A meeting of the Audit Committee of the Board of Trustees of the University of Vermont and State Agricultural College was held on Monday, April 29, 2013 at 10:00 a.m. in room 427A Waterman Building.

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

MEMBER ABSENT: Christopher Bray

OTHER TRUSTEES PRESENT: None

REPRESENTATIVES PRESENT: Faculty Representative Albert Joy*, Staff Representative Wendy Coy, Alumni Representative Bill Cimonetti, and Graduate Student Representative Cornell Woodson

REPRESENTATIVES ABSENT: Student Representative Chris Juaire, and Tanya Moorehouse of the State Auditor’s Office.

PERSONS ALSO PARTICIPATING: President Thomas Sullivan, Vice President for Finance and Administration Richard Cate, Chief Internal Auditor William Harrison, Chief Compliance and Privacy Officer Anna Drummond, Information Security Officer Dean Williams, University Controller Claire Burlingham, Senior Strategist for Enterprise Risk and Planning Al Turgeon, and Director of the Department of Risk Management Mary Dewey.

* Participated via teleconference call

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 February 7, 2013, meeting minutes.

Chief Internal Auditor Update

Chief Internal Auditor William Harrison began by providing a brief summary of the audits listed in his written status report provided in advance to the Committee. Since the February 7 meeting, the Office of Audit Services (OAS) has issued four reports that included five recommendations. Mr. Harrison provided a summary of two recent audits; i) an Audit of Senior Management Travel and Business Meal Expenses and ii) an Audit
of the Grant Proposal Process. The audit reports included a total of eight recommendations classified as “useful”.

Next, Mr. Harrison presented the Committee with an update on the restructuring of the Office of Compliance and Privacy Services. The research completed by the Office of Compliance and Privacy Services shows that the University’s compliance program has been developed and implemented in a way generally consistent with the essential compliance program components at other schools. Using the results of their research, the Compliance Office has drafted a revised program description as well as draft charters for an Executive Compliance Committee and an Operational Compliance Committee. Mr. Harrison added that approximately sixty percent of the institutions reviewed had some type of Compliance Committee Structure in place. He plans to have a recommendation for the Committee at the July 8, 2013, meeting.

Moving on, Mr. Harrison reviewed the FY 2013 internal audit plan. The estimated completion dates for the General Information Technology Controls/IT Governance, Physical and Electronic Building Access Controls, and Inventory and Monitoring of Portable Devices Audits are the end of the Fiscal Year. Several planned audits will carry-forward into FY 2014 due to the deputy internal auditor vacancy and unplanned work that includes ten EthicsPoint reviews and three additional audits requested by management.

Mr. Harrison concluded his presentation with a preview of agenda items planned for the July 8, 2013, Audit Committee meeting. These items include summary reports of Presidential travel and housing expenses and a detailed report of all significant and essential internal audit recommendations.

Ms. Drummond responded to Vice Chair Rocheleau’s question about the restructuring of the compliance program by confirming that the University does not currently have an official Ethics Program outside of the Ethics and Compliance Reporting and Help Line and President Sullivan’s Statement on Ethics and Integrity, which she worked on with the President upon his arrival. Her revised program proposal includes a more robust Ethics Program.

Chair Young and Vice Chair Rocheleau will not be available to present the Audit Committee summary report at the May Board of Trustees meeting. Arrangements will be made with the Board Office.

For planning purposes, Chair Young requested three hours be allotted for the July 8 Audit Committee to accommodate planned agenda items.

Chief Compliance and Privacy Officer Update

Ms. Drummond began with an update on the FY 2013 Compliance Work Plan. She provided a summary of her Office’s work with the University’s Institutional Review Board (IRB) and the Research Protections Office (RPO). She explained that due to the inherent risks of research involving human subjects and the significant consequences that
may arise from a failure to apply adequate protections, this regulatory area has consistently been ranked as high risk in the annual risk assessment conducted by the Compliance Office.

