program planning, administration, and evaluation are informed by standards and best practices published by NAFSA: Association of International Educators, the Forum on Education Abroad, and UVA’s Institutional Review Boards.

- Data sources for risk assessment include Overseas Security Advisory Council (OSAC); iJet/WorldCue; Alert-24; Medex Worldwatch; U.S. Embassies and Consulates abroad; Embassies and Consulates of other nations, e.g., the UK; the Centers for Disease Control; the World Health Organization; news services, e.g., BBC; and local experts.

- Training for faculty and staff involved with student international travel for university related purposes; required in-person training pre-departure, four sessions/year. Student international travel registry: confidential and secure database for maintaining key travel information about students traveling that forms the basis for the University’s emergency response protocols and communications strategy (e.g., alerts, warnings, evacuation notices) when responding to an emergency or critical incident abroad.

- Health and emergency assistance insurance requirement for students who travel internationally for university related purposes: students must confirm that they have insurance that provides 1) medical evacuation, 2) security evacuation, 3) repatriation of remains, 4) emergency assistance, and 5) overseas health insurance.

- Smart Traveler Enrollment Program (STEP): students who are U.S. nationals must be enrolled with STEP.

- *Risk Management Plan for Education Abroad*: guides the response of faculty and staff abroad and the response of University leaders, administrators, faculty and staff in Charlottesville to matters involving the health, safety, and security of UVA students abroad and faculty and staff traveling with them.
- Training for students: students enrolling in study abroad must complete the online study abroad workshop and attend a pre-departure orientation, each addressing health, safety, and security.

- *UVa Education Abroad Student Handbook*: comprehensive resource for students that addresses planning, resources, policies and procedures, and matters related to health, safety, and security.

- *Cultural Orientation, Reflection, and Engagement (CORE)*: ISO program that offers a menu of workshops and short classes to help students prepare for their time, succeed while abroad, and re-integrate post-return.

- The Office of Export Controls monitors the University's research and educational activities for compliance with export control and sanction restrictions through policy, procedures, training, and support for regulated activities, including but not limited to international travel and shipping.

<table>
<thead>
<tr>
<th>Due Date</th>
<th>Action Plans</th>
<th>Responsible Person</th>
</tr>
</thead>
<tbody>
<tr>
<td>March 2016</td>
<td>• Implement travel system for faculty/staff with Duty of Care component and advanced information about travel.</td>
<td>Director, Procurement Services</td>
</tr>
<tr>
<td></td>
<td>• Capitalize on information available through the new travel system to provide export control and sanction guidance, support international travelers, and work with them assure compliance.</td>
<td>Export Compliance Officer</td>
</tr>
<tr>
<td>June 2016</td>
<td>• Increase use of emergency travel assistance program.</td>
<td>AVP for Compliance and ERM</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Key Performance Indicators</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 100% student compliance with established requirements for study abroad programs.</td>
<td>• ISO</td>
<td></td>
</tr>
<tr>
<td>• 100% utilization of new travel system for faculty on foreign travel.</td>
<td>• Procurement Services</td>
<td></td>
</tr>
</tbody>
</table>
UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: November 12, 2015

COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: II.C. 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 findings to the Board. Ms. Bianchetto will introduce Mr. Eric M. Sandridge, who will report on findings for the fiscal year 2014-2015 audit.

Mr. Sandridge is the Director of Higher Education Programs for the Virginia Auditor of Public Accounts and has served in that position since 2012. His responsibilities include management of the office's Higher Education Programs Specialty Team and project management oversight for audits of various agencies and institutions of the Commonwealth. Mr. Sandridge has served as audit director for the Virginia Community College System, Old Dominion University, Virginia Commonwealth University, Norfolk State University, University of Virginia, and the Department of Alcoholic Beverage Control annual audits.

Mr. Sandridge also coordinates required federal audits at the Commonwealth's institutions of higher education, which support Virginia's statewide Single Audit report. He received his B.B.A. in Finance from the College of William and Mary and is a Certified Public Accountant and a Certified Government Financial Manager.
UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: November 12, 2015

COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: IV. Auditor of Public Accounts' Findings

BACKGROUND: This resolution reflects discussion by the Committee, in Executive Session, of the findings of the Auditor of Public Accounts.

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

AUDITOR OF PUBLIC ACCOUNTS' FINDINGS

RESOLVED, the Auditor of Public Accounts' Findings for fiscal year 2014-2015, are approved as recommended by the Audit, Compliance, and Risk Committee.