CHRISTOPHER NEWPORT UNIVERSITY

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 Christopher Newport University as of and for the year ended June 30, 2024, and issued our report thereon, dated June 13, 2025. Our report, included in the University's Financial Report, is available at the Auditor of Public Accounts' website at www.apa.virginia.gov and at the University's website at www.cnu.edu. Our audit found:

- the financial statements are presented fairly, in all material respects;
- one internal control finding requiring management's attention; however, we do not consider it to be a material weakness;
- three matters involving internal control and its operation necessary to bring to management's attention that also represent instances of noncompliance with applicable laws and regulations or other matters required to be reported; and
- adequate corrective action with respect to the 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 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	1-5
INDEPENDENT AUDITOR'S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS	6-8
APPENDIX – FINDINGS SUMMARY	9
UNIVERSITY RESPONSE	10-11

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Improve IT Risk Management and Contingency Planning Program
Type: Internal Control and Compliance
Severity: Significant Deficiency
First Reported: 2023

In our prior report, we identified that Christopher Newport University (University) did not have an effective process to maintain its information technology (IT) risk management and contingency planning program in accordance with the Commonwealth's Information Security Standard, SEC530 (Security Standard). During audit planning, the University confirmed that it plans to complete corrective actions to remediate the prior year finding by May 2025. As the University plans to complete corrective action after the fiscal year under review, we will evaluate whether the corrective actions achieved the desired results during the fiscal year 2025 audit.

Improve Physical and Environmental Security Program Documentation
Type: Internal Control and Compliance
Severity: Significant Deficiency

The University has not implemented certain minimum physical and environmental security requirements outlined in its Building Access Policy and the Security Standard to adequately protect its sensitive IT systems. The University has a server room that houses IT infrastructure assets containing confidential and mission-critical data. We identified the following physical and environmental security control weaknesses:

- The University does not document its review of the Building Access Policy, which is based on the Security Standard. The Building Access Policy requires the University to review and update its physical and environmental protection policy annually and after any environmental changes. Without documentation of the review, the University lacks a formal record that the review was conducted. Additionally, by not reviewing and revising the Building Access Policy as required, the University may not document, implement, and communicate the controls and processes needed to prevent unauthorized access to the data center and protect University data.

- The University does not include certain required provisions and procedures, as mandated by the Security Standard, in its Building Access Policy. Specifically, the Building Access Policy does not require visitors to be escorted by authorized personnel; visitor access to the data center to be recorded; visitor access records to be retained for a specified period; physical access audit logs to be maintained; physical access to the facility to be monitored; or physical access logs and visitor access records to be reviewed. Furthermore, the Building Access Policy does not document the University's environmental controls and the processes for monitoring and maintaining environmental controls. Without implementing these requirements mandated by the Security Standard, the risk of unauthorized access to sensitive, restricted areas increases, which may lead to a compromise of physical IT infrastructure and operational

disruptions. Additionally, without adequate documentation of environmental controls and processes to monitor and maintain them, the University may not be able to reasonably respond to environmental conditions that could damage, degrade, or destroy organizational systems or system components.

- The University does not document its review of the list of individuals with authorized access to the data center to verify that everyone continues to need access. The Building Access Policy requires the University to review authorized access to the facility at the end of each academic term. Additionally, the Security Standard requires a review of the access list detailing authorized facility access by individuals on an annual basis and following an environmental change. Without documentation of an annual review of individuals with authorized access to the data center, the University increases the risk of unauthorized access to critical or restricted areas, which, in turn, raises the likelihood of physical asset compromise. Furthermore, insider threats, such as former employees, students, or contractors, may retain access beyond their authorized time period.

- The University does not document its reviews of visitor access records or physical access logs to the data center. The Security Standard mandates that visitor access records be reviewed at least once every 30 days. Furthermore, the Security Standard requires that physical access logs be reviewed at least once every 30 days and upon the occurrence of organization-defined events or potential indications of events. While the University sends monthly physical access and visitor access records reports to the University Information Security Officer (ISO) for review via their visitor management system, there is no documentation supporting that the ISO has reviewed the reports. Additionally, while the ISO verbally communicates to the responsible parties the anomalies and discrepancies identified, such as unauthorized access; the ISO does not document these events. An absence of documentation demonstrating the review of visitor access records and physical access logs increases the risk that the University will not identify unauthorized access events and may lead to security breaches and compromise of sensitive assets.

