COMMUNITY COLLEGE OF VERMONT
VERMONT STATE UNIVERSITY

VERMONT
STATE COLLEGES SYSTEM

OFFICE OF THE CHANCELLOR
PO BOX 7
MONTPELIER, VT 05601
P (802) 224-3000

MEMORANDUM

TO:

Committee Members	**Committee Liaisons**
Sue Zeller, Chair	William Carey, CCV faculty
David Durfee, Vice-Chair	Ryan Dulude, CCV staff
Gwen Bailey-Rowe	Jen Jones, VTSU staff
Bob Flint	Dennis Reilly, VTSU faculty
David Silverman	

FROM: Sharron Scott, Chief Financial & Operating Officer

RE: VSC Board of Trustees Audit & Risk Management Committee Meeting
May 11, 2026

DATE: May 7, 2026

The VSC Board of Trustees Audit & Risk Management Committee is scheduled to meet on Monday, May 11, 2026 at 9:00 a.m. virtually at vsc.edu/botzoom.

The Audit & Risk Management Committee meeting will cover public comment, approval of previous minutes, a review of the FY2026 audit planning schedule with Zach LaFlash from Withum, and an evaluation of the Information Technology Team's Written Information Security Program. The committee will decide whether to recommend WISP approval to the Board of Trustees for the June 8, 2026 meeting.

Note: Please be advised that the committee has four members. The quorum to start the meeting and to take any action is three members of the committee.

The board assistant, Kayla Dewey, may be reached at (802) 224-3021 for any questions.

CC: Business Affairs Council
Council of Presidents
Vermont Department of Libraries
VSC Board of Trustees

Vermont State Colleges Board of Trustees
Audit & Risk Management Committee Meeting
Monday, May 11, 2026 at 9:00 a.m.
Live meeting: vsc.edu/botzoom
Stream: vsc.edu/live

AGENDA

1. Call to Order
2. Public Comment[1]
3. Approval of February 23, 2026 minutes
4. Review: FY2026 Audit Planning with Withum
5. Review & Recommend: Written Information Security Program (WISP)
6. Other Business
7. Adjourn

MATERIALS

1. February 23, 2026 Minutes
2. FY2026 Audit Plan
3. Written Information Security Program

[1] Sign up to make a comment at vsc.edu/signup. Commenters must be logged in to the live session at www.vsc.edu/botzoom to make a comment.

Minutes of February 23, 2025

Minutes of the VSC Board of Trustees' Audit & Risk Management Committee meeting held Monday, February 23, 2026 at 11:00 a.m. virtually at vsc.edu/botzoom. – UNAPPROVED

Note: These are unapproved minutes, subject to amendment and/or approval at the subsequent meeting.

The VSC Board of Trustees Audit & Risk Management Committee met on Monday, February 23, 2026 at 11:00 a.m. virtually at vsc.edu/botzoom.

Attendance

Committee Members:	Sue Zeller (Chair), David Durfee (Vice Chair), Bob Flint, David Silverman
Other Trustees:	Megan Cluver, Lynn Dickinson
Liaisons:	William Carey (CCV faculty), Ryan Dulude (CCV staff)
Chancellor:	Beth Mauch
Presidents:	David Bergh, VTSU Joyce Judy, CCV
Other Attendees:	Charles Bombard, Manager of Data Center/Systems Admin. Kayla Dewey, Executive Assistant, Board of Trustees Wilson Garland, Chief Information Officer Jennifer Jones, AVP of Academic Support and Ed Op. Programs Jason Kaiser, VTSU Learning Spaces Technology Specialist Zach LaFlash, CPA, Withum Nicole Mace, CCV Dean of Administration Sharron Scott, Chief Financial and Operating Officer Toby Stewart, Controller Patty Turley, General Counsel Littleton Tyler, AVP Finance and Compliance Meg Walz, Deputy CIO

1. Call to Order

Chair Zeller called the meeting to order at 11:00 a.m.

2. Public Comment

There was no public comment.

3. Approval of October 30, 2025 minutes

Trustee Zeller moved and Trustee Durfee seconded the motion to approve the October 30, 2025 meeting minutes. The motion was approved unanimously.

