A meeting of the Audit Committee of the Board of Trustees of the University of Vermont and State Agricultural College was held on Monday, July 8, 2013 at 9:00 a.m. in room 427A Waterman Building.

MEMBERS PRESENT: Chair Mark Young, Vice Chair Dale Rocheleau, Carolyn Branagan, Christopher Bray**, David Potter*, Raj Thakrar*, and Jeff Wilson*

MEMBERS ABSENT: None

OTHER TRUSTEES PRESENT: None

REPRESENTATIVES PRESENT: Staff Representative Wendy Coy, Alumni Representative Bill Cimonetti, Graduate Student Representative Lane Manning (filling on behalf of Jason Fuchs), and Doug Hoffer and Tanya Morehouse* of the State Auditor’s Office

REPRESENTATIVES ABSENT: Faculty Representative Albert Joy, Student Representative Joshua Barry

PERSONS ALSO PARTICIPATING: Vice President for Finance and Treasurer Richard Cate, Chief Internal Auditor William Harrison, Chief Compliance and Privacy Officer Anna Drummond, Information Security Officer Dean Williams, University Controller Claire Burlingham, Chief Risk Officer Al Turgeon, Chief Information Officer & Dean of Libraries and Learning Resources Mara Saule, Vice President for Legal Affairs and General Counsel Francine Bazluke, and Renee Bourget-Place and Sara Timmerman of KPMG

* Participated via teleconference call
** Joined the meeting at 9:30 a.m. via teleconference call

Chair Young called the meeting to order at 9:03 a.m.

Approval of Minutes

Chair Young began the meeting by thanking Trustee David Potter for presenting the Audit Committee summary report to the Board of Trustees at the May meeting.

A motion was made, seconded and voted to approve the April 29, 2013, meeting minutes.
Chief Internal Auditor Update

Chief Internal Auditor William Harrison began his presentation by referring to the first of five tables in his written status report provided in advance to the Committee. The Office of Audit Services (OAS) completed twenty reports and work products in FY 2013. This includes eleven EthicsPoint reports and four related control reports. In addition to planned work in process, the OAS has five open EthicsPoint reviews.

Moving on to table two, Mr. Harrison reviewed the FY 2013 Audit Plan and the proposed plan for FY 2014. Of the internal audits proposed last year, four were completed, four are in process, and three will carry-forward into FY 2014. The FY 2014 plan includes five audits to begin in FY 2014 or FY 2015. Mr. Harrison offered the Committee a brief overview of the methodology used to create the FY 2014 Audit Plan noting the direct correlation between the plan and the Enterprise Risk Management (ERM) draft risk and opportunity portfolio.

Next, Mr. Harrison provided a status report on internal audit recommendations. Referencing the Audit Recommendations definitions beginning on page 3 of his report, Mr. Harrison provided a brief summary of the classification and status reporting process. He also reviewed tables 3 through 5 which detailed all recommendations classified as essential, significant, or not rated as the recommendation was made prior to implementation of the rating system. Since the February 7, 2013 Audit Committee meeting, management has reported 16 recommendations as closed. The OAS is confirming the closed status of six of these recommendations.

Mr. Harrison concluded his presentation with an update on the recruitment for the Senior Auditor position. He is currently interviewing candidates and will make a selection in about a month.

Mr. Harrison confirmed for Chair Young that management is still considering their course of action and timelines for some of the Gift and Endowment Audit recommendations.

Chair Young expressed concern about the number of corrective actions to be completed by the fall of 2013. Vice President Cate commented that he felt this was a reasonable timeline. Both Mr. Harrison and Vice President Cate noted the new organizational chart effective July 1, 2013, and that some of the corrective actions have been assigned to new Responsible Officials.

Chief Compliance and Privacy Officer Update

As background for the first item of her report, the FY 2014 Compliance Work Plan, Ms. Drummond provided context by reminding the Committee that a compliance program is meant to assist both the Board of Trustees and management: helping management with its obligation to comply with the law and its own policies, and providing an assurance activity for the Board of Trustees, so that each Trustee can discharge their responsibility
for oversight of compliance. Part of that oversight responsibility is to ensure that systems are in place within the organization for compliance information (i.e. gaps in compliance, mitigation efforts), to be communicated to senior management and to the Board of Trustees. The Office’s Work Plan efforts are meant to evidence those systems and that oversight.

