



THE COLLEGE OF WILLIAM & MARY IN VIRGINIA

REPORT ON AUDIT FOR THE YEAR ENDED JUNE 30, 2021

Auditor of Public Accounts
Staci A. Henshaw, CPA

www.apa.virginia.gov

(804) 225-3350



AUDIT SUMMARY

We have audited the consolidated basic financial statements of The College of William & Mary in Virginia, as of and for the year ended June 30, 2021, and issued our report thereon, dated April 28, 2022. The consolidated basic financial statements of The College of William and Mary in Virginia include the financial activity of The College of William and Mary in Virginia (William & Mary), Virginia Institute of Marine Science, and Richard Bland College (Richard Bland), which report to the Board of Visitors of The College of William and Mary in Virginia. Our report, included in the consolidated basic financial statements, is available at the Auditor of Public Accounts' website at www.apa.virginia.gov and at William & Mary's website at www.wm.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–

Pages

AUDIT SUMMARY

STATUS OF PRIOR YEAR FINDINGS AND RECOMMENDATIONS

1-2

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

3-7

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

8-10

WILLIAM & MARY AND RICHARD BLAND RESPONSES

11-12

WILLIAM & MARY AND RICHARD BLAND OFFICIALS

13

STATUS OF PRIOR YEAR FINDINGS AND RECOMMENDATIONS

Improve Internal Controls over Conflict of Interests Act Requirements

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: Partial (first issued in fiscal year 2020)

During the fiscal year 2020 audit, we determined William & Mary did not have a sufficient process to identify and track individuals in a position of trust, which is necessary to ensure such individuals satisfy Statement of Economic Interest (SOEI) form requirements as specified in §§ 2.2-3114 and 2.2-3118 of the Code of Virginia. Additionally, William & Mary did not maintain adequate internal records to monitor and ensure employees completed ethics and conflict of interest training required by §§ 2.2-3129 and 2.2-3130 of the Code of Virginia.

We communicated our original audit finding to management during the fiscal year 2020 audit on April 21, 2021. William & Mary has made progress to identify and track individuals in a position of trust, which is necessary to ensure such individuals satisfy SOEI form requirements. However, due to the timing between when we issued the original finding and the end of the period under audit, William & Mary's implementation of processes and controls to maintain adequate internal records to monitor and ensure employees complete ethics and conflict of interests training required by the Code of Virginia was ongoing at the end of the fiscal year. As a result, we will review the implementation of management's completed corrective actions during our fiscal year 2022 audit.

Properly Complete Verification Prior to Disbursing Federal Financial Aid

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: Partial (first issued in fiscal year 2020)

During the fiscal year 2020 audit, we determined the William & Mary Financial Aid Office did not properly complete the verification process for certain financial aid recipients in accordance with Title 34 Code of Federal Regulations (CFR) 668.54 and 34 CFR 668.56 prior to disbursing aid, which resulted in overawards of Pell grant funds to students.

As part of audit procedures performed during the fiscal year 2021 audit, we tested to ensure that William & Mary complied with all verification requirements. For two out of 25 students tested (8%), we determined the Financial Aid Office did not complete all the required verification procedures; however, the Financial Aid Office confirmed these instances did not result in changes to the student's award or estimated family contribution, resulting in no overawarding of Pell grant funds.

We communicated our original audit finding to management during the fiscal year 2020 audit on April 6, 2021. Due to the timing between when we issued the original finding and the end of the period under audit, William & Mary had not fully implemented all corrective actions related to this finding.

Properly Complete Exit Counseling for Direct Loan Borrowers

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: Partial (first issued in fiscal year 2020)

During the fiscal year 2020 audit, we determined the William & Mary Financial Aid Office did not confirm that certain Federal Direct Loan borrowers who had withdrawn had completed online exit counseling in accordance with 34 CFR 685.304(B)(3). Consequently, the Financial Aid Office did not provide the required exit counseling materials to these students.

