THE UNIVERSITY OF VERMONT AND STATE AGRICULTURAL COLLEGE
BOARD OF TRUSTEES

AUDIT COMMITTEE

Members: Chair Shap Smith, Vice Chair Jodi Goldstein, Matt Devost, Katelynn Giroux, Ed Pagano, Kristina Pisanelli, and Catherine Toll

Representatives: Faculty Representative Barbara Arel, Staff Representative Mindy Bean, Graduate Student Representative Jaiden Capozzi, Alumni Representative (vacant), Student Representative Matt Sorensen, and Representative Doug Hoffer of the State Auditor's Office

Monday, September 16, 2024

10:00 a.m. – 11:30 a.m.
Memorial Lounge, 338 Waterman Building

AGENDA

	Item	Enclosure/ Exemption	Discussion Leader(s)	Times*
	Call to Order			***10:00 am.**
1.	Approval of April 11, 2024 meeting minutes	Attachment 1	Shap Smith	10:00-10:05
2.	Fiscal year 2024 financial statement/uniform guidance audit status report	Attachment 2	David Gagnon Sara Timmerman, KPMG	10:05-10:15
3.	Internal audit update	Attachment 3	Bill Harrison	10:15-10:30
4.	Report on expenses incurred by the University under the President's Official Residence university operating procedure	Attachment 4	Bill Harrison	10:30-10:40
5.	Review and approval of revisions to the Audit Committee charge and charter	Attachment 5; Appendices A&B	Bill Harrison	10:40-10:50
6.	Information Security Report (Enterprise Risk Management Risk #14 Update)	Attachment 6	Darcy Pientka Scott Carbee	10:50-11:00
7.	Gramm-Leach-Bliley Act (GLBA)	Attachment 7	Darcy Pientka Scott Carbee	11:00-11:10

	Item	Enclosure/ Exemption	Discussion Leader(s)	Times*
8.	Other business		Shap Smith	11:10-11:15
	Motion to enter executive session**	**Exemption**		
9.	Performance evaluation of Chief Internal Auditor	The appointment or employment or evaluation of a public officer or employee	Shap Smith Suresh Garimella	11:15-11:30
	Motion to go out of executive session		Shap Smith	
	Motion to adjourn			**11:30 a.m.**

* Time is approximate.

** The Chair will entertain a motion to enter into executive session for the purpose of discussing the appointment or employment or evaluation of a public officer or employee. No action is anticipated following.

AUDIT COMMITTEE
BOARD OF TRUSTEES
UNIVERSITY OF VERMONT AND STATE AGRICULTURAL COLLEGE

A meeting of the Audit Committee of the Board of Trustees of the University of Vermont and State Agricultural College was held on Thursday, April 11, 2024, at 3:00 p.m. in room 230 Waterman Building.

MEMBERS PRESENT: Chair Shap Smith, Vice Chair Jodi Goldstein[1], Matt Devost[1], Katelynn Giroux[1], and Catherine Toll[1]

MEMBERS ABSENT: Ed Pagano and Kristina Pisanelli

OTHER TRUSTEES PRESENT: Board Chair Ron Lumbra[1]

REPRESENTATIVES PRESENT: Faculty Representative Barbara Arel[2], Staff Representative Mindy Bean[2], Alumni Representative Susan Higgins, and Student Representative Matt Sorenson

REPRESENTATIVES ABSENT: Graduate Student Representative Vanessa Ballard and Vermont State Deputy Auditor Tim Ashe (on behalf of Vermont State Auditor Douglas Hoffer)

PERSONS ALSO PARTICIPATING: Vice President for Finance and Administration Richard Cate, Chief Safety and Compliance Officer Michael Schirling[3], Director of Compliance Services and Chief Privacy Officer Tessa Lucey, and David Gagnon, and Sara Timmerman of KPMG

[1] Joined via remote conferencing.
[2] Joined the meeting at 3:04 p.m.
[3] Joined the meeting at 3:29 p.m.

Chair Shap Smith called the meeting to order at 3:02 p.m. He began by welcoming new committee members Matt Devost and Katelynn Giroux.

Approval of minutes

A motion was made, seconded, and voted to approve the February 8, 2024, meeting minutes.

Presentation of the Fiscal Year (FY) 2024 external audit engagement plan

Referring the committee to attachment 2, Lead Audit Engagement Partner David Gagnon provided an overview of KPMG's plan for the FY 2024 audit engagement. He started by reviewing the required communications and client service team.

Next, Senior Audit Manager Sara Timmerman offered an overview of the audit materiality, timeline, preliminary risk assessment as well as KPMG's audit approach. KPMG plans to audit one major program, the student financial assistance cluster, under the Uniform Guidance for federal awards.

In conclusion, Mr. Gagnon explained how KPMG utilizes technology to enhance the audit experience and provide a quality audit. He also described KPMG's professional responsibilities including the responsibility to maintain and monitor independence.

Higher education industry update

Mr. Gagnon offered a high-level summary of KPMG's 2024 higher education industry update included in attachment 2 of the meeting materials.

Following Mr. Gagnon's presentation, Chair Smith presented the following resolution for approval:

> **Resolution authorizing retention of external audit firm for the FY 2024 mandatory annual audits**
>
> WHEREAS, on April 11, 2022 the Audit Committee recommended, and the Board of Trustees approved, authorizing the Vice President for Finance and Administration to enter into a contract with KPMG, LLP to obtain external audit services to conduct the annual financial statement audit and other related audits of the university for five consecutive years during the period April 1, 2022, through March 31, 2027, at a total contract price not to exceed $2,160,000, with continuation of said contract subject to an annual performance review by the Audit Committee; and
>
> WHEREAS, the Audit Committee recommends retention of KPMG, LLP for the FY 2024 mandatory audits;
>
> BE IT RESOLVED, that the annual audit shall be conducted in compliance with the requirements of the University Bylaws and state and federal law.

