VIRGINIA COMMONWEALTH UNIVERSITY

REPORT ON AUDIT
FOR THE YEAR ENDED
JUNE 30, 2017

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 Virginia Commonwealth University (the University) as of and for the year ended June 30, 2017, and issued our report thereon dated December 4, 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.vcu.edu.

Our audit of Virginia Commonwealth University for the year ended June 30, 2017, 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.

Our audit also included testing over the major federal program of the Research and Development Cluster for the Commonwealth's Single Audit as described in the U.S. Office of Management and Budget Compliance Supplement; and found no internal control findings requiring management's attention or instances of noncompliance in relation to this testing.

–TABLE OF CONTENTS–

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Improve Risk Management and Continuity Planning Documentation
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

The University does not maintain effective Risk Management and Continuity Planning documentation, which may result in unnecessary delays when attempting to restore IT services to some business functions. Specifically, the University does not have a Business Impact Analysis (BIA) to evaluate the University's essential and non-essential business functions and its dependence on information technology (IT) systems. Currently, the University uses a server inventory and the system security plan (SSP) to track IT risk management information. Although the University requires an annual update for the server inventory, the SSP's on file are only reviewed and updated when there are significant system changes. Consequently, some information in the SSPs, particularly related to individual points of contact, can be inconsistent with the information presented in the University's server inventory. The distributed storage of this information and inconsistencies between both sources can require additional time to identify the critical system and contact information in an emergency event.

As specified by the business continuity management system standard, ISO 22301:2012, organizations should complete a cycle of the BIA process before selecting business continuity strategies. The International Organization for Standardization offers guidance for establishing, implementing, and maintaining a BIA in ISO/TS 22317:2015.

The University's IT Risk Management Standard requires system owners to periodically review and update SSPs for systems. Additionally, the University's adopted information security standard, ISO/IEC 27002:2013, section 17.1.3, requires the University to verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations. This includes organizational, technical, procedural, and process changes, which applies to the University's SSPs, as they can lead to changes in information security continuity requirements.

Without a BIA, the University is unable identify its mission-critical and non-essential business functions and reliance on one or more IT systems. This leads to the risk that the University's continuity management documentation is not based on the information evaluated in the BIA and may result in the application of unnecessary or ineffective controls. By not having consistent and updated risk management documentation, the University is unable to quickly evaluate changes to systems and associating risks and vulnerabilities within the IT environment. This can ultimately lead to the University not implementing appropriate security controls in a timely fashion to prevent new risks and vulnerabilities from gaining unauthorized access to the sensitive information.

The University's absence of a documented BIA is the result of no established organization-wide requirements or processes to develop a formal BIA that evaluates each business function and its impact

on business continuity. The University's lack of updating the SSPs are due to differing review and update requirements for the server inventory database and the SSPs.

The University should incorporate a BIA process that evaluates a more comprehensive set of business functions and risk factors than its current Continuity of Operations Plan. The University should then use the information derived from the BIA and other risk analysis documents, such as the SSPs, to update its business continuity plans. Finally, the University should define a frequency for performing SSP reviews to ensure consistency with the server inventory database.

Improve Management Oversight of Wage Employee Timekeeping

Type: Internal Control
Severity: Significant Deficiency
Repeat: No

The University recently installed a new timekeeping management system that requires wage employees to track time through automated timesheets. The system has notifications and reports to identify errors such as employees with long shifts, conflicting shifts, unapproved time, and missed punches. If desired, timesheet approvers can use these notifications and reports to assist them in reviewing timesheets, but the system does not prevent them from approving timesheets without resolving the system-identified error. In addition, timesheet approvers can adjust employee timesheets, either intentionally or unintentionally, which can result in pay for hours not worked, and the error may go unnoticed. Further, timesheet approvers can use the system's mass approval feature, as opposed to individually reviewing and approving employee timesheets, which further bypasses the system's error notification process.