The absence of certain requirements and procedures in the Building Access Policy contributed to the identified weaknesses, such as a lack of documented annual reviews of authorized individuals with access to the data center, as well as documented monthly reviews of visitor access and physical access records. Furthermore, insufficient management oversight resulted in the lack of revision and review of the Building Access Policy and procedures.

The University should review and update the Building Access Policy to include the requirements of the Security Standard and develop procedures to support the implementation of an effective physical and environmental security program. Additionally, the University should establish an annual process to review and revise the Building Access Policy. The University should also document its review of physical access lists and access logs to ensure it consistently monitors authorized individuals in restricted areas, to identify suspicious events for future reference. Implementing these corrective actions will help protect the confidentiality, availability, and integrity of the University's sensitive and mission-critical data.

Improve Change Management
Type: Internal Control and Compliance
Severity: Significant Deficiency

Christopher Newport University does not consistently perform information technology changes in accordance with its Change Management Standard and Procedures, as well as its Change Management Policy. Our review identified the following weaknesses:

- The University has not reviewed its Change Management Policy since January 2022. The Change Management Policy requires the University to perform a review of the policy on an annual basis. Additionally, the Security Standard requires the University to review and update the current configuration management policy on an annual basis. Without reviewing its Change Management Policy on an annual basis, the University increases the risk that the policy becomes outdated and may not include all necessary elements to ensure adequate implementation of change management controls that meet Security Standard requirements.

- The University does not consistently evaluate and document the security risk level and risk assessment level for each change in accordance with its Change Management Standard and Procedures. As a result, 20 out of 30 (67%) sampled changes did not include an analysis of the security risk level and risk assessment level. Without consistently performing an analysis of the security risk level and risk assessment level for each change, the University increases the risk that it may not identify existing vulnerabilities or weaknesses before implementing a change which could compromise the confidentiality, availability, and integrity of the University's sensitive data.

- The University does not consistently obtain approvals for each change in accordance with its Change Management Standard and Procedures. As a result, 20 out of 30 (67%) sampled changes did not include documented approval by the Change Management Board, Chief Information Officer, or Deputy Chief Information Officer. Without consistently following its change management process, the University increases the risk of unauthorized changes that may weaken cybersecurity defenses, as poorly managed changes could lead to unintended data deletion or corruption impacting the University.

- The University does not ensure proper segregation of duties for all changes. As a result, ten out of 30 (33%) sampled changes did not include evidence that someone different than the developer migrated the change to the production environment, or an approval happened prior to the migration. Without ensuring segregation of duties for all changes, the University increases the risk of an employee making an unauthorized change that compromises security controls.

The University's Change Management Standard and Procedures were recently implemented in June 2024. As a result of this recent implementation, there are still some aspects of the new process that the University is implementing into the change process, such as the evaluation and documentation of the security risk level and risk assessment level. Additionally, the University's Change Management

Standard and Procedures is a working document that the University will update to more accurately reflect the processes for different change types, such as development changes.

The University should dedicate the resources necessary to complete the implementation of its new Change Management Standard and Procedures to ensure the University follows all elements of the process for each change type. Improving its change management process will help protect the confidentiality, integrity, and availability of the University's sensitive and mission critical data.

Strengthen Controls Over Financial Reporting
Type: Internal Control
Severity: Significant Deficiency

The University's Comptroller's Office did not perform an adequate review of its financial statements to accurately report new and complex financial events. Due to our identification of errors in the financial statements, management made the following adjustments to accurately present account balances and related activity in accordance with generally accepted accounting principles (GAAP):

- Reclassified $61.9 million in unearned revenue from current liabilities within the Statement of Net Position to capital appropriations within the Statement of Revenues, Expenses, and Changes in Net Position. Fiscal year 2024 was the first year in several years this type of activity was applicable for the University to report.

- Reclassified $3.6 million from operating expense to scholarship allowance due to the exclusion of tuition and fee waivers from the development of the scholarship allowance estimate in the Statement of Revenues, Expenses, and Changes in Net Position. The University changed its methodology for estimating scholarship allowance in accordance with the National Association of College and University Business Officers' recommendation.

