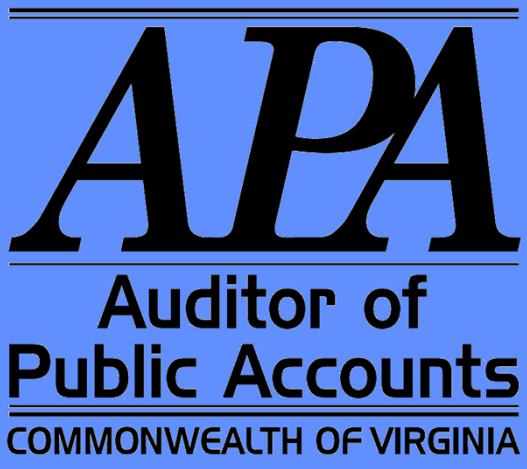
LONGWOOD UNIVERSITY

REPORT ON AUDIT

FOR THE YEAR ENDED

JUNE 30, 2010



AUDIT SUMMARY

Our audit of Longwood University for the year ended June 30, 2010, found:

- the financial statements are presented fairly, in all material respects, with generally accepted accounting principles;

- certain matters involving internal control findings requiring management's attention; however, we do not consider them to be material weaknesses; and

- no instances of noncompliance or other matters required to be reported under Government Auditing Standards.

In addition, we have audited the basic financial statements of Longwood University as of and for the year ended June 30, 2010 and issued our report thereon dated June 8, 2011. Our report, included in the University's basic financial statements, is available at the Auditor of Public Accounts' website at www.apa.virginia.gov.

- T A B L E O F C O N T E N T S -

INTERNAL CONTROL FINDINGS AND RECOMMENDATIONS

Implement Third Party Monitoring and Review Processes

The University does not monitor and review that TouchNet, a third-party credit card processing vendor, only accesses or changes student data in the University's Banner system necessary for processing payments. The University allows TouchNet to access sensitive data in the student accounting system and post payment information directly to a student's account.

This process reduces University time and labor in posting payment information; however, the University needs to verify that TouchNet only accesses or changes student data necessary to process payments.

Best practices indicate that the University should maintain sufficient overall control and visibility into all security aspects for sensitive or critical information or information processing facilities accessed, processed, or managed by a third party. In addition, this best practice requires the University's review of third-party audit trails and records of security events, operational events, and failures and tracing of faults and disruptions related to services delivered.

So that the University is aware of all the intentional and unintentional uses of its sensitive student information, we recommend that the University implement a monitoring and review process for TouchNet and all other third party processors in accordance with their approved security standard. The University should turn on the system feature that allows monitoring and review of data transmission periodically to validate the data elements sent between its Banner system and TouchNet.

Improve Risk Management and Contingency Planning

As noted also in last year's audit, the University last completed a comprehensive update and review of their Risk Assessment in 2006 and since that time, there have been changes to their IT environment, including an upgrade to Banner 8. While the University did update their Continuity of Operations (COOP) and Disaster Recovery Plan (DRP), these updates are incomplete and based on an outdated Risk Assessment. Therefore, any tests of the COOP or DRP do not capture the current risks to the University's information systems and security. University standards specify a review of the Risk Assessment when significant changes occur in the IT environment, in addition to a periodic review.

Without performing a complete sequential update of the Risk Assessment, COOP and DRP, the University cannot competently test and guarantee the availability of these systems to continue operations in the event of an emergency. We recommend that the University allocate the necessary resources to update the Risk Assessment, COOP and DRP and test both the COOP and the DRP to help ensure the availability of mission critical systems.

Strengthen Firewall Configuration

The University does not use vendor recommended settings to secure its firewall that protects its administrative network. We recommend that the University develop and implement a policy that requires the periodic network device scanning against security control best practices and broaden regular vulnerability scans beyond reviewing only access control lists to include scanning for weak security control settings.

Commonwealth of Virginia

Walter J. Kucharski, Auditor

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

June 8, 2011

The Honorable Robert F. McDonnell
Governor of Virginia

The Honorable Charles J. Colgan
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 the financial statements of the business-type activities and discretely presented component units of **Longwood University** as of and for the year ended June 30, 2010, which collectively comprise the University's basic financial statements and have issued our report thereon dated June 8, 2011. Our report includes a reference to other auditors. We conducted our audit in accordance with 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. 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, we considered the University's internal control over financial reporting as a basis for designing our auditing procedures for the purpose of expressing our opinion 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 controls 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 significant deficiency, or 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 by the entity's internal control over financial reporting.

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 that might be deficiencies, significant deficiencies or material weaknesses. We did not identify any deficiencies in internal control over financial report that we consider to be material weaknesses, as defined above. However, we identified certain deficiencies in internal control over financial reporting entitled "Implement Third Party Monitoring and Review Processes", "Improve Risk Management and Contingency Planning" and "Strengthen Firewall Configuration", which are described in the section titled "Internal Control and Compliance Findings and Recommendations," that we consider to be significant deficiencies in internal control over financial reporting 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.

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, and 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 no instance of noncompliance and other matters that are required to be reported under Government Auditing Standards.

The University's response to the findings identified in our audit is included in the section titled "University Response". We did not audit the University's response and, accordingly, we express no opinion on it.

