GEORGE MASON UNIVERSITY
AUDIT, RISK, AND COMPLIANCE COMMITTEE OF THE BOARD OF VISITORS

November 19, 2024
AGENDA

I. Call to Order

II. Approval of Audit, Risk, and Compliance Committee Minutes

A. Approval of Committee Minutes for September 26, 2024 Meeting **(ACTION)**

III. New Business

A. Auditor of Public Accounts Examination Discussion

B. Information Technology Update (includes **CLOSED SESSION** regarding security of information technology systems (Code of Virginia: §2.2-3711.A.19))

C. Review of Audit, Risk, and Compliance Committee Charter

D. Approval of Office of Audit and Compliance Charter **(ACTION)**

IV. Reports

A. Report of Approved Waivers of Contractual Conflicts of Interest

B. Report of Compliance with Gramm-Leach-Bliley Act Safeguards Rule

C. Office of University Audit Summary Report

D. Review of Office of University Audit Planning

E. Enterprise Risk Management Program Summary Report

F. Office of Institutional Compliance Summary Report

G. Information Technology Risk and Control Infrastructure Program Update

V. Adjournment

The November 19, 2024 meeting of the Audit, Risk, and Compliance Committee will be held virtually, and may be viewed at https://bov.gmu.edu/live/. In the event of a disruption or failure in the live stream, please call (703)-993-8704 and inform Mason staff of the disruption. Gallery seating and viewing of the session will also be available in Merten Hall 1201. Should the meeting format change, a subsequent notice will be issued in accordance with Virginia Code 2.2-3707.

Written comments will be accepted until the full board meeting adjourns on December 5, 2024. To submit a written public comment, please complete the form at the following link: https://forms.office.com/r/9AcSrVQwiz. Written comments will be entered into the public record of this meeting. ***No oral public comment will be taken at this meeting.***

DRAFT – Subject to Revision

GEORGE MASON UNIVERSITY
AUDIT, RISK, AND COMPLIANCE COMMITTEE
OF THE BOARD OF VISITORS

September 26, 2024
MINUTES

PRESENT: Chair Oberoi, Vice Chair Alacbay, Visitors Brown, Marcus, and Meese.

ABSENT: Visitor Blackman.

ALSO PRESENT: Rector Stimson; Visitors Burke, Pence, Peterson, Short, and Thompson; President Washington; Provost and Executive Vice President Antony; Vice President and Chief Diversity Officer Artis; Undergraduate Student Representative Cuesta; Executive Vice President of Finance and Administration Dickenson; Staff Senate Chair Gautney; Special Advisor Healy; Vice President of Finance Heinle; Graduate Student Representative Hoffman; Vice President and Chief Information Officer Madison; Vice President for Research, Innovation, and Economic Development Marshall; Associate University Counsel Schlam; Faculty Senate President Simmons; Assistant Vice President and Deputy Chief Information Officer Spann; Executive Vice President for Strategic Initiatives and Chief of Staff Walsh; Interim Senior Vice President and Chief Risk Officer Zobel; Chief Audit and Compliance Officer Dittmeier; and Associate Vice President for Institutional Compliance Lacovara.

I. Chair Oberoi called the meeting to order at 9:30 a.m.

II. Approval of Minutes

Chair Oberoi called for any corrections to the minutes of the May 2, 2024 Audit, Risk, and Compliance Committee meeting. Hearing none, the **MINUTES STOOD APPROVED AS WRITTEN.**

III New Business

A. Enterprise Risk Management Program Update

Dr. Zobel reviewed with the Committee highlights related to the enterprise risk management program.

She reminded the Committee the program’s purpose is to identify risks; plan, facilitate, and oversee implementation of response strategies; and provide communication to the President and the Committee. Since the prior Committee meeting, the program has worked with senior leaders and risk owners to facilitate development of mitigation action plans for each of the ten enterprise risks. Ongoing monitoring of internal and external changes in the risk environment has also continued. Funding resources, competition, and cybersecurity remain the high-priority risks for the university. Risk drivers and mitigation actions for these risks were discussed with the Committee. The Committee discussed with management the factors influencing the trends in risk levels for the high priority risks, including the competitive environment for students and for high-performing faculty.

IV. Reports

Chair Oberoi asked for the highlights of the reports received by the Committee to be discussed:

Mr. Dittmeier reported that Derek Butler joined George Mason earlier in September as Deputy University Auditor, succeeding Wendy Watkins who retired recently. Mr. Butler has more than 30 years of internal audit leadership experience, most recently as Chief Auditor of Washington Gas Light, and holds professional certifications as a Certified Internal Auditor and Certified Information Systems Auditor. The portfolio of audit work is being transitioned to Mr. Butler's leadership. Mr. Dittmeier also highlighted that there has been a recent uptick of allegation reports which require investigation; he stated that it was too early to tell whether the uptick represents any systemic concern.

Mr. Lacovara noted there were no significant compliance reports, external reviews, or other matters since the prior Committee meeting. Assessment work is continuing and Institutional Compliance is working with several groups to develop response strategies and action plans related to the Institutional Compliance and Ethics enterprise risk, including assessing the Code of Ethics as well as processes for developing policies, surfacing concerns, and addressing instances of non-compliance.

Dr. Madison described recent IT Risk and Control Infrastructure Program accomplishments which include automation of security awareness training enforcement through password resets, and the establishment and use of domain councils to facilitate governance in George Mason's distributed environment.

VI. Adjournment

Chair Oberoi adjourned the meeting at 9:50 a.m.

Edward R. Dittmeier
Secretary pro tem

ITEM NUMBER: III.A. Auditor of Public Accounts Discussion

PURPOSE OF ITEM: Brief the Audit, Risk, and Compliance Committee regarding the upcoming financial statement audit for the year ended June 30, 2024.

NARRATIVE: The Commonwealth's Auditor of Public Accounts is responsible for auditing the accounts of every state department, officer, board, commission, institution, or other agency handling any state funds. Among other things, the Auditor of Public Accounts determines that state agencies are providing and reporting appropriate information on financial and performance measures.

Zach Borgerding is representing the Auditor of Public Accounts.

ACTION: Receive briefing and discuss.

