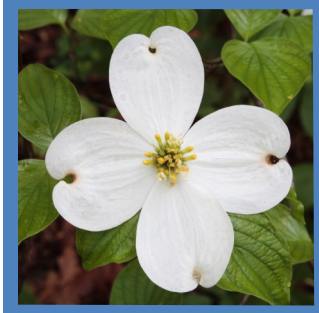


THE COLLEGE OF WILLIAM & MARY IN VIRGINIA

REPORT ON AUDIT FOR THE YEAR ENDED JUNE 30, 2023

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, 2023, and issued our report thereon, dated June 17, 2024. 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;

- ten internal control findings requiring management's attention, nine of which represent instances of noncompliance or other matters required to be reported under Government Auditing Standards; however, we do not consider them to be material weaknesses; and

- adequate corrective action with respect to prior audit findings and recommendations identified as complete in the Findings Summaries included in the Appendix.

Our audit also included testing over federal Student Financial Assistance at Richard Bland in accordance with the U.S. Office of Management and Budget Compliance Supplement Part 5 Student Financial Assistance Programs; and found internal control deficiencies requiring management's attention and instances of noncompliance in relation to this testing.

In the section titled "Internal Control and Compliance Findings and Recommendations," we have included our assessment of the conditions and causes resulting in the internal control and compliance findings identified through our audit as well as recommendations for addressing those findings. Our assessment does not remove management's responsibility to perform a thorough assessment of the conditions and causes of the findings and develop and appropriately implement adequate corrective actions to resolve the findings as required by the Department of Accounts in Topic 10205 – Agency Response to APA Audit of the Commonwealth Accounting Policies and Procedures Manual. Those corrective actions may include additional items beyond our recommendations.

-TABLE OF CONTENTS-

	Pages
AUDIT SUMMARY	
INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS	1-12
INDEPENDENT AUDITOR'S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS	13-15
APPENDIX – FINDINGS SUMMARIES	16
WILLIAM & MARY RESPONSE	17
RICHARD BLAND RESPONSE	18-19

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

WILLIAM & MARY

Improve IT Service Provider Oversight
Applicable to: William & Mary
Type: Internal Control and Compliance
Severity: Significant Deficiency

The College of William & Mary (William & Mary) does not maintain sufficient oversight of all its information technology (IT) third-party service providers hosting sensitive and protected data in accordance with William & Mary's Application Hosting Policy and Procedures (Hosting Policy), as well as its adopted security standard, the International Organization for Standardization and International Electrotechnical Commission Standard, ISO/IEC 27002 (ISO Standard). William & Mary has 96 IT service providers, including 23 IT service providers hosting sensitive data, 24 IT service providers hosting protected data, and 49 IT service providers hosting nonsensitive data. William & Mary currently obtains and reviews independent audit assurance reports validating the operating effectiveness of security controls for some but not all of its IT service providers hosting sensitive data. For IT service providers hosting protected data, William & Mary did not receive and review the Higher Education Community Vendor Assessment Toolkit (HECVAT) for one of its IT service providers hosting protected data.

William & Mary's Hosting Policy defines the process for oversight of IT service providers hosting sensitive and protected data and does not require oversight of nonsensitive IT service providers hosting public data. The Hosting Policy requires that IT service providers hosting sensitive data must sign a contract addendum that obligates the IT service provider to implement an effective information security program that meets or exceeds the information security standards of William & Mary. Further, the Hosting Policy requires IT service providers hosting sensitive data to provide an independent auditor's report, such as a System and Organization Controls (SOC) report, for review and evaluation, or provide evidence of an industry standard certification, as specifically defined in the Hosting Policy. For IT service providers hosting protected systems, the Hosting Policy requires that William & Mary annually obtain and review a HECVAT for the service provider. The ISO Standard requires William & Mary to regularly monitor, review, evaluate, and manage IT service providers to ensure compliance with established information security controls and requirements. *(ISO Standard: section 5.19 Information security in supplier relationships, section 5.20 Addressing information security in supplier agreements, section 5.21 Managing information security in the ICT supply chain, section 5.22 Monitoring, review and change management of supplier services, and section 5.23 Information security for use of cloud services).*

William & Mary did not receive independent audit assurance reports from two IT service providers hosting sensitive systems because the IT service providers have not responded to William & Mary's requests. For 13 IT service providers identified, William & Mary received and relied upon various certifications for each IT service provider; however, these certifications do not provide an opinion over the operating effectiveness of the IT service providers' controls.