Ms. Drummond provided a brief description of the historical context that led to the development of regulations to provide for the protection of human subjects. The 1978 Belmont report, issued in response to abuses involving human subjects in medical research, including the Tuskegee Study, proposed creating a federal system of review entailing self-regulation and governmental oversight. The Office for Human Research Protection (OHRP) was created under the Department of Health and Human Services (HHS). The OHRP “Common Rule” together with Food and Drug Administration (FDA) regulation, and the Health Insurance Portability and Accountability Act (HIPAA) provide the regulatory framework for how research is to be conducted involving human subjects, including requirements for informed consent, ethics, confidentiality and the mitigation of risk to subjects. Each institution, including UVM, enters into a Federal Wide Assurance (FWA), which is a form of contract, with OHRP for the protection of human subjects, certifying that the IRBs are organized and operated in compliance with applicable laws and regulation.

Ms. Drummond further explained that the UVM Research Protections Office (RPO) is responsible for the administration of the University’s IRB. The IRB’s role is to review and approve proposed non-exempt research before the involvement of human subjects and to provide continuing review of the research until the research protocol is closed.

The Compliance Office work efforts included the development, in conjunction with the RPO, of an assessment tool developed from OHRP and FDA checklists. This tool included over 200 compliance items and 70 quality assurance items. The Compliance Office reviewed the IRB's processes and procedures and made recommendations concerning: (1) IRB documentation and guidance materials, (2) routine self-monitoring/audits, (3) expanding the Ethics and Compliance Reporting and Help Line system to accept reports related to human subject research, (4) committee roster controls and documentation, and (5) committee minutes documentation.

Finally, the Compliance Office worked with the RPO staff to prioritize the identified compliance enhancements and create a work plan and time line for implementation. Ms. Drummond noted that many of the recommended enhancements from her Office were already complete or well underway by the conclusion of her work. Additionally, Ms. Drummond commended the RPO office, the Associate Vice President for Research and the Vice President for Research and Dean of the Graduate College for their efforts and collaborative work with the Compliance Office.

Next, Ms. Drummond offered the Committee a summary of compliance work prompted by the results of internal audits. She reported that her Office continues follow up with Sponsored Program Administration (SPA) on compliance issues raised in the Subrecipient Monitoring Audit Report #12-010. SPA is on track and has completed all the elements set out to date in the Management Response to the Audit Report.
Concerning the compliance/privacy observation identified in the Access Control and Other Matters Audit Report #13-006M, corrective actions are moving forward by the Center for Health and Well Being as projected or slightly ahead of schedule.

With respect to consultations, the Office of Compliance Services continues to provide compliance and privacy consultations upon request. Referring to her written report, Ms. Drummond provided the Committee with an overview of the types of issues addressed in these self-generated consultations and discussed the importance of such consultations to the Office of Compliance Services and to the University. She described how the chart illustrates that privacy and research were significant areas and that student issues were also substantial. She noted that these consultations, as self-generated, are a valuable tool for measuring the areas about which the campus is seeking guidance. In particular, she noted an increase over the past year of questions involving ethics/conflicts of interest and document retention. The Office of Compliance Services has performed seventeen distinct compliance and privacy consultations for the period December 18, 2012 through April 4, 2013. This brings the cumulative total to 244 independent consults. In terms of outreach, the Office performed outreach efforts for the Associate Deans Council, Human Resource Services, and the Library.

Ms. Drummond moved on to provide an update and data on the Ethics and Compliance Reporting and Help Line (Help Line). As of April 4, 2013, there have been forty-one reports to the Help Line and twenty-six have been closed. Of the twenty-six closed reports, thirteen were substantiated or partially substantiated, and 10 were unsubstantiated. The remainder of the reports were not properly within the scope of the Help Line or were not allegations needing to be substantiated. Thirty-one of the forty-one reports were made anonymously. Ms. Drummond also noted that of those who self-identified by category, two were students, twenty-four were employees, and two were faculty. Referring to her written report, Ms. Drummond provided a summary of the types of issues that were reported and the administrative area within which the alleged activities took place. The three issue types with the greatest number of reports included: accounting and financial issues, human resources issues, and misuse of resources. The University areas about which the most reports were made included, Financial and Enterprise Services, Student and Campus Life, and the academic units.

