A meeting of the Audit Committee of the Board of Trustees of the University of Vermont and State Agricultural College was held on Monday, September 10, 2012 at 10:00 a.m. in room 427A Waterman Building.

MEMBERS PRESENT: Chair Mark Young, Vice Chair Dale Rocheleau, Bill Botzow**, Jeff Davis*, David Potter* and Dennis Mahoney

MEMBERS ABSENT: Carolyn Branagan

REPRESENTATIVES PRESENT: Faculty Representative Albert Joy, Staff Representative Marie Tiemann and Student Representative Chris Juaire

REPRESENTATIVES ABSENT: Alumni Representative Bill Cimonetti and Student Representative Cornell Woodson

PERSONS ALSO PARTICIPATING: Vice President for Finance and Administration Richard Cate, Vice President for Legal Affairs and General Counsel Francine Bazlute, Chief Internal Auditor William Harrison, Chief Compliance and Privacy Officer Anna Drummond, Information Security Officer Dean Williams, Chief Information Officer David Todd, Controller Claire Burlingham, Renee Bourget-Place of KPMG***, and Tanya Morehouse and Tom Salmon of the State Auditor’s Office

* Participated via teleconference
** Joined via teleconference call at 10:15 a.m.
*** Participated via teleconference until 11:25 a.m.

Chair Mark Young called the meeting to order at 10:00 a.m.

Approval of Minutes

A motion was made, seconded and voted to approve the July 9, 2012, meeting minutes.

Chief Internal Auditor Update

Chief Internal Auditor William Harrison began by referring to his written status report. Since June 30, 2012, the Office of Audit Services (OAS) has issued seven reports. These reports include an Audit of PeopleSoft Access Control, an Audit of Departmental Expenses, the General Information Technology (IT) Control Self-Assessment Questionnaire, and three EthicsPoint reports.

He moved on to review the status of OAS internal audit report follow-up. He reported that since the July 2012 Audit Committee meeting the Office closed 3 recommendations related to existing audits and issued two new reports containing 16 recommendations. Of the total number of open recommendations, 65% have been open for less than a year, 29% for one year, and 6% for more than two years.
Vice President Cate noted he would have management’s responses to the Banner Student Information System audit to Mr. Harrison by the end of the week.

Prompted by Vice Chair Rocheleau’s inquiry, Mr. Harrison clarified his determination of “satisfactory” progress when used to determine the status of audit report follow-up.

Tanya Morehouse, of the State Auditor’s Office, requested clarification on the relationship between Finance and Administration and the other units when responding to audit recommendations. Vice President Cate explained that all financial reporting goes through his office as well as the review of timelines for corrective action plans.

In conclusion, Vermont State Auditor Tom Salmon commended the University on its commitment and progress creating a culture of compliance over the past five years.

Chief Compliance and Privacy Officer Update

Chief Compliance Officer Anna Drummond began with an update on the FY 2013 Compliance Work Plan. She addressed the Office’s work on UVM’s compliance with the new Public Health Services (PHS) Conflict of Interest Rules. The University is required to comply with new requirements from the Public Health Service related to the disclosure and management of investigator financial conflicts of interest. Last year, PHS-funded research at UVM totaled approximately $65 million and is a very significant component of overall research funding.

These new federal rules are the result of recent public scandals involving conflicts of interest, increased legislative interest in transparency and accountability, increased collaboration of investigators with the private sector, and increased public expectations. On August 25, 2011, Health and Human Services (HHS) issued the final rules amending the PHS regulation on Responsibility of Applicants for Promoting Objectivity in Research with an effective date for implementation of August 24, 2012. This allowed the University one year to implement a compliance response to these complex new rules. To ensure the University met the implementation deadline, Associate Vice President for Research Administration Ruth Farrell (AVP for Research) put together a work group within her unit. The Compliance Office created a compliance matrix for use by that unit and reviewed with the AVP Research a work plan and timeline that was finalized by January 2012. In addition, the Compliance Office used the National Institutes of Health (NIH) created compliance checklist as an assessment tool to ensure that all policy and practice requirements within the check list were being met.

