VIRGINIA COMMONWEALTH UNIVERSITY

REPORT ON AUDIT
FOR THE YEAR ENDED
JUNE 30, 2025

Auditor of Public Accounts
Staci A. Henshaw, CPA
www.apa.virginia.gov
(804) 225-3350

AUDIT SUMMARY

We have audited the basic financial statements of Virginia Commonwealth University (University) as of and for the year ended June 30, 2025, and issued our report thereon, dated December 15, 2025. Our report, included in the University's basic financial statements, is available at the Auditor of Public Accounts' website at www.apa.virginia.gov and at the University's website at www.vcu.edu. Our audit found:

- the financial statements are presented fairly, in all material respects;

- three matters involving internal control and its operation requiring management's attention that also represent instances of noncompliance with applicable laws and regulations that are required to be reported under Government Auditing Standards; however, we do not consider the matters to be material weaknesses; and

- one additional internal control finding requiring management's attention; however, we do not consider it to be a material weakness.

In the section titled "Internal Control and Compliance Findings and Recommendations," we have included our assessment of the conditions and causes resulting in the internal control and compliance findings identified through our audit as well as recommendations for addressing those findings. Our assessment does not remove management's responsibility to perform a thorough assessment of the conditions and causes of the findings and develop and appropriately implement adequate corrective actions to resolve the findings as required by the Department of Accounts in Topic 10205 – Agency Response to APA Audit of the Commonwealth Accounting Policies and Procedures Manual. Those corrective actions may include additional items beyond our recommendations.

-TABLE OF CONTENTS-

	Pages
AUDIT SUMMARY	
INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS	1-3
INDEPENDENT AUDITOR'S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS	4-6
APPENDIX – FINDINGS SUMMARY	7
UNIVERSITY RESPONSE	8-9

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Improve Internal Controls Over Financial Reporting for Capital Assets
Type: Internal Control
Severity: Significant Deficiency
First Reported: Fiscal Year 2024

Virginia Commonwealth University (the University) has made progress in strengthening several aspects of its capital asset processes since the prior year, including improvements to capitalization practices and lease and subscription-based information technology arrangement identification and reporting. However, deficiencies remain in the execution and enforcement of certain capital asset controls, particularly related to asset disposals and the accuracy of the capital asset listing.

University staff in various departments are not following the current asset disposal policy and are removing assets from the capital asset system prior to the University physically disposing of the assets. During a review of ten asset disposals, we noted the following:

- For five assets (50%), staff did not maintain sufficient documentation to support the disposal method or disposal date, providing a Move and Surplus Form instead of a Disposal Form.

- Staff sent three assets (30%) to the warehouse for disposal without supporting documentation.

- Staff recorded the disposal of two assets (20%) in the capital asset system that remained in service.

In addition, testing we performed to locate assets included on the capital asset listing identified that five out of a sample of 24 assets (21%) recorded by departments on the capital asset listing did not physically exist, indicating continued weaknesses in maintaining accurate accounting records for capital assets.

The issues noted are primarily attributable to inconsistent adherence to established procedures at the departmental and custodian level, and reliance on forms that do not fully capture necessary disposal information. As a result, the University may remove capital assets from service prematurely or in the incorrect fiscal year, improperly remove assets from the capital asset system that remain in service, and continue to report assets that no longer exist. These conditions increase the risk of misstatement in capital asset balances and related disclosures. Additionally, if the University does not have a complete and accurate understanding of the assets it possesses, it cannot properly control or safeguard them, further increasing operational and financial risk.

University policy requires that capital assets be accurately tracked, safeguarded, and reported in financial statements, including proper documentation of disposals. These requirements are necessary to ensure the University reports assets in the correct fiscal year and that the capital asset listing remains

complete and accurate. While management has identified process gaps and is planning updates for the next fiscal year, staff have not consistently applied, and management has not enforced the current controls.

The University should continue building on the progress it has made since the prior year by finalizing and implementing the updated disposal process and ensuring it clearly documents the disposal date, method, and transfer of custody. Management should reinforce accountability for custodians to follow disposal requirements, including timely completion and documentation. The Controller's Office should also strengthen monitoring controls over the capital asset listing, including performing robust inventories and follow-up procedures to identify and resolve assets that no longer exist or are incorrectly classified. Continued training and communication with departments and custodians will be critical to ensure consistent execution of capital asset policies and sustain compliance with the University's standards.