- Reclassified $2.1 million from incorrect operating expense line items to depreciation and amortization expense due to management erroneously reporting lease activity in the wrong line item. The University recently implemented a new lease tracking system to aid financial reporting.

- Increased operating expenses by $1.8 million due to correction of the entry reversing prior year deferred outflows related to pensions.

Christopher Newport University management is responsible for designing and maintaining a system of internal control relevant to the preparation and fair presentation of financial statements that are free from material misstatement in accordance with GAAP. Misstatements increase the risk that users of financial statements may draw improper conclusions about the University's financial activities. While the Comptroller's Office has a mature financial reporting process for the University's ongoing activities, that process did not adequately address new financial activity and requirements that increase the risk of material misstatement and; therefore, require heightened scrutiny during financial statement preparation and review.

The Comptroller's Office should improve its financial statement preparation and review process to ensure the University reports new and complex financial activity in accordance with GAAP. Specifically, the University should enhance its financial statement review process to apply additional scrutiny to items affected by new transactions, standards, or systems to ensure the University produces financial statements that are free from material misstatement.

Commonwealth of Virginia

Auditor of Public Accounts

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

June 13, 2025

The Honorable Glenn Youngkin
Governor of Virginia

Joint Legislative Audit
and Review Commission

Board of Visitors
Christopher Newport University

William G. Kelly
President, Christopher Newport 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 **Christopher Newport University** of and for the year ended June 30, 2024, and the related notes to the financial statements, which collectively comprise the University's basic financial statements and have issued our report thereon dated June 13, 2025. Our report includes a reference to another auditor 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 auditor did not audit the financial statements of the component unit 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 IT Risk Management and Contingency Planning Program," "Improve Physical and Environmental Security Program Documentation," "Improve Change Management," and "Strengthen Controls Over Financial Reporting," 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 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 and recommendations titled "Improve IT Risk Management and Contingency Planning Program," "Improve Physical and Environmental Security Program Documentation," and "Improve Change Management."

The University's Response to Findings

We discussed this report with management at an exit conference held on June 3, 2025. 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. The University has taken adequate corrective action with respect to prior audit findings 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

SDB/clj

FINDINGS SUMMARY

Finding Title	Status of Corrective Action*	First Reported for Fiscal Year
Improve Operating System Security	Complete	2022
Improve IT Risk Management and Contingency Planning Program	Ongoing	2023
Improve Physical and Environmental Security Program Documentation	Ongoing	2024
Improve Change Management	Ongoing	2024
Strengthen Controls Over Financial Reporting	Ongoing	2024

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

CHRISTOPHER NEWPORT
UNIVERSITY

June 4, 2025

Staci Henshaw, CPA, CGMA
Auditor of Public Accounts
P.O. Box 1295
Richmond, VA 23218-1295

Dear Ms. Henshaw:

Christopher Newport University has reviewed the findings and recommendations provided by the Auditor of Public Accounts for fiscal year ended June 30, 2024. The University appreciates the effort and hard work the APA auditors put towards the audit this year and has the following response to the Internal Control and Compliance Matters:

INTERNAL CONTROL AND COMPLIANCE MATTERS

Improve IT Risk Management and Contingency Planning Program

The University IT Department has dedicated the necessary resources to implement the security controls for the operating system that meet the requirements of the Security Standard and best practices.

Improve Physical and Environmental Security Program Documentation

The University IT Department will review and update the policy to include the requirements of the Security Standard and develop procedures to support the implementation of an effective physical and environmental security program.

Improve Change Management

The University IT Department will dedicate the resources necessary to complete the implementation of its new Change Management Standard to help protect the confidentiality, integrity, and availability of the University's sensitive and mission critical data.

Office of the Chief Financial Officer/Associate Vice President
1 Avenue of the Arts, Newport News, VA 23606
Phone: 757-594-7222

Strengthen Controls Over Financial Reporting

The Comptroller's Office will improve its financial statement preparation and review process to ensure the University reports new and complex financial activity in accordance with GAAP. In addition, the financial statement review process will be revised to ensure the University produces financial statements that are free from material misstatement.

Sincerely,

Sarah Herzog

Sarah E. Herzog
Chief Financial Officer/Associate Vice President

Office of the Chief Financial Officer/Associate Vice President
1 Avenue of the Arts, Newport News, VA 23606
Phone: 757-594-7222