George Mason Audit, Risk, and Compliance Committee

2024 Financial Statement Audit Entrance Meeting

November 19, 2024

Zach Borgerding, Audit Director

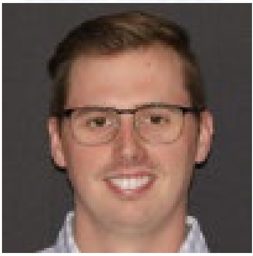
Auditor of Public Accounts

Our Team (Preliminary Staffing)

Zach Borgerding

Project Manager
- Director
- 16 years experience
- Served as GMU PM in 2016/2017
- Other HEI experience: RU, VT, VSU, ODU, VCCS
- Ultimately responsible for audit
- CPA, CISA, CGFM

Justin Rhodes



In-Charge
- Supervisor
- 6.5 years experience
- 4th year assigned to GMU and 3rd year as In-Charge
- Specializes in higher education
- Runs day-to-day audit operations
- CPA and CISA

Carter Ryder

Audit Staff
- Auditor
- 3 years experience (including prior employer)
- 2nd year assigned to GMU
- Specializes in acquisitions and contracts
- VCA and Masters of Accountancy

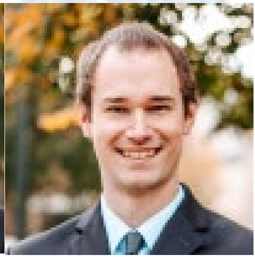
TBD

Audit Staff
- Audit staffing in progress – will add **two** additional general audit staff, at least one ISS auditor, a pension auditor, and a debt auditor
- To inform management when audit team is finalized

April Cassada

Data Reviewer
- Director
- 21 years experience
- Manages and reviews all data retrieval work
- BS in Accounting, CPA, CISA, and CITP

Brian Deveney



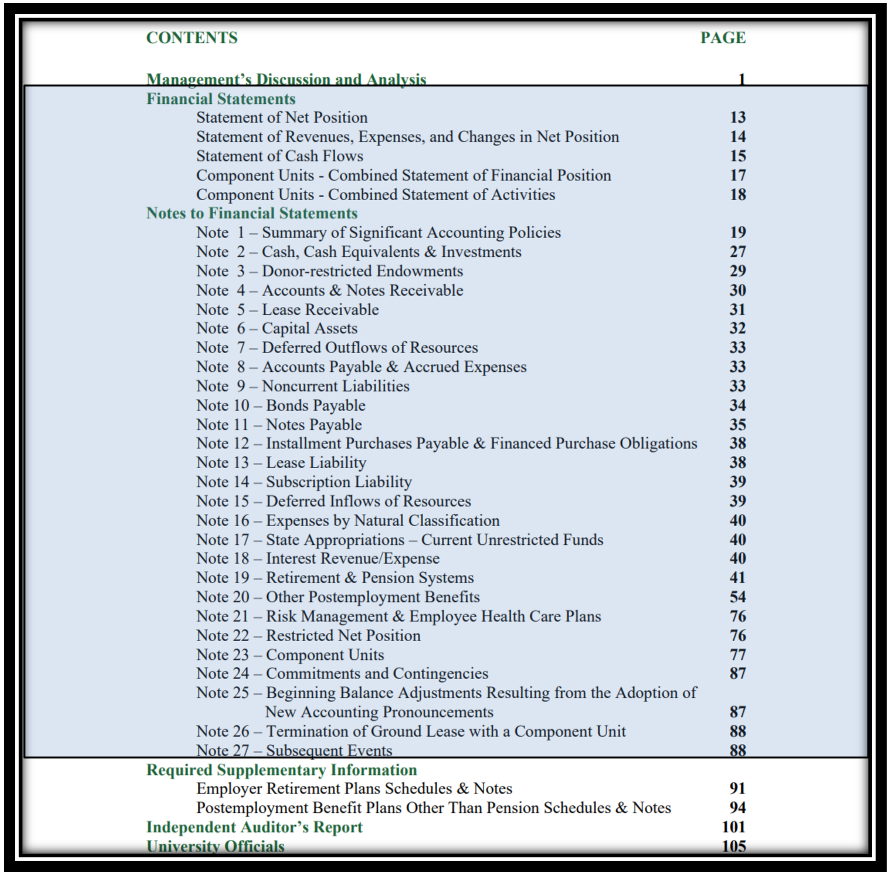
Pension/Debt Reviewer
- Manager
- 11 years experience
- Manages and reviews debt, pensions, and OPEBs for spring HEI projects
- CPA, CISA, Masters of Accountancy

Goran Gusavsson

ISS Reviewer
- Director
- 28 years experience
- Manages and reviews system security work
- BS in Electrical Engineering and Computer Science, MA in ISS, CISM, and CISSP

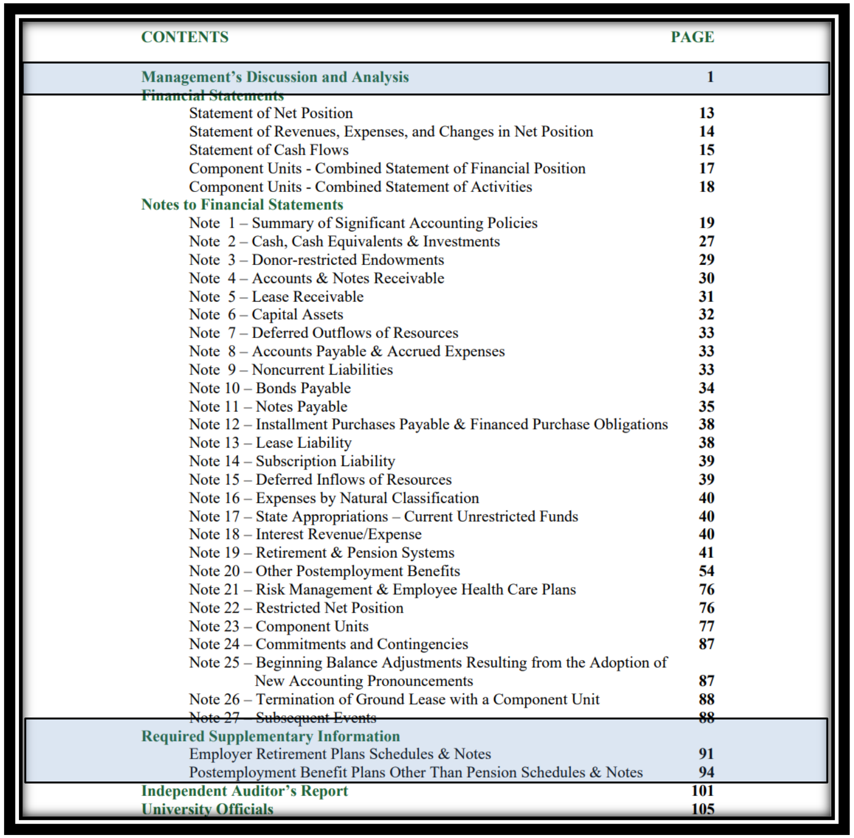
Audit Objectives

- **Basic Financial Statements**
  - Primary objective of audit is to provide an opinion on fair presentation in accordance with GAAP
  - We assess risk of material misstatement at the line item level and design an audit approach responsive to those risks
  - Procedures include a combination of tests of detailed transactions and balances, as well as internal control processes



Audit Objectives

- **Required Supplementary Information (RSI)**
  - We review for consistency with the basic financial statements
  - We perform limited procedures, including management inquiries and review of support
  - We do not provide an opinion concerning RSI



CONTENTS PAGE

Significant Risks

Management Override

- Risk is present at all organizations
- Access controls
- Segregation of duties
- Culture/tone at the top
- Whistleblower communication channels