As part of audit procedures performed during the fiscal year 2021 audit, we tested to ensure that, for applicable students, the Financial Aid Office provided required materials timely and documented completion of the required exit counseling. For six of 25 students tested (24%), we found that the Financial Aid Office did not provide the required materials to applicable students timely. We communicated our original audit finding to management during the fiscal year 2020 audit on April 6, 2021. Due to the timing between when we issued our original finding and the end of the period under audit, William & Mary had not fully implemented all corrective actions related to this finding.

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

WILLIAM & MARY

Improve Router Security

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: No

William & Mary does not manage its router in accordance with its Technical Vulnerability Management Policy, as well as its adopted security standard, the International Organization for Standardization and the International Electrotechnical Commission Standard, ISO/IEC 27002 (ISO Standard). We communicated two weaknesses to management in a separate document marked Freedom of Information Act Exempt (FOIAE) 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 William & Mary's information systems and data.

The reorganization of information technology (IT) senior management and unforeseen challenges related to the COVID-19 pandemic contributed to the department's lapse in following its policies and standards. The IT Department should remediate the issues identified over its router and continue to develop and implement policies and procedures to properly maintain and secure the router in accordance with the requirements of the ISO Standard. Implementing corrective action will help to ensure that William & Mary protects its sensitive and mission critical systems and data.

Improve Web Application Security

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: No

William & Mary does not manage a sensitive web application in accordance with its Technical Vulnerability Management Policy, as well as the ISO Standard. We communicated the weakness to management in a separate document marked FOIAE 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 William & Mary's information systems and data.

The reorganization of IT senior management and unforeseen challenges related to the COVID-19 pandemic contributed to the issues regarding the web application. William & Mary should remediate the weakness identified over the web application and continue to develop, document, and implement standard operating procedures and processes to properly maintain and secure the web application in accordance with the requirements of the ISO Standard. Implementing corrective action will help to ensure that William & Mary protects its sensitive and mission critical systems and data.

Formalize Policies and Procedures for Obtaining and Reviewing System and Organization Control Reports of Third-Party Service Providers

Type: Internal Control

Severity: Significant Deficiency

Repeat: No

William & Mary's Financial Reporting Office (Financial Reporting) does not document its review of third-party service providers' System and Organization Controls (SOC) reports, nor does it document how William & Mary's controls satisfy the objectives of the complementary user entity controls (CUECs) identified in SOC reports. Additionally, Financial Reporting does not document its evaluation and response to risks that may exist within the reports and was not able to provide documentation indicating that management reviewed the SOC reports.

Commonwealth Accounting Policies and Procedures (CAPP) Manual Topic 10305, published by the Commonwealth's Department of Accounts, requires agencies to have adequate interaction with third-party service providers to appropriately understand the provider's internal control environment. Agencies must also maintain oversight over the provider to gain assurance over outsourced operations. SOC reports are a key tool in gaining an understanding of a provider's internal control environment and maintaining oversight over outsourced operations.

Without documentation evidencing review and response to SOC reports, management may be unaware of risks related to its third-party service providers and may not be able to demonstrate that it maintains sufficient oversight over its third-party service providers. The process of documenting consideration of CUECs strengthens the control environment by ensuring proper internal control design, implementation, and operating effectiveness. Lastly, Financial Reporting may face challenges in demonstrating that it is properly addressing any internal control deficiencies, exceptions, or modified opinions noted in the SOC reports.

Financial Reporting requests SOC reports each year and regularly interacts with its third-party service providers. However, Financial Reporting does not have formalized policies and procedures for the review of SOC reports. In addition, there are no written policies or procedures describing William & Mary's required actions in considering CUECs or noting and evaluating risks related to issues identified in the SOC reports.

Financial Reporting should formalize its policies and procedures for obtaining, reviewing, assessing, and documenting the effectiveness of service providers' controls reported through SOC reports. In addition, Financial Reporting should utilize SOC reports as a component of its third-party service provider oversight activities to demonstrate compliance with the requirements outlined in the CAPP Manual and industry best practices. Finally, if Financial Reporting identifies issues or concerns within the SOC reports, it should document its evaluation of the noted issues, including whether additional compensating controls are necessary to mitigate risk until the provider implements appropriate corrective action.