Against this background, Ms. Drummond presented the FY 2014 Compliance Work Plan. Ms. Drummond explained the development process for the FY 2014 Compliance Work Plan, including the steps taken to create the Compliance Risk Assessment. She discussed her consultations with campus stakeholders (including the Chief Internal Auditor); involvement with the Enterprise Risk Management (ERM) process; invitational compliance exit interviews with those who have had significant compliance responsibility (in order to determine if they have any compliance concerns); reviews of internal and external audit reports; identification of issues and trends experienced through analysis of compliance consultation requests, Ethics and Compliance Reporting Line activity and Government Reviews; reviews of other university work plans and detailed discussions with other Compliance Officers (a list of which was provided in the Report); reviews of professional higher education organization publications; reviews of federal agency OIG work plans; and analyzing the compliance risks identified in accordance with a modified COSO (Committee of Sponsoring Organizations of the Treadway Commission) framework to prioritize risk.

Referring to page 8 of her Report, Ms. Drummond reviewed the Compliance Risk Assessment Heat Map with the Committee. She summarized the areas included in the FY 2014 Work Plan: (i) HR issues, including the Affordable Care Act and the USCIS Form I-9, (ii) privacy and data retention issues, including the new HIPAA Omnibus Rule requirements, and (iii) health and safety issues related to the Violence Against Women Act. The FY 2014 Work Plan also includes the continuation of multi-year projects carried forward from the prior year, including: (a) phase two of the general work being continued in the area of Privacy, Information Security and Records Retention, and (b) Export Controls. She also referred the Committee to the areas on the Heat Map that reflect compliance subject matter areas where the Compliance Office has completed work in prior years through past Work Plans. Ms. Drummond then described how, when taken together, this past body of work, the annual Risk Assessment and Work Plan, and the Work Plan progress reports made at each Committee meeting, provides assurance to management and the Trustees for the discharge of their respective responsibilities.

Following up on the Audit Committee’s request to see the status of open and outstanding recommendations and observations, Ms. Drummond reviewed attachment B of her report (the Compliance Work Plan Log). The Compliance Work Plan Log details the status of all compliance topics and related observations and recommendations that the Compliance Office has reported upon over the past three years. It identifies for each topic and observation: the year in which the work was done, the observations/recommendations, the risk ranking as at the time of the work (as depicted on the relevant year’s Heat Map), the priority, action status, timeline for completion, responsible official(s), and oversight official(s). Ms. Drummond explained that the closed items are identified as shaded on the
Compliance Work Plan Log, while open items remain unshaded and include the current status and projected timeline as provided by the responsible officials. Ms. Drummond walked the Committee through the status of several work areas including Laboratory Safety, PHS Conflicts of Interest, Human Subjects Research compliance, Immigration (SEVIS) compliance, NCAA compliance, and Compliance Education and Training (i.e. mandated compliance training) and how the Committee can view the progress of management, including the open and closed compliance items in each area. The Office will continue to monitor management’s progress on all open observations and will report progress to the Committee. Mark Young thought the Compliance Work Plan Log was what the Committee had requested, but noted that it was a little difficult to read.

Moving on, Ms. Drummond reported that she has participated in responding to thirty-eight government reviews during the period April 1, 2010 through June 17, 2013. Referring to the charts in her Report, she noted the subject areas most reviewed by government agencies related to research and employment/discrimination issues, and the next largest area was environmental/safety facilities. Additionally, she noted that the Federal Government conducted 79% of all recorded reviews. In additional data, the Office has performed nine distinct compliance and privacy consultations for the period April 5, 2013 through June 12, 2013 bringing the cumulative total to 253 independent consults. Consultations include such things as questions on records retention or queries on ethics issues, sometimes from senior management. The Office is able to refer individuals to applicable policies and provide support and analysis. Data from the consultations is used to identify trends for the Work Plan and is presented to the Committee. Ms. Drummond also provided data on the Ethics and Compliance Reporting and Help Line (Help Line). Since the April 29 Audit Committee meeting, there have been two reports to the Help Line. To date, there have been forty-three reports of which thirty-three have been closed. Of the ten open reports, nine were referred to Audit Services, and one was referred to the Affirmative Action Office.

