LONGWOOD UNIVERSITY

REPORT ON AUDIT
FOR THE YEAR ENDED
JUNE 30, 2015

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 Longwood University as of and for the year ended June 30, 2015, and issued our report thereon, dated July 27, 2016. Our report is included in the University's Annual Report, is available at the Auditor of Public Accounts' website at www.apa.virginia.gov and at the University's website at www.longwood.edu. Our audit found:

- the financial statements are presented fairly, in all material respects;
- internal control findings requiring management's attention; however, we do not consider them to be material weaknesses; and
- instances of noncompliance with applicable laws and regulations or other matters that are required to be reported under Government Auditing Standards.

-TABLE OF CONTENTS-

STATUS OF PRIOR YEAR FINDINGS

Improve Information Security Management and Prioritization

Longwood University (University) does not prioritize and manage information security for sensitive University information technology (IT) resources in accordance with the University's designated information security standard, ISO 27002 version 2013-10-01, as reported in our previous audit.

We also identified and communicated several areas of weaknesses to management in a separate document marked Freedom of Information Act Exempt under Section 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms.

We obtained a status update from Longwood on the corrective actions related to these weaknesses. As of our report date, some corrective actions were completed and some remain ongoing. The weaknesses that still have corrective action ongoing are included in this year's recommendations and will be reviewed during our next audit.

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Improve IT Change Management and Patch Management Policies and Procedures

The University is using an outdated IT change management policy from 2009 and does not have a sufficient patch management policy that sets consistent expectations for upgrading and patching sensitive IT systems.

The University's adopted security standard, ISO 27002:2013 (Security Standard), requires several configuration management controls to safeguard mission critical systems that contain or process sensitive data. The Security Standard defines minimum requirements for change control management, including but not limited to: segregation of duties enforcement, a clearly defined formal approval process, and testing a change in a segregated environment prior to implementation (*Security Standard Section: 14.2.2 System Change Control Procedures*). Specifically, the University's change policy does not include the following:

- A determination of how to differentiate between changes that should be tracked and documented as "maintenance" or "change."
- Clear procedures and guidelines for maintenance changes resulting in inconsistencies and unclear requirements.

Additionally, the University does not have a sufficient patch management procedure that defines requirements for all areas managed by Information Technology Services, such as:

- A process to identify when systems require patches;
- A determination of reasonable timeframes for the application of patches; and
- Establishing required patch windows.

The University's current patch management procedure provides guidance for the patching of Windows servers; however, the procedure does not define the requirements for identifying and applying patches for non-Windows systems, including the server operating systems supporting the primary financial management system.

An inadequate change management policy could result in inappropriate implementation of system changes that could result in a breach of sensitive data or system unavailability, which could include financial, legal, and reputational damages for the University. Also, without a sufficient patch management procedure, the University does not identify when systems require patches, apply the patches in a reasonable timeframe, or have an established patch window to apply required patches. Systems that are not up-to-date are at an increased risk for data compromise and system unavailability.

These weaknesses exist in the environment due to competing IT priorities and limited availability of resources. The University should dedicate the necessary resources to finish and implement an updated change control policy and update the patch management procedure to comply with the requirements defined in the Security Standard.

Improve Virtual Private Network Security

The University does not implement controls in its virtual private networks that are in accordance with its policies, its designated information security standard, ISO 27002:2013 (Security Standard), or that align with industry best practices. These policies and standards require the implementation of several security controls to safeguard mission critical systems that contain or process sensitive data.

We identified and communicated the specific control weaknesses to management in a separate document marked Freedom of Information Act Exempt (FOIAE) under Section 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms. In general, these areas consisted of weaknesses related to system monitoring, authentication, software patching, training, and definition of requirements.

The University should dedicate the necessary resources to mitigate the specific risks communicated in the FOIAE document. Improvements to the security posture of remote connections is required for compliance with the University's policy, the Security Standard, and to align with industry best practices. Improvements will also reduce risk associated with remote connections that access systems that contain sensitive data.

Improve Server Operating System Security

The University is missing some required and recommended security controls for the server operating system where the primary financial management system's database is installed. These missing controls are either required by the University's policy or its designated information security standard, ISO 27002:2013 (Security Standard), or recommended by industry best practices.

We identified and communicated the specific control weaknesses to management in a separate document marked FOIAE under Section 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms. In general, these areas consisted of weaknesses related to system patching, least functionality, system monitoring, and access controls.

The University should dedicate the necessary resources to mitigate the risks communicated in the FOIAE document. Improvements to the security controls of the operating system are required for compliance with the University's policy, the Security Standard, and to align with industry best practices and will reduce sensitive data safeguard risk associated with the system to ensure its confidentiality, integrity, and availability.

Improve Oversight of Third-Party Service Providers

The University does not maintain oversight of its third-party providers, including sub-service providers, to gain assurance over outsourced IT operations. Additionally, the University does not sufficiently document contractual agreements with service providers that establish requirements to protect sensitive data that meet the requirements of the University's designated information security standard, ISO 27002:2013 (Security Standard) and its policies. The University has outsourced two business functions that include transactions with sensitive data where sufficient assurance has not been obtained: one for student health services and one for student transcript services.

The Security Standard requires the implementation of controls to gain assurance and maintain oversight over contractors, that such controls include clearly documenting the security requirements a contractor must comply with, have a signed agreement over security requirements, and relevant regulations for sub-contracting (*Security Standard Section: 15.1 Information security in supplier relationships*). The University may obtain assurance over outsourced operations in various ways, including but not limited to, Service Organization Control (SOC) reports or other independent audit reports that cover the scope of security controls relied upon by the University and sufficient contractual language that holds the contractor accountable for compliance with the University's policy and the Security Standard.