4. Review & Recommend: DRAFT Single Audit

Chair Zeller invited Zach LaFlash to give an overview of the results of the FY25 Draft Single Audit. Mr. LaFlash reported that there was one finding related to the Written Information Security Plan, which VSC is in the process of resolving.

Trustee Zeller moved and Trustee Durfee seconded the motion to recommend acceptance of Resolution 2026-002 to the board. The motion passed unanimously.

5. Internal Audit Discussion

Chair Zeller introduced a recommendation by management to take a break from the internal audit to focus on the Workday project due to its significant complexities. Chief Financial and Operating Officer Sharron Scott provided additional context for the proposal including limited staff resources with the Workday implementation project. After the Workday implementation is completed, many processes will be changed, therefore an audit of these processes may not be useful.

6. Other Business

There was no other business.

7. Executive Session

At 11:27 a.m. Chair Zeller moved and Trustee Silverman seconded that the Committee enter executive session, pursuant to 1 VSA 313(a)6) to discuss records exempt from access to public records, it is appropriate for the Committee to enter executive session. Along with the members of the Board present at this meeting, in its discretion, the Committee invited the VSC Chancellor, VSC Chief Financial Officer, VSC Associate General Counsel, the Presidents of Community College of Vermont and Vermont State University, the Chief Information Officer, Deputy Chief Information Officer, and the Director of IT Infrastructure and Security. The motion was approved unanimously.

The committee exited executive session at 11:47 a.m.

8. Adjourn

Chair Zeller adjourned the meeting at 11:47 p.m.

Fiscal Year 2026 Planning Memo & Timeline

Memorandum

To: Vermont State Colleges – Audit Committee

From: WithumSmith+Brown, P.C.

Date: May 11, 2026

Re: Fiscal Year 6-30-26 Financial Statement and Single Audit Planning Discussion

---

Agenda:

- **WSB Introductions**
- **Discussion of prior year audit results - 6/30/25**
    - Prior Year Audit Approach
        - Completed 100% of the audit remotely.
        - Consistent communication.
    - Financial Statements – Unmodified Opinion was issued
    - Internal Controls over Financial Reporting and on Compliance – No material weaknesses/significant deficiencies were noted
    - No disagreements with management or difficulties encountered in performing the audit
    - Prior Year Audit Items of Note:
        - Single Audit:
            - Compliance supplement was delayed- late November release.
            - One finding noted within the Student Financial Aid (SFA) Cluster:
                - Finding No. 2024-001 – Written Information Security Plan (WISP)
            - Total of five major programs (including SFA).

- **Current Year Audit Approach - 6/30/26**
    - Audit Approach
        - Ongoing/continuous improvements in audit process, what has worked in past, what can be improved upon.
        - Expanded communication and strict timetables/deadlines with an emphasis on open items, and potential single audit findings.
            - Periodic check-in meetings between WSB and VSC
        - Remote Approach - complete the work remotely with scheduled meetings with management and scheduled open item/audit status updates built into the audit timeline.

- Meet the October deadline for both Financial Statements and Single Audit Report.
- Review and communication of process improvements and efficiencies as they are identified during the audit.

- Audit Risks
  - Going Concern Assessment - Forecasts and Financial Outlooks through 1 year after financial statements are issued (*Estimated* 10/15/27).
  - Material errors (i.e. Unusual or non-routine transactions) and/or fraud (both external or internal) and its impact on the financial statements and on compliance with federal and state programs.
  - Threats to Independence.
- Determining Major Programs for federal audit (known as the Single Audit).
  - Increase in major program threshold from $750,000 to $1,000,000.
  - Student Financial Aid (SFA) – makes up the majority of the federal expenditures (approx. $46.75m in FY2025) - will most likely need to be selected for FY2026 to obtain minimum coverage.
  - Additional major program selections will depend on the preliminary Schedule of Expenditures of Federal Awards, "SEFA".