Chair Smith offered an opportunity for discussion. There being none, a motion was made, seconded and the resolution was approved as presented.

Compliance update

Director of Compliance Services and Chief Privacy Officer Tessa Lucey offered a few highlights from her interim report and dashboards provided to the committee in attachments 4 and 5. As background for the new committee members, Ms. Lucey explained that the University's Compliance program is based on the Seven Elements of an Effective Compliance Program as outlined by the Federal Sentencing Guidelines. Her reports are structured around these seven elements to clearly articulate the effectiveness of the University's compliance program to the committee.

Continuing on, Ms. Lucey highlighted work plan efforts in the areas of foreign influence and improvements to the institutional policy process. She commented on how the policy modernization project is helping address the Enterprise Risk Management (ERM) register risk entitled "Insufficient Knowledge/ Understanding of Policy Expectations."

Next, Ms. Lucey advised the committee that the State of Vermont is in the process of developing a new privacy law that unanimously passed the house and is currently in front of the senate.

To finish, Ms. Lucey discussed the program's contingent activities. She reviewed compliance consultations noting that many were directly correlated to the ERM program. She also described how her office continues to monitor and track helpline reports.

Emergency preparedness & institutional continuity report (ERM Risk #29 update), and campus threats/mass casualty report (ERM Risk #7 update)

Chief Safety and Compliance Officer Michael Schirling provided a brief status update on the ERM emergency preparedness & institutional continuity risk, and the campus threats/mass casualty risk which were provided in the summary reports included as attachment 6 of the meeting materials. Mr. Schirling provided an overview of work that has been done to date and described work that is being planned but not yet completed.

Adjournment

There being no further business, the meeting was adjourned at 3:50 p.m.

Respectfully submitted,

Shap Smith, Chair

Attachment 2

KPMG

University of Vermont State and Agricultural College Audit Committee

2024 Audit status update

September 16, 2024

Introduction

To the Audit Committee of the University of Vermont State and Agricultural College (UVM):

We are pleased to have the opportunity to meet with you on September 16, 2024 to discuss the status of the audit of the financial statements of UVM as of and for the year ended June 30, 2024, and the Single Audit in accordance with 2 CFR 200 for the year then ended.

This document, which outlines the status of our audit procedures performed to-date, is being provided to you in advance of the meeting to allow you sufficient time to consider the key matters and formulate your questions.

We believe the contents of this document should provide a good platform for our discussions when we do meet. We will be pleased to elaborate further on matters covered in this document at the meeting.

Content	Page(s)

Financial statement audit update

Procedures performed and other observations:

- Performed procedures to obtain an understanding of entity-level controls and performed analytical procedures and risk assessment on certain accounts through interim dates.
- Preliminarily discussed changes to discretely presented component units presentation and disclosure as a result of JVs.
- Interviewed key personnel to understand the risks faced by the University (including fraud risks) and to understand the control environment from their perspective.
- Non-GAAP policies were identified and are consistent with prior years. We will summarize the significant policies in our final report to the Audit Committee along with the impact to the financial statements, if required.
- Performed detailed tuition testing at interim. No exceptions noted.
- Reviewed management's enhancements to the presentation of discounts to student services revenues and the determination of scholarship expenses.

Year-end substantive detail testing began on 9/3/24.

Single audit update

- Completed preliminary major program determination based on federal expenditure discussions with the University as of 3/31/24:
  - Preliminarily identified one major program for testing: Student Financial Assistance Cluster (SFA)
  - Possible additional major program(s) to be determined based upon final draft schedule of expenditures of federal awards (SEFA) through 6/30/24 to be provided by management in mid September 2024.

Procedures performed on SFA

- Inquired with University personnel to understand the risks faced by the University and to gain an understanding of the control environment
- Began documenting our initial understanding of controls in place for several direct and material compliance requirements
- Reviewed applicable University policies and procedures over the administration of the program
- Compliance testing in progress for certain compliance requirements
- The liquidation of the Perkins Loan program will be tested as an additional compliance requirement specific to FY24

Information technology update

- Process and walkthrough meetings completed in June and July 2024
- Key IT application reviewed:
    - Banner – student system
    - General IT review performed over Banner

Questions?

For additional information and audit committee resources, including National Audit Committee Peer Exchange series, a Quarterly webcast, and suggested publications, visit the KPMG Audit Committee Institute (ACI) at www.kpmg.com/ACI

This presentation to the Audit, Risk, and Compliance Committee is intended solely for the information and use of the Audit, Risk, and Compliance Committee and management and is not intended to be and should not be used by anyone other than these specified parties. This presentation is not intended for general use, circulation or publication and should not be published, circulated, reproduced or used for any purpose without our prior written permission in each specific instance.

---

kpmg.com/socialmedia

Internal Audit Update

Summary of Reports and Work Plan Status

Board of Trustees - Audit Committee
September 16, 2024

Prepared By
William Harrison, Chief Internal Auditor

Update Notes

Audit Reporting

Since the February meeting, we issued final and draft reports on the following:

- Complex Systems Center – Final (Report No. 24-009).
- PurCard Review – Final (Report No. 24-010).
- IT Risk Assessment – Final (Report No. 24-011).
- ADA Assessment – Final (Report No. 24-012).
- Farm Safety Assessment – Final (Report No. 25-001).
- President's Official Residence – Final (Report No. 25-002).
- Data Breach Notification Policy – Draft.
- Helpline Report No. 0022aa23 – Draft.
- Rubenstein School Facility Management Advisory Project – Draft.