Ms. Drummond commended Sponsored Project Administration, the AVP for Research, and the Vice President for Research Domenico Grasso for their proactive efforts and diligence in meeting these compliance requirements. In addition, Ms. Drummond commended the VP for Research for setting the right “tone at the top” for the research enterprise. The VP for Research communicates to both his staff and to University researchers the importance of compliance and of integrity, professionalism and ethical conduct.

Ms. Drummond described the Compliance Office’s extensive work reviewing and advising the AVP for Research on the new policy and procedures developed to meet compliance in this area and then she briefly described the results of the compliance assessment performed utilizing the previously noted NIH checklist. She provided a summary of each requirement and the University's response. Areas included required training, disclosure, review and monitoring requirements, reporting
requirements to the PHS/NIH, maintenance of records, required enforcement mechanisms and remedies for noncompliance, sub-recipient requirements as well as public accessibility requirements.

When asked, Ms. Drummond provided Chair Young with an example of a research conflict of interest. She noted that the significant financial interest would also need to be a financial conflict of interest, essentially impacting the research, itself. Only a small number of potential such conflicts of interest are anticipated at UVM.

In response to Vice Chair Rocheleau's question about compliance with the new rules giving the University an advantage, Ms. Drummond noted that while all institutions are expected to be compliant, the existence of a compliance function and an anonymous reporting line would be beneficial for the University in any audit process.

Moving on to discuss compliance work prompted by the results of an internal audit, Ms. Drummond reported that her Office continues to meet monthly with Sponsored Program Administration on compliance issues raised in the Subrecipient Monitoring Audit Report #12-010. Under the guidance of the AVP Research, the unit is engaged in meeting the goals outlined in the Management Response to the Audit Report.

With respect to consultations, the Office of Compliance Services continues to provide compliance and privacy consultations upon request or in response to new regulatory requirements. The Office of Compliance Services has performed twelve distinct compliance and privacy consultations or outreach activities for the period May 31, 2012 through August 2, 2012 and since our previously reported cumulative data. This brings the cumulative total to 202 independent consults.

Next, Ms. Drummond reported there were no new Government Reviews that arose in the period since the last Audit Committee meeting. The Chief Compliance Officer continues to participate in open reviews.

Ms. Drummond moved on to provide an update on the Ethics and Compliance Reporting Help Line. Four reports have been received since the July 9 Audit Committee meeting. There have been a total of twenty-eight reports made to date, eighteen of which have been closed. Eight of the outstanding reports were referred to Audit Services, one was referred to both the Affirmative Action Office and Human Resources, and the remaining report was referred to management.
Ms. Drummond concluded her presentation with an update on the Privacy Program. In addition to providing advice and outreach on privacy issues and application of the Privacy policy, the Privacy Office has updated the Privacy Procedures to include provision for the use of biometric identifiers. The Office, with the Information Security Officer and Chief Information Officer, has been working with the Athletics Office regarding appropriate privacy and security safeguards for the adoption of a pilot system using biometric identifiers for access to certain recreational sports facilities. For instance, certain disclosures are being required to be made and the system is totally voluntary with an ability to discontinue use at any time.

Responding to Chair Young's concern about a breach of biometric identifiers, both Ms. Drummond and Mr. Williams explained some of the technical features of the system being piloted and noted that the risk for this particular system were deemed to be low.

Chair Young commented on the use of such an advanced technology for access to an athletic facility. Ms. Drummond explained that this technology was being utilized more to address convenience rather
than security issues. Mr. Williams noted in more secure environments, additional security measures including two-factor authentication are used.

Other work on the Privacy Program includes revisions to the Records Retention policy. Ms. Drummond plans to report at the November Audit Committee meeting on this work.

Lastly, Ms. Drummond reported that since the July Audit Committee meeting, the Office has responded to two data security incidents in accordance with the Data Breach Notification policy.

Ms. Drummond addressed Chair Young’s concerns about Ethics and Compliance Help Line (the HelpLine) report follow-up when reports are referred to other departments. The Chief Compliance Officer noted that the current practice is for Compliance to follow up on the status of reports and to track the outcomes of reviews, but that the offices to which reports are referred utilize their own processes and procedures to perform the reviews. She noted that some investigations take longer than others and that her office does not set any kind of timeframe for conclusion of an investigation, but that it does follow up with the individual departments to ensure that they are still actively investigating. Vice President Francine Bazluke noted the Vice President of Executive Operations, Vice President for Legal Affairs and General Counsel, Chief Compliance and Privacy Officer, and Chief Internal Auditor meet to close every report once the departments had completed their investigations, under the newly changed processes of the HelpLine.