Our non-statistical sample of timesheets identified a ten percent (2 out of 21 items tested) error rate that resulted in $120 in overpayments to one employee. Because this was a non-statistical sample, we cannot project the error rate or overpayments to the population, but believe the ability to change employee time, mass approve timesheets, and approve timesheets with system-identified errors, without a minimum post-approval error review process, indicates the approval process lacks sufficient controls to minimize the likelihood of employee overpayments.

Management should evaluate solutions to improve controls to prevent the overpayment of employees. Possible solutions include disabling the mass approval button, requiring managers to approve time on a more frequent basis so they increase their ability to resolve errors, and developing a lag pay process which would allow managers and timekeepers the time to properly review timesheets and clear all exceptions noted by the timekeeper and the system.

Comply with Commonwealth Requirements for Wage Employees

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

The University should improve their process for monitoring non-benefit employee work hours to ensure compliance with Chapter 836 §4-7.01g of the 2017 Virginia Acts of Assembly. The University is responsible for implementing policies and procedures to ensure employees who are not eligible for benefits do not work more than 29 hours per week on average over a 12-month period. The University has policies and procedures in place to monitor this, but current procedures do not prevent departments from allowing an employee to exceed the requirement. For non-benefit employees reviewed during the measurement period of May 1, 2016 to April 30, 2017, ten employees exceeded the requirement.

For certain Commonwealth employees, Chapter 836 §4-7.01 g of the 2017 Virginia Acts of Assembly requires that they may not work more than 29 hours per week on average over a twelve month period. To implement this requirement, Human Resource Policy 2.20, developed by the Department of Human Resource Management, states that wage employees are limited to working 1,500 hours per agency per year. The Commonwealth developed this policy to ensure compliance with the requirements of the Patient Protection and Affordable Care Act, which requires employers to provide health benefits to certain employees and could bring penalties for noncompliance.

To avoid penalty payments and ensure compliance with state and federal requirements, the University Office of Human Resources should reinforce to departments and employees the importance of not exceeding the annual hour requirement. This includes not allowing employees who have reached the limit to work again until the beginning of the next measurement period.

Implement Newly Developed Policies over Information Technology Third-Party Service Providers

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

The University is implementing a formal process to obtain and review independent audit assurance that its third-party service providers (Providers) have secure IT environments to protect sensitive University data on an ongoing basis. Providers are entities that perform outsourced tasks or functions on behalf of the University.

The University's adopted information security standard, ISO/IEC 27002 (Security Standard), section 15.2.1, requires organizations to regularly monitor, review, and audit Providers to ensure they comply with information security requirements.

Without a formal process implemented to gain assurance on a regular basis over Providers' IT environments, the University cannot consistently validate that those Providers have effective IT controls to protect its sensitive data.

The Technology Services, Procurement, and business divisions recently developed formal policies and procedures to maintain a central list of its Providers and evaluate independent audit assurance of Providers' IT security controls on an annual basis. While the University approved the policies and procedures, the University requires additional time to implement the recently approved framework across its business segments. The University estimates completing this progress by June 30, 2018.

The University should dedicate the necessary resources to implement the formal framework to obtain and evaluate independent audit assurance over its Providers. This will ensure providers have appropriate IT security controls in place and operating effectively to protect sensitive University data. The University should also maintain oversight over this process after implementation to confirm compliance with the University's policy and 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

December 4, 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
Virginia Commonwealth 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 **Virginia Commonwealth University** as of and for the year ended June 30, 2017, and the related notes to the financial statements, which collectively comprise the University's basic financial statements and have issued our report thereon dated December 4, 2017. 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.

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 Risk Management and Continuity Planning Documentation", "Improve Management Oversite of Wage Employee Timekeeping", "Comply with Commonwealth Requirements for Wage Employees", and "Implement Newly Developed Policies over Information Technology Third-Party Service Providers," which are described in the section titled "Internal Control and Compliance Findings and Recommendations."

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 Risk Management and Continuity Planning Documentation," "Comply with Commonwealth Requirements for Wage Employees," and "Implement Newly Developed Policies over Information Technology Third-Party Service Providers."