Without annually receiving and reviewing independent audit assurance reports that provide an opinion over the operating effectiveness of the controls for each IT service provider hosting sensitive data, William & Mary cannot validate that the IT service providers have effective IT controls to protect William & Mary's sensitive data. By relying on other types of certifications that do not provide an opinion on the operating effectiveness of IT security controls, William & Mary may not be able to identify relevant subservice providers, identify exceptions and complementary user entity controls, and perform other verification required by the ISO Standard to monitor control compliance of IT service providers. Additionally, without receiving and reviewing an annual HECVAT for IT service providers hosting protected systems, William & Mary may not appropriately identify and manage risks to maintain an effective security posture. Unidentified weaknesses in IT service provider controls may expose William & Mary to an increased risk of a breach or possible data disclosure.

William & Mary should modify its Hosting Policy to include a requirement to obtain and review an independent audit assurance report for all IT service providers hosting sensitive data that provides an opinion on the operating effectiveness of the IT service provider's controls, such as a SOC report. William & Mary should then ensure that it obtains the reports annually for each IT service provider classified as sensitive, subsequently performs and documents an annual security assessment based on its evaluation of the provided independent audit assurance, and follows up with the IT service provider for any identified issues. In circumstances where using a specific vendor without an independent audit assurance report is unavoidable, William & Mary should document its evaluation of the risk to confidentiality, integrity, and availability of data hosted by the vendor, and the mitigating processes and controls William & Mary should implement to reduce risk to an acceptable level. Additionally, William & Mary should ensure that it obtains and reviews a HECVAT for all IT service providers hosting protected data as required by the Hosting Policy. Implementing these changes will help William & Mary ensure that IT service providers hosting sensitive or protected data implement an effective information security program that protects the confidentiality, integrity, and availability of William & Mary's data.

RICHARD BLAND

Improve Firewall Security
Applicable to: Richard Bland
Type: Internal Control and Compliance
Severity: Significant Deficiency
First Reported: Fiscal Year 2021

Richard Bland College (Richard Bland) has made progress since the prior audit to secure its firewall by conducting vulnerability scans against the firewall. However, Richard Bland continues to not have a formal policy that establishes the minimum requirements and timeframe for performing vulnerability scans over the firewall and subsequently evaluating and remediating any identified vulnerabilities within 90 days in accordance with the Commonwealth's Information Security Standard, SEC501 (Security Standard). Additionally, while Richard Bland established a firewall standard operating procedure (firewall procedure) since the prior year audit to conduct firewall vulnerability scanning weekly and track vulnerabilities through its change management process, the firewall procedure does not detail a process that ensures Richard Bland remediates vulnerabilities within the required 90 days.

The Security Standard requires that organizations define a policy that establishes requirements for system and information integrity. The Security Standard also requires analyzing vulnerability scan reports and remediating legitimate vulnerabilities within 90 days in accordance with an organizational assessment of risk (Security Standard, sections: SI-1 System and Information Integrity Policy and Procedures and RA-5 Vulnerability Scanning). Not establishing and implementing a formal policy and procedure governing vulnerability management and subsequently evaluating and remediating vulnerabilities within 90 days exposes Richard Bland to increased risk of potential exploitation of vulnerabilities by malicious actors.

Richard Bland experienced significant turnover in its information technology and security positions. As a result, Richard Bland has hired a new Information Security Officer, Chief Information Officer, and Chief Operating Officer since calendar year 2023. Due to the significant turnover and lack of staff continuity, Richard Bland is working to evaluate and establish consistent policies and procedures.

Richard Bland should establish a formal vulnerability management policy that details the minimum requirements for performing vulnerability scans over its environment, and the requirements for evaluating and remediating identified vulnerabilities based on severity within 90 days. Richard Bland should update its firewall procedure to detail the process for remediating vulnerabilities in accordance with its policy. Richard Bland should then ensure it remediates vulnerabilities within 90 days, which will help to ensure the confidentiality, integrity, and availability of Richard Bland's sensitive information systems and data.

