LONGWOOD UNIVERSITY

REPORT ON AUDIT
FOR THE YEAR ENDED
JUNE 30, 2020

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 Longwood University (Longwood) as of and for the year ended June 30, 2020, and issued our report thereon, dated June 24, 2021. Our report, included in Longwood's Annual Report, is available at the Auditor of Public Accounts' website at www.apa.virginia.gov and at Longwood'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 or other matters required to be reported under Government Auditing Standards.

Longwood has not taken adequate corrective action with respect to two previously reported findings. Accordingly, we designated these findings with a "repeat" label in the section entitled "Internal Control and Compliance Findings and Recommendations." Longwood has taken adequate corrective action with respect to audit findings reported in the prior year that are not repeated in this report.

–TABLE OF CONTENTS–

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Continue to Improve Continuity of Operations Planning
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2016)

Longwood continues to implement its corrective action plan to address the weaknesses to improve its risk management and contingency planning process and documentation. Longwood is making progress to improve and update its continuity of operations plan (COOP) and information technology (IT) disaster recovery plan (DRP) and process to align with its adopted security standard, the International Organization for Standardization and the International Electrotechnical Commission Standard, ISO/IEC 27002 (ISO Standard). However, the following weaknesses remain:

- Longwood has not determined and documented the recovery time objectives (RTOs) for each of the four Tiers of IT systems defined in the *Information Technology Business Process Analysis (BPA)* to ensure that the RTOs align with those defined for the four Tiers in the *COOP Basic Plan.* Additionally, the Tier 1 and Tier 2 systems in the *Disaster Recovery Plan* do not align with the four Tiers in the *Information Technology BPA.* Finally, Longwood has not yet completed nine of the 38 Departments' BPAs and ten of the 29 completed BPAs do not document manual workarounds. The ISO Standard, section 17.1.2, requires that organizations establish, implement, and maintain processes, procedures, and controls to ensure the required level of continuity for information security during an adverse situation. Not documenting the RTOs for its IT systems, as well as manual workarounds for critical business processes may affect Longwood's ability to prioritize the restoration of critical and mission essential systems in the event of an outage or disaster.

- Longwood does not have risk assessments (RAs) for five of ten sensitive systems. Longwood also did not complete an annual review for one of the five completed RAs. Additionally, Longwood has seven hosted sensitive systems that require a RA, which Longwood handles as part of their new service provider oversight process; however, Longwood has not completed a RA for six of the seven hosted systems. The ISO Standard, section 0.2, requires that an organization identify threats to its assets, along with evaluating vulnerabilities and impact, by conducting a risk assessment. Without conducting a risk assessment for each sensitive system, management may not correctly prioritize information security risks and implement appropriate controls to help mitigate those risks. By not updating its risk assessments to reflect changes to its sensitive systems, Longwood increases the risk of not securing its sensitive systems adequately against known vulnerabilities that can affect data confidentiality, integrity, and availability.

- Longwood's most recent disaster recovery test is 2016. The ISO Standard, section 17.1.3, requires that organizations verify the established and implemented information security continuity controls via regular exercises and tests to ensure that they are valid and effective during adverse situations, and that organizations review and evaluate information security continuity measures at regular intervals. Without regular disaster recovery testing, Longwood cannot ensure processes exist and function properly to restore sensitive systems within RTOs in the event of a system failure or disaster.

Staff turnover in the information security office delayed updating the IT Risk Management and Contingency Planning documents. Specifically, Longwood lost two information security staff members in 2020, including the information security officer role, which have not yet been filled. Additionally, Longwood lost one security staff member in fiscal year 2019 and only recently filled the position in July 2020. The effects of the pandemic also affected Longwood's corrective action timeline.

The Longwood emergency management, IT, and information security groups should complete the IT Risk Management and Contingency Planning documents to ensure that the manual workarounds and RTOs align throughout the documents. In addition, Longwood should acquire the information security staff necessary to improve its risk management and contingency management processes. Once Longwood hires the necessary security staff, Longwood should develop a plan to complete RAs for all sensitive systems and develop processes to ensure the RAs receive an annual review and revision to ensure their validity. Further, Longwood should conduct and document the planned disaster recovery test. Doing this will help to ensure Longwood protects the confidentiality, integrity, and availability of its sensitive and mission critical systems.