- **New GASB Pronouncements – Effective FY2026**
  - GASB 103 – *Financial Reporting Model Improvements*
    - The objective is to improve key components of the financial reporting model. Key areas impacted are"
      - Management Discussion and Analysis (MD&A)
      - *Statement of Revenues and Expenses- grouping*
  - GASB 102 – *Disclosure of Certain Capital Assets*
    - The objective is to improve and expand on disclosures for capital assets, including assets held for sale.
- **Timeline for audit planning and audit field work, including Federal Single.**
  - **Audit Planning- Weeks of May 4th, May 11th and May 18th**
    - **Focus on Financial Statement Planning, Internal Control documentation and Single Audit testing**
  - **Audit Fieldwork- Weeks of August 17th and August 28th**
    - **Focus on year end audit procedures, substantiative audit testing and audit wrap-up.**
- **Other matters**
  - **Questions/comments**

PLASE NOTE, WE ARE FLEXIBLE IN OUR PLANNING DATES AND CAN MAKE CHANGES TO DATES AS NECESSARY BASED ON YOUR STAFF SCHEDULING NEEDS.

OCD Summary Timeline Template
Vermont State Colleges
June 30, 2026

	Timeline Event	*Deadline*	WSB task	VSC task	External Task	Note
1	Send Planning Samples (cash disbursements/payroll/revenue) and Single Audit Samples	ASAP	X	X		
2	Single Audit Testing and Audit Planning (Testing internal controls, plan for fieldwork, etc.)	May 4th to May 22nd	X	X		
3	Single Audit Testing (SFA)wrapup	May 26th to May 29th	X			
4	Send out Confirmations to Bank	1st week of July	X	X		
5	WSB to send Fieldwork Workpaper package to client	46227	X			
6	Wrap up of Single Audit Testing Open Items	46234	X			
7	Pre-audit fieldwork meeting	TBD - week of 8/3	X	X		
8	Actuary Report provided by Actuary	TBD			X	
9	Client provides audit packages and fieldwork workpaper package requests support	46251		X		
10	Audit fieldwork	08/17/2026-08/28/2026	X	X		
11	Audit Fieldwork Wrap-up Meeting with Client	46262	X	X		
12	Audit Fieldwork wrap-up meeting -WSB internally	46265	X			
13	WSB prepares & reviews Financial Statements	09/14/2026-09/18/2026	X			
14	Final partner workpaper review	09/14/2026-09/18/2026	X			
15	Client provides footnote support to complete financials	09/14/2026-09/18/2026		X		
16	WSB to send along final findings for Single Audit	46283	X			
17	Reviewed financials are sent to Technical Review	46290	X			
18	Client provides Management Discussion and Analysis	46296		X		
19	Financials to Technical Review	09/25/2026 to 10/02/2026	X			
20	TR points are cleared (Financials)	09/25/2026 to 10/02/2026	X			
21	TR approves cleared points (Short Form)	09/25/2026 to 10/02/2026	X			
22	Management provides single audit findings responses and Corrective Action Plan	46296		X		
23	Financials are sent to client for review	46304	X			
24	Single Audit is sent to Technical Review	46296	X			
25	TR Review reviews Single Audit and TR points are cleared	10/1/2026-10/10/26	X			
26	Withum sends Single Audit to Client	46305	X			
27	Audit committee meeting to present financials/Single Audit	46321	X	X		
28	Client sends Financials to State of Vermont	by 10/31/26		X		
29	Obtain signed representation letter	TBD	X	X		
30	Upload data collection form to the Clearinghouse	TBD	X	X		

Written Information Security Program

WRITTEN INFORMATION SECURITY PROGRAM

As identified in the 2025 Single Audit, applicable federal regulations, including 2 CFR 200.303 and the Federal Trade Commission Safeguards Rule (16 CFR 314), require institutions participating in Title IV programs to develop, implement, and maintain a comprehensive Written Information Security Program (WISP). This program must include administrative, technical, and physical safeguards appropriate to the sensitivity of institutional data and aligned with federal information security standards.

The audit noted that, while Vermont State Colleges maintains strong information security practices, the absence of a formally documented WISP created a gap in demonstrating compliance. Specifically, without a comprehensive, centralized policy, the institution faced increased risk related to inconsistent application of practices, insufficient documentation for audit purposes, and potential exposure to unauthorized access or data loss.