RICHARD BLAND

Develop and Implement a Service Provider Oversight Process

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: No

Richard Bland does not employ effective policies, procedures, and processes to monitor, on an ongoing basis, security control compliance by external service providers that do not qualify for the Virginia Information Technologies Agency's (VITA) Enterprise Cloud Oversight Services (ECOS). Additionally, Richard Bland does not have a formal documented process to manage its software as a service (SaaS) providers covered by VITA's ECOS. Providers are organizations that perform certain business tasks or functions on behalf of Richard Bland and the Commonwealth. Richard Bland uses 34 providers for mission critical business functions that include the processing and storing of sensitive data.

The Commonwealth's Hosted Environment Information Security Standard, SEC 525 (Hosted Environment Security Standard), Section 1.1, states that management remains accountable for maintaining compliance with the Hosted Environment Security Standard through documented agreements with external service providers and oversight of services provided. Section SA-9 requires that organizations employ appropriate processes, methods, and techniques to monitor effectiveness of external service providers' security controls on an ongoing basis. Additionally, Richard Bland signed a Memorandum of Understanding (MOU) with VITA's ECOS that requires Richard Bland to review and approve all documentation evidencing ECOS's performance of services to monitor compliance with the MOU.

Without a documented and established process to gain assurance over the internal controls of external service providers that do not qualify for VITA's ECOS service, Richard Bland cannot consistently validate that those providers have effective security controls to protect Richard Bland's mission-critical and confidential data. Without a formal process to obtain VITA's ECOS oversight services, and then review and maintain ECOS's documentation, Richard Bland cannot validate whether its SaaS providers implement security controls that meet the requirements in the Hosted Environment Security Standard to protect sensitive and confidential data.

Richard Bland was unaware of its oversight responsibilities in the MOU for VITA's ECOS, which led to the weaknesses described above. Limited staffing resources in its IT Department contributed to the incomplete external service provider oversight process. Richard Bland recently executed a contract to transition certain IT Department functions to a third-party service provider to help alleviate staffing resource constraints.

Richard Bland should dedicate the necessary resources to request and evaluate annual security assessment reports from each external service provider to ensure the provider employs effective operating controls to protect Richard Bland's sensitive data. During the evaluation, Richard Bland should identify control deficiencies, develop mitigation plans, and escalate issues of noncompliance, as needed. Further, Richard Bland should develop a formal process to procure VITA's ECOS oversight for all SaaS

providers, monitor and maintain oversight to ensure the providers comply with the Hosted Environment Security Standard, and ensure that VITA's ECOS satisfies its requirements as stated in the MOU. Effective external service provider oversight will help maintain the confidentiality, integrity, and availability of sensitive and mission critical data.

Improve Firewall Security

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: No

Richard Bland does not properly secure its firewall in accordance with the Commonwealth's Information Security Standard, SEC 501 (Security Standard). We communicated four control weaknesses to management in a separate document marked FOIAE under § 2.2-3705.2 of the Code of Virginia, due to it containing descriptions of security mechanisms. The Security Standard requires the documentation and implementation of certain controls that reduce unnecessary risk to the confidentiality, integrity, and availability of Richard Bland's information systems and data.

Limited staffing resources in the IT Department contributed to the control weaknesses communicated to management. Richard Bland recently executed a contract to transition certain IT Department functions to a third-party service provider to help alleviate staffing resource constraints.

Richard Bland should develop a plan to implement the controls discussed in the communication marked FOIAE in accordance with the Security Standard in a timely manner. Implementing corrective action will help to ensure Richard Bland secures its network to protect its systems and data.

Upgrade End-of-Life Technology

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: No

Richard Bland uses an end-of-life and end-of-support technology in its IT environment. Specifically, Richard Bland maintains a technology that supports mission-essential data on an IT system running software that its vendor no longer supports. We communicated the control weakness to management in a separate document marked FOIAE under § 2.2-3705.2 of the Code of Virginia, due to it containing descriptions of security mechanisms. The Security Standard prohibits agencies from using software that is end-of-life and which the vendor no longer supports, to reduce unnecessary risk to the confidentiality, integrity, and availability of information systems and data.