The University's Response to Findings

We discussed this report with management at an exit conference held on December 5, 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

KKH/clj

December 5, 2017

Finance and Budget
Office of the Vice President

McAdams House
914 W. Franklin Street
P.O. Box 843076
Richmond, Virginia 23284-3076

804 828-6116 • Fax: 804 828 0198
TDD: 1-800-828-11200
VPFB@vcu.edu
www.finance.vcu.edu

Karol Kain Gray
Vice President for Finance
and Budget

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

Dear Ms. Mavredes:

We have reviewed the audit findings and recommendations resulting from the fiscal year 2017 audit by the Auditor of Public Accounts (APA) and discussed during the exit conference.

Virginia Commonwealth University acknowledges and concurs with the audit findings. The following contains the APA findings and management's responses to the concerns and issues raised.

Findings of the Auditor:

1. Improve Risk Management and Continuity Planning Documentation

The University does not maintain effective Risk Management and Continuity Planning documentation, which may result in unnecessary delays when attempting to restore IT services to some business functions. Specifically, the University does not have a Business Impact Analysis (BIA) to evaluate the University's essential and non-essential business functions and its dependence on information technology (IT) systems. Currently, the University uses a server inventory and the system security plan (SSP) to track IT risk management information. Although the University requires an annual update for the server inventory, the SSP's on file are only reviewed and updated when there are significant system changes. Consequently, some information in the SSPs, particularly related to individual points of contact, can be inconsistent with the information presented in the University's server inventory. The distributed storage of this information and inconsistencies between both sources can require additional time to identify the critical system and contact information in an emergency event.

As specified by the business continuity management system standard, ISO 22301:2012, organizations should complete a cycle of the BIA process before selecting business continuity strategies. The International Organization for Standardization offers guidance for establishing, implementing, and maintaining a BIA in ISO/TS 22317:2015.

The University's IT Risk Management Standard requires system owners to periodically review and update SSPs for systems. Additionally, the University's adopted information security standard, ISO/IEC 27002:2013, section 17.1.3, requires the University to verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations. This includes organizational, technical, procedural, and process changes, which applies to the University's SSPs, as they can lead to changes in information security continuity requirements.

Without a BIA, the University is unable to identify its mission-critical and non-essential business functions and reliance on one or more IT systems. This leads to the risk that the University's continuity management documentation is not based on the information evaluated in the BIA and may result in the application of unnecessary or ineffective controls. By not having consistent and updated risk management documentation, the University is unable to quickly evaluate changes to systems and associating risks and vulnerabilities within the IT environment. This can ultimately lead to the University not implementing appropriate security controls in a timely fashion to prevent new risks and vulnerabilities from gaining unauthorized access to the sensitive information.

The University's absence of a documented BIA is the result of no established organization-wide requirements or processes to develop a formal BIA that evaluates each business function and its impact on business continuity. The University's lack of updating the SSPs are due to differing review and update requirements for the server inventory database and the SSPs.

The University should incorporate a BIA process that evaluates a more comprehensive set of business functions and risk factors than its current Continuity of Operations Plan. The University should then use the information derived from the BIA and other risk analysis documents, such as the SSPs, to update its business continuity plans. Finally, the University should define a frequency for performing SSP reviews to ensure consistency with the server inventory database.

VCU Response:

VCU currently requires the review and update of system security plans when systems undergo significant changes, such as the installation of a new service, change of the system function, or migration to a new operating system. These major changes and subsequent system security plan updates are enforced through the system and network provisioning process, of which the information security office is an integral part. Outside of the required process mentioned above, VCU requires its system owners to update a server inventory on an annual basis. The server inventory contains information on system contacts, system security classification, system status and network information among others. Information from the server inventory is then used as the source for the VCU vulnerability management system and the security and information event management system. Therefore among the two sources of information and emergency contact lists, VCU IT personnel can identify the sensitivity of a system, the expected security configuration, and the appropriate contact information within reasonable timeframe.