Audit Progress

1. We are drafting the report of our audit of the temporary employment process.
2. We started an internal audit of income and expense activity procedures. This audit was requested by management. The focus of the audit is on those activities that charge sponsored projects for internal supplies and services in compliance with university policies and procedures.
3. We started an internal audit of an international sponsored project. Mandated by the sponsor, we will perform interim and final audits of grant funds received and project expenditures.
4. We started an internal audit of the Affiliated Organizations (AO) policy. Affiliated organizations are entities that are legally distinct from the University but are organized and operated for the benefit and in support of the University and/or conduct activities that advance our mission. The planned focus of the audit will be on financial monitoring/oversight terms and conditions of AO agreements.

Audit Follow-Up

5. Regarding the aged and open information technology recommendations, we did not receive an update for this report. Further, specific action plans and action plan dates are not provided on several open recommendations. We will continue to request semiannual updates from management.

6. Overall, we issued new reports containing 15 recommendations, closed 30 recommendations, with 113 recommendations remaining open at the end of the reporting period.

Advisory Communications

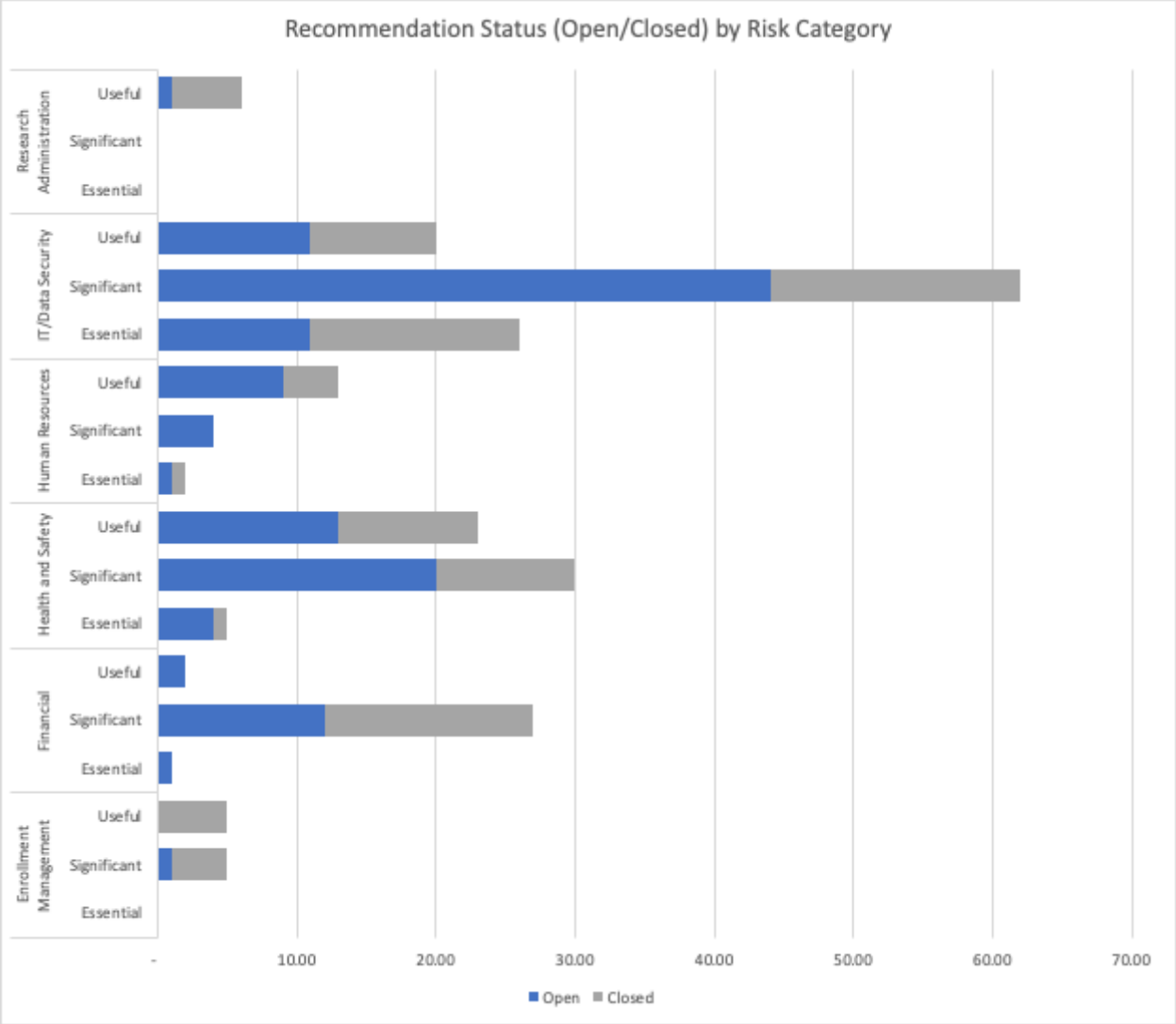
In addition to more formal reports, the Office often provides advice on internal controls and policy compliance, performs special projects, or shares the results of prior audits that may be of interest to responsible officials. In fiscal year 2024, we started more formally tracking these communications. In 2024, the Office provided 13 advisory communications related to the following ERM risk/opportunity areas: human resources (4), financial (2), health and safety (1), information technology (2), and operations (4).

New Audit Follow-Up Process

We are now tracking all new audit recommendations using SharePoint and have created SharePoint sites for all administrative divisions. Each site provides responsible officials with a dashboard of all open and closed recommendations and the ability to directly upload follow-up documents showing completion or modification of corrective action plans. These SharePoint sites allow us to more securely share information with responsible officials, monitor site access, and timelier track recommendation status.

