



UNIVERSITY OF MARY WASHINGTON

REPORT ON AUDIT FOR THE YEAR ENDED JUNE 30, 2016

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 the University of Mary Washington as of and for the year ended June 30, 2016, and issued our report thereon, dated August 14, 2017. 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.umw.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.

–TABLE OF CONTENTS–

| | <u>Pages</u> |
|--|--------------|
| AUDIT SUMMARY | |
| INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS | 1-4 |
| INDEPENDENT AUDITOR’S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS | 5-7 |
| UNIVERSITY RESPONSE | 8-9 |
| UNIVERSITY OFFICIALS | 10 |

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Improve Controls over Financial System Access

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: No

The University of Mary Washington (University) has not restricted access to critical application processes based on the principle of least privilege. Between two and 15 users had unnecessary access to the University's accounting and financial reporting system including the ability to access and make changes to student accounts including minimum and maximum rates, meal plans, dorm assignments and room rates. These users include student employees and numerous employees in the Registrar's Office. As the system generates student bills based on the rates entered, access should be restricted to employees responsible for the corresponding finance office functions. The system access class used for Registrar's Office employees mistakenly included access to these forms, which the University assigned during the initial system setup.

The Commonwealth's Information Security Standard, SEC 501-09 (Security Standard), requires that access rights be granted only to users with documented job responsibilities that require those rights (*Security Standard Section: AC-6 Least Privilege*). Additionally, University policy requires a review of system access twice a year to validate accounts, roles, and privileges of end users. University policy requires the Applications Database Administrator to contact all University data stewards requesting that they agree their system access records to database records and that they make any necessary changes to ensure that system access is appropriate. Sufficiently performing the required semi-annual access review and ensuring that all department data stewards have completed their reconciliation provides assurance that access is appropriate for users based on their current job responsibilities. Improper access to these forms could lead to improper or unauthorized changes to student financial information and could compromise sensitive information.

Management should complete a review of all system classes to ensure each class grants access to only necessary functionality. In addition, the semi-annual review process should include controls to ensure that all departments complete the review of user access to the system application and determine if assigned access is in accordance with the principle of least privilege.

Improve Database Security

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: No

The University's Information Technology (IT) Department does not secure a sensitive system's supporting database with some minimum security controls required the Security Standard and industry best practices.

We communicated the control weaknesses to management in a separate document marked Freedom of Information Act (FOIA) Exempt under Section 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms. The Security Standard and industry best practices require the implementation of certain controls that reduce unnecessary risk to data confidentiality, integrity and availability in systems processing or storing sensitive information.

The IT Department should dedicate the necessary resources to implement the controls discussed in the communication marked FOIA Exempt in accordance with the Security Standard and industry best practices in a timely manner.

Complete Implementation of the Process for Granting and Restricting Elevated Workstation Privileges

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: No

In May 2017, the University approved a policy establishing a formal authorization process to grant elevated workstation privileges to end users and also implemented a software vetting process. However, the IT Department has not yet completed the implementation of the formal authorization process for granting and restricting elevated workstation privileges. Both University policy and the Security Standard prohibit administrator rights unless the privileges are essential to perform tasks within the scope of the employee's job duties.

We have communicated the details of this finding 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.

The IT Department should complete the implementation process for granting and restricting elevated workstation privileges. Doing this will reduce the risks to the University's information technology environment and better protect the confidentiality, integrity, and availability of sensitive and mission critical data.

Improve IT Risk Management and Contingency Process

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: No

The University does not properly manage certain aspects of its IT Risk Management and Contingency Program in accordance with the Security Standard. The IT Risk Management and Contingency Program provides the baseline for the University to recover and restore mission critical and sensitive systems based on the university's identification, assessment, and management of information security risks. During our review, we identified the following control weaknesses.

- The IT Department does not perform periodic Disaster Recovery Plan (DRP) testing and has no schedule to conduct DRP tests. The University has a separate DRP for each of its fourteen

sensitive systems, including its accounting and financial reporting system, and documents testing requirements within each DRP. However, the IT Department has not performed any DRP tests since the accounting and financial reporting system DRP test performed in May 2015. The IT Department clones the production database for the accounting and financial reporting system on a monthly basis and relies on the cloning process in lieu of performing annual restoration testing. DRP testing is essential to ensure the appropriate processes exist and work to restore a system and its application(s) to full functionality in the event of a system failure or disaster. *(Security Standard: CP-1-COV Contingency Planning Policy and Procedures; and CP-4 Contingency Plan Testing and Exercise)*

- The IT Department does not have a consistent process to manage the IT systems inventory used to classify data and identify sensitive systems. Specifically, the IT Department does not assign an individual responsible for maintaining the IT systems inventory and has no formal process to consistently review and update the IT systems inventory as changes occur in the IT environment. As a result, the University misclassified five non-sensitive systems as sensitive systems. Since the identification of this weakness, the IT Department updated the IT systems inventory and accurately classified the five systems. Consistently and accurately classifying systems according to their data sensitivity is a critical security control to ensure the implementation of the necessary controls to protect its sensitive systems and data. *(Security Standard: Section 4 IT System and Data Sensitivity Classification)*

The IT Department has not performed periodic DRP testing, because it relied on the database cloning process rather than planning and executing formal, rotating DRP tests for each of their individual DRPs. The IT Department does not consistently manage the IT systems inventory, because it did not assign an individual responsible for managing its inventory following the departure of a key employee and did not develop a formal process to correctly classify the systems on the list.

Without performing DRP tests, there is an increased risk to the University that in the event of a disaster and activation of its continuity of operations plan, it may not be able to recover sensitive and mission critical systems in a timely manner. Without a process in place to maintain an accurate IT systems inventory, the IT Department may be unable to determine and implement proper protection, storage, and recovery requirements for University systems and data.

