



# VIRGINIA COMMONWEALTH UNIVERSITY

## REPORT ON AUDIT FOR THE YEAR ENDED JUNE 30, 2022

Auditor of Public Accounts  
Staci A. Henshaw, CPA

[www.apa.virginia.gov](http://www.apa.virginia.gov)

(804) 225-3350



## AUDIT SUMMARY

We have audited the basic financial statements of Virginia Commonwealth University (University) as of and for the year ended June 30, 2022, and issued our report thereon, dated December 7, 2022. Our report, included in the University's basic financial statements, is available at the Auditor of Public Accounts' website at [www.apa.virginia.gov](http://www.apa.virginia.gov) and at the University's website at [www.vcu.edu](http://www.vcu.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;
- three instances of noncompliance or other matters required to be reported under Government Auditing Standards; and
- the University has taken adequate corrective action with respect to audit findings reported in the prior year.

Our audit also included testing over the major federal program of the Education Stabilization Fund 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–

### Pages

AUDIT SUMMARY

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

1-2

INDEPENDENT AUDITOR’S REPORT ON INTERNAL CONTROL OVER  
FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS

3-5

UNIVERSITY RESPONSE

6-8

UNIVERSITY OFFICIALS

9

## INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

### **Improve IT Asset Management Process**

**Type:** Internal Control and Compliance

**Severity:** Significant Deficiency

**Repeat:** No

Virginia Commonwealth University (University) lacks certain controls to support the information technology (IT) asset management process in accordance with the University's adopted information security standard, the International Organization for Standardization, and the International Electrotechnical Commission Standard ISO/IEC 27002 (ISO Standard), as well as the University's standards and baselines.

We identified two control weaknesses and communicated them to management in a separate document marked Freedom of Information Act (FOIA) Exempt under § 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms. The ISO Standard requires the University to implement certain controls that reduce unnecessary risk to the confidentiality, integrity, and availability of the University's IT assets and data. Due to the University's decentralized environment, the University does not have a central enforcement measure to ensure each unit complies with the ISO Standard and baseline.

The University should ensure that it follows the required IT asset management process that meets the requirements of the ISO Standard, as well as the University's standards and baselines to help protect the University's confidential and sensitive information.

### **Improve Firewall Security**

**Type:** Internal Control and Compliance

**Severity:** Significant Deficiency

**Repeat:** No

The University does not properly secure the firewall that safeguards its secure internal network in accordance with the ISO Standard as well as University policies and best practices.

We identified four control weaknesses and communicated them to management in a separate document marked FOIA Exempt under § 2.2-3705.2 of the Code of Virginia, due to it containing descriptions of security mechanisms. The ISO Standard requires organizations to implement certain controls that reduce unnecessary risk to the confidentiality, integrity, and availability of the University's information systems and data.

The University should remediate the existing firewall weaknesses and develop procedures to maintain the firewall in accordance with the requirements of University policies and the ISO Standard to help secure its network to protect its systems and data.

## **Improve IT Change Management Procedures and Process**

**Type:** Internal Control and Compliance

**Severity:** Significant Deficiency

**Repeat:** No

The University does not follow an IT change management process that includes elements required by the ISO Standard, as well as University policies and procedures. Specifically, the following two control weaknesses exist:

- The University does not record or confirm the results of technical testing or user acceptance testing. The University's Change Management Standard (CM Standard) requires that the implementation team document all change management requests in detail, including specifying a test plan. However, the Change Management Process Guide (Process Guide) does not detail the steps that the University follows to meet the requirements for documenting testing. As a result, the change management requests do not detail the test plan or confirm the results of technical testing or user acceptance testing. The ISO Standard, Section 8.32, states that change control procedures should include tests and acceptance of tests for changes. Without ensuring that the implementation team performs and documents proper testing, the University increases the risk that critical systems may become unavailable due to the implementation of untested changes in production.
- The University's change management process does not verify that the technical implementation teams update supporting documentation to reflect the change. The University tasks individual implementation teams with managing and maintaining operating documentation and user procedures; however, the CM Standard and the Process Guide do not include requirements and a process to verify that the implementation teams update supporting documentation, when applicable, following a change. The ISO Standard, Section 8.32, states that change control procedures should ensure that the implementation team updates operating documentation and user procedures, as necessary, to remain appropriate. Without verifying updates to supporting documentation during the change management process, the University may not consistently update supporting documentation following changes, which could result in out-of-date or incorrect operating procedures or baseline configurations.