Develop and Implement a Service Provider Oversight Process

Applicable to: Richard Bland
Type: Internal Control and Compliance
Severity: Significant Deficiency
First Reported: Fiscal Year 2021

Richard Bland continues to not employ effective policies and procedures to monitor the effectiveness of external IT service providers on an ongoing basis for those that do not qualify for the Virginia Information Technologies Agency's (VITA) Enterprise Cloud Oversight Services (ECOS), and for IT service providers that do qualify for ECOS. IT service providers are organizations that perform certain business tasks or functions on behalf of Richard Bland and the Commonwealth. Richard Bland currently uses 32 IT service providers for mission-critical business functions, some of which include the processing and storing of sensitive data.

Since the fiscal year 2022 audit, Richard Bland developed its Third-Party Procedures that detail how Richard Bland requests IT service providers for ECOS oversight. However, these procedures do not detail a process for Richard Bland to effectively monitor its IT service providers as required by the Commonwealth's Hosted Environment Information Security Standard, SEC525 (Hosted Environment Security Standard), such as deliverables expected from ECOS oversight, or the steps Richard Bland must take if the IT service provider does not qualify for ECOS oversight.

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

Without a documented and established process to gain assurance over the internal controls of IT service providers that do not qualify for VITA's ECOS, Richard Bland cannot consistently validate that those IT service providers have effective security controls to protect Richard Bland's mission critical and confidential data. Similarly, without a formal process to review and maintain VITA's ECOS documentation, Richard Bland cannot validate whether its IT service providers under active ECOS oversight implement security controls that meet the requirements in the Hosted Environment Security Standard to protect sensitive and confidential data, which could result in third-party IT service providers with significant security risks and vulnerabilities that expose Richard Bland to potential breach or compromise of Richard Bland's sensitive systems and data.

Richard Bland experienced significant turnover in its IT and security departments since the prior audit. As a result, Richard Bland has hired a new Information Security Officer, Chief Information Officer, and Chief Operating Officer since calendar year 2023. Due to the significant turnover and lack of staff

continuity, Richard Bland chose to prioritize completing its Business Impact Analysis and risk assessment process before focusing on its IT service provider oversight process.

Richard Bland should dedicate the necessary resources to continue developing and implementing an IT service provider process and update its policies and procedures as necessary to align with the Hosted Environment Security Standard. Richard Bland should also dedicate the necessary resources to request and evaluate annual security assessment reports from each IT service provider that does not qualify for ECOS oversight to ensure it has 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 monitor and maintain oversight for IT service providers that qualify for VITA's ECOS to ensure they comply with the Hosted Environment Security Standard and ensure that VITA's ECOS satisfies its requirements as stated in the MOU. Effective IT service provider oversight will help maintain the confidentiality, integrity, and availability of Richard Bland's sensitive and mission-critical data.

Improve Database Security
Applicable to: Richard Bland
Type: Internal Control and Compliance
Severity: Significant Deficiency
First Reported: Fiscal Year 2022

Richard Bland has made limited progress to implement minimum security controls and processes to protect the database that supports its accounting and financial reporting system in accordance with its policies, the Commonwealth's Security Standard, and industry best practices, such as the Center for Internet Security's Benchmark (CIS Benchmark). We communicated six 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 and industry best practices, such as the CIS Benchmark, require Richard Bland to implement certain controls to reduce unnecessary risk to data confidentiality, integrity, and availability in systems processing or storing sensitive information.

Richard Bland experienced significant turnover in its IT and security departments. As a result, Richard Bland has hired a new Information Security Officer, Chief Information Officer, Chief Operating Officer, and lead Database Administrator since 2023. Due to the significant turnover and lack of staff continuity, Richard Bland has not yet had time to remediate all database weaknesses identified during the prior year's audit.

Richard Bland should develop policies and procedures and update its formal baseline configuration to align with the Security Standard and industry best practices, such as the CIS Benchmark. Richard Bland should then dedicate the necessary resources to address the weaknesses in the FOIAE communication. Implementing these security controls and processes to protect the database will help maintain the confidentiality, integrity, and availability of Richard Bland's sensitive and mission-critical data.

