



GEORGE MASON UNIVERSITY

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 basic financial statements of George Mason University (University) as of and for the year ended June 30, 2023, and issued our report thereon, dated May 30, 2024. Our report, included in the University's basic financial statements, is available at the Auditor of Public Accounts' website at www.apa.virginia.gov and at the University's website at www.gmu.edu. Our audit found:

- the financial statements are presented fairly, in all material respects;
- one internal control finding requiring management's attention; however, we do not consider it to be a material weakness; and
- no instances of noncompliance or other matters required to be reported under Government Auditing Standards.

Our audit also included testing over the Research and Development Cluster major federal program 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 or instances of noncompliance in relation to this testing.

In the section titled "Internal Control Finding and Recommendation," we have included our assessment of the conditions and causes resulting in the internal control finding identified through our audit, as well as the recommendation for addressing that finding. Our assessment does not remove management's responsibility to perform a thorough assessment of the conditions and causes of the finding and develop and appropriately implement adequate corrective actions to resolve the finding 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 recommendation.

- TABLE OF CONTENTS -

	<u>Pages</u>
AUDIT SUMMARY	
INTERNAL CONTROL FINDING AND RECOMMENDATION	1-2
INDEPENDENT AUDITOR'S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS	3-5
APPENDIX – FINDINGS SUMMARY	6
UNIVERSITY RESPONSE	7-8

INTERNAL CONTROL FINDING AND RECOMMENDATION

Improve IT Risk Management and Contingency Planning Program

Type: Internal Control

Severity: Significant Deficiency

George Mason University (University) does not conduct certain activities as part of its Information Technology (IT) Risk Management and Contingency Planning Program that are required by the University's IT Security Standard (2019) or generally considered requirements of industry standards and best practices. Specifically, we identified the following issues:

- The University does not have risk assessments for all its sensitive systems, including systems that store highly sensitive data or restricted data. The University's IT Security Standard (2019), section 3.11.1, requires the University to periodically assess the risk to organizational operations. By not performing risk assessments, the University increases the risk it will not identify and mitigate existing vulnerabilities before a bad actor could exploit such a vulnerability. A successful compromise could lead to a breach of data and create financial, legal, and reputational damage for the University.
- The University has not developed a System Security Plan (SSP) for all of its sensitive systems as required by its IT Security Standard (2019), section 3.12.4. The University has completed an SSP for the University's Enterprise Resource Planning (ERP) system. However, by not having an SSP for every sensitive system, the University increases the risk of not identifying and implementing proper security controls to secure its systems, and this could lead to a breach of data or unauthorized access to sensitive and restricted data.
- The University does not define recovery point objectives (RPOs) within the Continuity of Operations Plan (COOP) and Disaster Recovery Plan (DRP) for all critical IT applications and systems. Specifically, the University defines a recovery point objective for its ERP system but has not defined recovery point objectives for any other critical IT applications and systems. The University's IT Security Standard (2019), section 3.15.12, requires the University to define recovery time and recovery point objectives. Recovery point objectives are necessary to determine how the University will restore critical IT applications and systems in a prioritized and timely manner. Without defining recovery point objectives, the University may not establish data backup plans to ensure it has recent and accurate data available, recover its data, and resume operations following an incident.

Industry best practices recommend maintaining up-to-date IT Risk Management and Contingency Planning Program documentation to reduce risk related to recovering the essential and primary business functions required to operate effectively in the event of an outage or disaster.

The University is in the process of migrating all IT Risk Management and Contingency Planning Program documentation from the previous system of record to an Integrated Risk Management (IRM) Platform. The University began transitioning to the new IRM platform in 2021 and subsequently

purchased the IRM platform's disaster recovery and business continuity application in November 2022. After configuring the application, the University began moving documents into the IRM platform's disaster recovery and business continuity application in October 2023. Due to the time and resources needed to configure the base functionalities of the IRM platform, as well as the complexity of the transition to the disaster recovery and business continuity application, the University has not completed the migration. Additionally, the University documented and approved a new IT Security Standard in March 2024 to govern all internal policies. However, due to the scale of transferring the IT Risk Management and Contingency Planning Program to the new IRM platform, as well as the resources and interdepartmental coordination required for the transition, the University has not maintained complete and updated IT Risk Management and Contingency Planning Program documentation.

The University should continue to allocate resources to complete its migration to the new IRM platform and improve its IT Risk Management and Contingency Planning Program to include the elements required by its IT Security Standard and industry best practices. Strengthening the IT Risk Management and Contingency Planning Program will help to ensure the continued confidentiality, integrity, and availability of the University's sensitive systems and mission-essential functions.