CLASSIFICATION OF INTERNAL AUDIT RECOMMENDATIONS

The following is a ranked summary of open and closed recommendations by ERM risk category.



Classification of Internal Audit Recommendations

- Essential – implementation of the recommendation(s) would help to avoid a probable and potentially critical negative impact involving financial, operational, health and safety, information technology, compliance, and reputational risks or non-compliance with institutional policies and procedures.

- Significant – implementation of the recommendation(s) would help to avoid a possible and potentially significant negative impact involving financial, operational, health and safety, information technology, compliance, and reputational risks or non-compliance with institutional policies and procedures.

- Useful - implementation of the recommendation(s) would help to improve University processes and internal controls. These recommendations may be in writing or communicated orally to unit management at the exit conference.

STATUS (TIMELINESS) OF INTERNAL AUDIT RECOMMENDATIONS

The following is a summary of open recommendations by number of month open and status.

Report Number	Risk Category	Duration (months)	Red	Yellow	Green	Blue
15-004M	IT/Data Security	114		1		0
19-008	IT/Data Security	66		5		3
19-007	IT/Data Security	66		33		32
20-008	Health and Safety	53		2		4
21-006	Research Administration	42		1		5
21-010	Enrollment Management	41				10
21-014	Financial	39		2		14
23-005	Health and Safety	18		4		5
23-006	IT/Data Security	17		5		1
23-007	IT/Data Security	17		2		3
24-001	Health and Safety	12			6	20
24-003	IT/Data Security	11		1		0
24-004	Human Resources	10			5	1
24-006	Health and Safety	8			4	
24-007	IT/Data Security	6		10		3
24-008	Human Resources	5			0	9
24-009	Financial	4			5	6
24-012	Human Resources	2			4	
25-001	Health and Safety	2			12	
DRAFT	IT/Data Security	0			8	
DRAFT	Financial	0			3	

Status of Internal Audit Recommendations

- Green – the management update indicates that there has been progress towards implementation of the recommendation(s); the timeline for implementation is still within the agreed upon completion dates.
- Yellow – the management update indicates that there has been progress towards implementation of the recommendation(s); however, the timeline for implementation has been extended beyond the original agreed upon completion dates.
- Red – the management response or update is incomplete or indicates that there has been a lack of progress towards implementation of the recommendation(s).
- Blue – recommendations have been partially or fully closed.

Reports Issued, In-process, and Planned

The following is a summary of internal audit activity since July 1, 2023. The table also includes planned internal audits included in the 2023/ 2024 Internal Audit Work Plan and the status of audit recommendations on final reports.

Report Number	Report Title	Status	Total Recs	Closed Recs
25-00x	Department Level Controls Assessment	Planned		
25-00x	Privileged Access Controls	Planned		
25-00x	Changes to Vendor Master File	Planned		
25-00x	UVM Extension	Planned		
25-00x	Advisory Project – College of Arts and Sciences	Planned		
25-00x	Affiliated Organizations	In Process		
25-00x	Income and Expense Activities	In Process		
25-00x	Helpline Report No. 0008aa24	In Process		
25-00x	Helpline Report No. 0009aa24	In Process		
25-00x	Temporary Employees and Paid Non-employees	In Process		
25-00x	International Grant – College of Arts and Sciences	In Process		
25-00x	Advisory Project – Rubenstein School	DRAFT	0	0
25-00x	Helpline Report No. 0022aa23	DRAFT	3	0
25-00x	Data Breach Notification Policy	DRAFT	9	0
25-002	President's Official Residence (FY24)	08/13/24	0	0
25-001	Farm Safety Operations	06/10/24	12	0
24-012	Americans with Disabilities Act (ADA) Assessment	06/10/24	4	0
24-011	IT Security Risk Assessment	05/16/24	0	0
24-010	PurCard Review	04/17/24	0	0
24-009	Complex Systems Center (CEMS)	03/08/24	11	6
24-008	Background and Reference Checks	02/20/24	9	9
24-007	Information Technology (IT) Contract review process	01/19/24	12	3
24-006	Helpline Report No. 0003aa23	11/29/23	4	0
24-005	Cybersecurity Insurance	09/18/23	1	1
24-004	Helpline Report No. 0009aa22	09/13/23	5	1
24-003	Access Control – Privileged User Accounts	08/23/23	1	0
24-002	President's Official Residence (FY23)	08/22/23	0	0
24-001	Residential Life Key Control	07/07/23	26	20

University of Vermont

Office of Audit Services

August 13, 2024

To: Audit Committee of the Board of Trustees

From: Bill Harrison, Chief Internal Auditor

Subject: University Operating Procedure #5 – The President's Official Residence

---

In accordance with *The President's Official Residence* University Operating Procedure, below is the Chief Internal Auditor's report addressing all operating expenses incurred by the University related to the general maintenance and operations of the President's Official Residence for FY2024.

The President's Official Residence General Maintenance and Operating Expenses Fiscal Year 2024			
	Total Annual Budget	Actual Expense	Over/(under) Budget
Grounds Labor	$16,173	$2,565	($13,608)
Grounds Fringe	$7,118	$1,123	($5,995)
Utilities Labor	$744	$0	($744)
Utilities Fringe	$324	$0	($324)
Custodial Labor	$2,050	$2,975	$925
Custodial Fringe	$902	$1,303	$401
Misc. PPD Labor	$2,379	$5,004	$2,625
Misc. PPD Fringe	$1,047	$2,201	$1,154
PPD Other Supplies	$5,160	$4,778	($382)
Natural Gas	$5,238	$5,125	($113)
Electricity	$4,883	$5,125	$242
Water & Sewage	$911	$887	($24)
Cleaning	$2,500	$990	($1,510)
Exterminating	$300	$0	($300)
Repairs & Maint. Svcs (External)	$10,000	$11,453	$1,453
IC – CATcard Fees	$2,000	$1,950	($50)
IC - Phone Lines/Equip	$600	$600	$0
Printing & Publishing Services	$0	$40	($40)
Rental - External Facilities	$3,780	$3,780	$0
	$66,109	**$49,899**	**($16,210)**

In addition, below are the costs associated with management approved Englesby projects.

