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 12, 2011 at 10:00 a.m. in room 427A Waterman Building.

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

MEMBERS ABSENT: Carolyn Branagan and Brian Sozansky

OTHER TRUSTEES PRESENT: None

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

REPRESENTATIVES ABSENT: Alumni Representative Bill Cimonetti and Graduate Student Representative Daniel Sanchez

PERSONS ALSO PARTICIPATING: Vice President for Finance and Administration and University Treasurer Richard Cate, Chief Internal Auditor William Harrison, Chief Compliance and Privacy Officer Anna Drummond, Lead Auditor John Copoulos, Information Security Officer Dean Williams, University Controller Claire Burlingham, Renee Bourget-Place and Sarah Timmerman of KPMG and Tanya Morehouse of the State Auditor’s Office

*Participated via teleconference call

Chair Mark Young called the meeting to order at 10:05 a.m.

Approval of Minutes

A motion was made, seconded and voted to approve the April 25, 2011 meeting minutes with the correction of a few minor typing errors.

Chief Internal Auditor Update

Chief Internal Auditor William Harrison began by reviewing the summary of hours worked detailed in his status report which was submitted to Committee members in advance of this meeting. He was pleased to report that planned hours, unplanned hours, and other hours were in line with budgets.
Chair Mark Young inquired about the impact of special projects requested by the Board of Trustees on the Office of Audit Services (OAS) work plan. Mr. Harrison noted the large amount of his own time that was put into these projects.

Mr. Harrison moved on to a summary of internal audits. He commented on the overall positive experience working with UVM Extension, Enterprise Technology Services, the Print and Mail Center, the CATcard Center, and Athletics. Management was very responsive and willing to initiate corrective actions prior to the issuance of audit reports. The audit of the University of Vermont Extension Newport Office focused on internal controls over cash receipts. Findings included controls over cash receipts either did not exist or were not operating effectively, in violation of University policy. A review of management’s corrective actions is planned to begin in November of 2011. Mr. Harrison explained that follow up work is typically done six months after the completion of an audit. The follow up is akin to a mini audit of transactions to confirm management’s corrective actions have been put in place.

Continuing his summary, Mr. Harrison explained the Banner Student Information system is a purchased software package to support business processes related to the recruitment, admissions, registration, and billing of students. The scope of this audit focused on Banner system security and the integrity of the data within the system. Therefore, the general information technology (IT) controls reviewed related to logical access controls over infrastructure, applications, and data; program change management controls; and data center physical security controls. OAS recommended that management enhance segregation of duties in the change control process, develop a formal set of policies and procedures to document key IT support functions, and enhance the current tool used for tracking and documenting Banner changes. On August 10, 2011, Management provided OAS with a corrective action plan to address the report’s recommendations.

The CATcard Service Center is responsible for managing the campus identification card (smart card) program. Smart cards are used for personal identification, stored value (meal plans & CAT$cratch), access control to buildings and computer labs, library services, laundry, vending, and bus service. Closed Circuit Television equipment on campus is also maintained by the CATcard Service Center. In addition, the CATcard Service Center is a fee based provider of smart card services to three area colleges. Organizationally the CATcard Service Center is part of Administrative & Facilities Services. The purpose of the audit was to determine whether controls over cash receipts and disbursements were in compliance with UVM policies and procedures. After our preliminary risk assessment, the audit scope was expanded to include a review of CATcard System IT controls.

OAS noted opportunities for improvements in controls relative to data center physical security, segregation of CATcard IT duties, issuance of CATcards to external contractors, CATcard IT security risk assessment, and compliance with Payment Card Industry Data Security Standards. OAS noted that the contract with the CATcard Service Center’s smart card vendor currently exceeds both the $1 million and 5 year thresholds that trigger Board of Trustees involvement; however, the contract has not gone through adequate internal review or the Board’s approval process. Contracts with two of three area colleges
for the provision of smart card services have not been formally reviewed or updated since their inception in FY 2004.

OAS also found that the CATcard Service Center processed almost $50,000 of UVM departmental CAT$cratch purchases without first verifying that transactions were consistent with University policy. The CATcard Service Center did not maintain an up-to-date Memorandum of Understanding (MOU) or follow a formal documented business planning and risk assessment process. Finally, checks were not always deposited at least twice a week as required by UVM Policy although no timing issues were noted with daily cash deposits. Accounting reconciliation documentation needs improvement.

Chair Young questioned why the CATcard smart card vendor contract needing Board approval was not detected prior to the audit. Discussion ensued about improving internal controls over contract approvals in the Procurement Office as well as in the departments where contracts originate.

Chair Young inquired if Champlain College, one of the schools serviced by the CATcard Center, notified its users about using a third party servicer. Mr. Harrison responded that he did not know.

Trustee Bill Botzow requested an example of the prizes mentioned in the CATcard Service Center report. Mr. Copoulos, Lead Auditor, provided an example.

