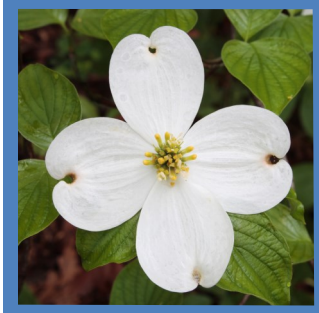


CHRISTOPHER NEWPORT UNIVERSITY

REPORT ON AUDIT

FOR THE YEAR ENDED

JUNE 30, 2023

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 (University) as of and for the year ended June 30, 2023, and issued our report thereon, dated August 12, 2024. 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.cnu.edu. Our audit found:

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

- 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 these to be material weaknesses; and

- adequate corrective action with respect to prior audit findings and recommendations 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 –

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Improve Operating System Security
Type: Internal Control and Compliance
Severity: Significant Deficiency
First Reported: Fiscal Year 2022

Christopher Newport University (University) does not implement certain security controls for its server operating system in accordance with the Commonwealth's Information Security Standard, SEC501 (Security Standard) and best practices, such as the Center for Internet Security Benchmark. We identified and communicated the specific 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 mechanisms.

The control weaknesses were the result of the University applying settings and permissions without evaluating the settings and permissions against best practices and recommendations. The University should dedicate the necessary resources to implement the security controls for the operating system as communicated in the FOIAE recommendation that meet the requirements of the Security Standard and best practices. Implementing the required controls will help ensure the University maintains the confidentiality, integrity, and availability of sensitive and mission-critical data.

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

The University does not have an effective process to maintain its information technology (IT) risk management and contingency planning program. Specifically, the University does not meet the following requirements in the Security Standard:

- The University does not define each data class as sensitive or non-sensitive in order to identify systems as sensitive or non-sensitive. The University identifies the data stored, processed, or transmitted by each system. The University also classifies the data handled by each system as Class 1-Restricted, Class 2-Confidential (Moderate Sensitivity), Class 3-Confidential (Low Sensitivity), or Class 4-Public. However, the University does not define the sensitivity of each of the four data classes as either 'sensitive' or 'non-sensitive.' (*Security Standard, section 4 – IT System and Data Sensitivity Classification*)

- The University has not conducted a system risk assessment of each of its sensitive systems. The University conducted a system risk assessment of one of its critical systems, and the University conducted nine of 39 departmental risk assessments that included 32 of the 52 Class 1 and Class 2 systems used across the nine departments. However, the University has not conducted individual system risk assessments for each of its sensitive systems. (*Security Standard, section 6.2 Risk Assessment*)

- The University does not have a System Security Plan (SSP) for any of its sensitive systems. The University developed an SSP template to use following the completion of system risk assessments. However, the University has not yet completed any SSPs. (*Security Standard, section PL-2 System Security Plan*)

- The University does not always prevent conflicts of interest and adhere to the security concept of separation of duties when assigning system owner, data owner, system administrator, and data custodian roles. Specifically, the University designated the Information Security Officer as the data owner for nine of its 96 active systems. *(Security Standard section 2.4.10.b – Agency Head)*

- The University has not completed a comprehensive Business Impact Analysis (BIA) to evaluate the University's essential and non-essential business functions and their dependence on information technology systems. The University completes departmental BIAs but has only completed a BIA for nine out of 39 departments. Specifically, the University's Business Impact Analysis Standard requires that system owners complete a Business Impact Analysis Intake form; however, the University obtained Business Impact Analysis Intake forms from nine out of 39 departments rather than obtaining Business Impact Analysis Intake forms from each System Owner. *(Security Standard, section 3 – Business Impact Analysis)*

- The University identifies primary business functions and the associated Business Process Analysis for each primary business function in the Continuity of Operations Plan (COOP). However, although the University updated the COOP in September 2023, the University has not reviewed the Business Process Analysis for each Primary Business Function since January 2022 and March 2022. *(Security Standard section 3.2 – Business Impact Analysis)*