Continue to Maintain Oversight of Third-Party Service Providers
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2019)
Prior Title: Maintain Oversight of Third-Party Service Providers

Longwood continues to not gain assurance that IT-related third-party service providers who host University data have secure IT environments. Third-party providers are organizations that perform outsourced business tasks or functions on behalf of the University. Longwood has identified 38 IT service providers in its *System Name Master List*, including seven that host sensitive and mission critical data. Longwood has a process in place to manage these third-party providers but has not completed the oversight process.

Specifically, Longwood has not completed an Institutional Data Elements Form (IDF) for six of the 38 service providers. Additionally, Longwood has not completed a risk assessment for six of the seven providers that process sensitive and mission critical data. Further, for five of the seven providers that process sensitive and mission critical data, Longwood has not performed regular security audits of the provider's IT environment, or reviewed and evaluated independent audit reports, such as System and Organization Controls (SOC) reports on a regular basis to determine that agreed upon security controls

are in place and operating effectively. Finally, three service providers that perform outsourced business tasks for Longwood are not listed in the *System Name Master List* and therefore not yet included in the oversight process.

Longwood's Information Technology Services (ITS) Project Management Office Procedure requires that Longwood complete an IDF for each provider, which classifies the system as sensitive or not based on the data processed by the system. For any systems that process sensitive and mission critical data, Longwood's ITS Project Management Office procedure and the Service Security Controls Review (SSCR) procedure require that the data owner and Information Security Office work together to complete a risk assessment of the system. Longwood also requires its providers to contractually agree to a Data Protection Addendum wherein the providers agree to adhere to certain security requirements. The addendum states that for providers hosting sensitive and mission critical data, Longwood has the right to conduct audits of the vendor at any time, and that the vendor must conduct, or have conducted, an annual independent security audit that attests to the vendor's security policies, procedures, and controls. The addendum further states that the vendor must provide to Longwood the results of independent security audits at Longwood's request, and that the vendor must modify its security measures, based on the results of the audit, to meet the controls agreed upon in the addendum. The SSCR requires the Information Security Office to annually review the providers' audits.

By not gaining adequate assurance over third-party service providers' IT environments, Longwood cannot validate the effectiveness of the providers' IT controls to protect Longwood's sensitive and mission critical data.

Longwood began implementing the oversight process as established in their ITS Project Management Office Procedure and their SSCR procedure in early 2020 and has had some unexpected setbacks. Longwood did not complete the required risk assessments and gain adequate assurance over third-party service providers' IT environments due to limited information security resources. The complex nature of the collaborative effort required to complete the process contributed to the delay.

The Information Security Office should work with the various departments to identify providers currently performing outsourced business tasks to ensure they are included in the oversight process. Longwood should complete an IDF for each provider performing outsourced business tasks, including the remaining six providers on the *System Name Master List*. Longwood should dedicate its limited information security resources to complete the required risk assessments. Additionally, Longwood should gain assurance that each of their IT-related third-party providers have secure IT environments to protect sensitive and mission critical data. To do this, Longwood should perform an annual security audit of the provider's IT environment, or obtain and evaluate SOC reports, or other independent audit reports, to confirm that each provider maintains effective IT controls to protect its sensitive and mission critical data.

Improve Operating System Security
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

Longwood is missing certain security controls for the server operating system that hosts the database for the primary financial management system. Longwood's information security standard, the ISO Standard, requires these controls to reduce risk to data confidentiality, integrity, and availability.

We communicated the details of the control weaknesses to Longwood in a separate document marked Freedom of Information Act (FOIAE) under Section 2.2-3705.2 of the Code of Virginia, due to its sensitivity and description of security mechanisms. In general, the critical controls relate to missing policies and procedures that outline requirements, as well as critical processes for server operating systems that store sensitive data.

Longwood should prioritize and dedicate the necessary resources to address the concerns communicated in the FOIAE document.

Improve Internal Controls Over Capitalizing Software Purchases
Type: Internal Control
Severity: Significant Deficiency
Repeat: No

Longwood does not have adequate internal controls over capitalizing software purchases. Financial Operations staff did not adhere to policies and procedures in place for capitalizing software purchases resulting in a $222,000 (approximately) understatement in net depreciable capital assets. In addition, Financial Operations staff did not adequately research software purchases to ensure that they consistently record all software purchases with a license agreement exceeding one year as capital assets in the capital asset system in accordance with Longwood and Commonwealth requirements.

Financial Operations staff indicated that the software purchases tested were annual subscriptions. However, after more research the staff determined that the software purchases were license agreements exceeding one year. While Longwood does not own subscriptions or licenses, they are capitalizable, including hosted software if Longwood pays to use it over a period greater than one year. Improper recording of capital assets increases the risk of misstating asset balances within the capital asset system and the financial statements.