Mr. Harrison concluded his summary by reviewing findings from the Print and Mail and Athletic Ticket Sales audits. Both shared similar issues in terms of deposit handling and timing, restrictive check endorsement and segregation of duties.

Finally, Mr. Harrison concluded this presentation with an explanation of the OAS’s new Audit Quality Survey. The first survey was sent out to the UVM Extension Office. The average score was 6.71 on a scale of 7 (with 7 being most favorable). The survey questions focus on timeliness, communication and professionalism. The Office plans to use this survey after most of its audits.

Trustee Botzow asked Mr. Harrison if the survey allowed participants the opportunity to provide comments. Mr. Harrison confirmed that it did and noted that his office previously initiated plans to improve certain communications in response to the last survey.

**Chief Compliance and Privacy Officer Update**

Ms. Drummond began with an update on the FY 2012 Compliance Work Plan and work done on two multi-year efforts: (i) laboratory safety and environmental practices, and (ii) privacy, information security, and data retention.

In the area of privacy, information security and data retention, Ms. Drummond first addressed the Office’s work in assisting the Chief Information Officer and Information Security Officer with their draft Information and Security Policy and Procedures. As a part of this work, the Office removed the “privacy” content from the prior Information
Security Policy, and developed a stand-alone Privacy Policy and Procedure which has been submitted to Interim President Bramley for approval.

Much work has been done by the Office in regard to the Health Insurance Portability and Accountability Act (HIPAA); specifically, the Office has continued the University’s commitment to ensuring the privacy and security of protected personal information by drafting a framework for improved compliance with HIPAA and the Health Information Technology for Economic and Clinical Health Act (HITECH). In collaboration with the Office of General Counsel, “covered components” of the University that have been identified by counsel have been engaged in a conversation to clarify expectations, assist in identification of their responsibilities and have been provided with suggestions for the steps needed to be completed in order to demonstrate compliance. A periodic assurance process is being developed for future utilization with each of the covered components.

Additionally, the Chief Privacy Officer has joined a network of Chief Privacy Officers in Higher Education. Ms. Drummond believes this network will assist UVM in adopting best practices in the area of privacy. Also, in the area of privacy, the Office has dedicated part of its website to the Office of Privacy Services. When complete, the Privacy Policy and Procedure, as well as other privacy information useful to the University community will be available.

In the area of laboratory safety, the Compliance Office has completed its assessment of laboratory safety and structural issues regarding the Cook Physical Sciences Building. The report recommends that the University create: (a) enhanced communication and collaboration between academicians and the administrative staff, (b) greater clarification of oversight, enforcement and accountability processes (through clearer policies and procedures), (c) enhanced training delivery and documentation/tracking of such training, and (d) better identifiable reserves/budgeting for laboratory safety compliance items of a facilities nature, as well as continuing the coordination of larger improvements with the latter, where applicable. The report, prepared at the request and direction of counsel, was shared with the Interim President, Provost, General Counsel, Vice President of Finance and Administration, Vice President for Research and Dean of the Graduate College, Interim Dean of the College of Arts and Sciences, Chief Internal Auditor, Associate Vice President of Administrative and Facilities Services, Chairs of both the Chemistry and Physics Departments, and the Director of Risk Management.

The Office continues its work with the Work Group on Laboratory Safety. A new Draft Laboratory Safety Policy has been drafted by that group, which focuses on responsibility, oversight, communication and enforcement. Also being drafted, or significantly revised, are procedures addressing specific safety requirements for certain types of laboratories or certain types of hazards. The long-term goal is to have one website with procedures and information related to laboratory safety that currently exists in multiple locations across the University. The Director Risk Management, Mary Dewey, is working to provide this resource to the University community.
Work on the FY 2012 work plan has also begun since the last Audit Committee meeting. In particular work has continued in the area of the Program Integrity Rules. The Department of Education (DOE) promulgated the “Program Integrity Rules” in October of 2010 with rolling effective dates. These rules apply to all Title IV eligible institutions and are intended to promote integrity in higher education programs by protecting students as consumers. In collaboration with the Office of General Counsel, a matrix of the compliance requirements of the Program Integrity Rules has been created, and the Office is working with each of the responsible offices to assess compliance. Specific compliance areas have included the required complaint mechanism, incentive compensation, and state authorization. Ms. Drummond plans to provide an extensive report on the Program Integrity Rules to the Committee at a future date.

Ms. Drummond moved on to discuss new federal guidance regarding sexual harassment. In April 2011, the Department of Education published guidance clarifying sexual violence as a form of sexual harassment that is prohibited as a form of discrimination under Title IX of the Education Amendments of 1972. The guidance describes additional institutional obligations for ensuring compliance with the application of Title IX to incidents of sexual violence and, ultimately, to prevent this form of discrimination. The Office has begun the work for an assessment of the University’s policies on discrimination, harassment and sexual assault to determine what, if any, changes are necessary to meet compliance under the new guidelines. The Office will be closely working with the appropriate University personnel in respect of these issues and will provide a more fulsome report on this issue to the Committee at a future date.