Revenue Recognition

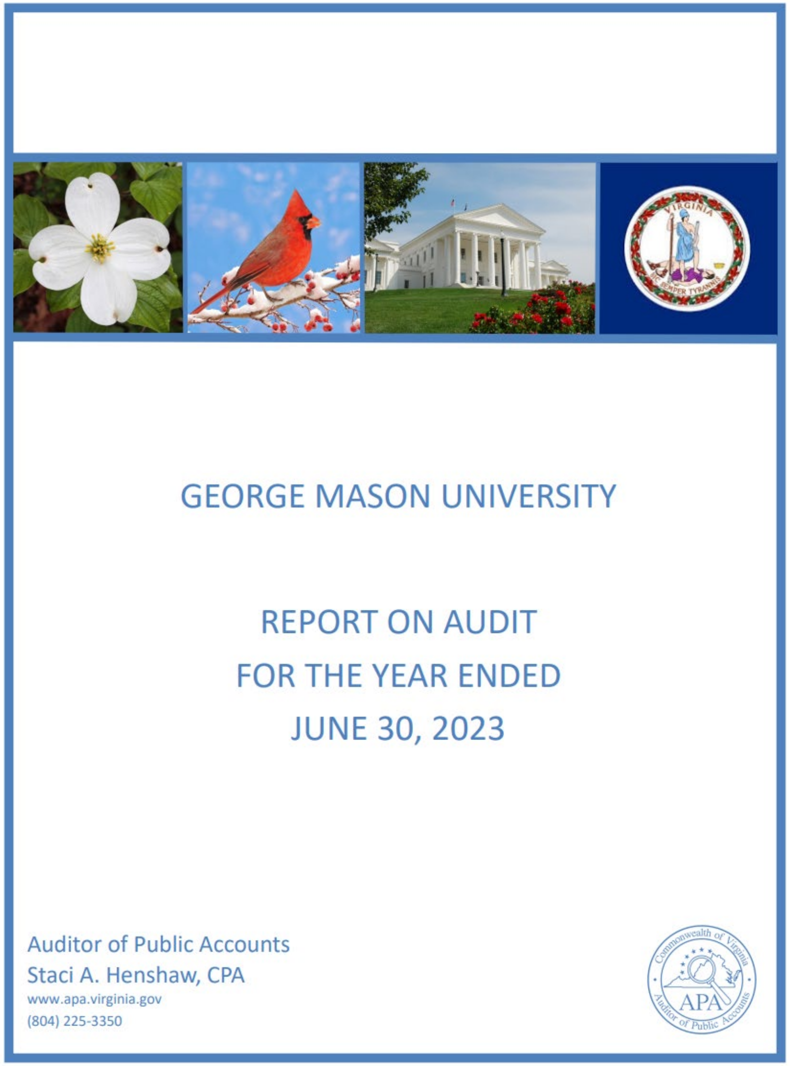
- Risk is present at all universities
- Tuition and fees and auxiliary enterprises demand most attention
- Scholarship allowance moderately complex
- Grants and contracts generally follow non-exchange recognition criteria

Transactions with Component Units

- Purchase of Vernon Smith Hall assets from GMUF is significant ($107 million), infrequent, and moderately complex
- GMUF gifted $58 million to support key University initiatives

Audit Objectives

- **Report on Internal Controls and Compliance**
  - We do not provide an opinion on internal controls
  - We are required to report any findings that we deem to be significant deficiencies or material weaknesses
  - Though not required, we plan to issue this report the same week we release the audit opinion

