



VIRGINIA COLLEGE SAVINGS PLAN

REPORT ON AUDIT FOR THE YEAR ENDED JUNE 30, 2024

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 the Virginia College Savings Plan (Virginia529) as of and for the year ended June 30, 2024, and issued our report thereon, dated November 14, 2024. Our report, included in Virginia529's Annual Report, is available at the Auditor of Public Accounts' website at www.apa.virginia.gov and at Virginia529's website at www.virginia529.com. Our audit found:

- the financial statements are presented fairly, in all material respects; and
- two internal control findings requiring management's attention; that also represent instances of noncompliance or other matters required to be reported under Government Auditing Standards; however, we do not consider them to be material weaknesses.
- adequate corrective action with respect to a prior audit finding identified as complete in the Findings Summary included in the Appendix.

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 audits 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 developing and appropriately implementing adequate corrective actions to resolve the findings. Those corrective actions may include additional items beyond our recommendations.

- TABLE OF CONTENTS -

	<u>Pages</u>
AUDIT SUMMARY	
INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS	1-2
INDEPENDENT AUDITOR'S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS	3-4
APPENDIX – FINDINGS SUMMARY	5
AGENCY RESPONSE	6

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Improve IT Service Provider Oversight

Type: Internal Control and Compliance

Severity: Significant Deficiency

Virginia529 does not consistently maintain adequate oversight of information technology (IT) service providers to gain assurance over outsourced operations in accordance with the *Virginia529 System and Services Acquisition Policy* (Acquisition Policy) and the Commonwealth's Information Security Standard, SEC 530 (Security Standard). Service providers are organizations that perform outsourced business tasks or functions on behalf of Virginia529 and the Commonwealth. Virginia529 uses service providers to manage access to, process, and store data used by its critical business functions but has not fully implemented certain policies and procedures required by the Security Standard to safeguard its outsourced IT operations. Specifically, Virginia529 does not consistently establish certain required vendor expectations or perform certain required monitoring activities over its IT service providers.

The Acquisition Policy requires the Information Security Officer to monitor security control compliance by external service providers. Additionally, the Security Standard, section SA-9 requires that Virginia529 employ the processes, methods, and techniques to monitor control compliance of external service providers on an ongoing basis, as per the control requirements detailed in sections SA-9 Control Enhancements, SA-9-COV-1, SA-9-COV-2, and SA-9-COV-3.

By not consistently gaining adequate ongoing annual assurance over IT service providers' operating controls, Virginia529 cannot validate that each provider has effective information security controls. Ineffective IT service provider controls can impact Virginia529's ability to ensure the confidentiality, integrity, and availability of hosted systems. The Commonwealth revised the Security Standard during the fiscal year which added new requirements for IT service provider oversight that Virginia529 has not addressed through its documented procedures. Additionally, Virginia529 has not adequately documented and approved deviations from the Security Standard in instances when management is relying on various levels of compensating controls to manage the risks to its hosted systems.

Virginia529 should revisit its sensitivity classifications of hosted systems to ensure accurate assessments of risk. Virginia529 should further develop documented procedures to ensure effective implementation of its Acquisition Policy, including establishing expectations during procurement, requesting annual security assessment reports from each provider, and documenting its evaluation to ensure the provider has effective operating controls in order to meet the requirements of the Security Standard. During the evaluation, Virginia529 should identify control deficiencies, develop mitigation plans, and escalate issues of non-compliance, as necessary. By gaining adequate assurance over IT service providers, Virginia529 will ensure the ongoing confidentiality, integrity, and availability of its hosted systems.

Improve Change Control and Configuration Management Procedures

Type: Internal Control and Compliance

Severity: Significant Deficiency

Virginia529 does not document and implement configuration change control in accordance with the Security Standard. We identified weaknesses, including insufficient documented guidance, resulting in documentation and procedural inconsistencies relating to changes to components of sensitive information systems. We communicated the details of the control weaknesses to management in a separate document marked Freedom of Information Act Exempt (FOIAE) under § 2.2-3705.2 of the Code of Virginia due to its sensitivity and description of security controls.

The Security Standard, section CM-3 Configuration Change Control, requires that Virginia529 must determine and document the types of changes to a system that are configuration change controlled. Section CM-3 further defines the types of changes that should be configuration change controlled. For these types of changes, section CM-3 details the change control processes that Virginia529 should perform.

Virginia529 should implement corrective controls as discussed in the communication marked FOIAE to meet the requirements in the Security Standard.



Commonwealth of Virginia

Auditor of Public Accounts

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

November 14, 2024

The Honorable Glenn Youngkin
Governor of Virginia

Joint Legislative Audit
and Review Commission

Members of the Board
Virginia College Savings Plan

Mary Morris, Chief Executive Officer
Virginia College Savings Plan

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 (the Enterprise Fund) and the fiduciary activities (the Private Purpose Trust Fund) of the **Virginia College Savings Plan** (Virginia529) as of and for the year ended June 30, 2024, and the related notes to the financial statements, which collectively comprise Virginia529's basic financial statements, and have issued our report thereon dated November 14, 2024.

Report on Internal Control Over Financial Reporting

In planning and performing our audit of the financial statements, we considered Virginia529'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 Virginia529's internal control. Accordingly, we do not express an opinion on the effectiveness of Virginia529'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 deficiencies in internal control titled “Improve IT Service Provider Oversight” and “Improve Change Control and Configuration Management Procedures,” 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 Virginia529’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 are required to be reported under Government Auditing Standards and which are described in the section titled “Internal Control and Compliance Findings and Recommendations” in the findings titled “Improve IT Service Provider Oversight” and “Improve Change Control and Configuration Management Procedures.”

Virginia529’s Response to Findings

We discussed this report with management at an exit conference held on December 3, 2024. Government Auditing Standards require the auditor to perform limited procedures on Virginia529’s response to the findings identified in our audit, which is included in the accompanying section titled “Agency Response.” Virginia529’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 Finding

Virginia529 has taken adequate corrective action with respect to the prior audit finding identified as complete 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

ZLB/vks

FINDINGS SUMMARY

Finding Title	Status of Corrective Action*	First Reported for Fiscal Year
Improve IT Risk Management Program and Contingency Planning	Complete	2023
Improve IT Service Provider Oversight	Ongoing	2024
Improve Change Control and Configuration Management Procedures	Ongoing	2024

* A status of **Complete** indicates adequate corrective action taken by Virginia529 during the fiscal year. **Ongoing** indicates new and/or existing findings that require management's corrective action as of fiscal year end.



December 6, 2024

Ms. Staci Henshaw
Auditor of Public Accounts
101 N. 14th Street, 8th Floor
Richmond, Virginia 23219

Dear Ms. Henshaw:

We appreciate the time and effort you and your staff dedicated to our operations during the fiscal year 2024 audit. We acknowledge the importance of the audit function and its elemental role in continuous improvement. By fostering a culture that values continuous improvement Commonwealth Savers strives to promote transparency, accuracy, and consistency in all our processes.

In response to the two findings in the audit report for the fiscal year ending June 30, 2024, Commonwealth Savers understands the importance that documentation of business processes has in ensuring consistent performance and accountability. We commit to continue our on-going work to enhance documentation with respect to oversight of outsourced IT service providers as well as change control and configuration management, addressing sensitivity rankings and documentation of mitigating internal controls.

Sincerely,

A handwritten signature in black ink, appearing to read 'Mary G. Morris', with a horizontal line extending to the right.

Mary G. Morris

cc: Carolyn Bishop, COO
Vivian Shields, CFO
Mike Henry, CTO
Rosario Igharas, ISO
Sherri Wyatt, CCO