Next, Ms. Drummond discussed the Office’s work with Audit Services. Under the new configuration of Compliance Services and Audit Services, the Office follows up with management on compliance issues identified by audits conducted by Audit Services. Compliance works with management to address the identified issues and, at six months post-audit, the Office reports on management’s compliance progress to the Audit Committee. Audit Services can then calendar a subsequent audit to test for compliance, beginning the cycle anew.

The first time this process was implemented appears to have been a success. Office of Audit Services Report #11-001, “Compliance with Certain Provisions of FLSA”, was issued in December 2010. The report reviewed compliance with the Fair Labor Standards Act (FLSA) in one specific University unit, as well as recommended changes for enhanced compliance of long-term existing practices on a University-wide basis.

Beginning in January of 2011, the Chief Compliance Officer convened a series of meetings with Human Resources, the Controller, and the Director of the Business Practices and Planning, amongst others, to review the auditor’s recommendations and develop a plan to enhance certain University practices involving FLSA compliance. The group reevaluated the existing record keeping and time reporting processes for non-exempt employees at the University along with certain accounting practices and procedures. A plan was then developed to implement enhancements to current systems by adding electronic functionality that will better ensure consistent compliance.
Management plans to have these enhancements in place by December 31, 2011. Additional, more long-term changes are planned to occur by 2013, involving certain upgrades to PeopleSoft Version 9.1. Ms. Drummond took the opportunity to thank Mr. Cate for his assistance and support in this process.

The Office continues to conduct outreach with the University community in order to discuss compliance issues and further create a culture of compliance. Since the last Committee meeting, the Chief Compliance Officer has spoken to the Office of Human Resource Services staff, the President’s Campus Accessibility Task Force, and the Academic Business Managers.

Ms. Drummond continued on to discuss the Office’s communications plans. As previously noted, the Office’s website has been redesigned to provide distinct content for both the compliance and privacy programs. Plans are also in place to resume the Offices work on the Compliance Services/Code of Conduct awareness survey in September.

The Office of Compliance Services continues to provide compliance and privacy consultations upon request or in response to new regulatory requirements. The Office has performed twenty-five distinct compliance and privacy consultations for the period April 1, 2011, through August 25th, 2011, bringing their cumulative total to over 100 consultations.

Ms. Drummond summarized the Office’s work on University policy administration. In collaboration with General Counsel and the Vice President for Executive Operations, the Office is working to review University policies with the goal of making existing policies more effective in communicating the rights and responsibilities of our community members. The group is working to ensure: (i) closure of policy gaps, (ii) appropriate prioritization of new policies, and (iii) the overall effectiveness of our existing policies and policy processes. A new policy queue identifying and prioritizing policy gaps has been developed by General Counsel, the Compliance Office and the Vice President for Executive Operations. In addition, templates for the format of new University Operating Procedures have been created in addition to mechanisms for posting such documents on the Policy website. A new Policy on the Adoption of Policies will reflect new categories of “rule” and changes in the “rule making” process.

Next, Ms. Drummond provided an update on the Ethics and Compliance Reporting Help Line. One new report has been received since the prior report to the Audit Committee. Thus, there have been a total of twelve reports made to date, ten of which have been closed. Of the two outstanding reports, one was referred to Audit Services for investigation, while the other is being addressed by the applicable management group.

Finally, since the April 2011 Audit Committee meeting, the Office of Privacy Services has responded to two privacy incidents. The new Data Breach Notification Policy covering breaches, as well as privacy incidents that do not rise to the level of a breach, was followed.
Information Security Officer Update

Dean Williams offered his first report to the Committee in his role as Information Security Officer. Although the information security officer position is new, information security is not. There is a strong desire across the University to protect individuals’ privacy. However, securing information can be inconvenient, labor-intensive and expensive. Mr. Williams explained that the University of Vermont’s network architecture divides administrative, enterprise, academic and residence halls network services. Access to enterprise information systems is controlled by using strong passwords and core system access requires “two-factor” authentication. Additionally, networks are scanned for vulnerabilities.

Protecting laptops, desktop workstations, and mobile devices has risen to the top of Mr. Williams’ list. Planned work in this area includes; replacing virus protection software, implementing patch management software and laptop hard drive encryption. People are considered the weakest link in information security. In response to this, Mr. Williams has taken a proactive approach educating the University’s community, such as providing training to new employees at orientation sessions. Additionally, he is targeting groups to attend a web-based video series on the theme of “Securing the Human”. The new Information Security Policy also helps to provide user awareness by defining responsibilities in depth. He noted he had read hacking has become “big business” and cybercrime accounts for about four hundred billion dollars per year.

