MEMORANDUM

TO: The Audit and Compliance Committee:

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

and

The Remaining Members of the Board and Senior Advisor:

Allison Cryor DiNardo  
Helen E. Dragas  
Marvin W. Gilliam Jr.  
William H. Goodwin Jr.  
John A. Griffin  
Stephen P. Long, M.D.  
Edward D. Miller, M.D.  
Timothy B. Robertson  
Blake E. Blaze  
Leonard W. Sandridge Jr.

FROM: Susan G. Harris

SUBJECT: Minutes of the Meeting of the Audit and Compliance Committee on February 21, 2014

The Audit and Compliance Committee of the Board of Visitors of the University of Virginia met, in Open Session, at 8:37 a.m., on Friday, February 21, 2014, in the Board Room of the Rotunda; Hunter E. Craig, Chair, presided.

Present were Kevin J. Fay, Frank E. Genovese, Victoria D. Harker, John L. Nau III, and Linwood H. Rose.

Adelaide Wilcox King, Faculty Consulting Member, was present as well.
Also present were Allison Cryor DiNardo, Helen E. Dragas, William H. Goodwin Jr., John A. Griffin, Stephen P. Long, M.D., Timothy B. Roberson, and Leonard W. Sandridge Jr.

Present, too, were Paul J. Forch, Susan G. Harris, Teresa A. Sullivan, Susan A. Carkeek, Donna Price Henry, Patrick D. Hogan, R. Edward Howell, David W. Martel, Marcus L. Martin, M.D., Anthony de Bruyn, Barbara J. Deily, Karen Helderman, Gary S. Nimax, Lori J. Strauss, and Debra D. Rinker.

Mr. Craig began by introducing the four presenters: Ms. Deily, Ms. Helderman, Mr. Nimax, and Ms. Strauss.

Corporate Compliance and Privacy Office Status Report for Fiscal Year 2013-2014

Ms. Lori Strauss reported on the Corporate Compliance and Privacy Office’s 40 scheduled projects. She said 18, or 45%, are complete, with six projects, or 15%, in process. She anticipates having all scheduled projects in process by the end of the fiscal year and — ideally — completed by that time.

Ms. Strauss brought to the Board’s attention that during the first two months of this fiscal year the Office’s full-time analyst position was vacant and the senior analyst had been in her position for only six months; these circumstances limited their ability to begin projects due to associated learning curves and training needs for new employees. They continue to prioritize projects and coordinate with the Audit Department and other Medical Center departments to ensure coverage in as many areas as possible given the available resources.

She said one of the seven elements of an effective compliance program as identified in the Office of the Inspector General’s Compliance Program Guidance documents for hospitals is to develop and implement a regular, effective education and training program for all affected employees. The Corporate Compliance and Privacy Office prepares the compliance and privacy training modules for all new employees and it revises the mandatory annual retraining compliance and privacy content for all employees. The retraining content incorporates trends or issues that are identified during visits to departments, through questions from staff or management, and through the Office’s auditing and monitoring program.

Ms. Strauss said employees in the Health System are undergoing training to prepare for the conversion to the International
Classification of Diseases 10th Revision, ICD-10, on October 1, 2014. ICD-10 will replace ICD-9 resulting in expanding code selections from approximately 16,000 codes today to approximately 150,000 codes on October 1, 2014. Aside from the structural changes to the codes, there is greater specificity in the codes, which will require greater specificity in the documentation.

Ms. Strauss said the Health System’s Notice of Privacy Practices that HIPAA – the Health Insurance Portability and Accountability Act - requires that we explain to patients how their medical information may be used and disclosed, as well as how to access that information. The Office updated the Notice to be compliant with the federal Omnibus Final Rule changes to the HIPAA Privacy Rule that became effective on September 23, 2013.

Report on Enterprise Risk Management (ERM)

Mr. Nimax said in 2008 the University began to conduct an initial assessment of the University’s current framework for assessing and managing the University’s strategic and high-level operational risks. The University explored the feasibility and desirability of developing a framework that could link the different risk management programs that are already in place. At the beginning of that project, the University conducted interviews with several members of the Board of Visitors and numerous University officials to begin developing a portfolio of top risks.

In order to control the scope of the project, the University focused solely on the academic division. Phase I did not include the medical center, College at Wise, and University-related foundations, but clearly will need to incorporate those areas going forward. Mr. Nimax said they have discussed risk mitigation with the larger university-related foundations. Since they began that project they have given regular reports to the BOV regarding ERM.

Mr. Nimax said three years have passed since the current list of top risks was identified. The University will be updating its risk register given the turnover in senior administration and board members, the new strategic plan, internal financial model, and changes in the higher education landscape.