The President's Official Residence Management Approved Project Costs[1] Fiscal Year 2024				
Project Name	Budget	FY 2023 Actual	FY 2024 Actual	Over/ (under) Budget
Englesby House Stair Removal	$7,500	$0	$3,196	($4,304)
Englesby House Columns	$56,000	$28,564	$11,933	($15,503)

[1] Project costs do not include annual operating expenses.

AUDIT COMMITTEE

September 16, 2024

Resolution approving Audit Committee Charge and Charter revisions

WHEREAS, the Audit Committee annually reviews its Charge and Charter and Guidelines and recommends to the Board revisions thereto;

BE IT RESOLVED, that the Audit Committee hereby approves housekeeping changes to the Audit Committee Charge and to the Audit Committee Charter and Audit Committee Guidelines, as included in Appendices A and B, for recommendation to the Board.

Appendix A

UNIVERSITY OF VERMONT AND STATE AGRICULTURAL COLLEGE

BOARD OF TRUSTEES

AUDIT COMMITTEE

The Audit Committee is responsible for overseeing the quality and integrity of the University's financial statements including the selection of, and effective interaction with, the independent auditor; and promoting the development and monitoring the effectiveness of ~~institutional~~ systems ~~of~~for enterprise risk management, internal controls, accounting procedures, and compliance with laws and regulations.

The Audit Committee has full authority over the internal audit function including the appointment, evaluation, and termination of the chief internal auditor.

The Committee will review and monitor progress on annual plans for audits and related services ensuring that the plans encompass significant and material aspects of University operations; assess the quality and timeliness of management's response to audit findings and investigations; and review and make recommendations to the Board regarding institutional policies relevant to the Committee's charge, such as conflict of interest, fraudulent conduct, whistleblower protection, and documents retention.

A specification of Committee responsibilities shall be set forth in a Charter approved by the Board of Trustees. The Charter shall be revised from time to time in light of accounting industry and legal developments applicable to non-profit corporations and institutions of higher education.

The Board of Trustees shall annually appoint at least 5 of its members to the Audit Committee. Its members shall be independent of management and the University including its component units and affiliated organizations. Pursuant to the University Bylaws, the President shall not serve as an ex officio member of this Committee.

Approved by the Board of Trustees: September 9, 2006
Revised by the Board of Trustees: October 26, 2013
Approved by the Board of Trustees: October 18, 2014
Amended by the Audit Committee: September 16, 2024

UNIVERSITY OF VERMONT AND STATE AGRICULTURAL COLLEGE BOARD OF TRUSTEES

AUDIT COMMITTEE

Charter

This Charter sets forth the responsibilities of the University Board of Trustees Audit Committee.

I. Principal Responsibilities

The principal responsibilities of the Committee shall include:

a. promoting the development and monitoring the effectiveness of ~~an institutional~~ systems ~~of~~for enterprise risk ~~assessment~~ management and internal controls. At least annually, reviewing with management the University's processes for identifying, prioritizing, mitigating, and reporting institutional opportunities and risks;

b. reviewing and, as appropriate, making recommendations to the Board, regarding institutional policies relevant to the scope of Committee responsibilities, including conflict of interest, ethical and fraudulent conduct, whistleblower protection, cybersecurity, and document retention;

c. ensuring that audit plans encompass significant and material aspects of University operations;

d. full authority and oversight of the internal audit function including appointment decisions, performance evaluations, and employment termination of the chief internal auditor;

e. implementing a selection process to retain the independent auditor and making a recommendation to the Board of Trustees for approval. Recommending such additional audits as the Committee and/or the Board must approve under the Board's reserved authority;

f. maintaining direct and effective communication with independent auditors on behalf of the Board;

g. reviewing the results of internal and external audits (including the annually audited financial statements), and assessing the quality and timeliness of management's response and corrective actions;

h. reviewing the effectiveness of the University's practices related to monitoring its

compliance with laws and regulations;

i. reviewing the results of management's investigation and resolution of any reported, or otherwise discovered, significant instances of noncompliance;

j. evaluating the scope and quality of internal and independent audit services, and the degree of coordination and appropriate degree of independence between them;

k. reporting regularly and promptly to the Board regarding matters within the scope of the Committee charge; and,

l. periodically reviewing expense reimbursements, or summaries thereof that have been submitted by the President and reviewed and certified by the Vice President for Finance & Administration and Treasurer, who serves as the Chief Financial Officer ("CFO") of the University.

II. Membership

The University of Vermont Board of Trustees shall annually appoint at least 5 of its members to the Committee. Its members shall be independent of management and the University including its component units and affiliated organizations. For the purposes of this charter, "independence" is defined as rendering a Trustee ineligible for Committee service if ~~he or she~~they (1) ~~is~~are employed by the University; (2) ~~is~~are a partner or employee of a firm retained to conduct an audit of the University; (3) held such University employment or audit engagement at any time during the previous three years; or (4) ~~is~~are receiving consulting, advisory, or other compensatory fees for services provided to the University. Members of the ~~Investment Subcommittee~~Board who serve as Managers of the University of Vermont Investment Management Company, LLC -are eligible for appointment to the Audit Committee, but no such member may serve as its Chair or Vice Chair. The University President is ineligible for service as a member, ex officio or otherwise, of the Audit Committee, as a University official and employee.