- The University does not coordinate contingency plan testing with organizational elements responsible for related plans, including the COOP and Disaster Recovery Plan (DRP). Specifically, the University conducted a COOP test in June 2023 that evaluated a departmental relocation to an alternative location; however, the test did not include Information Technology Services to determine the effectiveness of the related plans and ensure availability of IT components and resources. *(Security Standard section CP-4 – Contingency Plan Testing)*

- The departments responsible for risk management and contingency planning do not collaborate to verify that IT related disaster recovery planning efforts adequately support the mission essential business functions of the University. Specifically, the Department of Emergency Management requests that departments complete a Business Process Analysis form and Information Technology Services requests that departments complete a Business Impact Analysis Intake form; however, the Department of Emergency Management and Information Technology Services do not ensure that the information obtained from the two forms align prior to completing the COOP and IT DRP. *(Security Standard section CP-1-COV-1.2 Contingency Planning Policy and Procedures)*

Without maintaining complete and effective IT risk management and contingency planning documentation, the University puts at risk the ability to recover the essential and primary business

functions required to operate effectively in the event of an emergency or disaster. By not conducting risk assessments for sensitive systems in a timely manner, the University may not adequately identify risks for its sensitive systems or identify and implement appropriate security controls for its IT systems and environment to address those risks. Unaddressed system security risks can lead to a potential compromise of the University's sensitive information. Without having a system security plan for each sensitive system, the University increases the risk of not identifying and implementing proper security controls to secure the system. Inconsistencies within risk management and contingency planning artifacts increase the risk of the University not having all the necessary requirements within the artifacts to recover systems and business process in required timeframes to support its mission essential functions. Without implementing the concept of separation of duties when assigning roles, the University increases the risk of operational inefficiencies, errors, and mismanagement which could result in the compromise of the University's sensitive data.

In 2023, the University experienced turnover of multiple executive level positions, including the Chief Information Officer and Director of Emergency Management, which contributed to inconsistent IT risk management and contingency planning documentation. Additionally, significant resource constraints contributed to the above issues.

The University should dedicate the necessary resources to improve oversight of its risk management and contingency planning process and documentation. Proper oversight includes developing a formal process to ensure the information within the documents is consistent, reflects the current environment, and addresses the weaknesses identified. Improving its risk management and contingency planning efforts and documentation will help the University to effectively respond to disasters and interruptions in IT operations within management's expected timeframes and assist in ensuring the confidentiality, integrity, and availability of its mission-critical data.

Commonwealth of Virginia

Auditor of Public Accounts

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

August 12, 2024

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** (University) as of and for the year ended June 30, 2023, and the related notes to the financial statements, which collectively comprise the University's basic financial statements and have issued our report thereon dated August 12, 2024. 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 Operating System Security" and "Improve IT Risk Management and Contingency Planning Program," 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 Operating System Security" and "Improve IT Risk Management and Contingency Planning Program."

The University's Response to Findings

We discussed this report with management at an exit conference held on June 6, 2024, and provided a draft of this report for management's review on August 9, 2024. 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. The University has taken

adequate corrective action with respect to prior audit findings and recommendations 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/vks

CHRISTOPHER NEWPORT
UNIVERSITY

August 12, 2024

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

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, 2023. 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 Operating System Security

The University will dedicate the necessary resources to implement the security controls for the operating system as communicated in the FOIAE recommendation that meet the requirements of the Security Standard and best practices.

Improve IT Risk Management and Contingency Planning Program

The University will dedicate the necessary resources to prioritize the oversight function for our risk management and contingency planning process and documentation to ensure the information within the documents is consistent, reflects the current environment and addresses any weaknesses identified.

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

FINDINGS SUMMARY

Finding Title	Status of Corrective Action*	First Reported for Fiscal Year
Improve Database Audit Logging and Monitoring	Complete	2022
Improve Internal Controls Over Terminated Employees	Complete	2022
Improve Operating System Security	Ongoing	2022
Improve IT Risk Management and Contingency Planning Program	Ongoing	2023

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