Management concurred with the audit finding. Over the past two years, information security practices have been strengthened in response to evolving industry standards, insurance requirements, and obligations under the Gramm-Leach-Bliley Act. However, these practices had not been consolidated into a single, formalized program document that could be readily evidenced during the audit process.

The Information Technology team has now completed the development of a formal Written Information Security Program that aligns documented policy with current operational practices and regulatory requirements.

The WISP is presented to the Audit & Risk Management Committee for review and recommendation to the Board of Trustees at its June 8, 2026 meeting.

Written Information Security Program (WISP) for Protection of Protected Information

General

A. Objective of WISP

The objective of the development and implementation of this comprehensive Written Information Security Program (WISP), is to create effective administrative, technical, and physical safeguards for the protection of Protected Information and to comply with the Vermont State Colleges' (the "Institution") obligations with applicable regulations.

The WISP sets forth procedures for evaluating electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting Protected Information, in alignment with the VSC Information Sensitivity Policy.

For purposes of this WISP, "Protected Information" includes the following, whether in paper, electronic or other form:

1. Social Security number;
2. driver's license number or state-issued identification card number; or
3. credit card holder data.

The VSC Information Sensitivity Policy includes further examples of Protected Information.

B. Purpose of WISP

The purpose of this WISP is to:

1. ensure the security and confidentiality of Protected Information;
2. protect against threats or hazards to the security or integrity of such information; and
3. protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft or fraud.

C. Scope of WISP

In formulating and implementing this WISP, the intended scope is to do the following:

1. identify reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing Protected Information;
2. assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Protected Information;
3. evaluate the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risks to Protected Information;
4. design and implement a WISP that puts safeguards in place to minimize those risks, consistent with regulatory requirements; and
5. regularly monitor the effectiveness of those safeguards.

D. Data Security Coordinator

The Vermont State Colleges has designated the Director of Infrastructure and Information Security to be the Data Security Coordinator. That individual may name an alternate designee in writing. They will be responsible for implementing, supervising and maintaining this WISP, including:

1. initial implementation of the WISP;
2. training of the following persons regarding the WISP and Protected Information security:
   a. all employees;
   b. independent contractors with access to Protected Information; and
   c. any other person involved with the Institution who has or will have access to Protected Information;
3. regular testing of the WISP's safeguards, including backup restoration, tabletop exercises, and penetration tests;
4. evaluating the ability of each of the Institution's third-party service providers to implement and maintain appropriate Protected Information security measures for the Protected Information to which the Institution has permitted them access, and requiring such third-party service providers by contract to implement and maintain appropriate Protected Information security measures;
5. reviewing the scope of the Protected Information security measures in the WISP at least annually, or whenever there is a material change in the Institution's business practices that may implicate the security or integrity of records containing Protected Information.

Protections Against Internal Data Security Breach

To combat internal risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing Protected Information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures are mandatory and are effective immediately:

A. Information and Access

1. The amount of Protected Information collected shall be limited to that amount reasonably necessary to accomplish the Institution's legitimate business purposes, or necessary to the Institution to comply with other state or federal regulations.
2. Access to records containing Protected Information shall be limited to those persons who are reasonably required to know such information in order to accomplish the Institution's legitimate business purpose or to enable the Institution to comply with other state or federal regulations.
3. Access to electronic Protected Information shall be restricted to active users and active user accounts only.
4. Access to electronically stored Protected Information shall be electronically limited to those employees having a unique log-in ID with multi-factor authentication enabled.
5. The Institution will maintain a list of critical systems, including the type of data stored and transmitted in each system.
6. Paper or electronic records (including records stored on hard drives or other electronic media) containing Protected Information shall be disposed of only in the following manner:
    a. paper documents containing Protected Information shall be either redacted, pulverized or shredded so that Protected Information cannot practicably be read or reconstructed; and
    b. electronic media or other non-paper media containing Protected Information shall be destroyed or erased so that Protected Information cannot practicably be read or reconstructed.