Committee members shall otherwise be subject to the Conflicts of Interest Policy in the conduct of their work.

Members of the Committee shall receive orientation appropriate to their Committee membership. All members should have a general understanding of general accounting, business and finance principles, including the ability to read and understand institutional financial statements, whether gained preceding service on this Board of Trustees or during Committee orientation. At least one member of the Committee should possess accounting or financial expertise.

III. Authority

The Committee is authorized to investigate any matter within the scope of its Charter, with full and direct access to all pertinent University records, personnel, independent auditors and consultants.

IV. Adoption of Charter

This Charter shall be effective as of the date of its approval by the Board. The Committee will annually review the Charter and recommend to the Board revisions thereto, in view of evolving accounting standards, legal developments and experience gained.

Audit Committee Guidelines

These Guidelines serve as an operational supplement to the Audit Committee Charter. They are intended to reflect generally accepted accounting industry standards and practices applicable to non-profit corporations and higher education institutions.
The Guidelines shall be reviewed annually by management, and management shall report annually to the Committee regarding the status of the Guidelines. The Committee shall make revisions to the Guidelines as necessary or appropriate in view of evolving accounting standards and practices, legal developments and experience gained.

I. Retention of the Independent Audit Firm

a. The Committee shall annually authorize and direct the Committee Chair to retain the independent audit firm to conduct the mandatory annual audit of the financial statements and/or compliance audits. In conjunction with such retention, the Committee will assess the independence and objectivity of the firm by obtaining statements from the firm on relationships between the firm and the University. The Committee will review and assess any relationships disclosed that may impact auditor objectivity and independence.

b. The Committee shall solicit requests for proposals relative to the mandatory annual audit of the financial statements and/or compliance audits from qualified independent audit firms no less than once every five years.

c. The Committee shall ensure the proper rotation of the lead audit partner, in accordance with standards of the profession.

II. Retention of Other Audit Services

a. The independent audit firm retained to conduct the mandatory annual audit of the financial statements and/or compliance audits generally shall not be eligible for University engagements to perform non-audit services that would violate the U.S. Government Accountability Office Independence Standard. If, due to extenuating circumstances, and in the exercise of its reasonable discretion, management deems it to be in the best interests of the University to retain the independent audit firm for non-audit services, the proposed retention is subject to review and action by the Committee where the retention will result in fees of $25,000 or more.

b. Contracts for non-audit services with independent audit firms not already retained by the University to conduct the mandatory annual audit of the financial statements and/or compliance audits are subject to review and recommendation by the Committee and subsequent Board consideration and action when such retentions will result in fees of $1,000,000 ~~250,000~~ or more and notice to the committee of agreements of $500,000 or more.

III. Oversight of Audits

The Committee will, no less than once annually, and otherwise periodically as necessary or desirable:

a. review annual audit plans developed by the Office of Audit Services, and receive regular progress reports relative to such plans;

b. review audit plans developed in consultation with independent audit firms, including (i) the critical accounting policies and practices to be used; (ii) all alternative treatments of financial information discussed with management, ramifications of alternative treatment and the treatment preferred by the firm; (iii) other material communications between the firm and management; and (iv) required communications from the firm under Auditing Standards AU-C Section 250;

c. subject to subsequent Board consideration and action, review and accept the mandatory annual audit of the financial statements. Review the Uniform Guidance audit, and the financial agreed upon procedures report of institutional National Collegiate Athletic Association programs;

d. resolve disagreements between management and the independent audit firm regarding financial reporting;

e. review the independent audit firm management letter comments regarding institutional financial and information technology and security internal controls, accounting policies and procedures, and management's response to those comments;

f. review with management and the independent audit firm their respective judgments about the quality of University accounting principles; the consistency, and the degree of aggressiveness or conservatism, in the application of accounting principles; the reasonableness of significant accounting judgments; and the clarity and completeness of the financial statements and related disclosures;

g. confirm with management that the annual financial statements disclose all material off-balance sheet transactions, arrangements, obligations, and other relationships of the University with unconsolidated entities or other persons that may have a material current or future effect on institutional financial condition, and the results of operations, liquidity, capital expenditures, capital resources, or significant components of revenues or expenses;

h. receive reports from management, the Office of Audit Services and the independent audit firm, regarding new and significant accounting standards to understand their impact on institutional financial statements;

i. receive reports from the Office of Audit Services regarding any findings of fraud which, in single incident or aggregate, results in an institutional uninsured or

insured loss in excess of $10,000, or potentially significant reputational damage to the university;

j. review the organizational structure, qualifications, independence, scope of services inclusive of office charter, and adequacy of resources of the University's Office of Audit Services;

k. annually review the appointment, evaluate the performance and set the salary of the chief internal auditor;

l. identify and document specific administrative responsibilities relevant to the routine operations of the office of chief internal auditor that are assigned to the President;

m. ensure that regular quality assessment reviews of the internal audit operations are performed in accordance with Institute of Internal Auditors standards; and,

n. meet separately with both the internal and external auditors without management representatives present subject to the requirement of the Vermont open meeting laws.

IV. Internal Controls

The University's executive management and the Board of Trustees Audit Committee have adopted the Committee of Sponsoring Organizations (COSO) Internal Control – Integrated Framework to help assess and enhance its internal control systems.

a. Certifications

i. The Committee will receive periodic reports from management on representations it is rendering in conjunction with mandatory annual audit of the financial statements and/or compliance audits as well as significant and material debt financing, such as issuance of bonds.

ii. Without limitation on IV a(i), the Committee will receive from the ~~Chief Financial Officer (~~CFO~~)~~ a record of certification along with the annual financial statement report that:

a. The CFO has approved the financial statements,

b. Based on the CFO's knowledge, the report does not contain any material errors or omissions,

c. Based on the CFO's knowledge, the financial statements materially present the financial condition and result of operations,

d. The CFO is responsible for establishing and maintaining a system of internal controls over financial reporting, and that,

e. The CFO has disclosed to the auditors and the Audit Committee all significant internal control deficiencies and changes that could

materially affect financial data.

b. Policy Review.