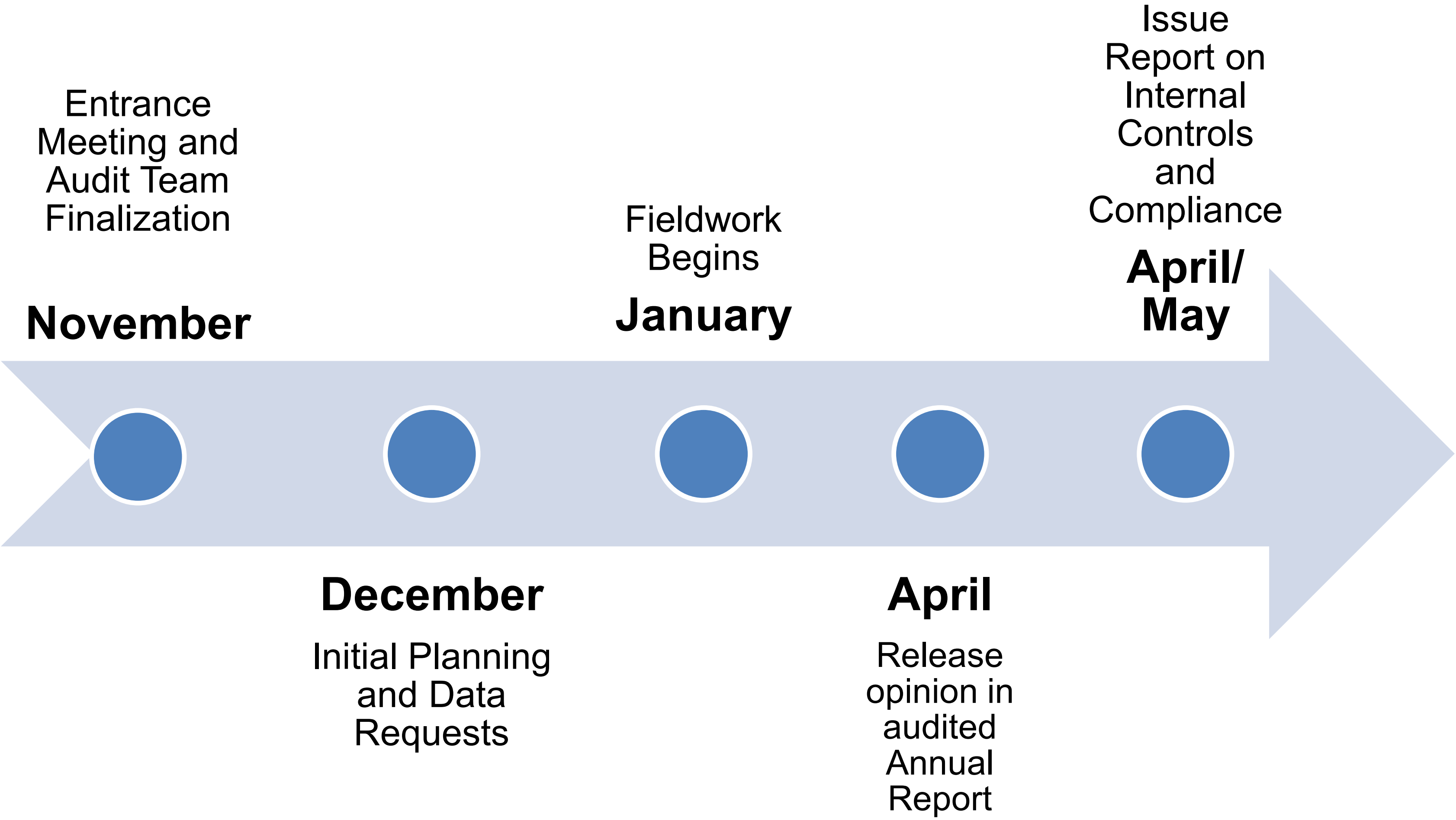


GEORGE MASON UNIVERSITY

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 Timeline



Entrance Meeting and Audit Team Finalization

November

December

Initial Planning and Data Requests

Fieldwork Begins

January

April

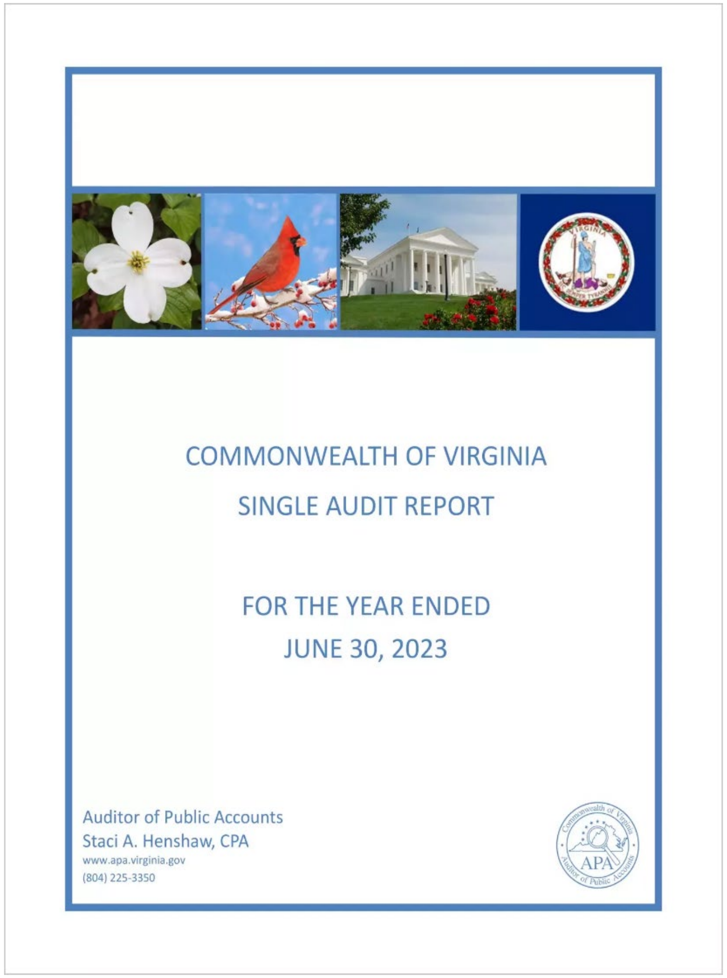
Release opinion in audited Annual Report

Issue Report on Internal Controls and Compliance

April/ May

Other Audit/Attest Engagements

- **Single Audit**
  - The Single Audit report includes our audit of federal funds received by the Commonwealth and serves as the internal control report for the Commonwealth's Annual Comprehensive Financial Report
  - A separate APA audit team is currently auditing the Student Financial Assistance (SFA) Programs Cluster (including George Mason) and will issue a stand-alone report
  - Findings included in the stand-alone SFA report will be carried forward to the Single Audit report
  - Deadline for Single Audit is February 15th



COMMONWEALTH OF VIRGINIA

SINGLE AUDIT REPORT

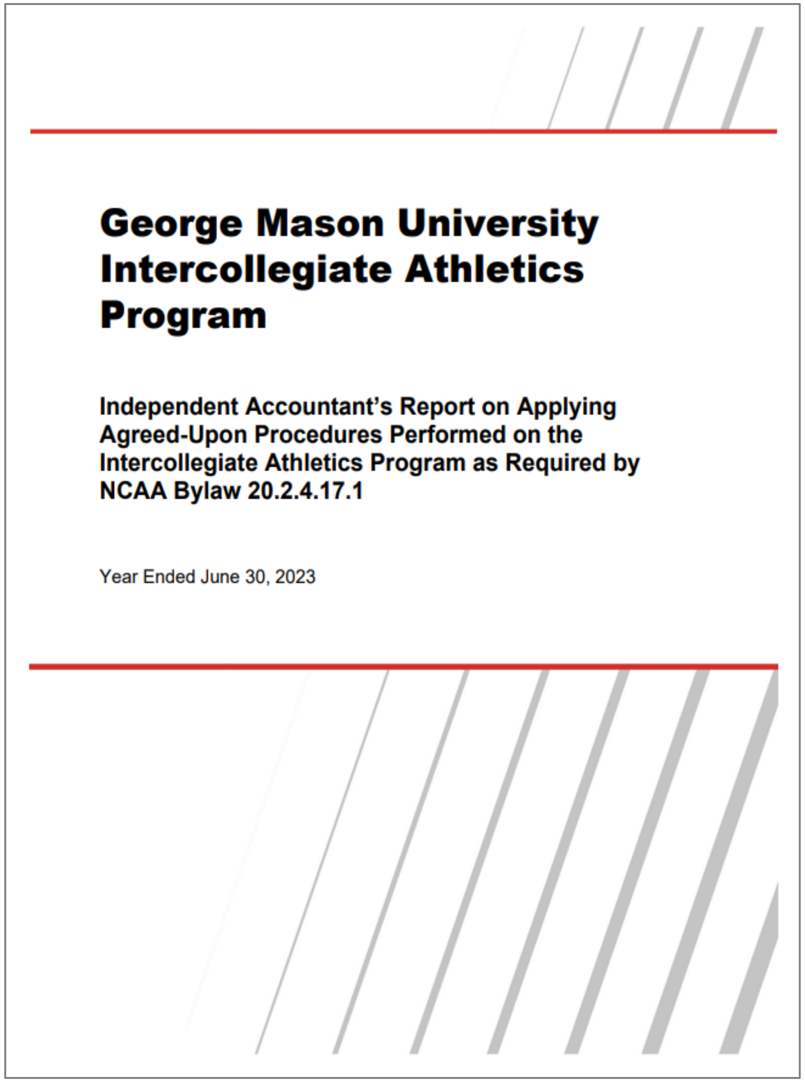
FOR THE YEAR ENDED

JUNE 30, 2023

Auditor of Public Accounts
Staci A. Henshaw, CPA
www.apa.virginia.gov
(804) 225-3350

Other Audit/Attest Engagements

- **Agreed-upon Procedures Report for Athletics**
  - Performed by Forvis Mazars
  - Describes procedures over Statement of Revenues and Expenses and related notes
  - Nearing Completion
  - Preliminary report is provided to APA for review prior to issuance
  - Deadline for submission to NCAA is January 15th



George Mason University Intercollegiate Athletics Program

Independent Accountant's Report on Applying Agreed-Upon Procedures Performed on the Intercollegiate Athletics Program as Required by NCAA Bylaw 20.2.4.17.1

Year Ended June 30, 2023

Management Communication

- Entrance/Exit with Management
- Periodic status updates
- When potential concerns are noted:
  - Confirm condition
  - Obtain response
  - Evaluate magnitude and pervasiveness

Audit, Risk, & Compliance Committee Communication

- If you are aware of risks our audit should address, please share those with us

- Unless there are findings requiring your immediate attention, we will present our results to you at the conclusion of the audit

- If earlier communication is warranted, we will coordinate with management to ensure the Committee is informed in a timely manner

Other Significant Correspondence

- Management will separately agree to the terms of the audit engagement and copy the Committee Chair on the communication

- Management will make written representations to us at the end of the audit and copy the Committee Chair on the communication

Intended Use Statement

This presentation is intended solely for the information and use of those charged with governance and management, and is not intended to be, and should not be, used by anyone other than these specified parties.

