UNIVERSITY OF VIRGINIA

REPORT ON AUDIT

FOR THE YEAR ENDED

JUNE 30, 2013

www.apa.virginia.gov | (804) 225-3350 | reports@apa.virginia.gov

AUDIT SUMMARY

Our audit of the University of Virginia for the year ended June 30, 2013, 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
- no instances of noncompliance or other matters required to be reported under Government Auditing Standards.

We have audited the basic financial statements of the University of Virginia as of and for the year ended June 30, 2013, and issued our report thereon, dated November 1, 2013. Our report is included in the President's Annual Report that the University anticipates releasing in December 2013.

–TABLE OF CONTENTS–

INTERNAL CONTROL FINDINGS AND RECOMMENDATIONS

Improve User Access Controls

University

The University must improve its policies and controls regarding user access to the Oracle e-Business Suite.

Policies

During our audit, we found that the University's user access policies reside in different areas that were not intuitive to business managers. Navigating the University's website to locate the policies and procedures should be effortless for business managers if they are expected to understand how to request, terminate, and periodically review user access. At the conclusion of our audit the University reorganized its user access policies, but we did not review the reorganization for effectiveness.

Additionally, we found the University never requires users to change their Oracle e-Business passwords. This creates a risk if an employee's password becomes known to others who can use it to log-in and execute transactions. Forcing regular password changes limits the amount of time that a lost, stolen, or forged password can be used by someone else. We recommend the University set its Oracle e-Business Suite password controls to require password changes at a regular intervals, such as quarterly.

Finally, University policies do not require an annual user access review, even though one is regularly performed. We recommend the University modify its current Administrative Data Access policy to formally require an annual review.

User Access Reviews

The University conducts annual reviews of Oracle user access by requiring Data Access Approvers (DAA) to certify the accuracy of and need for the responsibilities assigned to employees within the DAA's area. Our audit of user access to the Oracle Finance module found users that had incompatible responsibilities and users who were allowed to certify their own access as reasonable. As a result, we are concerned about the effectiveness of the current DAA annual certification process.

Many employees have only a few responsibilities which are confined to only one business unit and for these employees we found the DAA annual review process to be effective. Complexity and risk is added when an employee has multiple responsibilities or responsibilities administered by several business units. In these cases, the DAA may not be qualified to independently certify responsibilities granted by other business units; nonetheless, the DAA is expected to research the unfamiliar responsibilities to identify and understand any segregation of duties concerns that the responsibilities can create.

In addition, business units may be unaware that there are employees with critical responsibilities which are typically restricted to only employees actively working within their business unit. This typically results from employees transferring to other departments without having their old responsibilities revoked, or when a business unit data steward authorizes an exception for someone outside their unit to have a responsibility. Some exceptions were granted several years ago and data stewards are not periodically asked to review these exceptions for continued need.

First, we recommend the University adopt a policy requiring that Human Resources terminate all user responsibilities whenever an employee transfers to another department and require the new department to request new responsibilities.

Second, we recommend that the University prohibit employees from serving as their own primary or backup approver (DAA) and Information Technology Services should run periodic reports to validate compliance. We also recommend the automated system that is used to facilitate the annual review be configured to capture the DAA user ID, as well as a time/date stamp, to provide evidence that a DAA review was completed.

Third, we recommend the University shift away from a responsibility driven annual review and instead focus on functionality and segregation of duties concerns. This would require business departments to collaborate and identify incompatible functionality (such as creating and approving transactions) and may require that multiple DAA's and data stewards review and approve an employees' access. Business managers have identified some incompatible responsibilities on the Integrated Systems website and instruct managers to avoid assigning them to the same individual. Given that these conflicts are known, we recommend that Information Technology Services provide periodic reports to business managers that identify users with incompatible responsibilities and ask them to confirm the risk is acceptable and that access is still necessary for the employee to perform their job. These reports would be faster and more accurate than relying on a DAA to identify them annually.

Fourth, we recommend the University incorporate other aspects of authority into its annual access review, such as transaction limits and transaction approvers. In addition, Information Technology Services should provide periodic reports to Human Resources that show users whose transaction approver has terminated so a new approver can be assigned timely.

Finally, we recommend that Information Technology Services improve their understanding of how to obtain data from Oracle's security tables. Gaining a strong understanding would allow them to automate the review process by providing exception reports that identify users with inappropriate or incompatible functionality based on the business rules. Additionally, this would facilitate a more focused and effective review rather than spending time certifying the hundreds of users who have responsibilities that pose little to no risk.