Improve IT Risk Management Program
Applicable to: Richard Bland
Type: Internal Control and Compliance
Severity: Significant Deficiency
First Reported: Fiscal Year 2022

Richard Bland continues to not properly manage certain aspects of its IT risk management and contingency planning program in accordance with the Commonwealth's Security Standard, and the Commonwealth's IT Risk Management Standard, SEC520 (IT Risk Management Standard). The IT risk management and contingency planning program provides the baseline for Richard Bland to recover and restore mission-critical and sensitive systems based on the college's identification, assessment, and management of information security risks. Risk management documents include Richard Bland's Business Impact Analysis (BIA) and IT system risk assessments. Contingency planning documents include Richard Bland's Continuity of Operations Plan (COOP) and Disaster Recovery Plan (DRP).

Since the prior year audit, Richard Bland partially remediated one of three identified weaknesses. The following items reflect the remaining weaknesses and one additional weakness identified during the current year's audit:

- Richard Bland reviewed and updated its Risk Assessment Policy, Richard Bland Information Security Standard, COOP, IT COOP, and DRP since the prior year audit. However, Richard Bland continues not to conduct a full revision of the BIA at least every three years and an annual review thereafter to validate the information is accurate and revise as needed to reflect Richard Bland's current environment (*Security Standard, section 3.2 Business Impact Analysis; IT Risk Management Standard, section 4.2 Business Impact Analysis*).

- Richard Bland does not have an updated IT System and Data Sensitivity Classification. As a result, Richard Bland is unable to confirm the total number of sensitive systems to conduct risk assessments and System Security Plans (SSP). The Security Standard requires that Richard Bland complete an IT System and Data Sensitivity Classification to verify and validate that Richard Bland reviews and classifies all IT systems and data as appropriate for sensitivity (*Security Standard, sections: 4.1 IT System and Data Sensitivity Classification, 4.2 Requirements*).

- While Richard Bland has completed risk assessments for two sensitive systems since the prior year audit, it has not completed a risk assessment for the remaining systems previously classified as sensitive in fiscal year 2022. The Security Standard and IT Risk Management Standard require Richard Bland to conduct and document a risk assessment for each sensitive system no less than once every three years and conduct an annual self-assessment to determine the continued validity of the risk assessment (*Security Standard, section 6.2 Risk Assessment; IT Risk Management Standard, section 4.5.3 Performance of Risk Assessments*).

- Richard Bland has completed SSPs for two sensitive systems since the prior year audit, but it has not completed an SSP for the remaining systems previously classified as sensitive in fiscal

year 2022. The Security Standard and IT Risk Management Standard require that Richard Bland develop a security plan for the information system based on the results of the risk assessment, including all existing and planned IT security controls for the system (*Security Standard, section PL-2 System Security Plan; IT Risk Management Standard, section 4.6 System Security Plan*).

Without conducting a full BIA every three years and annual reviews thereafter, Richard Bland cannot accurately identify the IT systems and resources that support its mission-essential and primary business functions, which may cause Richard Bland to have inaccurate or insufficient information to conduct an IT System and Data Sensitivity Classification. Without an updated IT System and Data Sensitivity Classification, Richard Bland cannot properly identify which IT systems contain sensitive data and therefore classify them as sensitive systems. Improper planning can lead to spending too many resources on insignificant controls or having insufficient controls to protect sensitive information. By not conducting risk assessments for all sensitive systems and documenting SSPs based on the results of those risk assessments, Richard Bland may not adequately identify risks for its sensitive systems or identify and implement appropriate security controls for its IT systems and environment to address those risks. Unaddressed system security risks can lead to a potential compromise of Richard Bland's sensitive information.

Richard Bland experienced significant turnover in its IT and security departments. As a result, Richard Bland hired a new Information Security Officer, Chief Information Officer, and Chief Operating Officer since calendar year 2023. Due to the significant turnover and lack of staff continuity, Richard Bland has not yet completed its reviews and updates of all risk management documents.