Mr. Nimax said during discussions, some individuals want to focus immediately on safety risks or financial risks, but he said we want to make sure we are considering the full breadth of risks that the University faces.
Mr. Nimax said they are currently working with Mr. Craig and Mr. Hogan to develop a survey tool. This phase of the project is focused on completing the risk register for the Academic Division, which includes identifying the most important strategic, legal, financial, operational, and reputational risks now and in the immediate future. In that regard, they are seeking input from the Board members on the risks considered to be the most important Academic Division risks.

Next steps will include updating the risk register with survey responses and documenting mitigation strategies. The survey will be sent to the Board, vice presidents, and deans. Individual survey responses will be anonymous. Mr. Nimax said they are using a third-party survey tool, Question Pro, to collect and summarize survey data, so they will not have access to individual responses.

The survey includes a list of 18 specific risks to rate, summarized from the key risks identified by the prior ERM project, and other potential risks related to topics the Board has discussed recently. Each recipient will be asked to indicate a rating for the likelihood of risk occurrence, as well as the potential impact to the University of each risk, using a rating scale of low, moderate, and high. It is considered a best practice to have the Board provide input and evaluate institutional risks based on those two scales.

He said there are also spaces to record information regarding other risks that should be considered among the University’s top risks. If a risk is added in this section, there is also a need to rate the likelihood and impact of that risk.

Once the results of the survey are received, the University will provide additional information and related mitigation strategies regarding top risks at the June meeting. These will represent the key risks that merit further BOV understanding and discussion. Certainly there will remain other more operational risks that various units will manage, but these are the ones that rise to the level of the Board and its related initiatives.

There was some concern expressed by members of the committee about completing a survey, and Mr. Nimax and Mr. Hogan were asked to look at this again.

---

Audit Department Status Report for Fiscal Year 2013-2014

Ms. Deily said the Audit Department has a goal of completing 33% of their projects by December 31, and they have come in at 36% overall for the department, which is the same as at this time last
She said they usually complete 80-90% of their scheduled audits (after adjustments) by June 30th and they have a goal of completing 90% for the year so it still looks like they will be able to do that given that over 70% of their projects are in process as of December 31.

She said they have an audit manager vacancy and have decided to defer an audit of the College at Wise until the 2014-15 fiscal year. The Audit Department is currently filling that position with one of their senior auditors to allow that person some experience in the position. They also had to temporarily reduce the effort of the University audit director to half-time. This reduction is due to family medical leave. With the adjustment in the schedule by deferring one regular project, she believes that they will still be able to meet their goals.

Ms. Deily highlighted several audit reports in open session. She said these reports focus on various aspects of University and Health System information technology activities. Overall, these reports were very positive, but they did make some recommendations to improve certain security policies and procedures and to formalize a service agreement. She said they also made several suggestions to enhance operating practices. Management agreed to address the findings and to consider their suggestions.

---

Auditor of Public Accounts (APA) Audit and Management Letter

Ms. Helderman is an Audit Director for the Auditor of Public Accounts (APA). The APA has responsibility for reviewing all state operations for fiscal integrity. Ms. Helderman serves as the Project Manager for the U.Va. audit. She is a Certified Public Accountant, a Certified Information Systems Auditor, and a Project Management Professional with over 27 years of audit experience.

Ms. Helderman said the APA has issued an unqualified opinion on the University’s financial statements for the year ended June 30, 2013. She said their opinion is included in the University’s fiscal year 2013 Financial Statement Report. They have also issued a separate report on Internal Controls and Compliance that was distributed to the Board of Visitors. They obtained a sufficient understanding of internal control to plan their audit and to determine the nature, timing, and extent of testing performed.

The APA audit identified four matters that were considered to be significant internal control deficiencies, but not material weaknesses in internal controls.
The first area had to do with user access, primarily related to the Oracle Access e-Business Suite. Five recommendations came out of this finding: 1) adopt a policy requiring that Human Resources terminate all user responsibilities whenever an employee transfers to another department and require the new department to request new responsibilities; 2) the University should prohibit employees from serving as their own primary or backup approver and Information Technology Services (ITS) should run periodic reports to validate compliance; 3) the University should shift away from a responsibility-driven annual review and instead focus on functionality and segregation of duties concerns; 4) the University should incorporate other aspects of authority into its annual access review, such as transaction limits and transaction approvers; 5) ITS should improve their understanding of how to obtain data from Oracle's security tables.

The second area dealt with controls over termination of access to facilities and systems. She said both the University and the Medical Center had instances of employees with inappropriate access. In most cases, the departments had not notified Human Resources of the need to terminate access. The Medical Center plans to convert the employee notification process to an electronic form through Peoplesoft to allow for the prompt removal of terminated employees. The University implemented an off-boarding toolkit on October 1, 2013 to ensure proper processing of employees leaving the University.