Improve Router Security
Type: Internal Control and Compliance
Severity: Significant Deficiency

The University does not properly secure the routers that route and manage traffic within the University's network in accordance with its adopted information security standard, the International Organization for Standardization and the International Electrotechnical Commission Standard ISO/IEC 27002 (ISO Standard). We communicated five separate control weaknesses to management in a separate document marked Freedom of Information Act Exempt (FOIAE) under Section 2.2-3705.2 of the Code of Virginia, due to it containing descriptions of security mechanisms.

The ISO Standard requires the documentation and implementation of certain controls that reduce unnecessary risk to the confidentiality, integrity, and availability of the University's information systems and data. Failure to implement these controls may result in compromise of the University's sensitive network and information. Lack of resources and the need to prioritize other projects that required available personnel, as well as management oversight, resulted in the control weaknesses identified.

The University should remediate the issues discussed in the communication marked FOIAE to properly maintain and secure the router in accordance with the requirements of the ISO Standard in a timely manner. Implementing corrective action will help to ensure that the University protects its sensitive and mission critical systems and data.

Improve Physical and Environmental Security Policy and Processes
Type: Internal Control and Compliance
Severity: Significant Deficiency

The University does not require and has not implemented certain physical and environmental security elements in accordance with the ISO Standard. We identified five control weaknesses and

communicated them to management in a separate document marked FOIAE under §2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms.

The ISO Standard requires the University to implement certain controls that reduce unnecessary risk to the confidentiality, integrity, and availability of the University's mission critical systems and data. Management oversight and a lack of monitoring resulted in the University not requiring or implementing the required physical and environmental security controls. Without adequate documentation and implementation of these physical and environmental security controls, the University may have inconsistent implementation of key controls that increase the risk to secure areas. Additionally, the University increases the risk of not identifying abnormal patterns and behavior to appropriately respond.

The University should implement the controls required to address the weaknesses identified in the FOIAE communication, which will help ensure the University protects the confidentiality, integrity, and availability of its sensitive and mission critical data.

Improve IT Risk Management Security Procedures and Process

Type: Internal Control and Compliance
Severity: Significant Deficiency

The University does not require, and has not implemented, certain aspects of its Information Technology (IT) Risk Management and Contingency Program in accordance with the ISO Standard. We identified two control weaknesses and communicated them to management in a separate document marked FOIAE under §2.2-3705.2 of the Code of Virginia, as it contains descriptions of security mechanisms.

The ISO Standard requires the University to document and implement certain controls that reduce unnecessary risk to the confidentiality, integrity, and availability of the University's mission-critical systems and data. Management oversight and prioritizing other significant projects resulted in the University not requiring or implementing the required controls within its IT Risk Management and Contingency Program. Without appropriate documentation and implementation of these IT Risk Management and Contingency Program controls, the University may not consistently execute recovery processes. Additionally, the University increases the risk of a potential operational disruption in the event of an emergency.

The University should implement the required controls to address the weaknesses identified in the FOIAE communication. Implementing the required controls will help ensure that the University is able to recover sensitive and mission critical systems in a timely manner, without disrupting its operations.

Commonwealth of Virginia

Auditor of Public Accounts

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

December 15, 2025

The Honorable Glenn Youngkin
Governor of Virginia

Joint Legislative Audit
and Review Commission

Board of Visitors
Virginia Commonwealth University

Michael Rao
President, Virginia Commonwealth University

INDEPENDENT AUDITOR'S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS

We have audited, in accordance with the auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in Government Auditing Standards, issued by the Comptroller General of the United States, the financial statements of the business-type activities and aggregate discretely presented component units of the **Virginia Commonwealth University** (University) as of and for the year ended June 30, 2025, and the related notes to the financial statements, which collectively comprise the University's basic financial statements and have issued our report thereon dated December 15, 2025. Our report includes a reference to other auditors who audited the financial statements of the component units of the University, as described in our report on the University's financial statements. The other auditors did not audit the financial statements of the component units of the University in accordance with Government Auditing Standards, and accordingly, this report does not include reporting on internal control over financial reporting or compliance and other matters associated with the component units of the University.