Ms. Drummond went on to discuss the Privacy Program. The Office continues to work with the Chief Information Officer and Information Security Officer to address sensitive information through working with individual offices around the University, and most recently, on certain procurement forms. In addition, the Office has worked toward the creation of confidentiality agreements in a number of areas within the University that have access to PRISM or other third-party databases with sensitive information, including protected health information. As a result, numerous UVM employees will now sign a confidentiality agreement with UVM in addition to the requirements mandated by Fletcher Allen Health Care (FAHC) as part of their annual credentialing process for access to certain electronic records at FAHC. Ms. Drummond confirmed for Chair Mark Young that privacy efforts have included Information Security Officer Dean Williams, Chief Information Officer David Todd, and Deputy Compliance Officer Erica Heffner. The group works closely to address both privacy and security issues.

Ms. Drummond briefly reviewed the areas of policy administration and communications. As part of the Office’s communication efforts, a Compliance Calendar is now available
on the Compliance Services website. The calendar serves to assist in tracking the University’s reporting and filing obligations to the various federal agencies.

In conclusion, regarding the proposed changes related to the realignment in the Compliance Program’s reporting structure, draft revised program documents were shared with the President on May 30, 2013. The Chief Internal Auditor and Chief Compliance Officer discussed these documents with the President July 1, 2013. Chair Mark Young noted the President would like to continue the discussion at the September 9, 2013 Audit Committee meeting.

Chair Mark Young commented on how he continues to be impressed by Ms. Drummond’s Work Plan and the thorough process she uses in developing it. Vice Chair Dale Rocheleau also commended Ms. Drummond on how she adjusts the Heat Map to reflect the modified risk level after a work area is completed.

**Information Security Officer Update**

Information Security Officer (ISO) Dean Williams began his report to the Committee with a summary of the security assessment and penetration test of a nonproduction instance in the PeopleSoft system. Audit Services, Enterprise Technology Services (ETS), and the ISO Team completed the evaluation of vendor proposals and selected the vendor Secure Ideas, LLC.

Before testing began a mutual agreement on the scope and ground rules for the engagement were established. Secure Ideas performed vulnerability assessments and penetration tests both from the Internet and from within the University's campus network. The external, Internet-based tests began with reconnaissance of the Internet-facing components of the target environment, and were designed to ascertain whether an external attacker could gain unauthorized access to the PeopleSoft applications or data, while the testing from within the UVM network simulated whether an attacker working on campus could compromise the security or confidentiality of PeopleSoft systems or data. The campus-based tests were also designed to show what a remote (Internet-based) attacker could accomplish after having illegitimately obtained UVM credentials, which can occur through “phishing” attacks on UVM students, faculty, and staff.

Mr. Williams further explained that Secure Ideas tested the security of all layers of the infrastructure supporting the PeopleSoft system. Additionally, they carried out social engineering attacks in several forms against a group of personnel who have elevated system privileges.

Mr. Williams thanked Audit Services, ETS, and the ISO Team for their assistance and cooperation during the engagement. This group will work to prioritize future vulnerability analysis and tests.

A copy of the Secure Ideas draft report has been distributed to everyone involved in the penetration testing process. At Chair Young’s request, Mr. Williams will also provide him
with a copy of the report. Representative Tanya Morehouse of the State Auditor's Office recommended having Secure Ideas discuss their findings with the Audit Committee as a way to limit distribution of the report. The idea was discussed and the Committee concluded they would determine their next steps after the executive session.

Moving on, Mr. Williams offered an update on the University’s compliance with Payment Card Industry Data Security Standards (PCI DSS) requirements. The most recent periodic review of Self-Assessment Questionnaire (SAQ) status reflected that 28 of 36 merchants passed their SAQs.

Mr. Williams next offered an overview of the CampusGuard Qualified Security Assessor’s (QSA) report that validated the overall design and implementation of the Actively Secured Private Network (ASPN) that protects cardholder data. The report focused on the CatCard Office and ETS resources that support the CatCard System. The QSA identified 57 PCI DSS requirements or sub-requirements that needed attention, 4 that needed correction, and 226 that were satisfied. The CatCard system was found to be fully compliant in 6 of the 12 major PCI DSS compliance areas. Many of the items require only documentation of policies and procedures and most of the requirements related to the technical security of the environment have been met. The ISO Team will be working over the summer on tasks related to the ASPN system, in addition to assisting merchants with completion of their own compliance tasks.