The IT Department should develop a schedule for performing annual DRP testing according to the requirements detailed in their individual DRPs. Once it establishes a DRP testing schedule, the IT Department should perform annual DRP tests to provide assurance it can recover sensitive and mission critical systems in a timely manner and without disrupting University operations. Additionally, the IT Department should designate an accountable individual to manage the IT systems inventory and establish a process to consistently review and update the IT systems inventory as changes occur in the University environment.

Improve Continuity of Operations Plan Testing

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: No

The University does not test certain aspects of its Continuity of Operations Plan (COOP) to determine whether it can successfully implement manual workarounds to resume business operations during an emergency in the absence of critical information systems such as the accounting and financial reporting system.

The University has an approved COOP that works in tandem with the Crisis and Emergency Management Plan (CEMP). In fiscal year 2016, the University activated its CEMP during a winter storm and used the COOP as a supporting document to obtain contact information for key personnel needed in the emergency. By activating and documenting its crisis and emergency management process during the storm, the University may meet the Virginia Department of Emergency Management testing requirements. However, the University has not planned and conducted exercises of the COOP to test its ability to continue mission essential business functions without critical information systems. Not periodically testing the COOP to ensure that employees can efficiently execute roles and responsibilities during an emergency could result in potential delays in resuming business operations in the event of an emergency and may increase the likelihood that the University will not meet its pre-determined recovery time objective expectations.

The University did not perform COOP testing because it emphasized CEMP testing during an actual event, which focused on human safety in an emergency. Additionally, the University has not documented a testing plan and accompanying schedule to drive tests of its ability to continue with business processes without critical information systems.

The University should develop a schedule to test its processes for manual workarounds to continue mission essential functions that require information systems when those systems are not available. Subsequently, it should evaluate the results of these exercises and revise the COOP to reflect any lessons learned. Conducting and documenting COOP testing will help ensure the University can carry on business operations with minimal disruption during an emergency.



Martha S. Mavredes, CPA
Auditor of Public Accounts

Commonwealth of Virginia

Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

August 14, 2017

The Honorable Terence R. McAuliffe
Governor of Virginia

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

Board of Visitors
University of Mary Washington

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 unit of the **University of Mary Washington** as of and for the year ended June 30, 2016, and the related notes to the financial statements, which collectively comprise the University's basic financial statements and have issued our report thereon dated August 14, 2017. Our report includes a reference to another auditor. 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 unit of the University, which was audited by another auditor 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 Controls over Financial System Access," "Improve Database Security," "Complete Implementation of the Process for Granting and Restricting Elevated Workstation Privileges," "Improve IT Risk Management and Contingency Process," and "Improve Continuity of Operations Plan Testing," 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 Controls over Financial System Access," "Improve Database Security," "Complete Implementation of the Process for Granting and Restricting Elevated Workstation Privileges," "Improve IT Risk Management and Contingency Process," and "Improve Continuity of Operations Plan Testing."

The University's Response to Findings

We discussed this report with management at an exit conference held on August 22, 2017. 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

EMS/clj



August 5, 2017

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

Subject: Management response to the Audit Recommendations for Fiscal Year 2016

Dear Ms. Mavredes,

I am pleased to send you University of Mary Washington's response to the internal control findings and recommendations identified during the audit of the fiscal year ended June 30, 2016. Management's responses are as follows.

Improve Controls over Financial System Access

Finance agrees with this recommendation and unnecessary access has been removed from the critical access forms. Finance will coordinate with data stewards and continue to perform semi-annual access reviews to ensure only necessary access is granted.

Improve Database Security

IT concurs with the findings. Regarding item one of the finding, IT has completed the first 2017 access review and will complete the second access review by December 31, 2017. Items two through six have been remediated and completed. Regarding item seven, IT will complete this control by March 31, 2018.

Complete Implementation of the Process for Granting and Restricting Elevated Workstation Privileges

IT concurs with the finding. A plan is in place to complete implementation of the recommended control by December 31, 2018.

Improve IT Risk Management and Contingency Process

IT concurs with the finding; and will enhance the disaster recovery failover process by establishing a schedule of annual disaster recovery testing for all critical systems to include documenting the results. Implementation of the recommended controls will be completed by July 31, 2018.

IT will designate an individual to manage the IT systems inventory and will establish a process to consistently review and update the IT systems inventory. Implementation of the recommended controls will be completed by December 31, 2018.

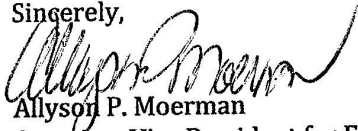
1301 College Avenue
Fredericksburg, VA 22401-5300
www.umw.edu

Improve Continuity of Operations Plan Testing

Emergency Management and Safety concurs with the finding. Implementation of correction will be completed by June 30, 2018.

If you have any questions or need additional information, please do not hesitate to contact me by phone at (540) 654-1212 or by email at amoerman@unw.edu.

Sincerely,



Allyson P. Moerman
Associate Vice President for Finance

UNIVERSITY OF MARY WASHINGTON

As of June 30, 2016

Board of Visitors

Holly T. Cuellar, Rector

Mark S. Ingrao, Vice Rector

Tara C. Corrigall, Secretary

Theresa Young Crawley

Kenneth Lopez

Heather M. Crislip

Fred M. Rankin, III

Carlos Del Toro

Davis C. Rennolds

R. Edward Houck

Lisa D. Taylor

Rhonda S. VanLowe

Administrative Officers

Richard V. Hurley

President

Richard R. Pearce

Vice President of Administration and Finance and CFO

Allyson P. Moerman

Associate Vice President for Finance and Controller

Tera Kovanes

Director of Internal Audit