Richard Bland should allocate appropriate resources to update its IT Risk Management and Contingency Planning Program. In doing so, Richard Bland should conduct a full BIA every three years and subsequently review and update its BIA at least annually thereafter to ensure the documentation reflects Richard Bland's current IT environment and business processes. Additionally, Richard Bland should complete its IT System and Data Sensitivity Classification based on the IT information documented in the BIA to determine Richard Bland's sensitive IT systems. Richard Bland should then conduct a risk assessment and document an SSP for each of its sensitive systems to identify risks, vulnerabilities, security controls in place, and controls needed to address the identified risks. Finally, Richard Bland should maintain its IT Risk Management and Contingency Planning Program through annual reviews, updates, testing, and other exercises as required by the Security Standard and IT Risk Management Standard to protect the confidentiality, integrity, and availability of sensitive and mission-critical data.

Improve Reporting to National Student Loan Data System

Applicable to: Richard Bland
Type: Internal Control and Compliance
Severity: Significant Deficiency

Richard Bland personnel did not report accurate and/or timely enrollment data to the National Student Loan Data System (NSLDS) for students that had graduated, withdrawn or had an enrollment-

level change. Insufficient management oversight in the enrollment reporting process is the underlying cause for the inaccurate and/or untimely reporting. During a review of twenty students, we noted the following noncompliance:

- Inaccurate enrollment status for eight students (40%);
- Inaccurate effective date for eight students' enrollment status (40%);
- Untimely enrollment status change reporting for nine students (45%); and
- Inaccurate information for at least one critical field for nine students (45%).

In accordance with Title 34 Code of Federal Regulations (CFR) § 685.309 and further outlined in the NSLDS Enrollment Guide published by the U.S. Department of Education (ED), Richard Bland must report enrollment changes to NSLDS within 30 days when attendance changes, unless it will submit a roster file within 60 days. The accuracy of Title IV enrollment data depends heavily on information reported by institutions. Untimely and inaccurate data submitted to NSLDS can affect the reliance placed on the system by ED for monitoring purposes. Noncompliance may affect an institution's participation in Title IV programs and can potentially impact loan repayment grace periods and/or loan subsidies for students.

Richard Bland personnel should enhance oversight of the enrollment reporting process, and if necessary, strengthen its procedures, to ensure that the college reports timely and accurate information regarding student enrollment status to the NSLDS.

Properly Perform Return of Title IV Calculations
Applicable to: Richard Bland
Type: Internal Control and Compliance
Severity: Significant Deficiency

Richard Bland personnel did not properly perform return of Title IV calculations for the Fall 2022 and Spring 2023 semesters. The underlying cause of the errors is an insufficient review process related to calculation inputs, specifically, not omitting scheduled break days from the period of enrollment calculation for each semester, as required by federal regulation. As a result of using the incorrect number of days for the period of enrollment, Richard Bland incorrectly calculated the return of Title IV funds for 14 out of 14 applicable students (100%) requiring a calculation. In addition, we identified the following instances of noncompliance within the sample:

- For three students, Richard Bland returned more to ED rather than the calculated amount, resulting in total overpayments of $2,471; and
- For one student, Richard Bland returned $85 less than required.

In accordance with 34 CFR § 668.22, when a recipient of Title IV grant or loan assistance withdraws from an institution during a period of enrollment in which the recipient began attendance, the institution must determine the amount of Title IV grant or loan assistance that the student earned as of the student's withdrawal date. The total number of calendar days in a payment period or period of enrollment includes all days within the period that the student was scheduled to complete, except that scheduled breaks of at least five consecutive days are excluded from the total number of calendar days in a payment period or period of enrollment and the number of calendar days completed in that period. As noted in Volume five of the Federal Student Financial Aid Handbook, for institutions with a scheduled break from Monday through Friday, the weekend before and weekend after must be included in the calculated number of scheduled break days unless classes were offered the prior Saturday or Sunday.

Management should improve its review process to ensure that Richard Bland properly records scheduled breaks of five or more consecutive days in its accounting and financial reporting system to ensure compliance with the calculation requirements.

Return Unearned Title IV Funds Timely
Applicable to: Richard Bland
Type: Internal Control and Compliance
Severity: Significant Deficiency

Richard Bland personnel did not return unearned Title IV aid timely to ED. Richard Bland process for identifying withdrawals includes producing a list of withdrawn students at the end of the semester, rather than frequently throughout the semester. By performing this process at the end of the semester, Richard Bland delayed returning unearned funds for three out of four applicable students (75%) selected for testing.