The change management process does not include adequate documentation of technical testing, documentation of user acceptance testing, and verification of updates to supporting documentation due to an oversight in establishing the CM Standard and Process Guide. The University should update the Process Guide to include requirements for documentation of tests for changes, including acceptance of tests. The University should also update the CM Standard and Process Guide to include requirements for verification of updates made to supporting documentation resulting from a change. Additionally, the University should include fields in the change ticket form that require the University to document testing information, as well as updates made to supporting documentation. Doing so will help ensure the confidentiality, integrity, and availability of the University's mission critical data.



# Commonwealth of Virginia

*Auditor of Public Accounts*

Staci A. Henshaw, CPA  
Auditor of Public Accounts

P.O. Box 1295  
Richmond, Virginia 23218

December 7, 2022

The Honorable Glenn Youngkin  
Governor of Virginia

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, 2022, 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 7, 2022. Our report includes a reference to other auditors who audited the financial statements of the component units of the University, as described in our report on the University's financial statements. The other auditors, excluding those of Dentistry@VCU, did not audit the financial statements of those component units of the University in accordance with Government Auditing Standards, and accordingly, this report does not include reporting on internal control over financial reporting or compliance and other matters associated with those component units of the University. Additionally, this report does not include the results of the other auditors' testing of internal control over financial reporting or compliance and other matters for Dentistry@VCU, that are reported on separately by those auditors.

## **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 (internal control) as a basis for designing audit procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the University's internal control. Accordingly, we do not express an opinion on the effectiveness of the University's internal control.

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

Our consideration of internal control was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and therefore, material weaknesses or significant deficiencies may exist that were not identified. Given these limitations, during our audit we did not identify any deficiencies in internal control that we consider to be material weaknesses. We did identify certain deficiencies in internal control titled "Improve IT Asset Management Process," "Improve Firewall Security," and "Improve IT Change Management Procedures and Process," 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 financial statements. 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 titled "Improve IT Asset Management Process," "Improve Firewall Security," and "Improve IT Change Management Procedures and Process."

### **The University's Response to Findings**

We discussed this report with management at an exit conference held on December 6, 2022. Government Auditing Standards require the auditor to perform limited procedures on the University's response to the findings identified in our audit, which is included in the accompanying section titled "University Response." The University's response was not subjected to the other auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on the response.

### **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 Auditing Standards in considering the entity's internal control and compliance. Accordingly, this communication is not suitable for any other purpose.

Staci A. Henshaw  
AUDITOR OF PUBLIC ACCOUNTS

JMR/clj





December 13, 2022

Staci Henshaw, CPA  
Auditor of Public Accounts  
P.O. Box 1295  
Richmond, VA 23218

Patricia Perkins  
AVP of Finance and University  
Controller  
912 West Franklin Street  
Box 842035  
Richmond, Virginia 23284-2512  
804 828-5474

Dear Ms. Henshaw:

We have reviewed the audit findings and recommendations resulting from the fiscal year 2022 audit by the Auditor of Public Accounts and discussed during the exit conference.

**Improve IT Asset Management Process**

Virginia Commonwealth University (University) lacks certain controls to support the information technology (IT) asset management process in accordance with the University's adopted information security standard, the International Organization for Standardization, and the International Electrotechnical Commission Standard ISO/IEC 27002 (ISO Standard), as well as the University's standards and baselines.

We identified two control weaknesses and communicated them to management in a separate document marked Freedom of Information Act (FOIA) Exempt under § 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms. The ISO Standard requires the University to implement certain controls that reduce unnecessary risk to the confidentiality, integrity, and availability of the University's IT assets and data. Due to the University's decentralized environment, the University does not have a central enforcement measure to ensure each unit complies with the ISO Standard and baseline.

The University should ensure that it follows the required IT asset management process that meets the requirements of the ISO Standard, as well as the University's standards and baselines to help protect the University's confidential and sensitive information.

VCU Response:

VCU will coordinate an effort within all of its units to strengthen the IT asset management process across the university and ensure IT assets are adequately tracked and maintained throughout the lifecycle.

Responsible Person: Dan Han, Chief Information Security Officer

Completion Date: June 30, 2023

Page 2  
Ms. Staci Henshaw, CPA  
December 13, 2022

### **Improve Firewall Security**

The University does not properly secure the firewall that safeguards its secure internal network in accordance with the ISO Standard as well as University policies and best practices.