In response to Chair Young’s question about compliant transactions, Mr. Williams confirmed that 43% of the transactions at the University are in compliance. When the Bookstore’s three merchants are compliant, that will move the University up to 97% of sales being made by compliant merchants.

Mr. Williams concluded his presentation by highlighting a few of the ISO team’s security related projects listed in his report to the Committee.

**New Chief Information Officer**

Chair Young introduced Mara Saule as the new Chief Information Officer & Dean of Libraries and Learning Resources. The Committee welcomed and congratulated Ms. Saule on her new role at the University.

**FY 2013 Financial Statement/A-133 Audit Status Report**

Renee Bourget-Place of KPMG provided a status report on the FY 2013 financial statement and OMB Circular A-133 audits. All scheduled interim works has been completed as planned. The majority of the compliance test work has been completed with no significant control or compliance findings. There will be no change to the year-end audit work.

Ms. Bourget-Place reviewed KPMG’s work with management in a number of areas. These efforts included the implementation of GASB 63 and discussions about early
implementation of GASB 65, which management has decided to implement next year. Ms. Bourget-Place also noted KPMG’s work with Jennifer Gagnon and her team at Sponsored Project Administration providing subrecipient monitoring training.

Chair Young questioned if the changes to GASB will affect the University’s refinancing or reissuance of bonds. Controller Burlingham responded the changes would not. She added that she would provide the Committee with a presentation about the changes to the financial statements at the September meeting. Ms. Bourget-Place suggested also educating the Committee on the new GASB 65 requirements.

**Laboratory Safety Update**

Vice President for Finance Richard Cate provided the Committee with an update on the status of management’s corrective actions related to laboratory safety issues. Risk Management & Safety has implemented the audit software Lab Cliq and since its implementation in April, they have completed 44 laboratory audits. The laboratory audits have found no issues of imminent danger, however, Vice President Cate noted approximately half of the labs had kept chemical waste longer than the six months that are allowed and did not have up-to-date training. Overall, Vice President Cate is pleased with the laboratory improvements and believes that the regular audits will help create better compliance.

Vice President Cate also provided the Committee with developments in the area of laboratory safety training. In order to manage a new Occupational Safety & Health Administration (OSHA) requirement for chemical safety training, as well as to encourage all lab personnel to become current in their trainings, the University offered the first *Annual Refresher* training. Within the first two months, almost 200 people have completed this on-line training. Additionally, a new work group has been created and a campus-wide system to identify employees and students requiring training is expected to be operational by December 2013.

Responding to Chair Young’s question about who will replace him as the Responsible Official for laboratory safety, Vice President Cate explained that this would be announced before the next Audit Committee meeting.

Chair Young also commented on the value of the second annual Chemistry Safety day. This day-long break allows lab personnel to update their chemical inventory information, purge unused chemicals, attend trainings and clean their labs.

Committee member Carolyn Branagan thanked Vice President Cate for his efforts in the area of laboratory safety. She stressed the significance of laboratory safety as the University works to become a premier research university and noted the importance of eliminating risks in labs. Vice President Cate added that the President’s proposal to build a new laboratory facility and renovate the Cook Physical Science building would have a huge impact on improving laboratory safety as well as promoting the University as a research institution.
Chair Young commented that laboratory safety not only protects students, teachers and researchers but also educates the next generation and provides them with valuable skills to bring with them into the workforce. He also noted the variety of facilities that are considered laboratories and the different levels of risk they carry.

Vice President Cate clarified for Vice Chair Rocheleau that all 500 labs on campus are audited within a three year cycle. Mary Dewey, Director of Risk Management, explained the risk-based approach used to audit the laboratories.

**Enterprise Risk Management (ERM) Update**

Chief Risk Officer Al Turgeon began his presentation by noting he will now report to the Vice President for University Relations and Administration Thomas Gustafson. Mr. Turgeon has drafted the ERM Work Plan for FY 2014 and will be taking it to Vice President Gustafson by July 22, 2013. Key components of the plan include the President’s request to conduct risk assessments on the higher education funding model and administrative unit efficiency. Additionally, Mr. Turgeon and Director of Risk Management Mary Dewey are working with Associate Vice President for Administration and Facility Services Bill Ballard and Vice President for Student Affairs Annie Stevens, who run the University’s emergency operations group, to take a look at all the hazard related risks that could affect the institution and require an emergency response so that they can prepare for any emergencies the University may face.