In accordance with 34 CFR § 668.22 (b)(1), when a student ceases attendance at an institution that is required to take attendance, the student's withdrawal date is the last date of academic attendance as determined by the institution from its attendance records. Further, the Federal Student Financial Aid Handbook, Volume five, Chapter one states, "Institutions that are required to take attendance are expected to have a procedure in place for routinely monitoring attendance records to determine in a timely manner when a student withdraws. Except in unusual instances, the date of the institution's determination that the student withdrew should be no later than 14 days (less if the school has a policy requiring determination in fewer than 14 days) after the student's last date of attendance as determined by the institution from its attendance records. The 14 days includes holidays, breaks, and weekends." Additionally, 34 CFR § 668.22 (j)(1) requires that "an institution must return the amount of Title IV funds for which it is responsible as soon as possible but no later than 45 days after the date of the institution's determination that the student withdrew."

Management should revise its current process to ensure that Richard Bland identifies withdrawn students within 14 days of a student's last date of attendance and subsequently returns unearned funds within 45 days of determining the date of withdrawal.

Implement Information Security Program Requirements for the Gramm-Leach-Bliley Act
Applicable to: Richard Bland
Type: Internal Control and Compliance
Severity: Significant Deficiency

Richard Bland does not comply with certain elements of the Gramm-Leach-Bliley Act (GLBA) related to its information security program. Public Law 106-102, known as the GLBA, considers institutions of higher education to be financial institutions because of their engagement in financial assistance programs. Related regulations at 16 CFR §§ 314.3 and 314.4 require organizations to develop, implement, and maintain the information security program to safeguard customer information.

Specifically, Richard Bland does not comply with the following three elements required by GLBA:

- Richard Bland does not base its written information security program on a risk assessment that identifies security risks to customer information. As a result, Richard Bland cannot evaluate and adjust its information security program based on the results of the risk assessment. GLBA requires that Richard Bland base its information security program on a risk assessment that "identifies reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assesses the sufficiency of any safeguards in place to control these risks." GLBA also requires that Richard Bland adjust its information security program based on the results of the risk assessment. Not basing Richard Bland's information security program on a risk assessment could result in unidentified risks that pose a threat to the college's sensitive customer information and data (*16 CFR §§ 314.4(b) and 314.4(g)*).

- Richard Bland does not have a formally written requirement as part of its information security program to encrypt customer information on its information systems and when in transit. GLBA requires that Richard Bland include, as part of its written information security program, a requirement for encrypting customer information on its systems and when in transit. Not including this requirement could result in a lack of encryption of Richard Bland's sensitive customer information and data, which could lead to a potential compromise of the confidentiality, integrity, and availability of Richard Bland's sensitive customer information and data (*16 CFR § 314.4(c)(3)*).

- Richard Bland does not have a formally written requirement as part of its written information security program to implement multi-factor authentication for anyone accessing customer information on any of Richard Bland's systems. GLBA requires that Richard Bland include as part of its written information security program a requirement for implementing multi-factor authentication for anyone accessing customer information on Richard Bland's systems. Not including this requirement could result in a lack of multi-factor authentication on Richard Bland's systems, which could result in a potential compromise of the confidentiality, integrity, and availability of Richard Bland's sensitive customer information and data (*16 CFR § 314.4(c)(5)*).

Richard Bland experienced significant turnover in its IT and security departments. As a result, Richard Bland has hired a new Information Security Officer, Chief Information Officer, and Chief Operating Officer since calendar year 2023. Due to the significant turnover and lack of staff continuity, Richard Bland has not had the resources to conduct risk assessments and implement its information security program as required by GLBA.

Richard Bland should allocate resources to conduct a comprehensive information security program risk assessment that identifies risks to the security, confidentiality, and integrity of Richard Bland's customer information. Richard Bland should then assess safeguards in place to ensure they are sufficient to address the risks identified in the risk assessment and revise its information security program as necessary based on the results of the risk assessment. Additionally, Richard Bland should update its policies and procedures to include written requirements for encryption of customer information on Richard Bland's systems, including when in transit, and require multifactor authentication for anyone accessing customer information on any Richard Bland system. Completing the requirements outlined by GLBA will assist Richard Bland in evaluating its information security program and protecting the confidentiality, integrity, and availability of customer information within its environment.