The Committee will receive for its review and comment and, if necessary, its recommendation to the Board, institutional policies relevant to its scope of work, including conflict of interest, code of conduct and ethical standards, whistleblower protection, and documents retention.

c. Required Disclosures and Compliance Monitoring.

The Committee shall oversee compliance with the Board Reserved Rights and Delegated Authority resolution. Violations of the Board Reserved Rights and Delegated Authority resolution identified by management or the internal audit office shall be reported to the Committee.

d. Confidential Reporting.

The committee will ensure that the University has a mechanism that permits confidential communications from employees and others regarding potential financial or accounting improprieties or nonfeasance.

V. Enterprise Risk Management

a. Oversee management's enterprise risk management process on behalf of the Board.

b. Receive periodic updates on management's process to identify, prioritize, mitigate, and report institutional risks including the process to map risks to relevant Board Committees.

VI. Compliance and Privacy

a. Review with the Office of Compliance and Privacy Services, and management the effectiveness of the University's practices related to monitoring compliance with laws and regulations;

b. Review with the Office of Compliance and Privacy Services and management, findings of internal compliance auditing and monitoring activities;

c. Review with the Office of Compliance and Privacy Services and management, findings of government agency audits, investigations, reviews and monitoring activities that the Director considers significant, that are initiated by a government agency as a result of a whistleblower report, or on a for-cause basis, or that result in a fine, penalty, refund, disallowance or questioned cost in excess of $10,000;

d. Review with the Office of Compliance and Privacy Services and management, the process for communicating the Code of Conduct and Ethical Standards to University personnel and for monitoring compliance therewith;

e. Receive periodically, but not less than annually, reports from the Office of Compliance and Privacy Services on its activities;

f. Receive updates from the Office of Compliance and Privacy Services, and management on new and emerging compliance issues, including their impact to the University; and,

g. Receive as needed, through the Audit Committee Chair, compliance matters communicated directly by the Chief Internal Auditor or Director of Compliance Services and Chief Privacy Officer.

As approved by the Board of Trustee: November 13, 2004
Approved as amended by the Board of Trustees: September 8, 2007
Revised by the Audit Committee: November 12, 2007
Approved as amended by the Board of Trustees: December 1, 2007
Revised by the Audit Committee: April 28, 2009
Approved by the Board of Trustees: May 16, 2009
Revised by the Audit Committee: October 11, 2010
Approved by the Board of Trustees: October 30, 2010
Revised by the Audit Committee: November 14, 2011
Approved by the Board of Trustees: February 4, 2012
Revised by the Audit Committee: September 15, 2014
Approved by the Board of Trustees: October 18, 2014
Revised by the Audit Committee: September 12, 2016
Approved by the Board of Trustees: October 22, 2016
Revised by the Audit Committee: July 10, 2017
Approved by the Board of Trustees: October 21, 2017
Revised by the Audit Committee: September 14, 2020
Approved by the Board of Trustees: September 25, 2020
Revised by the Audit Committee: September 16, 2024

University of Vermont

OFFICE OF COMPLIANCE AND PRIVACY SERVICES
www.uvm.edu/erm
284 East Avenue, Burlington, VT 05405
P: (802) 656-3086 • E: erm@uvm.edu

Enterprise Risk Management

Enterprise Risk Management Update

Board of Trustees – Audit Committee
September 16, 2024

Prepared By
Tessa Lucey, Director of Compliance and Chief Privacy Officer

---

In February 2023, the Board of Trustees received a biennial report on Enterprise Risk Management assessment results. Throughout the year, committees will receive status updates on risks and opportunities that fall under their purview. Included in this report is the update on the following:

- Information and Cyber Security

AUDIT COMMITTEE

Risk – Information and Cyber Security

Intentional and unintentional acts can compromise the confidentiality, integrity, or availability of UVM's information systems or building control systems infrastructure, leading to potential disruptions, data breaches, and financial, legal, or reputational damage. The exposure of sensitive information could result in significant penalties, identity theft, and legal liabilities.

UVM's Information Security Office (ISO), along with the Larner College of Medicine's dedicated team, continues to coordinate cybersecurity efforts across the University, focusing on enhancing detection, prevention, and response capabilities. Over 2022-2024, leadership changes and targeted audits, such as the Data Breach audit in collaboration with Internal Audit and a Cyber Hygiene assessment with CISA, have provided a clearer understanding of vulnerabilities and helped us solidify our cybersecurity goals. These efforts have driven improvements across most cybersecurity domains, particularly in spam and phishing detection, identity management, and intrusion detection.

In response to the evolving threat landscape, UVM is investing in secure enclaves designed from the ground up to meet federal security standards. These enclaves feature advanced security measures, including next-generation detection and prevention systems, heightened monitoring, and comprehensive security awareness training. The initial focus is on research security but the implementation process adds opportunities for more and targeted enclaves by creating a playbook for expansion of these enclaves throughout the enterprise.

The ISO recommends ongoing risk assessments, the implementation of automated vulnerability detection systems, and enhancements to firewall and desktop security practices. Continuing investment in staffing, training, and advanced systems is a vital part of our strategy. These initiatives are crucial for advancing our cybersecurity maturity.