VCU is currently working on further integrating both systems so that system and risk assessment information can be better tracked and organized, allowing this information to be maintained more consistently and accessed in an even faster and more streamlined fashion. Additionally, VCU recognizes the need to strengthen its business continuity planning and has recently purchased a business continuity software tool to help identify enterprise level risk, conduct BIAs, identify recovery strategies and support overall business continuity programming. This process will be on-going through 2018 with a full University BIA available by the end of the calendar year.

Responsible Person: Dan Han, Information Security Officer

Completion Date: December 31, 2018

2. Improve Management Oversight of Wage Employee Timekeeping

The University recently installed a new timekeeping management system that requires wage employees to track time through automated timesheets. The system has notifications and reports to identify errors such as employees with long shifts, conflicting shifts, unapproved time, and missed punches. If desired, timesheet approvers can use these notifications and reports to assist them in reviewing timesheets, but the system does not prevent them from approving timesheets without resolving the system-identified error. In addition, timesheet approvers can adjust employee timesheets, either intentionally or unintentionally, which can result in pay for hours not worked, and the error may go unnoticed. Further, timesheet approvers can use the system's mass approval feature, as opposed to individually reviewing and approving employee timesheets, which further bypasses the system's error notification process.

Our non-statistical sample of timesheets identified a ten percent (2 out of 21 items tested) error rate that resulted in $120 in overpayments to one employee. Because this was a non-statistical sample, we cannot project the error rate or overpayments to the population, but believe the ability to change employee time, mass approve timesheets, and approve timesheets with system-identified errors, without a minimum post-approval error review process, indicates the approval process lacks sufficient controls to minimize the likelihood of employee overpayments.

Management should evaluate solutions to improve controls to prevent the overpayment of employees. Possible solutions include disabling the mass approval button, requiring managers to approve time on a more frequent basis so they increase their ability to resolve errors, and developing a lag pay process which would allow managers and timekeepers the time to properly review timesheets and clear all exceptions noted by the timekeeper and the system.

VCU Response:

VCU has a large number of employees with varying shifts as well as unique needs that require employees to work excess hours at times. Therefore, managers are ultimately responsible for reviewing, correcting and approving hours worked for their employees. In addition to managers, timekeepers, who have been trained on timekeeping and leave reporting policies as well as system notifications and reports, play a key role in assuring policy is enforced in the system. To supplement these controls, payroll is now using a report to identify hours worked over 12 hours in one day. The payroll department is contacting the managers of the employees with segments totaling over 12 hours before processing the payroll. Managers and timekeepers will also be reminded periodically to use the system-provided alerts and reports.

Responsible Person: Amy Barnes, Payroll Director

Completion Date: June 30, 2018

3. Comply with Commonwealth Requirements for Wage Employees

The University should improve their process for monitoring non-benefit employee work hours to ensure compliance with Chapter 836 §4-7.01g of the 2017 Virginia Acts of Assembly. The University is responsible for implementing policies and procedures to ensure employees who are not eligible for benefits do not work more than 29 hours per week on average over a 12-month period. The University has policies and procedures in

place to monitor this, but current procedures do not prevent departments from allowing an employee to exceed the requirement. For non-benefit employees reviewed during the measurement period of May 1, 2016 to April 30, 2017, ten employees exceeded the requirement.

For certain Commonwealth employees, Chapter 836 §4-7.01 g of the 2017 Virginia Acts of Assembly requires that they may not work more than 29 hours per week on average over a twelve month period. To implement this requirement, Human Resource Policy 2.20, developed by the Department of Human Resource Management, states that wage employees are limited to working 1,500 hours per agency per year. The Commonwealth developed this policy to ensure compliance with the requirements of the Patient Protection and Affordable Care Act, which requires employers to provide health benefits to certain employees and could bring penalties for noncompliance.