Improve Controls for Accounting and Reporting for Right-to-Use Subscription Assets
Applicable to: Richard Bland
Type: Internal Control
Severity: Significant Deficiency

Richard Bland did not adequately prepare for the implementation of Governmental Accounting Standards Board (GASB) Statement No. 96, effective for fiscal year 2023, which prescribes the applicable accounting standards for proper accounting and financial reporting of right-to-use subscription assets or Subscription-Based Information Technology Arrangements (SBITA). While Richard Bland did perform some procedures to identify and record SBITAs, limited documentation exists to support implementation efforts resulting in the following deficiencies:

- Richard Bland did not develop policies and procedures to fully comply with GASB Statement No. 96. Richard Bland identified and reported three short-term SBITAs with a total present value of approximately $161 thousand. We performed a review over one of these SBITAs, with a present value of approximately $98 thousand. Richard Bland personnel were unable to provide sufficient documentation to support that they recorded the SBITA in accordance with GASB Statement No. 96 requirements. GASB Statement No. 96 defines a short-term SBITA as an arrangement with a term that is less than one-year. GASB Statement No. 96 does not require the recognition of an asset or liability in the financial statements for short-term SBITAs. Given these considerations and lack of policies and procedures for identifying, tracking, recording, and reporting SBITAs, we did not perform further review of the two other short-term SBITAs.

- Our review also included an analysis of expenses to identify potential SBITAs requiring recognition. During this review, we identified purchases with two vendors that appear to

qualify as SBITAs. Richard Bland evaluated these arrangements during its implementation of GASB Statement No. 96, but due to the complexity of the contracts, Richard Bland did not make a final determination on whether the arrangements qualified as SBITAs. Further, Richard Bland did not retain any documentation to support its evaluation.

Due to limited financial staff, Richard Bland did not dedicate sufficient resources to gain an adequate understanding of GASB Statement No. 96 requirements and did not develop sufficient controls to appropriately identify, track, record, and report SBITAs. These deficiencies do not have a material impact on the consolidated financial statements for fiscal year 2023; however, if Richard Bland establishes more significant arrangements with vendors in the future, SBITAs could have a more significant effect on the financial statements.

Richard Bland should dedicate the necessary resources to gain an adequate understanding of GASB Statement No. 96 requirements and should develop and implement policies and procedures related to identifying, tracking, recording, and reporting SBITAs. Additionally, Richard Bland should conduct and document a thorough review of its current contracts to properly identify potential SBITAs. Implementing effective corrective action will help ensure accurate and complete financial reporting in accordance with GASB Statement No. 96 during preparation of future fiscal year financial statements.

Commonwealth of Virginia

Auditor of Public Accounts

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

June 17, 2024

The Honorable Glenn Youngkin
Governor of Virginia

Joint Legislative Audit
and Review Commission

Board of Visitors
The College of William and Mary in Virginia

Katherine A. Rowe
President, 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** (the University) as of and for the year ended June 30, 2023, and the related notes to the financial statements, which collectively comprise the University's consolidated basic financial statements and have issued our report thereon dated June 17, 2024. 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 did not audit the financial statements of the 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 the component units of the University.

Report on Internal Control Over Financial Reporting

In planning and performing our audit of the consolidated 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 opinions 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. 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 Service Provider Oversight," "Improve Firewall Security," "Develop and Implement a Service Provider Oversight Process," "Improve Database Security," "Improve IT Risk Management Program," "Improve Reporting to National Student Loan Data System," "Properly Perform Return of Title IV Calculations," "Return Unearned Title IV Funds Timely," "Implement Information Security Program Requirements for the Gramm-Leach-Bliley Act," and "Improve Controls for Accounting and Reporting for Right-to-Use Subscription Assets," 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 and recommendations titled "Improve IT Service Provider Oversight," "Improve Firewall Security," "Develop and Implement a Service Provider Oversight Process," "Improve Database Security," "Improve IT Risk Management Program," "Improve Reporting to National Student Loan Data System," "Properly Perform Return of Title IV Calculations," "Return Unearned Title IV Funds Timely," and "Implement Information Security Program Requirements for the Gramm-Leach-Bliley Act."