GEORGE MASON UNIVERSITY®

Information Technology Update

Board of Visitors – Audit, Risk, & Compliance Committee Meeting – November 19, 2024

Agenda

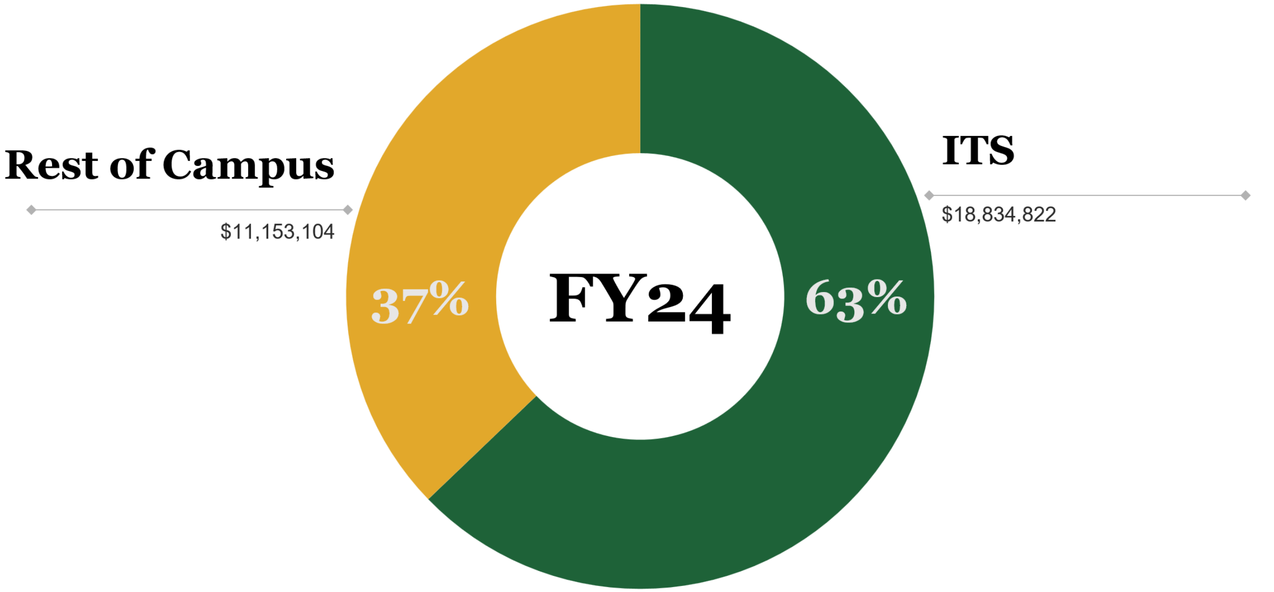
- Mason Information Technology Overview
- Cybersecurity Strategy
- Information Technology Risk and Control Infrastructure Program
- Security Threat Landscape
- Questions and Answers

Information Technology at George Mason University

Mason operates in a distributed IT environment with shared governance

- University Research is conducted within Schools, sometimes with shared IT functions (compute, administration)
  - Schools and Colleges, and some units have IT departments
- Demarcations in governance, roles/responsibility not always clearly defined

Information Technology Expenditures – Annual VITA Report



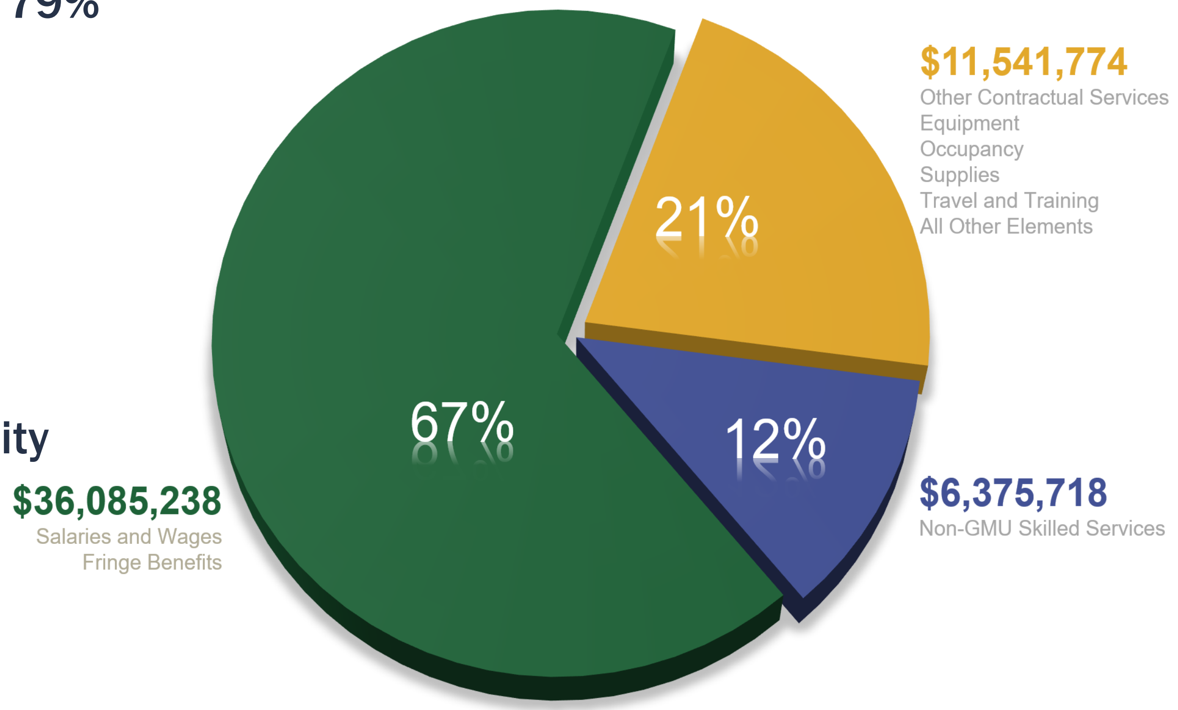
Note: The following accounts codes have been used for comparison: 73720, 73740, 73750, 73760, 73775, 74874, 74883, 74884, 76870, 76873, 76874, 76875, 76876, and 76878.

ITS manages ERP/CRM/HR/PR/LMS/Student

Information Technology Services Structure

- ITS salaries and contractors account for roughly 79% of ITS spend
- ITS employs 269 FTE , 80 student wage, 36 contractors and 28 wage employees
- ITS Units; Academic Strategies, Enterprise Applications, Enterprise Infrastructure Services, Enterprise Service Delivery, Learning Support Services, Information Technology Security Office

ITS Expenditures – Labor vs. Non-Labor E&G Comparison



George Mason Cybersecurity Strategy

Our vision is to establish a robust, proactive cybersecurity strategy that not only protects the integrity, confidentiality, and availability of our data but also fosters a secure environment for learning, research, and innovation.