Gramm-Leach-Bliley Act (GLBA)

Annual status report of the GLBA Information Security Program

Board of Trustees - Audit Committee
September 16, 2024

Prepared By
Scott Carbee, Information Security Officer, Enterprise Technology Services
Joey Catania, Assistant Director of Compliance, Student Financial Services

Background:

The Gramm Leach Bliley Act (GLBA) is a law that applies to financial institutions and includes privacy and information security provisions that are designed to protect consumer financial data. This law applies to how higher education institutions collect, store, and use student financial records (e.g., records regarding tuition payments and/or financial aid) containing personally identifiable information. GLBA regulations include both a Privacy Rule (16 CFR 313) and a Safeguards Rule (16 CFR 314), both of which are enforced by the Federal Trade Commission (FTC) for higher education institutions. Colleges and universities are deemed to be in compliance with the GLBA Privacy Rule if they are in compliance with the Family Educational Rights and Privacy Act (FERPA). The Safeguards Rule was promulgated in 2002, with compliance required in May 2003.

In early 2017, the federal Office of Management and Budget (OMB), working with the Department of Education's office of Federal Student Aid (FSA), announced that a GLBA Safeguards Rule audit objective would be included in the federal single audit process that most colleges and universities have to follow.

On December 9, 2021, the FTC issued final regulations (Final Rule) to amend the Standards for Safeguarding Customer Information (Safeguards Rule), an important component of the GLBA's requirements for protecting the privacy and personal information of consumers. The effective date for most of the changes to the Safeguards Rule was June 9, 2023.

https://www.uvm.edu/sites/default/files/UVM-Policies/policies/GLBA.pdf

https://library.educause.edu/topics/policy-and-law/gramm-leach-bliley-act-glb-act

Applicability to The University of Vermont:

The University's scope of covered accounts under GLBA is limited to its role as a lender for Institutional Loans and the former Federal Perkins Loan Program. Students may have borrowed from multiple loan programs and therefore the total count of loans borrowed annually and in repayment may result in double-counting of students so the following figures represent the maximum number of loans, not the total number of covered accounts, the total number of covered accounts would be less.

The following represents total institutional loans outstanding as of August, 2024, including loans for in-school students, loans in grace period, and loans in repayment:

	Number of Loans	Total Principal Outstanding Debt
In-School	890	$6,338,161.00
In Grace	476	$3,729,749.00
In Repayment	2354	$11,595,621.00
Total	3720	$21,663,53100

The total number of new loans originated in 2023-24 is 688 representing $3,296,487 of total principal. The total of new loans for the most recently completed academic year (2022-23) is 655.

Risk Analysis:

Student Financial Services and Enterprise Application Services have an annual review of all users who have access to student financial information. This review removes access for those who no longer require access or are no longer employed by the university. Employees that still need access are required to complete an annual review of GLBA rules as well as other applicable privacy policies and procedures.

The University conducts various assessments to analyze its risks related to information security. Conducted assessments are often scoped to specific University environments in order to best identify and address risks, at the correct granularity and focus, appropriate to a particular topic. While our assessments this year have been general in nature and focused more on the overall health of the University enterprise than specifically targeting GLBA, by addressing this overall health, we are also addressing GLBA.

Over the course of 2022-24, we had a turnover in the leadership of the Information Security Office and since replacing the Information Security Officer in 2023 have made progress toward assessing our cybersecurity maturity and planning upgrades that will help us better meet the University's requirements. In conjunction with Internal Audit we have undergone a Data Breach audit with the results of solidifying our cybersecurity goals both in general and in focus with GLBA regulations.

Enterprise Technology Services (ETS) also conducted a cyber hygiene assessment with the Federal Cybersecurity and Infrastructure Security Agency (CISA) with an

end toward understanding our level of vulnerability to common attacks. Since the last audit report we have made improvements across most cybersecurity domains which ties directly to the cyber defense capabilities within Student Financial Services (SFS). It is important to note that all nonpublic personal information (NPI) covered under GLBA is related to SFS lending activities.

Detection of spam and phishing emails has improved greatly through our incorporation of cloud-based email storage and management. This has also been supported through the implementation and broad adoption of multi-factor authentication helping us cut down the numbers of compromised accounts and adding to the overall Identity and Access management, strengthening individual account protections. Finally, we have also made strides in tuning our intrusion detection systems to be more flexible and report anomalies in account access and usage at a more granular level, making our staff more capable of rapid responses to any intrusions or compromises.

This year, we have also received funds to build our own secure enclaves. These enclaves will be a "green field" (or from scratch) design that supports a security model based on Federal requirements. These enclaves will have secure servers, next generation detection and prevention capabilities, heightened monitoring of activity, and critically, security awareness training to help users understand the risks to data and their role is the overall security of the information to which they have access. Our initial work will be oriented on research security, but the application of this technology will help us move toward a similar model for SFS (and others), allowing us to better protect critical information and systems without the monumental task of performing these activities across the entire University enterprise. Our recommendations made in 2019 still form the core of our efforts to improve our security within the assessment based on Federal Financial Institutions Examination Council – Cybersecurity Assessment Tool (FFIEC-CAT) which still finds us to be at a minimal inherent risk level, though it is worth noting that our overall footprint and financial offerings help us greatly in this regard. We will maintain a maturity level of "Baseline" with an eye toward improving to "Evolving" primarily through the improvements to controls directly affected by the secure enclaves project. Additionally, improvements can be made to internal procedures and processes that will drive improved compliance with regulations.

Recommendations include:

- Incorporating regular risk assessments and incorporation of automated systems that detect and report vulnerabilities.
- Improve our current firewalling and detection systems to move to a "next-generation" model.

- Document and track cybersecurity awareness training for all users of the SFS environment and conduct periodic assessments of user awareness of threats.
- Improve monitoring and detection of cyber events and proactively resolve imminent threats where possible.
- Improve desktop security practices limiting administrative access, software installations, and patching frequency.