Medical Center

The Medical Center had instances of employees with inappropriate access to both PeopleSoft Finance and Human Resources roles. The Medical Center's annual user access review process failed to identify the inappropriate access because reviewers were not provided sufficiently detailed information regarding role functionality.

We recommend the Medical Center continue their current efforts to provide reviewers with more detailed information regarding role functionality. Having this detailed information will help managers more easily identify instances of inappropriate or unnecessary access.

Strengthen Controls over Termination of Access to Systems and Facilities

The University and the Medical Center are not ensuring terminated employees have their system access privileges revoked timely. Removing terminated employees system and facility access promptly is essential in reducing the University and Medical Center's exposure to improper transactions, misappropriations of assets, and unauthorized access to sensitive data and physical areas.

- For the Medical Center, we found that 16 percent of terminated employees tested continued to have access to systems and facilities ranging from 5 to 334 days after their termination date because their managers did not notify Human Resources timely.

- For the University, we found that 100 percent of the terminated salaried employees tested continued to have access to systems through the time we performed the audit. Some employees had terminated as much as 14 months prior to our audit and in all cases, none of the departments had notified Human Resources to terminate the employees' access.

The Medical Center plans to convert the employee termination notification process to an electronic form through PeopleSoft. This will allow for the prompt removal of system and facility access for terminated employees, provided managers complete the electronic form.

On October 1, 2013, the University implemented an Off-boarding Toolkit which is applicable to all wage and salaried staff employees who terminate employment. Human Resources has communicated the new Toolkit to the University and made presentations to various management groups. In addition, Human Resources plans to perform random audits at least quarterly to ensure departments comply with the new Off-boarding Toolkit.

We recommend that both the University and Medical Center Human Resources Departments implement the new processes they have developed and perform regular audits to evaluate department compliance. We also recommend that Human Resources periodically compare terminated employees according to the payroll records to the systems access termination records to identify instances where departments did not notified them to terminate systems access.

Complete and Approve Reconciliations Timely

The University is not completing and approving reconciliations timely. In a sample of 55 reconciliations, five were prepared late and not approved, seven were prepared timely but not approved, five were prepared and approved late, and three were neither prepared nor approved.

Reconciliations should be prepared and approved timely because they are an important internal control to promptly detect, correct, and report errors and irregularities. Late reconciliations and unreconciled accounts put the University at risk of making financial and administrative decisions based inaccurate information.

We recommend the University improve internal controls to monitor and enforce the timely preparation and approval of reconciliations. The University should ensure information captured in the Recon@UVA system is used to send electronic reminders to both the reconciliation preparer and approver when reconciliations are incomplete or becoming late.

Comply with University Sole Source Policy

Procurement Services is not following University policy and; therefore, risks allegations of unfairly awarding sole source contracts. In a sample of five sole source contracts, one lacked justification for a purchase over $5,000 and one lacked the consideration of alternate vendors through a market survey. We recommend Procurement Services improve controls that will ensure sole source purchases adhere to University policy.

Commonwealth of Virginia

Auditor of Public Accounts

Martha S. Mavredes, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

November 1, 2013

The Honorable Robert F. McDonnell
Governor of Virginia

The Honorable John M. O'Bannon, III
Chairman, Joint Legislative Audit
and Review Commission

Board of Visitors
University of Virginia

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 the **University of Virginia** as of and for the year ended June 30, 2013, and the related notes to the financial statements, which collectively comprise the University's basic financial statements and have issued our report thereon dated November 1, 2013. Our report includes a reference to other auditors. We did not consider internal controls over financial reporting or test compliance with certain provisions of laws, regulations, contracts, and grant agreements for the financial statements of the component units of the University, which were audited by other auditors in accordance with auditing standards generally accepted in the United States of America, but not in accordance with Government Auditing Standards.

Internal Control Over Financial Reporting

In planning and performing our audit of the financial statements, we considered the University's internal control over financial reporting to determine the audit procedures that are appropriate in the circumstances for the purpose of expressing our opinions on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the University's internal control over financial reporting. Accordingly, we do not express an opinion on the effectiveness of the University's internal control over financial reporting.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Our consideration of internal control over financial reporting was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control over financial reporting that might be material weaknesses or significant deficiencies and therefore, material weaknesses or significant deficiencies may exist that were not identified. Given these limitations, during our audit we did not identify any deficiencies in internal control over financial reporting that we consider to be material weaknesses. However, material weaknesses may exist that have not been identified. We did identify certain deficiencies in internal control over financial reporting which are described in the section titled "Internal Control 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 no instances of noncompliance or other matters that are required to be reported under Government Auditing Standards.