Ms. Drummond responded to a question posed by President Sullivan clarifying that of the forty-one reports made through the Help Line about half of the closed reports at any one time have been, at least, partially substantiated.

Ms. Drummond went on to discuss the Privacy Program. The Office continues to work with the Chief Information Officer (CIO) and Information Security Officer (ISO) to mitigate risk regarding private and/or sensitive University information and its utilization. Other work in the area of privacy included: (1) working with the Office of Clinical Trials Research and the College of Medicine to address data access and confidentiality issues, (2) reviewing privacy related training for the Vermont Children’s Health Improvement Program (VCHIP), (3) meeting with the Library faculty and staff to provide advice on the retention of several types of library records, (4) working with the Admissions Office to
eliminate the collection of admitted student SSNs through a web based form, (5) ongoing work with Human Resources regarding the collection of SSN on HR forms, and (6) working with the CIO, the ISO, the Director of Procurement and the Business Process Re-engineering Team regarding SSNs on certain procurement forms.

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

In conclusion, Ms. Drummond provided an update on policy administration. In accordance with the annual policy process, the list of policies and procedures to be reviewed or developed for the 2013-2014 academic year is almost finalized. The final list will be circulated to Responsible Officials by July 1, 2013.

**Information Security Officer Update**

Information Security Officer (ISO) Dean Williams provided a summary of his Office’s work since the February 7 Audit Committee meeting. He began with an overview of the Information Security Operations Team’s contributions to the planned security assessment and penetration test of the PeopleSoft system. A detailed analysis of the vendor proposals is currently underway. The engagement for testing has been moved into May due to scheduled PeopleSoft updates in April and complexity of the vendor proposals.

Moving on, Mr. Williams highlighted a few of his team’s education efforts to promote information security awareness at the University. The ISO Team offered two educational sessions at UVM’s annual staff development event, edu@UVM. They are also working with the Learning Services Team to incorporating information security concepts into Learning Services’ courses. For Information Technology (IT) professionals three “First Friday Informal InfoSec” lunch sessions were offered throughout the semester and the UVM@RISK digest was resumed to provide UVM-specific security information. For general audiences, the ISO team is developing weekly security "Quick Tips" as well as continuing to provide security alerts to the campus community.

Next, Mr. Williams offered an update on the University’s compliance with Payment Card Industry Data Security Standard (PCI DSS) requirements. All of the UVM Bookstore’s equipment that processes payment card transactions has been moved into the Actively Secured Private Network (ASPN). Eleven of the twelve merchants that require ASPN’s protection are now within that environment. This accounts for 99% of sales by dollar amount. Twenty-seven of the University’s thirty-five merchants have passed their annual Self-Assessment Questionnaires (SAQs). The ISO Team expects to complete the compliance elements for which they are responsible during the summer and continue working with the Controller’s Office to help the remaining merchants become fully compliant.

Following recommendations from CampusGuard and the Office of Audit Services, a Qualified Security Assessor (QSA) from CampusGuard came to campus April 8 to 10 to
complete a Report on Compliance (ROC) for the CatCard Service Center. The QSA also reviewed the design and implementation of ASPN and provide guidance for SAQ D merchants completing work needed for full compliance. Mr. Williams felt the QSA’s visit was generally positive and does not anticipate recommendations in the QSA’s written report to require significant changes to infrastructure or processes.

Moving on, Mr. Williams referred the Committee to the list of other ISO team projects provided in his report to the Committee. He highlighted this team’s work with Procurement Services, the Office of General Counsel, University departments, and vendors evaluating several new information systems to ensure that appropriate security provisions are in place and the University is contractually protected against liability for any vendor data breaches.