5 Foundational Pillars

- **Data Protection & Privacy** – Safeguarding sensitive personal, academic, and research data is a top priority.
- **Security Awareness & Training** – A well-informed community is our first line of defense
- **Cutting Edge Cybersecurity Research** – As a hub of innovation, we are committed to advancing the field of cybersecurity through interdisciplinary research
- **Technology & Infrastructure** – Our strategy involves continuous investment in cutting-edge cybersecurity technologies, including AI-driven threat detection, network security, and incident response systems, to ensure the university's infrastructure remains resilient and adaptive to evolving threats.
- **Collaboration & Partnership** – We aim to build strong partnerships with government agencies, industry leaders, and other educational institutions to share knowledge, best practices, and resources in cybersecurity. Together, we can stay ahead of emerging cyber threats.

GEORGE MASON UNIVERSITY®

IT Risk and Control Infrastructure Program

November 2024

Information Technology Risk and Control Infrastructure Program
Strategic Programs of Focus

Most outstanding IT Security audit findings have common structural roots in underlying business processes and systems

- George Mason Scoped and Tailored NIST 800-53-Based Security Compliance Framework
- Portfolio and Project Management
- IT Security Program Management
- Change and Configuration Management
- Identity Management and Access Control
- Risk Assessment and Remediation

George Mason Scoped and Tailored NIST 800-53-Based Security Compliance Framework

FY2024 Activities/Accomplishments

- George Mason Scoped and Tailored NIST 800-53-Based Security Compliance Framework published and beginning of operationalization through release of the updated IT Security Standard.
- In partnership with Risk, Safety, and Resilience team, start of transition of Business Continuity and Disaster Recovery (BC/DR) and Continuity of Operations (COOP) documentation from Kuali to Archer Integrated Risk Management (IRM) platform.
- Banner Core controls assessment conducted to the updated framework and baselines.

FY2025 Planned Initiatives

- Operationalize risk workflows in Archer.
- Focus on APA MP01 remediation activities.

Portfolio and Project Management

FY2024 Activities/Accomplishments

- Introduction of the Domain Councils (DC) concept and operationalization.
- Project Management Module moved into TeamDynamix (TDX) to establish linkage between TDX Project Intake and Project Process Methodology.

FY2025 Planned Initiatives

- Work towards operationalizing Enterprise and the Provost Administration Domain Councils.
- Prepare to launch the Schools & Colleges Domain Council (SCDC) by FY25 Q3.
- Align processes of Facilities, Space, and IT project requests to support Executive Administration Committee (EAC).
- Roll out TeamDynamix automation to support DC1 and DC2 of the Domain Council process to streamline intake and review of requests.

IT Security Program Management

FY2024 Activities/Accomplishments

- Launched project to achieve compliance enforcement for mandatory IT Security Awareness training through automated mechanism.
- Rubrik backup services implemented for Microsoft 365 service.
- Review conducted to evaluate existing Microsoft 365 controls for enhancements and industry best practices.

FY2025 Planned Initiatives

- Completed project for mandatory IT Security Awareness training automated enforcement. As of July 2024, the process is live and operational.
- Finalize the scope and the statement of work for the penetration test.

Change and Configuration Management

FY2024 Activities/Accomplishments

- Transitioned the Change Management process from the legacy Change Management Database (CMDB) to TeamDynamix to align with industry best practices and compliance requirements.
- Banner Change Advisory Board (CAB) established.
- Center for Internet Security (CIS) benchmark-based Windows 11 consensus security baselines created.

FY2025 Planned Initiatives

- Enhance the current Service Catalog to enable search of ITS.gmu.edu across TeamDynamix and WordPress catalogs providing better results and user experience.

Identity and Access Management

FY2024 Activities/Accomplishments

- Socialized and championed the need for an Identity Access Management program.
  - Project #867: Selection and implementation of an Identity Access Governance tool.
  - Project #866: Establish an IAM program.

FY2025 Planned Initiatives

- Both projects associated with this program area are currently on hold for funding and resource prioritization approvals.

Risk Assessment and Remediation Program

FY2024 Activities/Accomplishments

- Began workflow enhancements in Archer IRM to support risk assessments and issues management.
- Creation of FAR 52-204.21 compliance security plan template for the Hopper High Performance Cluster (HPC) to position Mason to be able to support research grant requests that require compliance to the FAR 52-204.21 controls.

FY2025 Planned Initiatives

- Completed – GLBA and FTI assessment
- MP01 remediation activities for the finding issued by the Virginia Auditor of Accounts (APA) continue to be prioritized. These activities include conducting system risk assessments, creating System Security Plans (SSPs), and documenting Recovery Point Objectives (RPOs) for systems that meet the categorization criteria.

GEORGE MASON UNIVERSITY

Motion:

I move that the Audit, Risk, and Compliance Committee go into Closed Session under the provisions of Section 2.2-3711.A.19 of the Code of Virginia to discuss the security of university information technology systems.

GEORGE MASON UNIVERSITY

Motion:

I move that the Audit, Risk, and Compliance Committee go back into Public Session and further move that by ROLL CALL VOTE we affirm that only public business matters lawfully exempted from the open meeting requirements under the Freedom of Information Act were heard, discussed or considered in the Closed Meeting, and that only such business matters that were identified in the motion to go into a Closed Meeting were heard, discussed, or considered in the Closed Meeting. Any member of the Committee who believes that there was a departure from the requirements as stated above, shall so state prior to taking the roll call, indicating the substance of the departure that, in their judgment, has taken place.

Questions

ITEM NUMBER: III.C. Review of Audit, Risk, and Compliance Committee Charter

PURPOSE OF ITEM: This item facilitates the Committee’s review of its charter.

NARRATIVE: The Audit, Risk, and Compliance Committee’s charter was last approved in September 2023.

- The charter requires the Committee to review the charter annually and update as necessary.

No revisions are recommended to the Committee.

The charter continues to align with the university’s bylaws which have not changed since the last approval in September 2023.

RECOMMENDATION: Review Audit, Risk, and Compliance Committee Charter. No action is recommended.

GEORGE MASON UNIVERSITY BOARD OF VISITORS
AUDIT, RISK, and COMPLIANCE COMMITTEE CHARTER

I. PURPOSE

The purpose of the Audit, Risk, and Compliance Committee is to assist the Board of Visitors in fulfilling its oversight responsibilities for:

- the financial reporting process;
- the system of internal controls;
- internal and external auditing;
- institutional compliance processes that monitor compliance with laws and regulations; and
- enterprise risk management processes that assess significant risks to the University and the steps management has taken to monitor and control such risks.