Without establishing documented agreements and exercising oversight of the services provided, the University cannot gain reasonable assurance and validate that service providers have implemented effective internal controls that at a minimum meet the requirements outlined in the Security Standard and its policies for protecting sensitive data.

The University has not enforced compliance requirements for third-party providers because it has not established a formal documented process in its information security program for identifying third-party providers, establishing documented agreements with each service provider, and employing appropriate oversight of the services provided. Additionally, the University has not established a collaborative relationship between IT security and procurement to ensure adequate contractual language is included to address information security requirements.

Since the identification of this issue, the University has taken steps towards compliance, including communication with the Office of the Attorney General and its Material Management Office. The University is working on a contract addendum draft that aims to address contractor accountability for the implementation of security controls to protect the University's data.

The University should implement an approach to obtain assurance over third-party service providers, maintain oversight, and include adequate contractual language to hold the contractor accountable for the implementation of security controls. To facilitate the implementation of these controls, the University should develop a formal procedure to establish documented contractual agreements with third-party providers directing that the vendor comply with the requirements of its policy and the Security Standard; proactively and timely request the appropriate assurances from its

service providers; implement a structured review process to evaluate the service provider's internal controls and performance; document its evaluation of the service provider's internal controls and performance including any areas identified as weaknesses, then apply compensating controls accordingly; and document agency head approval of the services provided.

Commonwealth of Virginia

Auditor of Public Accounts

Martha S. Mavredes, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

July 27, 2016

The Honorable Terence R. McAuliffe
Governor of Virginia

The Honorable Robert D. Orrock, Sr.
Chairman, Joint Legislative Audit
and Review Commission

Board of Visitors
Longwood 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 Longwood University as of and for the year ended June 30, 2015, and the related notes to the financial statements, which collectively comprise the University's basic financial statements and have issued our report thereon dated July 27, 2016. 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 Information Security Management and Prioritization" and in the section titled "Status of Prior Year Findings," and "Improve IT Change Management and Patch Management Policies and Procedures," "Improve Virtual Private Network Security," "Improve Server Operating System Security," and "Improve Oversight of Third-Party Service Providers," 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 which are included within the section titled "Status of Prior Year Findings," in the finding entitled "Improve Information Security Management and Prioritization" and in the section titled "Internal Control and Compliance Findings and Recommendations," in the findings entitled "Improve IT Change Management and Patch Management Policies and Procedures," "Improve Virtual Private Network Security," "Improve Server Operating System Security," and "Improve Oversight of Third-Party Service Providers."

The University's Response to Findings

We discussed this report with management at an exit conference held on July 27, 2016. 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

With respect to all audit findings reported in the prior year, the University has completed some correction actions, while others remain ongoing. Accordingly, we included the status in the section entitled "Status of Prior Year Findings."

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

JRQ/alh

LONGWOOD
UNIVERSITY

201 High Street
Farmville, Virginia 23909
tel: 434.395.2016
fax: 434.395.2635
trs: 711

Office of the Vice President for Administration and Finance

July 27, 2016

Ms. Martha Mavredes
Auditor of Public Accounts
P.O. Box 1295
Richmond, VA 23218-1295

Dear Ms. Mavredes:

Longwood University has reviewed the Internal Control Findings and Recommendations provided by the Auditor of Public Accounts for fiscal year ending June 30, 2015 and is in agreement, in principle, with all of the findings submitted.

Attached for your consideration is a brief update as to where the campus is with respect to progress on the findings. The formal Corrective Action Workplan will be submitted within thirty days as required by CAPP Manual Section 10205. Please contact me should you have any questions or require additional information.

On behalf of Longwood University, please extend my appreciation to all of your staff for their professional audit work and recommendations.

Sincerely,

Mr. P. Kenneth Copeland, Jr.
Vice President for Administration and Finance

FY 2015 –Internal Control Findings and Recommendations

Improve IT Change Management and Patch Management Policies and Procedures

- The ITS department has reviewed the findings, concurs and is implementing corrective actions which will be completed August 1, 2016.

Improve Virtual Private Network Security

- The ITS department has reviewed the findings, concurs and is implementing corrective actions which will be completed August 1, 2016.

Improve Server Operating System Security

- The ITS department has reviewed the findings, concurs and is implementing corrective actions which will be completed May 31, 2017.

Improve Oversight of Third-Party Service Providers

- The ITS department and Materiel Management department have reviewed the finding and is finalizing a contract terms and conditions that will address contractor accountability for the implementation of security controls to protect Longwood data. These terms and conditions will be posted to the Materiel Management website by August 31, 2016, for inclusion in all future solicitations. As contract modifications and renewals are exercised for current contracts these terms and conditions will be included.

LONGWOOD UNIVERSITY

Farmville, Virginia

As of June 30, 2015

BOARD OF VISITORS

Colleen McCrink Margiloff
Rector

Robert S. Wertz, Jr.
Vice Rector

Eileen M. Anderson
Katherine Elam Busser
David H. Hallock
Eric Hansen
Thomas A. Johnson
Stephen L. Mobley
Marianne M. Radcliff
Brad E. Schwartz
Lucia Anna Trigiani
Shelby Jones Walker
Lacy Ward, Jr.

UNIVERSITY OFFICIALS

W. Taylor Reveley, IV
President

Kenneth Perkins
Provost and Vice President for Academic Affairs

Ken Copeland
Vice President for Administration and Finance

Richard Bratcher
Vice President for Facilities Management and Real Property

Tim Pierson
Vice President for Student Affairs

Victoria Kindon
Vice President for Strategic Operations

Courtney Hodges
Interim Vice President for University Advancement