Commonwealth of Virginia

Auditor of Public Accounts

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

May 30, 2024

The Honorable Glenn Youngkin
Governor of Virginia

Joint Legislative Audit
and Review Commission

Board of Visitors
George Mason University

Gregory Washington
President, George Mason 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 **George Mason University** (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 basic financial statements and have issued our report thereon dated May 30, 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 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 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 a deficiency in internal control titled "Improve IT Risk Management and Contingency Planning Program," which is described in the section titled "Internal Control and Compliance Finding and Recommendation," that we consider to be a significant deficiency.

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 no instances of noncompliance or other matters that are required to be reported under Government Auditing Standards.

The University's Response to Findings

We discussed this report with management at an exit conference held on June 11, 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.

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 SUMMARY

Finding Title	Status of Corrective Action	Fiscal Year First Issued
Improve IT Risk Management and Contingency Planning Program	Ongoing	2023

*A status of **Ongoing** indicates a new or existing finding that requires management's corrective action as of fiscal year end.



4400 University Drive, Fairfax, Virginia 22030
Phone: 703-993-1000; Web: <https://fiscal.gmu.edu/>

June 20, 2024

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

Dear Ms. Henshaw:

We have reviewed the audit findings and recommendations resulting from the fiscal year 2023 audit by the Auditor of Public Accounts (APA) and discussed during the exit conference.

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

Improve IT Risk Management and Contingency Planning Program

George Mason University (University) does not conduct certain activities as part of its Information Technology (IT) Risk Management and Contingency Planning Program that are required by the University's IT Security Standard (2019) or generally considered requirements of industry standards and best practices. Specifically, we identified the following issues:

- The University does not have risk assessments for all its sensitive systems, including systems that store highly sensitive data or restricted data. The University's IT Security Standard (2019), section 3.11.1, requires the University to periodically assess the risk to organizational operations. By not performing risk assessments, the University increases the risk it will not identify and mitigate existing vulnerabilities before a bad actor could exploit such a vulnerability. A successful compromise could lead to a breach of data and create financial, legal, and reputational damage for the University.
- The University has not developed a System Security Plan (SSP) for all of its sensitive systems as required by its IT Security Standard (2019), section 3.12.4. The University has completed an SSP for the University's Enterprise Resource Planning (ERP) system. However, by not having an SSP for every sensitive system, the University increases the risk of not identifying and implementing proper security controls to secure its systems, and this could lead to a breach of data or unauthorized access to sensitive and restricted data.
- The University does not define recovery point objectives (RPOs) within the Continuity of Operations Plan (COOP) and Disaster Recovery Plan (DRP) for all critical IT applications and systems. Specifically, the University defines a recovery point objective for its ERP system but has not defined recovery point objectives for any other critical IT applications and systems. The University's IT Security Standard (2019), section 3.15.12, requires the University to define recovery time and recovery point objectives. Recovery point objectives are necessary to determine how the University will restore critical IT applications and systems in a prioritized and timely manner. Without defining recovery point objectives, the University may not establish data backup plans to ensure it has recent and accurate data available, recover its data, and resume operations following an incident.



Industry best practices recommend maintaining up-to-date IT Risk Management and Contingency Planning Program documentation to reduce risk related to recovering the essential and primary business functions required to operate effectively in the event of an outage or disaster.


The University is in the process of migrating all IT Risk Management and Contingency Planning Program documentation from the previous system of record to an Integrated Risk Management (IRM) Platform. The University began transitioning to the new IRM platform in 2021 and subsequently purchased the IRM platform's disaster recovery and business continuity application in November 2022. After configuring the application, the University began moving documents into the IRM platform's disaster recovery and business continuity application in October 2023. Due to the time and resources needed to configure the base functionalities of the IRM platform, as well as the complexity of the transition to the disaster recovery and business continuity application, the University has not completed the migration. Additionally, the University documented and approved a new IT Security Standard in March 2024 to govern all internal policies. However, due to the scale of transferring the IT Risk Management and Contingency Planning Program to the new IRM platform, as well as the resources and interdepartmental coordination required for the transition, the University has not maintained complete and updated IT Risk Management and Contingency Planning Program documentation.

The University should continue to allocate resources to complete its migration to the new IRM platform and improve its IT Risk Management and Contingency Planning Program to include the elements required by its IT Security Standard and industry best practices. Strengthening the IT Risk Management and Contingency Planning Program will help to ensure the continued confidentiality, integrity, and availability of the University's sensitive systems and mission-essential functions.

Management's Response

The University concurs with the recommended controls and corrective actions. George Mason has a multi-year effort underway that commenced in December 2021, to make comprehensive improvements in IT risk management and contingency planning programs, and will continue to allocate resources to this effort. Senior leaders and the Board of Visitors' Audit, Risk, and Compliance Committee receive regular reports of the progress of these. The program enhancements include steps towards addressing the items cited in this report.

Sincerely,

DocuSigned by:

787A38257099417
Deb Dickenson
Executive Vice President, Finance and Administration