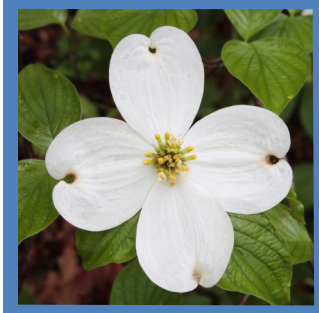


CHRISTOPHER NEWPORT UNIVERSITY

REPORT ON AUDIT

FOR THE YEAR ENDED

JUNE 30, 2021

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 (the University) as of and for the year ended June 30, 2021, and issued our report thereon dated May 27, 2022. 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 of the University for the year ended June 30, 2021, found:

- the financial statements are presented fairly, in all material respects;
- internal control findings requiring management's attention; however, we do not consider these to be material weaknesses;
- instances of noncompliance or other matters required to be reported under Government Auditing Standards; and
- adequate resolution of the prior year's audit finding.

Our audit also included testing over federal Student Financial Assistance performed in accordance with the U.S. Office of Management and Budget Compliance Supplement Part 5 Student Financial Assistance Programs; and found an internal control finding requiring management's attention that was also an instance of noncompliance required to be reported in relation to this testing.

–TABLE OF CONTENTS–

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Develop and Implement Database Configuration Procedures
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

The University does not document its own procedures to secure a database management system that supports one of its critical and sensitive applications. The University follows the vendor's compliance standards when configuring the database; however, the University does not create its own procedure by comparing and aligning the settings recommended by the vendor's standard to ensure they meet the requirements of the University's policy, the Commonwealth's Information Security Standard, SEC 501 (Security Standard), and industry best practices, such as the Center for Internet Security Benchmarks (CIS Benchmarks). Subsequently, we found one administrative account control, two password controls, three monitoring controls, and two configuration management controls that do not align with standards or best practices.

The Security Standard requires the University to perform the following for sensitive systems (*Security Standard, Section CM-6 Configuration Settings):*

- Establish and document configuration settings for information technology products employed within the information system using the Commonwealth of Virginia System Hardening Standards that reflect the most restrictive mode consistent with operational requirements.

- Implement the configuration settings.

- Identify, document, and approve any deviations from established configuration settings for information system components based on operational requirements.

- Monitor and control changes to the configuration settings in accordance with organizational policies and procedure.

Without a tailored and documented procedure applicable to the University's control expectations, the University increases the risk that the system will not meet minimum security requirements to protect data from malicious parties. The University did not document and implement a configuration procedure because it depended on the security practices published by the application's vendor.

The University should document and implement a configuration procedure based on Security Standard requirements and settings recommended by industry best practices, such as CIS Benchmarks. The configuration procedure should include deviations from recommended and expected security configurations and the University's business justification for the deviation. Additionally, the University

should develop a process to review the database's configuration against its established configuration procedure and CIS Benchmarks on a scheduled basis and after major changes occur to help detect and address potential misconfigurations timely. Establishing and implementing a procedure to standardize configurations will help protect the confidentiality, integrity, and availability of the University's sensitive data.

Develop and Implement a Process to Maintain Oversight over Service Providers

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

The University does not have a process for gaining continuing assurance that all information technology service providers (IT providers) have effective operating controls to protect the University's sensitive and confidential data after initial service procurement. IT providers are organizations that perform certain business tasks or functions on behalf of the University. The University has a process in place to assess and approve IT providers during contract negotiation and procurement but does not have any formal processes to gain assurance on an annual basis that agreed-upon security controls are in place and operating effectively. Specifically, the University does not have a documented process to obtain and review periodic service reports and annual independent audit assurance reports, such as System and Organization Controls (SOC) reports, from each IT provider.

The University requires all contracts with IT providers that may create, obtain, use, maintain, process, store, or dispose of University data to contain a security addendum wherein the IT provider agrees to adhere to certain security requirements. The addendum states that the IT provider shall provide an annual independent security audit that attests to the IT provider's security controls. The Security Standard states management remains accountable for maintaining compliance with the Security Standard through documented agreements with IT providers and oversight of services provided (*Security Standard, Section 1.1-Intent*). Additionally, the Commonwealth's Hosted Environment Information Security Standard, SEC 525 (Hosted Environment Security Standard), recognizes that organizations may procure IT equipment, systems, or services from third-party service providers and states that organizations must ensure that such providers meet the organization's established security requirements. Additionally, the Hosted Environment Security Standard requires that organizations define and employ processes to monitor security control compliance by external service providers on an ongoing basis (*Hosted Environment Security Standard, Section: SA-9 External Information System Services*).

By not defining, documenting, and employing a process to gain continuous assurance over IT providers' operating controls, the University cannot validate that the IT providers have effective IT controls to protect the University's sensitive and confidential data. Due to staffing constraints, the University has not developed and implemented a policy and process for maintaining oversight over IT providers, which impacted the University gaining assurance over outsourced operations.

The University should develop and document a policy and process to maintain oversight over IT providers and gain assurance over outsourced operations. The University should then request and

evaluate periodic service reports and annual independent audit assurance reports from each IT provider to ensure the IT provider has effective operating controls to protect the University's sensitive and confidential data. During the evaluation, the University should identify control deficiencies, develop mitigation plans, and escalate issues of noncompliance, as needed. Finally, the University should document its evaluation of the periodic service reports and annual assurance reports from each IT provider. If the University is unable to obtain a service report, it needs to document this consideration in its risk assessment and evaluate and implement the appropriate compensating controls to maintain security of its sensitive data. The University should evaluate its current staffing levels and assignments to determine if it needs to prioritize staff assignments differently or hire additional staff to ensure the University can implement information security controls timely and according to standards. Gaining sufficient assurance over IT providers' security controls will help to ensure the confidentiality, integrity, and availability of sensitive data.