The lack of a documented process to track end-of-life software and limited staffing resources in the IT Department led to the oversight. Richard Bland recently executed a contract to transition certain IT Department functions to a third-party service provider to help alleviate staffing resource constraints.

Richard Bland should dedicate the necessary resources to evaluate and implement the controls and recommendations discussed in the communication marked FOIAE in accordance with the Security

Standard. Proper planning for upgrading technology prior to the end-of-life and end-of-support date will increase Richard Bland's security posture and help to ensure the confidentiality, integrity, and availability of sensitive and mission critical data.



Staci A. Henshaw, CPA
Auditor of Public Accounts

Commonwealth of Virginia

Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

April 28, 2022

The Honorable Glenn Youngkin
Governor of Virginia

Joint Legislative Audit
and Review Commission

Board of Visitors
The College of William and Mary in 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 College of William and Mary in Virginia** (William & Mary) as of and for the year ended June 30, 2021, and the related notes to the financial statements, which collectively comprise William & Mary's consolidated basic financial statements and have issued our report thereon dated April 28, 2022. 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, 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 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 opinions on the financial statements, but not for

the purpose of expressing an opinion on the effectiveness of internal control. Accordingly, we do not express an opinion on the effectiveness of 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 Internal Controls over Conflict of Interests Act Requirements," "Properly Complete Verification Prior to Disbursing Federal Financial Aid," "Properly Complete Exit Counseling for Direct Loan Borrowers," "Improve Router Security," "Improve Web Application Security," "Formalize Policies and Procedures for Obtaining and Reviewing System and Organization Control Reports of Third-Party Service Providers," "Develop and Implement a Service Provider Oversight Process," "Improve Firewall Security," and "Upgrade End-of-Life Technology," which are described in the sections titled "Status of Prior Year Findings and Recommendations" and "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 consolidated financial statements are free of material misstatement, we performed tests of 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 sections titled "Status of Prior Year Findings and Recommendations" and "Internal Control and Compliance Findings and Recommendations" in the findings titled "Improve Internal Controls over Conflicts of Interest Act Requirements," "Properly Complete Verification Prior to Disbursing Federal Financial Aid," "Properly Complete Exit Counseling for Direct Loan Borrowers," "Improve Router Security," "Improve Web Application Security," "Develop and Implement a Service Provider Oversight Process," "Improve Firewall Security," and "Upgrade End-of-Life Technology."

William & Mary and Richard Bland's Response to Findings

We discussed this report with management at an exit conference held on April 13, 2022. The responses to the findings identified in our audit are described in the accompanying sections titled "William & Mary Response" and "Richard Bland Response." The responses were not subjected to the auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on them.

Status of Prior Findings

William & Mary did not complete corrective action during our audit period with respect to the previously reported findings "Improve Internal Controls over Conflict of Interests Act Requirements," "Properly Complete Verification Prior to Disbursing Federal Financial Aid," and "Properly Complete Exit Counseling for Direct Loan Borrowers." Accordingly, we included these findings in the section titled "Status of Prior Year Findings and Recommendations." William & Mary has taken adequate corrective action with respect to audit findings reported in the prior year that are not repeated in this report.

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

EMS/vks



WILLIAM & MARY

CHARTERED 1693

OFFICE OF UNIVERSITY OPERATIONS

May 19, 2022

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

Dear Ms. Henshaw:

After reviewing William & Mary's (University) fiscal year 2021 audit findings and recommendations, I hereby provide the following responses for inclusion in the audit report:

Improve Internal Controls over Conflict of Interests Act Requirements

Management agrees with the auditor's finding and the University has identified and tracks individuals in positions of trust. As of April 30, 2022, all of the employees identified in positions of trust for filing year 2022 have completed the required training and proper documentation exists to support the compliance requirement.

Properly Complete Verification Prior to Disbursing Federal Financial Aid

Management agrees with the auditor's finding and the Financial Aid Office has implemented a quality assurance process for compliance with verification requirements. The overawards for fiscal year 2020 were returned to the Department of Education promptly upon identification. Items from the fiscal year 2021 review had no impact on estimated family contribution or award amount and were addressed prior to the completion of the review.