The third area had to do with completing and approving reconciliations in a timely manner. The University needs to monitor and enforce the timely preparation and approval of reconciliations. This could be captured within the Recon@UVA system.

The final area noted was the compliance of the University sole source policy. In a sampling of five, one lacked justification for a purchase over $5,000, and another lacked consideration of alternate vendors. It was recommended that Procurement Services tighten up these controls to ensure compliance.

Institutional Response to APA Management Letter

Mr. Hogan responded on behalf of the University. He said as noted in November, the APA's review has found that the University's financial statements are presented fairly in all material respects; there are no internal control findings classified as material weaknesses, and no instances of noncompliance or other matters required to be reported under Government Accounting Standards. The APA did find several internal control weaknesses that, although not
material, require response and action. Mr. Hogan acknowledged the importance of strong and effective policies and practices around user access, termination of access to systems and facilities, completing and approving reconciliations, and the University sole source policy. The University is taking appropriate measures to strengthen oversight and management of these areas in response to the recommendations of the APA.

EXECUTIVE SESSION

After adopting the following motion, the voting members present plus Mr. Forch, Ms. Harris, and Ms. Rinker, participated in Executive Session at 9:22 a.m.:

That the Audit and Compliance Committee of the Board of Visitors go into Closed Session to discuss audits of University departments, and consult legal counsel, concerning performance of specific University personnel responsible for information security facilities and evaluation of performance of Medical Center departments and personnel with respect to medical record security and billing, and also to confer with the Auditor of Public Accounts on the performance of University management as permitted by Sections 2.2-3711 (A) (1), (7) and (19) of the Code of Virginia and where, in the case of the Medical Center, disclosure at this time would adversely affect the Medical Center's competitive position as permitted by Section 2.2-3711 (22) of the Code of Virginia.

At 9:50 a.m. the Committee left closed session and, on motion, adopted the following resolution certifying that the deliberations in closed session had been conducted in accordance with the exemptions permitted by the Virginia Freedom of Information Act:

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.

Action Item: Summary of Audit Findings

On motion, the committee approved the following resolution and recommended it for Board approval:
RESOLVED, the Summary of Compliance Projects for the period July 1, 2013 through December 31, 2013, as presented by the Chief Corporate Compliance and Privacy Officer, the Auditor of Public Accounts Findings for fiscal year 2012-2013, and the Summary of Internal Audit Findings for the period October 1, 2013 through December 31, 2013, as presented by the Chief Audit Executive, are approved.

---

On further motion, the committee adjourned at 9:50 a.m.

SGH:dr
These minutes have been posted to the University of Virginia’s Board of Visitors website. http://www.virginia.edu/bov/auditminutes.html
ATTACHMENT
<table>
<thead>
<tr>
<th>Area</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auditor’s Opinion</td>
<td>We have issued an unqualified opinion on the University’s financial statements for the year ended June 30, 2013. Our opinion is included in the University’s fiscal year 2013 Financial Statement Report.</td>
</tr>
<tr>
<td>Scope of Internal Control Work</td>
<td>We have also issued a separate report on Internal Controls and Compliance that was distributed to the Board of Visitors. We obtained a sufficient understanding of internal control to plan our audit and to determine the nature, timing, and extent of testing performed. Our audit identified four matters that we consider to be significant deficiencies, but not material weaknesses in internal control.</td>
</tr>
<tr>
<td>Compliance Testing</td>
<td>We found no instances of noncompliance that are required to be reported.</td>
</tr>
<tr>
<td>Fraud and Illegal Acts</td>
<td>We found no indications of fraudulent transactions or illegal acts.</td>
</tr>
<tr>
<td>Significant Audit Adjustments</td>
<td>All audit adjustments were reviewed with management and recorded in the audited financial statements.</td>
</tr>
</tbody>
</table>
| Accounting Policies, Principles, Methods, and Estimates | • We concur with management’s application of accounting principles.  
• We reviewed the basis for accounting estimates and these estimates appear to be reasonable based on available information and consistent with prior periods.  
• There were no material changes to accounting and reporting policies and standards during the year.  
• There were no material alternative accounting treatments identified as a result of the audit.  
• There were no unusual transactions or significant accounting policies in controversial or emerging issues.  
• There were no disagreements with management about auditing, accounting, or disclosure matters. |
NCAA Agreed-Upon Procedures

We also performed an agreed-upon engagement to assist the University in complying with NCAA Bylaw 3.2.4.16.1. All adjustments that we identified were properly corrected in the Schedule. Our separate report on this Agreed-upon Procedures engagement has been distributed to the Board of Visitors.