In conclusion, Mr. Williams provided the Committee with a staffing update noting Joshua Phillips joined the ISO team in March as an Information Technology Account Services Specialist.

**Enterprise Risk Management (ERM)**

Senior Strategist for Enterprise Risk and Planning Al Turgeon began by defining ERM as a consistent and continuous process across the whole organization for identifying, assessing, deciding on responses to and reporting on risks and opportunities affecting the institution’s competitiveness and strategic goals. He explained the process used to develop the University’s first risk and opportunity portfolio and register, the University’s ERM governance structure, and the assessment process for risks and opportunities. He reviewed the risk and opportunity portfolio with the Committee as well as the risk and opportunity register by strategic goal, President Sullivan’s strategic action plan areas, and institutional risk category.

Moving on, Mr. Turgeon reviewed the ERM timeline over the summer and process for finalizing and presenting the risk portfolio to the Board of Trustees. Next steps include the development of a management plan for each of the risks and opportunities in the portfolio, the development of a risk appetite and tolerance statement, and the development of a proposal for how to best identify and monitor emerging risks and opportunities.

Mr. Turgeon concluded his presentation with a note about efforts underway to address the high-risk area of business continuity and disaster recovery. Additionally, at the President’s request, the ERM office is preparing a recommendation of four to five risks or opportunities that could benefit from more in-depth assessments.

Chair Young commented on the significant undertaking the ERM initiative required. He thanked Mr. Turgeon for his efforts and outstanding work. He encouraged the Committee to review the risk and opportunity register and portfolio.
Vice Chair Rocheleau inquired of President Sullivan, what his impressions were of the ERM initiative and how he would use this tool for his engagement on risks and opportunities for the University as well as engaging the Board of Trustees. The President responded by first thanking Mr. Turgeon and his team for the thoroughness and the strategic nature of their work. He commented that he found the initiative very helpful and noted the importance of factoring risk assessment into each decision the University makes.

Vice Chair Rocheleau added that he agreed with Chair Young and President Sullivan on the high quality of the ERM program. He believes the program is a long term investment that provides the University with a framework for evaluating risks and opportunities that is disciplined, consistent, flexible and dynamic.

Vice President Cate remarked on the importance of creating an institutional culture of risk awareness. Mr. Turgeon added that the University should not be risk-averse and that the ERM program is designed to allow the University to evaluate opportunities as well as take prudent risks. Similarly, Vice Chair Rocheleau added that he felt an aspiration for the ERM program is to create a culture at the University that does think about risk and opportunities in the same vein and that everyone views themselves as an owner of risk and opportunities in their sphere of influence. Additionally, he felt that the University should think about risk and opportunities in a way that is consistent with what the ERM program is already doing. He commented on how such a culture could help the University in achieving its strategic initiatives.

Chair Young remarked on Mr. Turgeon’s work preparing for potential disasters and how he felt the ERM process would continue to be a useful tool for the University.

**Financial Statement/A-133 Audit Request for Proposal Process (RFP)**

The Request for Proposal Process agenda item was moved into the executive session.

**Overview of Risk Management Operations**

Chair Young thanked Director of Risk Management and Safety Mary Dewey for providing the Committee with an update on the University’s risk financing, risk control, and environmental, health and safety compliance efforts.