Vice Chair Rocheleau inquired as to whether the issues raised in HelpLine reports drive Compliance work plans. Ms. Drummond reiterated that these reports are taken into account in the development of the annual compliance work plan.

**Information Security Officer Update**

Information Security Officer (ISO) Dean Williams provided a summary of his Office’s work since the last Audit Committee meeting. Referring to his written report provided in advance to the Committee, he began with an update in the area of Payment Card Industry Data Security Standards (PCI DSS). The ISO team, along with Assistant Controller Kathy Snell and Administrative Professional Senior Sarah Bettencourt, has been reviewing the status of all merchants on campus to ensure they are on track for PCI DSS compliance. He reported that based on information assembled by Kathy Snell and Sarah Bettencourt, twenty-four out of thirty-three active UVM merchants (73%) have passed the applicable Self-Assessment Questionnaire (SAQ) requirements. Of the nine active merchants that are not fully compliant, four have not completed their annual SAQs, and five have not started their annual SAQs. One merchant has an SAQ that requires external scanning. Finally, two new merchants are not required to do an SAQ, at this time, because their e-commerce sites have not gone live.

The ISO team has continued to develop the Actively Secured Private Network (ASPN) to transmit cardholder data and work with UVM merchants to move into that network. Mr. Williams noted that due to the delayed arrival of new servers for the CatCard Center planning is underway to move existing servers into ASPN.

Mr. Williams will report to Chair Young concerning the number of transactions that are compliant with the applicable regulations. Ms. Drummond clarified that these “regulations” are industry standards rather than legal requirements.
Moving on, Mr. Williams updated the Committee on the Privacy, Information Security, and Data Retention Workgroup. The Chief Compliance and Privacy Officer (CPO), Chief Information Office (CIO), Information Security Officer, and Deputy Compliance and Privacy Officer met in July and determined that reducing the risk of social security number (SSN) disclosure would be its next area of focus. Analysis showed that Social Security numbers were reported to appear on 154 documents across 48 departments, with 128 in hard copy form and 103 in digital. The group’s goal will be to encourage departments to eliminate SSNs wherever possible, to destroy documents containing SSNs as soon as possible, when feasible obscure SSN’s, and to protect SSN’s wherever their use is necessary. Mr. Williams and Ms. Drummond believe many units across campus have already implemented corrective actions as a result of the Privacy, Information Security and Data Retentions workshops held last year.

Ms. Drummond addressed Trustee Botzow’s questions concerning historic documents containing SSN’s and how much risk they create for University by noting that adherence to the Records Retention policy should create a natural attrition. She also noted that this is an issue shared by many organizations and the efforts of the CPO, CIO and ISO are intended to provide a systematic and methodological approach to addressing this risk.

Next, Mr. Williams provided a brief summary of collaborations, consultations, and support work provided by his team. Enterprise Technology Services (ETS), Risk Management and Compliance and Privacy Services are performing a self-assessment as part of the process of investigating cyber liability insurance. Additionally, ETS and Audit Services are preparing next steps in helping decentralized Information Technology (IT) units with the security and appropriate controls for systems they manage.

Director of Risk Management Mary Dewey addressed Vice Chair Rocheleau’s question about whether the decision to look into cyber risk insurance was brought about by the Enterprise Risk Management (ERM) process. Ms. Dewey noted that she had requested this review as a standard best practice for risk management.

Trustee Botzow asked Mr. Williams if he was satisfied with the University’s practices related to penetration testing. Mr. Williams said that he was satisfied. Penetration testing for the University’s credit cards operations is done by Control Scan and internally as determined by management. A discussion of the benefit of third-party testing occurred and Mr. Williams agreed that more could be done in this area.

Mr. Williams confirmed for Chair Young that decentralized systems are owned by the University. He explained, however, that contracts for externally hosted services are reviewed to ensure the University is adequately protected.