Status of Prior Findings

The University has not taken adequate corrective action with respect to the previously reported finding "Improve Risk Management and Contingency Planning". Accordingly, we included this finding in the section entitled "Internal Control Findings and Recommendations". The University has taken adequate corrective action with respect to audit findings reported in the prior year that are not repeated in this report.

Report Distribution and Exit Conference

The "Independent Auditor's Report on Internal Control over Financial Reporting and on Compliance and Other Matters" is intended solely for the information and use of the Governor and General Assembly of Virginia, the Board of Visitors, and management, and is not intended to be and should not be used by anyone, other than these specified parties. However, this report is a matter of public record and its distribution is not limited.

We discussed this report with management at an exit conference held on June 8, 2011.

AUDITOR OF PUBLIC ACCOUNTS

LONGWOOD
UNIVERSITY

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

June 8, 2011

Office of the Vice President for Administration and Finance

Mr. Walter Kucharski
Auditor of Public Accounts
P.O. Box 1295
Richmond, VA 23218

Dear Mr. Kucharski:

The following are responses to the audit findings and recommendations issued to Longwood University following the recent audit of the University's June 30, 2010 financial statements.

Implement Third Party Monitoring and Review Processes

In section 10.2.2 Monitoring and review of third party services of the ISO 27002 standard it states that "Monitoring and review of third party services should ensure that the information security terms and conditions of the agreements are being adhered to, and that information security incidents and problems are managed properly."

As such, the University contract information security terms with TouchNet will be monitored and reviewed for compliance according to the following: Software License Agreement - Page 11, Section 13.2 Access, Section 13.3 Obligation of Confidentiality, and Addendum for Tuition Payment Services - Page 1, Section 3(b) Access to Student Information.

The scope of the monitoring and review will be limited to only data elements classified by the University as "restricted" according to the Data Classification Policy 6134 (see http://www.longwood.edu/vpaf/final_policy_base/6000/6134.htm) as this classification of data represents the greatest risk to the University if disclosed in an unauthorized manner. The reviews will be coordinated with the designated individual(s) responsible for managing the relationship with the third party and any other third party service contracts will be monitored and reviewed for compliance in a similar fashion.

A preliminary audit of TouchNet's access to restricted data elements in the Banner system was conducted on May 31, 2011 and resulted in no attempts. An additional audit will be performed at the end of June 2011 and then periodically from that point forward to ensure access is in compliance with contract information security terms.

Improve Risk Management and Contingency Planning

The University has not had an opportunity to complete a formal and systematic risk assessment. Since being granted Level II status in January 2010, we are currently transitioning from the VITA SEC501

standards to that of ISO 27002. Additionally, the Information Security Office suffered a loss of one of its staff in October of 2009 and did not replace the staff member until March 2010. The staff member who left was the primary lead on the new risk assessment process project. The APA auditor was supplied with significant amounts of evidence to show our progress towards approving a new risk assessment process compliant with the ISO 27002 standard and other sources of input such as EDUCAUSE in conjunction with University policies. The timeline indicated that after the initial framework was complete, testing would begin in April 2011. The plan is twofold. As soon as the new process is approved by management, all new systems will be assessed for risk prior to being implemented in production and an effort made to have all existing systems currently in production assessed for risk by June 30, 2012.

The new risk assessment process includes reminder statements to the appropriate system owners to update, where necessary, relevant information in COOP and Disaster Recovery Plans. During the initial implementation of the new process, additional emphasis will be placed on ensuring that consideration is given to updating these plans accordingly.

Contingency planning documents, such as the Continuity of Operations Plan are reviewed and updated at least annually. The Disaster Recovery Plan is reviewed and updated quarterly. Both plans are tested annually. These plans were last tested on October 11, 2010.

Strengthen Firewall Configuration

The University continuously evaluates vendor recommended settings and other security control best practices to secure its border firewall protecting the University networks and appropriately tailors those setting to the specific circumstances of the University.

The University is in the process of developing a new risk management policy in conjunction with the new risk assessment process. The new risk assessment process (described above - Improve Risk Management and Contingency Planning) will include the appropriate steps to document and ensure periodic vulnerability scanning of all systems and devices, including network devices such as the firewall. Additionally, the University already has a policy (see Firewall Policy 6130 - http://www.longwood.edu/vpaf/final_policy_base/6000/6130.htm) that states in section III.H. "IITS will review firewall configurations annually…."

If you have any questions or need additional information, please do not hesitate to contact me at (434) 395-2016 or worsterks@longwood.edu.

Sincerely,

Kathy S. Worster, MBA, MAcc, CPA
Vice President for Administration and Finance

LONGWOOD UNIVERSITY
Farmville, Virginia

BOARD OF VISITORS

Helen P. Warriner-Burke, Rector

John B. Adams, Jr.
Otis L. Brown
John W. Daniel, II
Robert E. Frye, Sr.
Chin Han Kim
M. Jane Brooke
Marjorie M. Connelly
George W. Dawson
Rita B. Hughes
Stephen Mobley
Susan E. Soza

OFFICIALS

Patricia P. Cormier
President

Wayne E. McWee
Provost and Vice President for Academic Affairs

Kathy S. Worster
Vice President for Administration and Finance

Richard W. Bratcher
Vice President for Facilities Management and Real Property

Tim J. Pierson
Vice President for Student Affairs

Francis X. Moore, III
Vice President for Information and Instructional Technology
Services and Chief Information Officer

K. Craig Rodgers
Vice President for University Advancement