Ms. Dewey began with a review of her Department’s four key mission points; i) to promote safety and accident prevention, ii) manage the protection of University assets, iii) minimize legal liabilities, and iv) support compliance with environmental health and safety regulations. She explained the University’s risk financing strategy includes the purchase of insurance from the commercial insurance market, participation in group purchase programs, self-insured high deductibles through funded claims reserves as well as participation in alternative risk financing arrangements, and risk retentions groups to which the University is a subscriber.
Continuing on, Ms. Dewey reviewed Genesis Limited and Pinnacle Consortium of Higher Education. General liability and automobile liability are the insurances that are covered through this captive arrangement. The University retains a $500,000 deductible for general liability and a $25,000 deductible for automobile liability. The University joined Genesis in 2003 and the shareholders organized Pinnacle in 2004. Pinnacle collects all of the premiums and is the first gatekeeper for all claims. Genesis is the reinsurer for Pinnacle. Pinnacle retains 5% of the risk and cedes 95% to Genesis. Shareholders are subject to dividends and assessments with the allocation based on individual institutions’ premium paid. UVM has not paid any assessments.

Moving on, Ms. Dewey reviewed other significant insurance coverage purchased by the University as well as a summary of premiums and self-insured claims. She explained that institutional claim reserves exist for general liability, automobile, property, employment practices and workers compensation exposures. All liability and workers compensation reserve funding is based on outside actuarial analysis every two years. The balance in all the reserves as of June 30, 2012, was $3,460,677. Finally, she provided a comparison of the most costly causes of on-the-job injuries, the University’s trends in liability claim costs over 10 years, uninsured exposures to risk, and risk reduction strategies.

Responding to Committee member Potter’s questions, Ms. Dewey explained that uninsured risks are addressed by Risk Management & Safety as well as through the ERM process. Mr. Turgeon added that the ERM process will look into any insurance opportunities. Additionally, Ms. Dewey noted that the one area not covered by insurance that she is most concerned about was cyber security risk. She is currently working with ISO Dean Williams to review insurance coverage options. She felt confident that all the other significant insurable risks on the University’s ERM portfolio and register were insured.

Chair Young asked if the other members of Pinnacle and the reinsurances have the same deductibles or if the University chooses their deductibles and the amount of risk they want to hold. Ms. Dewey responded that in Genesis and Pinnacle the members have the same deductibles. The group purchase programs in which the University participates may have varying deductibles. Ms. Dewey also commented that participation in Pinnacle and Genesis provided for an opportunity for a pooling of minds to develop best risk management practices.

Ms. Dewey clarified for Representative Cimonetti that all of the liability for the on-campus non-University residential facility has been transferred to the developer via contract with respect to the developer’s actions, inactions or negligence.

In response to Vice Chair Rocheleau’s question about how often insurance programs are reviewed and put out for bid, Ms. Dewey confirmed that she received competitive quotes for most non-captive insurances every year.

Vice Chair Rocheleau commented that an uninsured exposure that he has observed is unfunded mandates from new legislation that are imposed upon the institution.
Chair Young thanked Ms. Dewey for her report and asked that the Chair of the Budget, Finance and Investment Committee receive a copy of her report. Vice President Cate confirmed that a report has already been sent to Chair McAneny.

**Other Business**

Chair Young thanked retiring CIO David Todd for his attendance at the Audit Committee meetings and his service to the University.

At Chair Young’s request, Controller Burlingham provided the Committee with an update on the new purchasing card program. The Controller’s office is looking for a full conversion by July 1, 2013.

At 11:30 a.m., a motion was made, seconded and approved to go into executive session for the purpose of discussing contract matters, civil actions, the evaluation of public officers or employees, discussion of personnel records, and to receive the advice of Counsel. All in attendance were excused from the meeting, with the exception of Trustees, President Tom Sullivan, Vice President for Finance and Administration Richard Cate, Vice President and General Counsel Francine Bazluke, Chief Internal Auditor William Harrison, University Controller Claire Burlingham, and Assistant Controller Lindsey Donovan. Following the first executive agenda item, Chief Compliance and Privacy Officer Anna Drummond joined the meeting and Controller Claire Burlingham, and Assistant Controller Lindsey Donovan were excused.

**Adjournment**

The meeting was re-opened to the public at 12:00 p.m. There being no further business, the meeting was adjourned.

Respectfully submitted,

Mark Young, Chair