B. Employees

1. A copy of the WISP must be distributed to each employee and/or readily accessible on the Institution's website for each employee to access, including part-time, temporary and contract employees, and the Institution expects all employees to comply with the provisions of the WISP and all other record retention responsibilities.
2. There must be regular training of employees on the detailed provisions of the WISP. The Data Security Coordinator shall organize such training.
3. Employees are prohibited from keeping unsecured files containing Protected Information in their work area when they are not present, or otherwise failing to take reasonable measures to protect the security of Protected Information. All files and other records containing Protected Information must be secured in a manner that protects the security of Protected Information.
4. All employees are required to comply with the provisions of the WISP, and if the security provisions of the WISP are violated by an employee, Human Resources shall implement disciplinary procedures in accordance with the Institution's employee handbook or bargaining agreements.
5. Resigned or terminated employees must return all records containing Protected Information, in any form, that may be in the former employee's possession (including all such information stored on laptops or other portable devices or media, and in files, records, work papers, etc.), together with all other records of the Institution.
6. A resigned or terminated employee's physical and electronic access to Protected Information must be revoked when employment ends. Such resigned or terminated employee shall be required to surrender all keys, IDs or access codes or badges, business cards, and the like, that permit access to the premises or information. Moreover, such terminated employee's remote access to Protected Information (such as internet access, e-mail access, voice-mail access) must be disabled in accordance with the VSC Password and Access Management Policy.
7. Employees are expected to report any suspicious or unauthorized use of Protected Information to the Data Security Coordinator as soon as discovered.

Protections Against External Data Security Breach

To combat external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing Protected Information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures are effective immediately:

A. Vermont State Colleges' Computers and Electronic Information Systems

1. The wireless network at the Vermont State Colleges' locations shall always be encrypted.
2. All VSC-owned devices used by Institution personnel must be encrypted and password protected.
3. All portable devices used by employees of the Institution to send and receive their college e-mail shall be password protected, and shall be locked when not in use.
4. The Institution's computers and computer system, including any wireless system, shall, at a minimum, and to the extent technically feasible, have the following elements:
    a. Secure user authentication protocols including:
        i. control of user IDs and other identifiers;
        ii. a reasonably secure method of assigning and selecting passwords in accordance with the VSC Password and Access Management Policy;
        iii. multi-factor authentication required for login to all critical systems and elevated access;
        iv. restricting access to active users and active user accounts only; and
        v. blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system.
    b. Secure access control measures that:
        i. restrict access to records and files containing Protected Information to those who need such information to perform their job duties; and
        ii. assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls.
    c. Encryption of all transmitted records and files containing Protected Information that will travel across public networks, and encryption of all data containing Protected Information to be transmitted wirelessly.
    d. Reasonable monitoring of systems, including logs of users' activity, for unauthorized use of or access to Protected Information;
    e. Encryption of all Protected Information stored on laptops;
    f. For Protected Information on a critical system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the Protected Information.

g. Reasonably up-to-date versions of system security agent software installed and active at all times, which must include endpoint-protection, and reasonably up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.

5. New system and application purchases will be reviewed by the IT security team, risks documented, and added to the critical systems list as applicable. In-house developed systems with Protected Information will be similarly assessed.

Protected Information Security Breach

1. Employees must notify the Data Security Coordinator as well as cybersecurity@vsc.edu immediately in the event of a known or suspected Protected Information security breach or unauthorized use of Protected Information.
2. The Institution shall provide notice as soon as practicable and without unreasonable delay when the Institution (a) knows or has reason to know of a Protected Information security breach, or (b) knows or has reason to know that the Protected Information was acquired or used by an unauthorized person or used for an unauthorized purpose. The following notices shall be issued:
   a. Notice shall be provided to the individual(s) whose information was acquired or otherwise affected by an unauthorized person.
3. To the extent required by applicable regulations, notice shall be provided to the state Attorney General and other required regulatory bodies. Such notice shall include the nature of the breach of security or unauthorized acquisition or use, the number affected by such incident at the time of notification, and any steps the Institution has taken or plans to take relating to the incident, or other information required by law or regulation. Whenever there is a Protected Information security breach or unauthorized use of Protected Information, there shall be an immediate mandatory post-incident review of events and actions taken, if any, with a view to determining whether any changes in the Institution's security practices are required to improve the security of Protected Information for which the Institution is responsible.