We identified four control weaknesses and communicated them to management in a separate document marked FOIA Exempt under § 2.2-3705.2 of the Code of Virginia, due to it containing descriptions of security mechanisms. The ISO Standard requires organizations to implement certain controls that reduce unnecessary risk to the confidentiality, integrity, and availability of the University's information systems and data.

The University should remediate the existing firewall weaknesses and develop procedures to maintain the firewall in accordance with the requirements of University policies and the ISO Standard to help secure its network to protect its systems and data.

#### **VCU Response:**

VCU has corrected all identified weaknesses and will improve controls and monitoring procedures to minimize the likelihood of recurrence.

Responsible Person: Dan Han, Chief Information Security Officer

Completion Date: March 31, 2023

### **Improve IT Change Management Procedures and Process**

The University does not follow an IT change management process that includes elements required by the ISO Standard, as well as University policies and procedures. Specifically, the following two control weaknesses exist:

The University does not record or confirm the results of technical testing or user acceptance testing. The University's Change Management Standard (CM Standard) requires that the implementation team document all change management requests in detail, including specifying a test plan. However, the Change Management Process Guide (Process Guide) does not detail the steps that the University follows to meet the requirements for documenting testing. As a result, the change management requests do not detail the test plan or confirm the results of technical testing or user acceptance testing. The ISO Standard, Section 8.32, states that change control procedures should include tests and acceptance of tests for changes. Without ensuring that the implementation team performs and documents proper testing, the University increases the risk that critical systems may become unavailable due to the implementation of untested changes in production.

The University's change management process does not verify that the technical implementation teams update supporting documentation to reflect the change. The University tasks individual implementation teams with managing and maintaining operating documentation and user procedures; however, the CM Standard and the Process Guide do not include requirements and a process to verify that the implementation teams update supporting

Page 3  
Ms. Staci Henshaw, CPA  
December 13, 2022

documentation, when applicable, following a change. The ISO Standard, Section 8.32, states that change control procedures should ensure that the implementation team updates operating documentation and user procedures, as necessary, to remain appropriate. Without verifying updates to supporting documentation during the change management process, the University may not consistently update supporting documentation following changes, which could result in out-of-date or incorrect operating procedures or baseline configurations.

The change management process does not include adequate documentation of technical testing, documentation of user acceptance testing, and verification of updates to supporting documentation due to an oversight in establishing the CM Standard and Process Guide. The University should update the Process Guide to include requirements for documentation of tests for changes, including acceptance of tests. The University should also update the CM Standard and Process Guide to include requirements for verification of updates made to supporting documentation resulting from a change. Additionally, the University should include fields in the change ticket form that require the University to document testing information, as well as updates made to supporting documentation. Doing so will help ensure the confidentiality, integrity, and availability of the University's mission critical data.

VCU Response:

VCU built a robust change management process to record and track changes to key IT systems across the university. With the change request form, testing plans are often included in the implementation and recovery plan section, as demonstrated in samples reviewed during the audit. However, VCU will further clarify the change control form to specify the requirement for including test plans within the change request form. Additionally, VCU will review and update, as necessary, its change management process documentation to include additional guidance on testing of changes.

Further, while the change management process will track changes and their associated action, it currently does not remind change requesters to specify any documentation changes. VCU will include an indicator on the change management form to track any documentation updates, including whether a change requires a documentation update and, if so, then a brief description of the update.

Responsible Person: Dan Han, Chief Information Security Officer

Completion Date: June 30, 2023

Sincerely,

DocuSigned by:  
*Patricia Perkins*  
AB2B6C352A2449B...

Patricia Perkins  
Associate VP of Finance and University Controller  
Virginia Commonwealth University

## **VIRGINIA COMMONWEALTH UNIVERSITY**

As of June 30, 2022

### **BOARD OF VISITORS**

H. Benson Dendy, III, Rector

Carolina Espinal, Vice Rector

Clifton Peay	Tyrone E. Nelson
Peter Ferrell	Tonya Paris-Wilkins
Andrew C. Florance	Keith T. Parker
Todd P. Haymore	Ellen Fitzsimmons
Dale Jones	Anthony Bedell
Carmen Lomellin	Alexis Swann
Edward L. McCoy	Shantaram Talegaonkar

### **ADMINISTRATIVE OFFICERS**

Michael Rao, President

Karol Gray, Senior Vice President and Chief Financial Officer