Properly Complete Exit Counseling for Direct Loan Borrowers

Management agrees with the auditor's finding. The Financial Aid Office has implemented processes to ensure the timely completion of exit counseling communication in accordance with federal requirements. All students tested as part of the 2021 review did receive the required communications but not within the required timeframe. The majority of those identified were one day late due to a processing issue and that has been corrected.

Improve Router Security and Improve Web Application Security

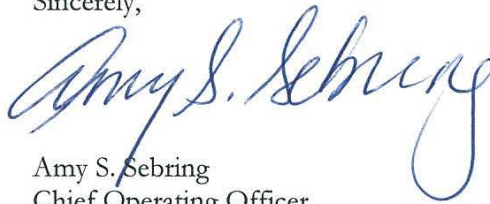
Management agrees with the auditor's findings and Information Technology will implement corrective action to address the concerns.

Formalize Policies and Procedures for Obtaining and Reviewing System and Organization Control Reports of Third-Party Service Providers

Management agrees with the auditor's finding. Financial Reporting currently requests and reviews Third Party Service Provider Reports. The department will develop a formalized policy to include the timing for requesting and reviewing the effectiveness of Third-Party Service Providers controls and to document the process.

Please contact me should you have any questions.

Sincerely,

A handwritten signature in blue ink, reading "Amy S. Sebring". The signature is fluid and cursive, with the first name "Amy" and last name "Sebring" clearly legible.

Amy S. Sebring
Chief Operating Officer

cc: Kent B. Erdahl
Melanie T. O'Dell
Ed Aractingi
Joe Dobrota
Pamela Mason



Richard Bland College of WILLIAM & MARY

Office of Finance

May 19, 2022

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

Dear Ms. Henshaw:

Richard Bland College has reviewed the Internal Control and Compliance Findings and Recommendations provided by the Auditor of Public Accounts for the fiscal year ended June 30, 2021. I hereby provide the following response for inclusion in the audit report:

Develop and Implement a Service Provider Oversight Process

Management concurs with the auditor's finding. Richard Bland will request and evaluate annual security assessment reports from each PaaS Provider to ensure it has effective operating controls to protect Richard Bland's sensitive data. During the evaluation, Richard Bland will identify control deficiencies, develop mitigation plans, and escalate issues of noncompliance, as needed. Further, Richard Bland will develop a formal process to procure VITA's ECOS oversight for all SaaS Providers, monitor and maintain oversight to ensure the Providers comply with the Hosted Environment Security Standard and ensure that VITA's ECOS satisfies its requirements as stated in the MOU.

Improve Firewall Security

Management concurs with the auditor's finding and Richard Bland will implement corrective action to address the concerns.

Upgrade End-of-Life Technology

Management concurs with the auditor's finding and Richard Bland will implement corrective action to address the concerns.

Please contact me should you have any questions.

Sincerely,

Paul S. Edwards
Chief Business Officer

11301 Johnson Road, South Prince George, Virginia 23805
804-862-6100|RBC.edu

THE COLLEGE OF WILLIAM & MARY IN VIRGINIA
RICHARD BLAND COLLEGE

As of June 30, 2021

BOARD OF VISITORS*

John E. Littel, Rector
William H. Payne, II, Vice Rector
Barbara L. Johnson, Secretary

Mari Carmen Aponte	Anne Leigh Kerr
Mirza Baig	Charles E. Poston
Victor K. Branch	Lisa E. Roday
S. Douglas Bunch	J.E. Lincoln Saunders
Sue H. Gerdelman	Karen Kennedy Schultz
James A. Hixon	H. Thomas Watkins, III
Cynthia E. Hudson	Brian P. Woolfolk

ADMINISTRATIVE OFFICIALS

The College of William and Mary in Virginia

Katherine A. Rowe, President

Amy S. Sebring, Chief Operating Officer

Richard Bland College

Debbie L. Sydow, President

*Only voting members included. Ex-officio and non-voting members not listed.