Implement Cybersecurity Requirements of the Gramm-Leach-Bliley Act
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

The University does not implement all cybersecurity requirements of the Gramm-Leach-Bliley Act (GLBA) and University policy for some systems containing customer information. Specifically, the University completed a risk assessment for five of 76 sensitive systems but does not have risk assessments for the remaining 71 sensitive systems. Additionally, the University has not evaluated each of its systems to determine which systems contain customer information specifically protected under the GLBA.

Federal regulations consider institutions of higher education, because of their engagement in financial assistance programs, to be financial institutions that must comply with Public Law 106-102, known as the GLBA. Related regulations within 16 U.S. Code of Federal Regulations (CFR) Part 314.4, require that organizations develop, implement, and maintain their information security programs to safeguard customer information and complete a risk assessment that includes consideration of risks in each relevant area of operation. Additionally, the University's *Information Technology Systems Risk Assessment Process,* requires the Chief Information Officer or the Information Security Officer to establish a schedule and perform risk assessments on a periodic basis.

Without implementing cybersecurity requirements of the GLBA for each system containing customer information, the University may not be able to ensure the security and confidentiality of customer information, protect against any anticipated threats or hazards, and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to the University's customers. Due to a lack of an internal risk assessment schedule and staffing constraints, the University has not yet completed the risk assessment process to meet the cybersecurity requirements of the GLBA for each system containing non-public customer information.

The University should evaluate its systems to determine which systems contain customer information, then document and complete a risk assessment for each of these systems. As part of the

risk assessment process, the University should identify controls and safeguards that are either in place or need to be implemented that mitigate the risks identified in the risk assessment. The University should evaluate its current staffing levels and assignments to determine if it needs to prioritize staff assignments differently or hire additional staff to ensure the University can implement information security controls timely and according to standards. Completion of required risk assessments and mitigation plans will help protect the security, confidentiality, and integrity of customer information and meet the requirements set forth in the GLBA.

Commonwealth of Virginia

Auditor of Public Accounts

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

May 27, 2022

The Honorable Glenn Youngkin
Governor of Virginia

Joint Legislative Audit
and Review Commission

Board of Visitors
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, 2021, and the related notes to the financial statements, which collectively comprise the University's basic financial statements, and have issued our report thereon dated May 27, 2022. Our report includes a reference to other auditors. We did not consider internal controls over financial reporting or test compliance with certain provisions of laws, regulations, contracts, and grant agreements for the financial statements of the component units of the University, which were audited by other auditors in accordance with auditing standards generally accepted in the United States of America, but not in accordance with Government Auditing Standards.

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 "Develop and Implement Database Configuration Procedures," "Develop and Implement a Process to Maintain Oversight over Service Providers," and "Implement Cybersecurity Requirements of the Gramm-Leach-Bliley Act," 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" for the findings titled "Develop and Implement Database Configuration Procedures," "Develop and Implement a Process to Maintain Oversight over Service Providers," and "Implement Cybersecurity Requirements of the Gramm-Leach-Bliley Act."

The University's Response to Findings

We discussed this report with management at an exit conference held on June 2, 2022. The University's response to the findings identified in our audit is described in the accompanying section titled "University Response." The University's response was not subjected to the auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on it.

Status of Prior Findings

The University has taken adequate corrective action with respect to the audit finding reported in the prior year.

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

LCW/vks

CHRISTOPHER NEWPORT
UNIVERSITY

May 27, 2022

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, 2021. 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

Develop and Implement Database Configuration Procedures

The University will document and implement a configuration procedure and process review that is based on Security Standard requirements and settings recommended by industry best practices. The configuration procedure will include justification for any deviations from recommended and expected security configurations.

Develop and Implement a Process to Maintain Oversight over Service Providers

The University will develop and document a Third-Party Risk Management Standard to maintain oversight over IT providers and gain assurance over outsourced operations. This standard will document the process to request and evaluate periodic reports from IT providers containing sensitive University data.

Office of the Vice President for Finance and Planning
1 Avenue of the Arts, Newport News, VA 23606
Phone: 757-594-7040 Fax: 757-594-7864

Implement Cybersecurity Requirements of the Gramm-Leach-Bliley Act

The Information Security team maintains and tracks systems identified as "sensitive" and their respective system owner, data owner, administrator and custodian responsibilities. As part of this process IT will consolidate system documentation to include modifications to identify data classification in compliance with the Graham-Leach-Bliley Act (GLBA).

Sincerely,

Jennifer B. Latour
Vice President for Finance and Planning/CFO

Office of the Vice President for Finance and Planning
1 Avenue of the Arts, Newport News, VA 23606
Phone: 757-594-7040 Fax: 757-594-7864

CHRISTOPHER NEWPORT UNIVERSITY

As of June 30, 2021

BOARD OF VISITORS

Robert R. Hatten, Rector

C. Bradford Hunter, Vice Rector

Terri M. McKnight, Secretary

Regina Brayboy
Lindsey Carney-Smith
William Ermatinger
Judy Ford-Wason
Maria Herbert
Steven Kast
Sean Miller
Gabriel Morgan, Sr.
Christy Morton
Lee Vreeland
Ella Ward

UNIVERSITY OFFICIALS

Paul Trible, President

David Doughty, Provost

Adelia Thompson, Chief of Staff

Jennifer Latour, Vice President for Finance & Planning

Christine Ledford, Vice President for Administration and Auxiliary Services