The University's Response to Findings

We discussed this report with management at an exit conference held on November 25, 2013. 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.

Martha S. Mavredes

AUDITOR OF PUBLIC ACCOUNTS

KKH/alh

UNIVERSITY of VIRGINIA
OFFICE OF THE ASSOCIATE VICE PRESIDENT FOR FINANCE

December 19, 2013

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

Dear Ms. Mavredes:

The University of Virginia has reviewed the management comments provided by the Auditor of Public Accounts for the period ending June 30, 2013. University management's response to each of these findings follows; in several instance, we are already taking action to strengthen internal controls over these areas.

#1 - Improve User Access Controls

University

The University must improve its policies and controls regarding user access to the Oracle e-Business Suite.

Policies

During our audit, we found that the University's user access policies reside in different areas that were not intuitive to business managers. Navigating the University's website to locate the policies and procedures should be effortless for business managers if they are expected to understand how to request, terminate, and periodically review user access. At the conclusion of our audit the University reorganized its user access policies, but we did not review the reorganization for effectiveness.

University Management Response

The University agrees that it is important for user access policies to be clearly and easily accessible. In October, after the completion of a usability study of Integrated System access instructions, the University implemented changes to the Integrated System website to improve clarity and accessibility to policies on the Integrated System website.

Additionally, we found the University never requires users to change their Oracle e-Business passwords. This creates a risk if an employee's password becomes known to others who can use it to log-in and execute transactions. Forcing regular password changes limits the amount of time that a lost, stolen, or forged password can be used by someone else. We recommend the University set its Oracle e-Business Suite password controls to require password changes at regular intervals, such as quarterly.

University Management Response

The University agrees that we must provide an appropriate level of control over unauthorized access. In order to provide strong controls, the University includes strong authentication controls on the Oracle e-Business Suite that greatly reduce the risk of unauthorized user access, including requiring the use of two-factor authentication based on PKI technology. Oracle e-Business Suite users must have their unique physical hardware token in their possession, know the password for the token, have the correct VPN filters assigned to their access, and know their Oracle e-Business Suite user

password before they can access the Oracle e-Business Suite application. Additionally, users must agree to use protected screen savers that lock their computing devices, and Oracle password timeouts are also in place. UVA will continue to reassess the risk level and cost of further mitigation strategies.

Finally, University policies do not require an annual user access review, even though one is regularly performed. We recommend the University modify its current Administrative Data Access policy to formally require an annual review.

University Management Response
It is the University's opinion that the Access Privileges, Responsibilities and Return of Property Policy, which includes a section requiring an annual audit of Oracle e-Business Suite and SIS responsibilities, sufficiently addresses the concern.

User Access Reviews
The University conducts annual reviews of Oracle user access by requiring Data Access Approvers (DAA) to certify the accuracy of and need for the responsibilities assigned to employees within the DAA's area. Our audit of user access to the Oracle Finance module found users that had incompatible responsibilities and users who were allowed to certify their own access as reasonable. As a result, we are concerned about the effectiveness of the current DAA annual certification process.

Many employees have only a few responsibilities which are confined to only one business unit and for these employees we found the DAA annual review process to be effective. Complexity and risk is added when an employee has multiple responsibilities or responsibilities administered by several business units. In these cases, the DAA may not be qualified to independently certify responsibilities granted by other business units; nonetheless, the DAA expected to research the unfamiliar responsibilities to identify and understand any segregation of duties concerns that the responsibilities can create.

In addition, business units may be unaware that there are employees with critical responsibilities which are typically restricted to only employees actively working within their business unit. This typically results from employees transferring to other departments without having their old responsibilities revoked, or when a business unit data steward authorizes an exception for someone outside their unit to have a responsibility. Some exceptions were granted several years ago and data stewards are not periodically asked to review these exceptions for continued need.

First, we recommend the University adopt a policy requiring that Human Resources terminate all user responsibilities whenever an employee transfers to another department and require the new department to request new responsibilities.

University Management Response
The University will evaluate possible options to determine the best means of addressing employees that transfer from one department to another. Currently, the Access Privileges, Responsibilities and Return of Property Policy and the Administrative Data Access Policy already require that the supervisors revoke access privileges when their employees no longer need these privileges, regardless of whether the employee has newly transferred into the department or has been a member of the organization for a longer term. As an additional precaution, a user access review is conducted annually to help ensure this requirement is met.

Second, we recommend that the University prohibit employees from serving as their own primary or backup approver (DAA) and Information Technology Services should run periodic reports to validate compliance. We also recommend the automated system that is used to facilitate the annual review be

configured to capture the DAA user ID, as well as a time/date stamp, to provide evidence that a DAA review was completed.

