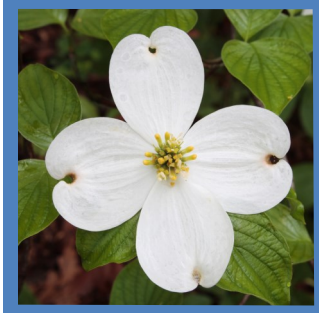


CHRISTOPHER NEWPORT UNIVERSITY

REPORT ON AUDIT
FOR THE YEAR ENDED
JUNE 30, 2018

Auditor of Public Accounts
Martha S. Mavredes, 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, 2018, and issued our report thereon, dated May 6, 2019. Our report is included in the University's Financial Statements that it anticipates releasing on or around June 7, 2019. Our audit found:

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

–TABLE OF CONTENTS–

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Improve Web Application Security
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

Christopher Newport University (University) does not properly secure a sensitive web application in accordance with its information security standard, the Commonwealth's Information Security Standard, SEC 501 (Security Standard).

We communicated five separate control weaknesses to management in a separate document marked Freedom of Information Act (FOIA) Exempt under §2.2-3705.2 of the Code of Virginia, due to it containing descriptions of security mechanisms. The Security 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.

The University should develop a plan to implement the controls discussed in the communication marked FOIA Exempt in accordance with the Security Standard in a timely manner. Doing this will help to ensure the University secures the web application to protect its sensitive and mission critical data.

Develop and Implement Information Security Policies
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

The University does not have certain policies to support its information security program. The Security Standard requires the University to develop and implement policies that prescribe the control requirements for sensitive applications and systems. The University lacks policies for the following areas:

- ***The University does not have a Patching Policy***

  The University does not have a patching policy to support the minimum patching requirements for sensitive applications and the network infrastructure components that support them. The University has patching procedures for certain environments, but the University lacks an overarching policy to define when and how the IT department will review and implement patches for critical and sensitive systems.

  The Security Standard, *Section SI-2: Flaw Remediation* requires the University to install security-relevant software and firmware updates within 90-days of the release of the updates. Without a policy to define the minimum requirements to install critical patches, the University increases the risk that vulnerabilities and security weaknesses will exist in its environment, which can lead to a breach of data or effect system availability.

- ***The University does not have a policy for Monitoring and Logging IT systems***

  The University does not have a policy to govern the minimum requirements for logging and monitoring sensitive systems and applications. The University uses a Security Information and Event Management (SIEM) tool to capture systems events on the network and produce reports to review suspicious activity and determine if vulnerabilities exist. The Information Security Officer (ISO) uses the SIEM to monitor information security activity; however, the University has no policy to detail the scope, roles, responsibilities, and the minimum system events to log and monitor for each system. The ISO is currently drafting a policy that will cover monitoring and logging requirements at the University.

  The Security Standard, *Section AU-1: Audit and Accountability*, requires the University to develop an audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and procedures to support the policy.

- ***The University does not have a policy for retaining IT system event logs***

  The University does not have a policy to establish the minimum requirements for retaining IT records, specifically system event logs. The SIEM stores IT system event logs and once the storage reaches the maximum capacity, the SIEM purges the oldest events logs with the most recent ones. The University's "SIEM Features and Storage" document states the overall retention time for IT system events is approximately three months depending on the activity level on the network. Three months is an insufficient period to maintain IT system events in the event the University needs to investigate a potential security incident.

  The University has a University-wide record retention policy that states, *"Retention periods are set by the State Library for state agencies in General Schedules (GS) 101 through GS 111. It is the responsibility of each department, with the assistance of the University Records Manager, to ensure that the retention schedules are being followed.*" In addition, the Security Standard, *Section AU-11 Audit Record Retention*, requires the University to retain audit records for consistency with the University's records retention policy to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

The lack of policies in these key areas is, at least in part, due to turnover in the ISO position, which led to the ISO position being vacant for several months during 2018. The University hired an ISO in November 2018, who is currently developing policies to address the issues discussed above. In addition, the University has procedures to support certain areas relating to patching and monitoring and logging, but due to other priorities, such as upgrading the University's financial system, it did not develop and implement policies for these specific areas.

The University should dedicate the necessary resources to develop and formally approve policies for these areas and implement them into their information security program. The policies should align

with the requirements in the Security Standard and prescribe effective security controls in the University's IT environment. Developing and implementing the policies will help to ensure the confidentiality, integrity, and availability of data and achieve compliance with the Security Standard.

Commonwealth of Virginia

Auditor of Public Accounts

Martha S. Mavredes, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

May 6, 2019

The Honorable Ralph S. Northam
Governor of Virginia

The Honorable Thomas K. Norment, Jr.
Chairman, 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** (the University) as of and for the year ended June 30, 2018, 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 6, 2019. 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 to determine the 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 over financial reporting. Accordingly, we do not express an opinion on the effectiveness of the University's internal control over financial reporting.

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 over financial reporting was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control over financial reporting 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 over financial reporting that we consider to be material weaknesses. We did identify certain deficiencies in internal control over financial reporting entitled "Improve Web Application Security" and "Develop and Implement Information Security Policies", 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 determination of financial statement amounts. 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 entitled "Improve Web Application Security" and "Develop and Implement Information Security Policies."

The University's Response to Findings

We discussed this report with management at an exit conference held on May 21, 2019. 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 audit findings 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 Audit Standards in considering the entity's internal control and compliance. Accordingly, this communication is not suitable for any other purpose.

AUDITOR OF PUBLIC ACCOUNTS

LCW/vks

CHRISTOPHER NEWPORT
UNIVERSITY

May 6, 2019

Martha S. Mavredes, CPA
Auditor of Public Accounts
P.O. Box 1295
Richmond, VA 23218

Dear Ms. Mavredes:

Christopher Newport University has reviewed the findings and recommendations provided by the Auditor of Public Accounts for fiscal year ended June 30, 2018. 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 Matter:

Internal Control and Compliance Matters

Improve Web Application Security

The University will ensure that the necessary controls are implemented in a timely manner, and in accordance with the Security Standard as proposed in the communication marked FOIA Exempt.

Develop and Implement Information Security Policies

The University will ensure that the security policies, to support our information security program, are developed and implemented in a timely manner.

Sincerely,

William L. Brauer
Executive Vice President

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

CHRISTOPHER NEWPORT UNIVERSITY

As of June 30, 2018

BOARD OF VISITORS

N. Scott Millar
Rector

Vicki Siokis Freeman
Vice Rector

C. Bradford Hunter
Secretary

Lindsey A. Carney
William R. Ermatinger
Robert R. Hatten
W. Bruce Jennings
Steven S. Kast
Terri M. McKnight
Gabriel A. Morgan, Sr.
Kellye L. Walker
Dr. Ella P. Ward
Judy Ford Wason
Junius H. Williams, Jr.

Dr. Brian Puaca
Faculty Representative

Kenneth Kidd
Student Representative

UNIVERSITY OFFICIALS

Paul S. Trible, President

Dr. David C. Doughty, Provost

Cynthia R. Perry, Chief of Staff

William L. Brauer, Executive Vice President

Kevin Hughes, Vice President of Student Affairs

Jennifer Latour, Vice President for Strategy and Planning

Dr. Lisa Duncan Raines, Vice President for Enrollment and Success

Adelia P. Thompson, Vice President of University Advancement