Mr. Williams went on to describe his Information Security Operations team. A fulltime security engineer will join his existing team of five in January of 2012. A major focus of the team has been to assist the Controller’s Office and other university departments in complying with the security requirements for accepting credit and debit card payments.

In conclusion, Mr. Williams noted the importance of collaborations and consortia. Internally, information security efforts intersect with work done in Audit Services, Compliance and Privacy, Enterprise Risk Management, Police Services, technical personnel, and units responsible for major collections of University information, such as Human Resource Services and the Registrar’s Office. Externally, information security is benefiting from memberships and affiliations with REN-ISAC, EDUCAUSE, SANS, NERCOMP, InCommon, Internet2, and Shadowserver.

Trustee Bill Botzow inquired as to how the Committee could measure the success of the Information Security Operations team in addition to the Offices of Audit and Compliance Services in securing the University’s resources. Richard Cate noted that these functions serve to minimize risks.

Trustee Botzow also inquired as to how “rich” of a target the University is. Ms. Drummond and Mr. Williams agreed that we are a rich source as is typical of most universities. Ms. Drummond noted that the unique environment of higher education tends to increase information security risks and that the breaches that have been reported on publically available clearinghouse websites support this.
Finally, Trustee Botzow questioned the effectiveness of the Data Breach Notification Policy. Ms. Drummond assured the Committee the system seems to be working well and responses have been very timely.

Chair Young expressed concerns about controls over terminated employees. Mr. Williams noted procedures were already in place to segregate duties and formalize departures from the University.

**KPMG FY11 Financial Statement/A-133 Audit Status Report**

Renee Bourget-Place of KPMG provided an interim report on the FY 2011 financial statement and OMB Circular A-133 audits. The Firm is about half way through the Financial Statements audit. Work is going well and being completed on target. So far, no major adjustments have been identified and much of the work on the A-133 audit is done. The Firm has just received the final schedule of federal awards. They are testing to make sure the programs they have chosen to test are the only programs they need to test.

KPMG will be looking at certain components of the information technology (IT) system with a particular emphasis on PeopleSoft and other systems used to create the financial statements. Ms. Bourget-Place concluded with a comment: IT, risk, governance and information security have been on every Audit Committee agenda she has seen. She expects this will continue and asked if there was anything KPMG could look at in the audit to help supplement areas of concern the Audit Committee may have.

Chair Young asked if the University had done external IT testing. David Todd, Chief Information Officer, indicated that no external testing had been done to date however; there are plans for external testing. Mr. Todd also noted that internal testing has been done for several years.

**Enterprise Risk Management (ERM) Update**

Due to time constraints Vice President Cate began by referring the Committee to his status report submitted in advance. He noted his newly added responsibility as the Responsible Official for Laboratory Safety. Chair Young expressed concern about the number of responsibilities Mr. Cate has been given and if this is putting the institution at risk. Mr. Cate responded by saying he is able to delegate some of this work to his very capable staff and knows his own limits.

Mr. Cate went on to explain that the Risk Assurance Group had held its first meeting on August 31, 2011. The Committee reviewed and discussed the charge, roles, responsibilities, as well as, membership. Additionally, the final draft of the Committee charter will be forwarded to Interim President Bramley for final approval. This group plans to meet every six to eight weeks.
A first draft of risks and opportunities identified through interviews with the Deans and Vice Presidents has been compiled in a “risk register”. The draft will be distributed for comment before being submitted to the President’s Advisory Committee on Enterprise Risk Management, the President and the Board of Trustees.

At the conclusion of Mr. Cate’s presentation, he noted that the Vice President for Finance and Administration, General Counsel, Chief Compliance and Privacy Officer, Director of Risk Management, Senior Strategist for Enterprise Risk and Planning, and Chief Internal Auditor plan to meet later this month to review a preliminary institutional risk register. The group will draft rating scales for assessing risks and opportunities based on impact and likelihood.

Trustee Botzow expressed his concerns about disclosures under open record laws and the implications for exposing the University’s risks to the public.

**Annual Review of Audit Committee Charter**

The Audit Committee Charter was discussed and due to lack of time a motion was made and seconded to continue the discussion at the November 2011 Committee meeting.

**Other Business**

At 11:30 a.m., a motion was made, seconded and approved to go into executive session to consider pending civil actions and discussion of a personnel matter. All in attendance were excused from the meeting, with the exception of Trustees, Tanya Morehouse of the State Auditor’s Office, Chief Internal Auditor Bill Harrison and Chief Compliance Officer Anna Drummond were present for both agenda items.

**Adjournment**

The meeting was re-opened to the public at 12:15 p.m. There being no further business, the meeting was adjourned.

Respectfully submitted,

Mark Young, Chair