Commonwealth Accounting Policies and Procedures Manual Topic 30325 "Software and Other Intangible Assets" provides policies and procedures for proper capitalization of software purchases. The policy indicates that software licenses with a license agreement exceeding one year and off the shelf software are capitalizable. In addition, Longwood's intangible assets policy states, "Software licenses owned by the University with a cost of $25,000 or greater and have a useful life of at least one year will be capitalized."

Financial Operations staff should capitalize all software purchases in accordance with Longwood and Commonwealth requirements. Staff should thoroughly research software purchases to ensure that they properly capitalize any purchases with a license agreement exceeding one year and the capitalization threshold.

Commonwealth of Virginia

Auditor of Public Accounts

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

June 24, 2021

The Honorable Ralph S. Northam
Governor of Virginia

The Honorable Kenneth R. Plum
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** (Longwood) as of and for the year ended June 30, 2020, and the related notes to the financial statements, which collectively comprise Longwood's basic financial statements and have issued our report thereon dated June 24, 2021. 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 Longwood, 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 Longwood'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 opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of Longwood's internal control. Accordingly, we do not express an opinion on the effectiveness of Longwood'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 entitled "Continue to Improve Continuity of Operations Planning," "Continue to Maintain Oversight of Third-Party Service Providers," "Improve Operating System Security," and "Improve Internal Controls Over Capitalizing Software Purchases," 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 Longwood'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 statement. 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 entitled "Continue to Improve Continuity of Operations Planning," "Continue to Maintain Oversight of Third-Party Service Providers," and "Improve Operating System Security."

Longwood's Response to Findings and Recommendations

We discussed this report with management at an exit conference held on June 25, 2021. Longwood's response to the findings and recommendations identified in our audit is described in the accompanying section titled "Longwood's Response." Longwood'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 and Recommendations

Longwood has not taken adequate corrective action with respect to the previously reported findings and recommendations "Continue to Improve Continuity of Operations Planning" and "Continue to Maintain Oversight of Third-Party Service Providers." Accordingly, we included these findings and recommendations in the section entitled "Internal Control and Compliance Findings and Recommendations." Longwood has taken adequate corrective action with respect to audit findings and recommendations reported in the prior year that are not repeated in this report.

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

DBC/clj

LONGWOOD
UNIVERSITY

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

Vice President for Administration & Finance

June 24, 2021

Ms. Staci Henshaw
Auditor of Public Accounts
P.O. Box 1295
Richmond, Virginia 23218

Dear Ms. Henshaw,

Longwood University has reviewed the Internal Control Findings and Recommendations provided by the Auditor of Public Accounts for fiscal year ending June 30, 2020 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,

Louise Waller
Vice President for Administration and Finance

FY 2020 – Internal Control Findings and Recommendations

Continue to Improve Continuity of Operations Planning

- Longwood's Department of Emergency Management will continuing to gather the data from various areas across campus and compiling the information. Information Technology Services (ITS) will continue to refine the COOP Information Technology Business Process Analysis (IT-BPA) and the Information Technology Disaster Recovery Plan (IT-DRP) so as to have the Recovery Time Objectives (RTO) align.

Continue to Maintain Oversight of Third-Party Service Providers

- ITS will examine Information Security Office staffing and place a high focus on completing Third-Party Service Provider risk assessments.

Improve Operating System Security

- ITS will examine Information Security Office staffing and will continue to improve upon the current logging and monitoring process and procedure.

Improve Internal Controls Over Capitalizing Software Purchases

- Financial Operations staff will begin capitalizing all software purchases in accordance with Longwood and Commonwealth requirements. The Fixed Asset Accountant will work closely with IT to research and identify software purchases, including those with a license agreement exceeding one year and the capitalization threshold, which should be capitalized.

LONGWOOD UNIVERSITY

Farmville, VA
As of June 30, 2020

BOARD OF VISITORS

Eric Hansen
Rector

Lucia Anna Trigiani
Vice Rector

Eileen M. Anderson
Katharine M. Bond
Michael A. Evans
Steven P. Gould
David H. Hallock, Jr.
Colleen McCrink Margiloff
Nadine Marsh-Carter
Larry Palmer
Polly H. Raible
Ricshawn Adkins Roane
N. H. Scott

LONGWOOD OFFICIALS

W. Taylor Reveley, IV
President

Louise Waller
Vice President for Administration and Finance

Cathryn Mobley
Associate Vice President for Administration and Finance