University Management Response

The University agrees that the annual review process does not currently prevent a DAA from re-approving his/her own access, although a supervisor's approval is required to approve initial access. To address this concern, UVa will explore options for configuring our online review tool to ensure that a DAA is not able to reapprove his/her own access, directing this approval to the DAA's manager. We will also look to date and time stamp each approval and show who designated the "keep" or "remove" responsibility.

Third, we recommend the University shift away from a responsibility driven annual review and instead focus on functionality and segregation of duties concerns. This would require business departments to collaborate and identify incompatible functionality (such as creating and approving transactions) and may require that multiple DAA's and data stewards review and approve an employees' access. Business managers have identified some incompatible responsibilities on the Integrated Systems website and instruct managers to avoid assigning them to the same individual. Given that these conflicts are known, we recommend that Information Technology Services provide periodic reports to business managers that identify users with incompatible responsibilities and ask them to confirm the risk is acceptable and that access is still necessary for the employee to perform their job. These reports would be faster and more accurate than relying on a DAA to identify them annually.

University Management Response

The University believes that current functionality prevents the *new* approval of system responsibilities with conflicting roles. The tool for processing new request for access automatically detects when an access request is made for a potentially conflicting responsibility. The system will suspend the workflow and issue a potential conflict notification for analysis by the appropriate approver(s). The access request workflow resumes only after this analysis is completed and the approver's decision (approval/denial) is recorded in the system. We do agree that some conflicting duties remain from requests approved prior to the new tool. In order to address this concern, the University will produce a one-time report of potential conflicts and resolve each issue as appropriate to remove unwarranted conflicts.

Fourth, we recommend the University incorporate other aspects of authority into its annual access review, such as transaction limits and transaction approvers. In addition, Information Technology Services should provide periodic reports to Human Resources that show users whose transaction approver has terminated so a new approver can be assigned timely.

University Management Response

The University agrees with this recommendation and will develop options to add the review of other aspects of authority, such as transaction limits and transaction approvers.

Finally, we recommend that Information Technology Services improve their understanding of how to obtain data from Oracle's security tables. Gaining a strong understanding would allow them to automate the review process by providing exception reports that identify users with inappropriate or incompatible functionality based on the business rules. Additionally, this would facilitate a more focused and effective review rather than spending time certifying the hundreds of users who have responsibilities that pose little to no risk.

University Management Response
The University agrees with this recommendation and will work with Oracle Support to obtain access and understanding the Oracle security tables.

Medical Center
The Medical Center had instances of employees with inappropriate access to both PeopleSoft Finance and Human Resources roles. The Medical Center's annual user access review process failed to identify the inappropriate access because reviewers were not provided sufficiently detailed information regarding role functionality.

We recommend the Medical Center continue their current efforts to provide reviewers with more detailed information regarding role functionality. Having this detailed information will help managers more easily identify instances of inappropriate or unnecessary access.

University Management Response
In response to the APA findings, the Medical Center has provided detailed role and function descriptions of each role to managers. This will ensure proper role assignments and functionality to employees within PeopleSoft. Employees identified during the audit as having inappropriate access relating to the role assigned were immediately corrected and assigned proper access as it relates to their current job roles. In addition, managers will review annually the accesses of their employee to ensure employees have the proper access and role within PeopleSoft.

#2 - Strengthen Controls over Termination of Access to Systems and Facilities
The University and the Medical Center are not ensuring terminated employees have their system access privileges revoked timely. Removing terminated employees system and facility access promptly is essential in reducing the University and Medical Center's exposure to improper transactions, misappropriations of assets, and unauthorized access to sensitive data and physical areas.

- For the Medical Center, we found that 16 percent of terminated employees tested continued to have access to systems and facilities ranging from 5 to 334 days after their termination date because their managers did not notify Human Resources timely.

- For the University, we found that 100 percent of the terminated salaried employees tested continued to have access to systems through the time we performed the audit. Some employees had terminated as much as 14 months prior to our audit and in all cases, none of the departments had notified Human Resources to terminate the employees' access.

The Medical Center plans to convert the employee termination notification process to an electronic form through PeopleSoft. This will allow for the prompt removal of system and facility access for terminated employees, provided managers complete the electronic form.

On October 1, 2013, the University implemented an Off-boarding Toolkit which is applicable to all wage and salaried staff employees who terminate employment. Human Resources has communicated the new Toolkit to the University and made presentations to various management groups. In addition, Human Resources plans to perform random audits at least quarterly to ensure departments comply with the new Off-boarding Toolkit.