The function of the Audit, Risk, and Compliance Committee is oversight. University management is responsible for (i) preparation, presentation, and integrity of the University's financial statements; (ii) maintenance and implementation of effective policies, procedures, and controls designed to assure compliance with generally accepted accounting principles and applicable laws and regulations; and (iii) identification, assessment, monitoring, and management of significant enterprise-level risks to the University.

II. COMPOSITION

The Audit, Risk, and Compliance Committee will consist of three or more Visitors determined annually by the Board of Visitors. The Rector shall appoint the Chair and Vice Chair subject to confirmation by the Board of Visitors. Each committee member shall be independent as defined by the Board of Visitors. At least one member shall be financially literate as defined by the Board of Visitors.

III. MEETINGS

The schedule of Committee meetings is determined annually by the Board of Visitors; additional meetings may occur as determined by the Committee Chair. The Committee Chair should meet with the Chief Audit and Compliance Officer as necessary and at least prior to each Committee meeting. Committee actions will be reported to the Board of Visitors with such recommendations as the Committee may deem appropriate. The Committee may meet in closed session in accordance with state law.

IV. RESPONSIBILITIES

In fulfilling its oversight responsibilities, the Audit, Risk, and Compliance Committee shall:

A. General

1. Adopt the Committee's Charter. The charter should be reviewed annually and updated as necessary.

2. Conduct or authorize its own investigations into issues related to its responsibilities and, as necessary, retain independent advisors to advise the Committee.

3. Approve the Office of Audit and Compliance Charter. The charter should be reviewed annually and updated as necessary.

B. Financial Reporting Oversight

1. Review and discuss with management and the University's independent auditors, the Auditor of Public Accounts:

   a. The University's annual financial statements, including footnotes, the University's significant accounting policies, and disclosures made in Management's Discussion and Analysis.

   b. The Auditor of Public Accounts' audit of the financial statements, including their report on internal control over financial reporting and on compliance and other matters.

   c. The effectiveness of the university's system of internal controls over financial reporting.

   d. Any difficulties or disputes with management encountered during the audit.

C. Enterprise Risk Management and Internal Control Oversight

1. Review and discuss with management and the Chief Audit and Compliance Officer:

   a. The effectiveness of the University's process for identifying and assessing significant enterprise-level risks or exposures and the steps management has taken to monitor and control such risks to the University.

   b. The effectiveness of the University's internal controls, including the status and adequacy of information systems and security.

c. The status and timing of management’s actions to monitor and control significant enterprise-level risks and implement recommendations related to internal controls.

2. Review and discuss with management the results of significant reviews by regulatory agencies or other external entities, or summaries thereof, and management’s responses.

D. Institutional Compliance Oversight

1. Review and discuss with management, the University Counsel, and the Chief Audit and Compliance Officer:

   a. The effectiveness of the institutional compliance processes for monitoring compliance with laws and regulations, including policies and processes related to ethics and conflicts of interest.

   b. The status and timing of management’s actions to monitor and control significant compliance risks.

2. Review and consult, as necessary, with the University Counsel and others regarding any legal or regulatory matters significant to the University.

E. Internal Auditing Oversight

1. Assess the internal audit function’s independence and reporting relationships.

2. Review and approve the process for establishing risk-based internal audit plans. Review and discuss with the Chief Audit and Compliance Officer the scope and plans for audits established under this process and factors, including the adequacy of financial and staffing resources, which may affect the effectiveness and timeliness of such audits.

3. Review significant reports to management prepared by the internal audit function, or summaries thereof, and management’s responses.

4. Review and discuss with the Chief Audit and Compliance Officer any difficulties encountered, such as restrictions on the scope of the work or access to information.

5. Review and approve the appointment, replacement, performance, and compensation of the Chief Audit and Compliance Officer, who shall report

directly to the Committee for functional purposes, but may report to the University President for administrative purposes.

V. BYLAWS

In the event of a conflict between this Audit, Risk, and Compliance Committee Charter and the Bylaws of the Board of Visitors, the Bylaws shall control.

Effective Date: September 28, 2023

ITEM NUMBER: III.D. Approval of Office of Audit and Compliance Charter

PURPOSE OF ITEM: This item requests Committee approval of the Office of Audit and Compliance charter.

NARRATIVE: The Committee's Charter requires the Committee to review annually, and update as necessary, the charter for the university's Office of Audit and Compliance.

- The charter was last approved in September 2023.
- The Institute of Internal Auditors has enhanced the International Professional Practices Framework via a comprehensive revision of the Global Internal Audit Standards, effective January 2025.
- The proposed changes to the charter are designed to conform to the revised Standards related to the Committee's approval and oversight of internal auditing at George Mason.
- The proposed changes will also align with the directives of the Office of the State Inspector General.

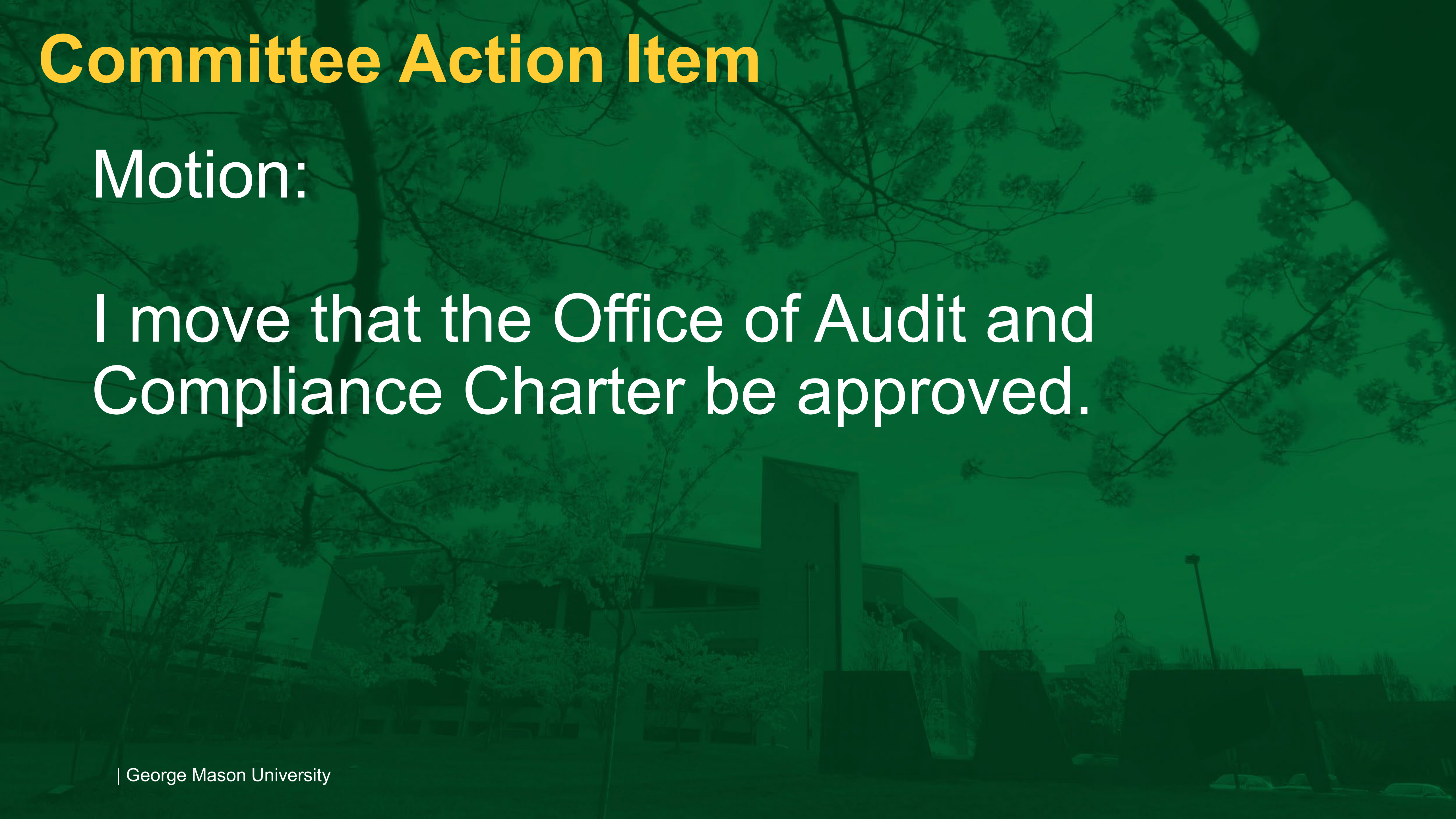
The proposed charter has been reviewed with President Washington; he is fully supportive of the charter and is committed to providing the Office of Audit and Compliance with the necessary independence, stature, and access to university personnel and resources to accomplish its responsibilities to the Audit, Risk, and Compliance Committee.