The University's Response to Findings

We discussed this report with management at an exit conference held on April 18, 2024, and provided a draft of this report for management's review on July 26, 2024. 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 not taken adequate corrective action with respect to the prior reported findings and recommendations identified as ongoing in the Findings Summaries included in the Appendix. The University has taken adequate corrective action with respect to prior audit findings and recommendations identified as complete in the Findings Summaries included in the Appendix.

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/clj

FINDINGS SUMMARIES

William & Mary

Finding Title	Status of Corrective Action*	First Reported for Fiscal Year
Improve IT Service Provider Oversight	Ongoing	2023

Richard Bland College

Finding Title	Status of Corrective Action*	First Reported for Fiscal Year
Improve Controls over Contract Administration and Management	Complete	2022
Improve Federal Financial Aid Reconciliation Controls	Complete	2022
Improve Firewall Security	Ongoing	2021
Develop and Implement a Service Provider Oversight Process	Ongoing	2021
Improve Database Security	Ongoing	2022
Improve IT Risk Management Program	Ongoing	2022
Improve Reporting to National Student Loan Data System	Ongoing	2023
Properly Perform Return of Title IV Calculations	Ongoing	2023
Return Unearned Title IV Funds Timely	Ongoing	2023
Implement Information Security Program Requirements for the Gramm-Leach-Bliley Act	Ongoing	2023
Improve Controls for Accounting and Reporting for Right-to-Use Subscription Assets	Ongoing	2023

* A status of **Complete** indicates adequate corrective action taken by management. A status of **Ongoing** indicates new and/or existing findings that require management's corrective action as of fiscal year end.

WILLIAM & MARY
CHARTERED 1693

FINANCIAL OPERATIONS

August 5, 2024

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

Dear Ms. Henshaw:

After reviewing William & Mary's fiscal year 2023 audit finding and recommendations, I hereby provide the following response for inclusion in the audit report:

Improve IT Server Provider Oversight

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

Please contact me should you have any questions.

Sincerely,

Melanie T. O'Dell
Chief Financial Officer

Cc: Michael Todd
Ed Aractingi
Kent B. Erdahl

P.O. Box 8795 **Williamsburg, VA 23187-8795** **(757) 221-3210**

Richard Bland College
of WILLIAM & MARY
Office of Finance

August 5, 2024

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, 2023. I hereby provide the following response for inclusion in the audit report:

Improve Firewall Security
Management concurs with the auditor's finding and Richard Bland continues to implement corrective action to address the concerns.

Develop and Implement a Service Provider Oversight Process
Management concurs with the auditor's finding. Richard Bland College is committed to developing and employing effective service provider oversight in alignment with applicable state policies and continues to take measures to improve the process.

Improve Database Security
Management concurs with the auditor's finding and Richard Bland continues to implement corrective action to address the concerns.

Improve IT Risk Management Program
Management concurs with the auditor's finding and Richard Bland continues to implement corrective action to address the concerns.

Improve Reporting to National Student Loan Data System
Management concurs with the auditor's finding and Richard Bland has taken corrective action to address the concerns.

Properly Perform Return of Title IV Calculations
Management concurs with the auditor's finding and Richard Bland has taken corrective action to improve the review process to address the concerns.

Return Unearned Title IV Funds Timely
Management concurs with the auditor's finding and Richard Bland has taken corrective action to improve the review process to address the concerns.

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

Richard Bland College of WILLIAM & MARY

Office of Finance

Implement Information Security Program Requirements for the Gramm-Leach-Bliley Act
Management concurs with the auditor's finding and Richard Bland has taken corrective action to address the concerns.

Improve Controls for Accounting and Reporting for Right-to-Use Subscription Assets
Management concurs with the auditor's finding and Richard Bland has taken corrective action to improve the review process to address the concerns.

Please contact me should you have any questions.

Sincerely,

Stacey A. Sokol
Chief Business Officer

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