We recommend that both the University and Medical Center Human Resources Department's implement the new processes they have developed and perform regular audits to evaluate department compliance. We also recommend that Human Resources periodically compare terminated employees according to the

payroll records to the systems access termination records to identify instances where departments did not notified them to terminate systems access.

University Management Response

The University and Medical Center concur and are in the process of implementing new processes to address the termination of access to systems and facilities by former employees.

The University recognized that controls over termination of access to systems and facilities by the Academic Division needed to be improved. Accordingly, in October, the University developed and implemented new procedures to strengthen controls for monitoring and documenting terminations, especially those controls designed to prevent unauthorized access to sensitive data. With the implementation of the new Off-boarding Toolkit and random quarterly audits, we are confident these changes will adequately address the issues that have been identified. The new controls have been well communicated to department management. We will provide additional training on the new policy and procedures and will implement actions to regularly monitor department compliance.

The Medical Center has initiated a three prong approach to address timely termination of access to systems and facilities. The Chief Financial Officer for the Medical Center communicated to Medical Center management the timeframe for terminating access of former employees, referring to policy No. 405 - Separation of Employment. Beginning January 2014, quarterly termination audits will be conducted by the Controller's Office to ensure termination notifications are received within 48 hours. In addition, the Medical Center plans to convert the employee termination notification to an electronic process through PeopleSoft, in order to streamline the notification process between Operations, Human Resources and HSTS.

#3 Complete and Approve Reconciliations Timely

The University is not completing and approving reconciliations timely. In a sample of 55 reconciliations, five were prepared late and not approved, seven were prepared timely but not approved, five were prepared and approved late, and three were neither prepared nor approved.

Reconciliations should be prepared and approved timely because they are an important internal control to promptly detect, correct, and report errors and irregularities. Late reconciliations and unreconciled accounts put the University at risk of making financial and administrative decisions based inaccurate information.

We recommend the University improve internal controls to monitor and enforce the timely preparation and approval of reconciliations. The University should ensure information captured in the Recon@UVA system is used to send electronic reminders to both the reconciliation preparer and approver when reconciliations are incomplete or becoming late.

University Management Response

The University agrees that the internal controls over the reconciliation process can be improved. Steps to do so are in place and are part of the next planned phase of the Recon@ system implementation, in early 2014. The Recon@ system has changed the old paper process to an online process, which has enabled monitoring capability not in place before. Since initial implementation in 2011, we have focused on improving system usability by adding enhanced functionality and additional reports. The next phase of the project is to turn on the workflow functionality, which will send out automatic notifications for reconciliations not completed within the established timeframe. After that, deans and vice presidents will be notified about outstanding reconciliations.

#4 - Comply with University Sole Source Policy

Procurement Services is not following University policy and therefore risks allegations of unfairly awarding sole source contracts. In a sample of five sole source contracts, one lacked justification for a purchase over $5,000 and one lacked the consideration of alternate vendors through a market survey. We recommend Procurement Services improve controls that will ensure sole source purchases adhere to University policy.

University Management Response

The University agrees that the sole source policy has not been followed in every case. Procurement Services will review the controls over the sole source process and put in place any improvements identified from that review.

Please contact me if any additional information is needed. On behalf of the University of Virginia, please extend my appreciation to all of your staff for their professional work and recommendations.

Sincerely,

Melody S. Bianchetto
Associate Vice President for Finance
University of Virginia

Larry Fitzgerald
Associate Vice President for Business Development and Finance
University of Virginia Medical Center

UNIVERSITY OF VIRGINIA
Charlottesville, Virginia

BOARD OF VISITORS

Helen E. Dragas
Rector

George Keith Martin
Vice Rector

Frank B. Atkinson
A. Macdonald Caputo
Hunter E. Craig
The Honorable Alan A. Diamonstein
Allison Cryer DiNardo
Marvin W. Gilliam Jr.
William H. Goodwin Jr.
Victoria D. Harker
Bobbie G. Kilberg
Stephen P. Long, M.D.
Vincent J. Mastracco Jr.
Edward D. Miller, M.D.
John L. Nau III
Timothy B. Robertson
Linwood H. Rose

Hillary A. Hurd, Student

Leonard W. Sandridge Jr., Senior Advisor to the Board

Susan G. Harris
Secretary to the Board of Visitors

ADMINISTRATIVE OFFICERS

Teresa A. Sullivan
President

Patrick D. Hogan
Executive Vice President and Chief Operating Officer