Report on Internal Control Over Financial Reporting

In planning and performing our audit of the financial statements, we considered the University's internal control over financial reporting (internal control) as a basis for designing audit procedures that are appropriate in the circumstances for the purpose of expressing our opinions on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the University's internal control. Accordingly, we do not express an opinion on the effectiveness of the University's internal control.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented or detected and corrected on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Our consideration of internal control was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and therefore, material weaknesses or significant deficiencies may exist that were not identified. Given these limitations, during our audit we did not identify any deficiencies in internal control that we consider to be material weaknesses. We did identify certain deficiencies in internal control titled "Improve Internal Controls Over Financial Reporting for Capital Assets," "Improve Router Security," "Improve Physical and Environmental Security Policy and Processes," and "Improve IT Risk Management Security Procedures and Process," which are described in the section titled "Internal Control and Compliance Findings and Recommendations," that we consider to be significant deficiencies.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the University's financial statements are free of material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the financial statements. However, providing an opinion on compliance with those provisions was not an objective of our audit and, accordingly, we do not express such an opinion. The results of our tests disclosed instances of noncompliance or other matters that is required to be reported under Government Auditing Standards which are described in the section titled "Internal Control and Compliance Findings and Recommendations" in the findings titled "Improve Router Security," "Improve Physical and Environmental Security Policy and Processes," and "Improve IT Risk Management Security Procedures and Process."

The University's Response to Findings

We discussed this report with management at an exit conference held on January 12, 2026. Government Auditing Standards require the auditor to perform limited procedures on the University's response to the findings identified in our audit, which is included in the accompanying section titled "University Response." The University's response was not subjected to the other auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on the response.

Status of Prior Findings

The University has not taken adequate corrective action with respect to the prior reported finding identified as ongoing in the Findings Summary included in the Appendix.

Purpose of this Report

The purpose of this report is solely to describe the scope of our testing of internal control and compliance and the results of that testing, and not to provide an opinion on the effectiveness of the entity's internal control or on compliance. This report is an integral part of an audit performed in accordance with Government Auditing Standards in considering the entity's internal control and compliance. Accordingly, this communication is not suitable for any other purpose.

Staci A. Henshaw
AUDITOR OF PUBLIC ACCOUNTS

ACS/clj

FINDINGS SUMMARY

Finding Title	Status of Corrective Action*	Fiscal Year First Reported
Improve Internal Controls Over Financial Reporting for Capital Assets	Ongoing	2024
Improve Router Security	Ongoing	2025
Improve Physical and Environmental Security Policy and Processes	Ongoing	2025
Improve IT Risk Management Security Procedures and Process	Ongoing	2025

* A status of **Ongoing** indicates new and/or existing findings that require management's corrective action as of fiscal year end.

Virginia Commonwealth University
Finance and Administration
Controller's Office
Stagg House
912 West Franklin Street
Box 843035
Richmond, Virginia 23284

Ph (804) 828-0388
www.controller.vcu.edu

January 16, 2026

Staci A. Henshaw
Auditor of Public Accounts
P.O. Box 1295
Richmond, VA 23218

Dear Ms. Henshaw:

We have reviewed the audit findings and recommendations resulting from the fiscal year 2025 audit by the Auditor of Public Accounts (APA) and discussed during the exit conference.

Virginia Commonwealth University acknowledges and concurs with the audit findings. The following contains the APA finding title and management's response to the concerns and issues raised.

Findings of the Auditor:

Improve Internal Controls over Financial Reporting for Capital Assets
Type: Internal Control
Severity: Significant Deficiency

VCU Response:
The Controller's Office has centralized the process of surplusage or disposing of fixed assets to administrative offices for ensuring compliance with policy and procedures. We have provided training and updated forms to capture required information to clarify proper treatment. Additionally, a process of central oversight has been added to the annual physical inventory count.

Responsible persons: Dessi Vetter, Associate Controller and Heather Seymour, Controller

Completion Date: September 30, 2026

Improve Router Security
Type: Internal Control and Compliance
Severity: Significant Deficiency

VCU Response:
The University will improve its administrative processes and documentation for router management. The university will continue with its current vulnerability management processes for its assets, including routers, and ensure the timely maintenance of its policies and standards.

Responsible persons: Dan Han, Chief Information Security Officer

Completion Date: January 31, 2026

Improve Physical and Environmental Security Policy and Processes
Type: Internal Control and Compliance

Severity: Significant Deficiency

VCU Response:

The University will implement processes to ensure consistent documentation of access reviews and record retention for its infrastructure facilities, and to ensure the timely maintenance of its policies and standards.

Responsible persons: Dan Han, Chief Information Security Officer and Keith Deane, Director Infrastructure Services and

Completion Date: March 31, 2026

Improve IT Risk Management Security Procedures and Process
Type: Internal Control and Compliance
Severity: Significant Deficiency

VCU Response:

The University will revise its disaster recovery plans and update the plan testing sections to reflect its current validation processes, and ensure the timely maintenance of its policies and standards.

Responsible persons: Dan Han, Chief Information Security Officer

Completion Date: January 31, 2026

Sincerely,

DocuSigned by:
Heather Seymour
5DFAA026B89C49F...

Heather Seymour
Controller, Virginia Commonwealth University