Mr. Turgeon went on to explain that he plans to move away from managing the ERM process and focus on outreach and consultant work with responsible officials. He also plans to take a more proactive approach in thinking about emerging risks; risks not on the register or portfolio but are known to be coming. In addition, at the President’s request, he will develop a process that will warn senior management and the Board of these emerging risks. He plans to continue to report on this concept of bringing emerging risks into the risk assurance process.

Moving on, Mr. Turgeon reviewed his plans to assess the ERM program. He is looking into a self-assessment tool to see if the ERM program is being implemented appropriately and is useful to senior management and the Board of Trustees. The product of the assessment will be a continuous improvement plan.

As a result of the organizational restructuring at the University, other ERM work included renegotiating who would be responsible for the portfolio and register level risks. The Responsible Officials are in the process of completing their response plans to the risk and opportunities in the portfolio. Responses are due in August and Mr. Turgeon plans to provide these as well as a high-level review to the Committee.

Next, Mr. Turgeon noted he has almost completed a first draft of a risk appetite statement and has started work on the risk tolerance statement. Work in this area may take longer than anticipated and he plans to provide progress reports to the Committee.
Mr. Turgeon concluded his presentation by commenting on the change in the risk awareness culture at the University. There has been a great collaboration between the risk assurance group, organizations on campus, and Responsible Officials.

Ms. Bourget-Place asked if the risk register indicated to which Board Committee a risk belonged. Mr. Turgeon explained the register indicates which Responsible Official is responsible for each risk or opportunity. In their response plans, Responsible Officials will identify to which committee they have been reporting. He will assimilate this data so that the Audit Committee will know where the risks are being managed.

Vice Chair Rocheleau commented that he was happy to hear Mr. Turgeon report positive changes in the risk culture at the University. Additionally, Vice Chair Rocheleau questioned where Mr. Turgeon thought the University’s ERM program was relative to peer institutions within the higher education community. Mr. Turgeon and Ms. Bourget-Place both felt that the University was in the middle of the pack to above average of those who have already implemented an ERM program.

At the request of the Committee, Mr. Turgeon will provide an ERM presentation to the full Board at the October meeting.

Mr. Turgeon confirmed for Chair Young that there is collaboration among the 25 institutions that have implemented ERM.

**PurCard Update**

University Controller Claire Burlingham offered the Committee an update on the status of the purchasing card program and conversion to the US Bank card vendor. Before the conversion, the University had 1,700 active purchasing cards and held $42.3 million in credit exposure. As of June 25, the University has reduced the number of cards to 1,100 and the monthly exposure to $17 million. The new purchasing card program also allows the University to further reduce monthly and per transaction spending limits based on a cardholder’s role at the University.

Continuing on, Ms. Burlingham provided an overview of the new purchasing card training and assessment tools. Cardholders are now tested on their knowledge of the Travel policy, Procurement policy and their responsibilities as a cardholder. Eight training sessions were offered in addition to individual training sessions provided to a number of University departments and Colleges.

Finally, Ms. Burlingham was pleased report how smoothly the conversion went and that the University had accomplished its goals to improve business process, program management, data analytics and reporting tools. She shared that the University’s successful conversion had been showcased in VISA’s summer publication.

Staff Representative Wendy Coy commented that she found the training and assessment very helpful. As a cardholder herself, she felt the transition was great.
Chair Young thanked Ms. Burlingham for her report and commented on how pleased he was with the transition. Ms. Burlingham will provide the Committee with a copy of VISA’s summer publication.

Other Business

Chair Young confirmed that the next Audit Committee meeting is scheduled for September 9, 2013.

At 10:30 a.m., a motion was made, seconded and approved to go into executive session for the purpose of discussing civil actions and security procedures and similar information the disclosure of which would threaten the safety of persons or the security of public property. All in attendance were excused from the meeting, with the exception of Trustees, Vice President for Legal Affairs and General Counsel Francine Bazluke, Chief Internal Auditor William Harrison, Chief Compliance and Privacy Officer Anna Drummond, Chief Information Officer Mara Saule, Information Security Officer Dean Williams and Tanya Morehouse of the State Auditor’s Office. Chief Information Officer Mara Saule and Information Security Officer Dean Williams were excused from the meeting following the first executive agenda item.

Adjournment

The meeting was re-opened to the public at 11:19 a.m. There being no further business, the meeting was adjourned.

Respectfully submitted,

Mark Young, Chair