In conclusion, Mr. Williams announced the selection of Sam Hooker as the new Information Security Engineer. Mr. Hooker is a former member of the Enterprise Technology Services System Architecture and Administration group. Mr. Williams is delighted Mr. Hooker will be joining his team.

**FY 2012 Financial Statement/A-133 Audit Status Report**

Ms. Bourget-Place of KPMG provided a brief status report on the FY 2012 financial statement and OMB Circular A-133 audits. KPMG is halfway through their fieldwork for the financial statements
audit. At this time, there are no significant adjustments to report. There was no change in the status of the A-133 audit since the July Audit Committee meeting.


At Vice President Cate’s request, Controller Claire Burlingham provided the Committee with a status report on the employee benefit reconciliations. A formal six-month process was completed in December 2011, for Blue Cross Blue Shield of Vermont. The reconciliation process identified a discrepancy less than $100,000. Going forward, a quarterly reconciliation will be performed on a regular basis.

In addition, both the University’s life insurance and disability insurance are being reconciled on a monthly basis. The next PeopleSoft upgrade will provide enhancements which will assist in the automation of the reconciliation process.

Chief Information Officer David Todd addressed the Information Technology observations. He commented on the balance between complex passwords and phishing threats. Mr. Todd confirmed for Chair Young that the University does maintain a history of passwords. In response to Trustee Botzow’s concerns about the strength of the University’s defense against attacks, Mr. Todd explained the well defined controls over what individuals can access electronically.

Moving on, Mr. Todd commented on the remaining IT observations related to access control, the change process, and separation of duties. Mr. Todd indicated that system infrastructure/network changes are now documented within the Footprints system. Staffing issues, however, have delayed implementation of periodic access control reviews and their ability to appropriately separate duties. In the meantime, staff engaged in PeopleSoft security monitor each other’s work and document their work in the tracking system. Finally, change management for Banner has been tested in production and will be fully implemented by the end of the second quarter.

**Information Security (IT) Security Program Presentation**

Chief Information Officer David Todd and Information Security Officer Dean Williams provided the Committee with an overview of the University’s IT security program. Mr. Todd began with a brief history of the five member ISO team that has been meeting over the past three years. The group’s first project was PCI DSS compliance.

Next, Mr. Williams presented the different challenges faced by the University in a decentralized environment. He explained how all universities are placing more reliance on information and communication technologies in all aspects of their operations. There is an expectation for ubiquitous connectivity. Today’s situation at UVM is comprised of a mature enterprise information system, storage and networks. It also includes a mix of centrally provided and decentralized information systems and support.

Mr. Williams explained the challenges created by the diverse information needs and range of activities at the University. He provided a brief summary of protections in place including firewalls, a firewall waiver process, network access and blocking network traffic. He completed his presentation by emphasizing the importance of IT security awareness education noting one of the biggest threats is users giving up their credentials.
Following Mr. William’s presentation, Chair Young asked if any external audits, testing, or IT supervision was contracted with outside vendors. Mr. Todd and Mr. William’s confirmed that no testing was done. Mr. Todd explained that Control Scan performs penetration testing for the University’s credit cards operations; however, there are no other requirements for penetration testing. He agreed that it was a good idea.

**Other Business**

At 11:50 a.m., a motion was made, seconded and approved to go into executive session for the purpose of discussing civil actions, attorney-client privileged information, and the evaluation of public officers or employees. For the first item, all in attendance were excused from the meeting with the exception of Trustees, Vice President and General Counsel Fran Bazluke, Chief Compliance, Privacy Officer Anna Drummond, and Tanya Morehouse of the State Auditor’s Office. For the second and third items, Chief Internal Auditor William Harrison joined the session and Chief Compliance and Privacy Officer Anna Drummond was excused. For the third item, Vice President and General Counsel Fran Bazluke was excused.

**Adjournment**

The meeting was re-opened to the public at 12:42 p.m.

Following a brief discussion, a motion was made, seconded, and approved requesting that the Chief Internal Auditor provide his recommendations regarding additional performance metrics to be reported to the Audit Committee on the follow-up status of internal audit recommendations.

There being no further business, the meeting was adjourned.

Respectfully submitted,

Mark Young, Chair