To avoid penalty payments and ensure compliance with state and federal requirements, the University Office of Human Resources should reinforce to departments and employees the importance of not exceeding the annual hour requirement. This includes not allowing employees who have reached the limit to work again until the beginning of the next measurement period.

VCU Response:

While it is ultimately the responsibility of hiring schools and divisions to ensure that 1500 work hours have not been exceeded, and it is the responsibility of managers within the schools and divisions to monitor compliance with these laws, VCU HR will continue to send automatic reports and consistent communication to the HR liaisons and will provide them with specific guidance to help them manage and monitor the hours of wage and hour employees who work in multiple departments.

Additionally, VCU HR will send another universal reminder regarding compliance with the laws, and the VCU HR Compliance Office will continue to monitor the quarterly hour reports. The VCU Compliance Office will direct the HR liaisons to immediately track and maintain a running account of any employee who looks to be close to 29 hours per week or who looks to be in potential violation of the 1500 annual hour limit.

Finally, in the 2017-2018 reporting year, VCU HR will continue to send the report containing the names of employees who have exceeded 1,200 hours to the relevant HR liaisons, but the VCU HR Compliance Office will also communicate directly with HR Professionals any time an hourly or wage worker exceeds 1,200 hours in the reporting period and will direct the respective HR Professional overseeing the HR liaisons to more closely monitor the matter. The VCU HR Compliance Office will also discuss with the HR Professionals ways to incorporate measures within the schools and divisions to determine if hourly employees are working in multiple positions and engage them in discussing ways they can better manage this situation among the schools and divisions.

Responsible Person: Ishneila Moore, Director of Employee Relations and Performance Management

Completion Date: June 30, 2018

4. Implement Newly Developed Policies over Information Technology Third-Party Service Providers

The University is implementing a formal process to obtain and review independent audit assurance that its third-party service providers (Providers) have secure IT environments to protect sensitive University data on an ongoing basis. Providers are entities that perform outsourced tasks or functions on behalf of the University.

The University's adopted information security standard, ISO/IEC 27002 (Security Standard), section 15.2.1, requires organizations to regularly monitor, review, and audit Providers to ensure they comply with information security requirements.

Without a formal process implemented to gain assurance on a regular basis over Providers' IT environments, the University cannot consistently validate that those Providers have effective IT controls to protect its sensitive data.

The Technology Services, Procurement, and business divisions recently developed formal policies and procedures to maintain a central list of its Providers and evaluate independent audit assurance of Providers' IT security controls on an annual basis. While the University approved the policies and procedures, the University requires additional time to implement the recently approved framework across its business segments. The University estimates completing this progress by June 30, 2018.

The University should dedicate the necessary resources to implement the formal framework to obtain and evaluate independent audit assurance over its Providers. This will ensure providers have appropriate IT security controls in place and operating effectively to protect sensitive University data. The University should also maintain oversight over this process after implementation to confirm compliance with the University's policy and the Security Standard.

VCU Response:

VCU has requested assessment and attestation documentation from the identified vendors and has received and completed documentation reviews for over 30% of the identified vendors. VCU expects to complete all annual reviews for identified vendors by June 30, 2018 and further refine the process for upcoming years.

Responsible Person: Dan Han, Information Security Officer

Completion Date: June 30, 2018

Sincerely,

Karol Kain Gray

Karol Kain Gray
Vice President for Finance and Budget

VIRGINIA COMMONWEALTH UNIVERSITY

As of June 30, 2017

BOARD OF VISITORS

John A. Luke, Jr., Rector

Phoebe Hall, Vice Rector

Carol Shapiro, Secretary

H. Benson Dendy, III
William M. Ginther
Robert D. Holsworth
Colette W. McEachin
Ronald McFarlane
Alexander B. McMurtrie, Jr.
Tyrone E. Nelson
Keith Parker
John W. Snow
Jacquelyn Stone
Shantaram Talegaonkar
G. Richard Wagoner
Steve L. Worley

ADMINISTRATIVE OFFICERS

Michael Rao, President

Karol Gray, Vice President of Finance and Budget