<u>Organizational Independence Confirmation:</u> Annually, the Chief Audit and Compliance Officer must confirm the organizational independence of the internal audit function.
It is.

- Clear functional reporting to the Audit, Risk, and Compliance Committee, with full and free access to the Committee.
- Demonstrated oversight by the Audit, Risk, and Compliance Committee.
- Freedom from interference in determining internal audit risk assessments; audit selection and scheduling; audit scope, procedures, frequency, and timing; and audit reporting.
- Unrestricted access to all functions, data, records, information, reports, property, and personnel.
- Non-performance of management or operational responsibilities, including directing any non-Office of Audit and Compliance personnel.

RECOMMENDATION: Approval of the Office of Audit and Compliance charter.

Committee Action Item



Motion:

I move that the Office of Audit and Compliance Charter be approved.

GEORGE MASON UNIVERSITY

OFFICE OF AUDIT AND COMPLIANCE CHARTER

Adopted by the Audit, Risk, and Compliance Committee of the Board of Visitors

Dolly Oberoi, Chairman,
Audit, Risk, and Compliance Committee

Date

University Management is fully supportive of the Office of Audit and Compliance in the accomplishment of its mission to assist the Board of Visitors and the Board's Audit, Risk, and Compliance Committee with fulfilling their oversight responsibilities through the provision of independent and objective risk-based assurance services; and planning and oversight of the university's institutional compliance and ethics program. Through its administrative reporting relationship, the Office of Audit and Compliance will have the necessary independence, stature, and access to university personnel and resources to accomplish its responsibilities to the Audit, Risk, and Compliance Committee.

Gregory Washington, President

11/4/24

Date

Purpose:

The Office of Audit and Compliance (OAC) provides risk-based assurance services through independent and objective internal audits; advisory activities; and planning and oversight of the university's institutional compliance and ethics program. It is designed to assist George Mason University's Board of Visitors and the Board's Audit, Risk, and Compliance Committee with fulfilling their oversight responsibilities.

Mission and Mandate:

OAC's mission is to strengthen George Mason's ability to create, enhance, protect, and sustain organizational value by providing risk-based assurance, advice, and insight as follows:

Audit:	Provides independent, objective, risk-based assurance and advisory services designed to add value and improve the university's operations. OAC utilizes a systematic, disciplined, and collaborative approach to evaluate and improve the effectiveness of university governance, risk management, control, and compliance processes.
Institutional Compliance:	Provide oversight of the university's institutional compliance program and the distributed processes that support compliance throughout the university by: • Planning, facilitating, and overseeing regular university-wide assessments of compliance risks, and ensuring management ownership for monitoring and managing compliance risks. • Advising risk owners in their design and implementation of risk-based distributed compliance programs, and evaluating the effectiveness of such risk-owner programs to monitor and manage compliance risks in consideration of legal and regulatory effectiveness requirements. • Ensuring the effectiveness of the institutional compliance program as well as significant compliance risks or exposures and the steps management has taken to monitor and control such risks are communicated to the President and the Audit, Risk, and Compliance Committee.
Ethics and Conflict of Interest Management:	Provide oversight of the university-wide processes that promote an ethical climate, including the university's code of ethics and policies for conflicts of interest and conflicts of commitment, and facilitating conflict evaluation and management processes.

Independence:

To provide for the independence of the OAC, the Chief Audit and Compliance Officer reports functionally to the Audit, Risk, and Compliance Committee of the Board of Visitors and administratively to the President.

The Audit, Risk, and Compliance Committee (i) approves the OAC Charter, and the appointment, replacement, performance, and compensation of the Chief Audit and Compliance Officer, and (ii) reviews the Chief Audit and Compliance Officer's confirmation of the organizational independence of the internal audit function; the internal audit process for establishing risk-based audit plans; the internal audit financial and staffing budget; and reports of significant findings and recommendations; among other things.

University management is responsible for, among other things, (i) the preparation, presentation, and integrity of the University's financial statements; (ii) the maintenance and implementation of effective policies, procedures, and controls designed to ensure compliance with generally accepted accounting principles and applicable laws and regulations; and (iii) the identification, assessment, monitoring, and management of significant enterprise-level risks to the University. OAC supports management by providing oversight, facilitation, coordination, advice, assurance, and reporting for the President and the Audit, Risk, and Compliance Committee. Accordingly, the OAC is prohibited from having management responsibility for any university operational areas and related management decisions. Administrative matters do not include, among other things, matters of audit risk assessments; audit selection and scheduling; audit scope, procedures, frequency, and timing; and audit reporting.

Authority:

The Chief Audit and Compliance Officer and OAC staff are authorized to:

- Have unrestricted access to all functions, data, records, information, reports, property, and personnel.
- Have full and free access to the Audit, Risk, and Compliance Committee.
- Allocate resources, set frequencies, select subjects, determine scope of work, and apply the techniques required to accomplish audit and institutional compliance program objectives.
- Obtain the assistance of university personnel as well as other specialized services from within or outside the university.

The Chief Audit and Compliance Officer and OAC staff are not authorized to:

- Perform any operational duties for the university.
- Initiate or approve accounting transactions external to the OAC.
- Direct the activities of any university personnel not employed by the OAC.

Standards of Practice:

The OAC conducts its internal audit work to conform to (i) the directives of the Commonwealth of Virginia's Office of the State Inspector General and (ii) the mandatory elements of the Institute of Internal Auditors' International Professional Practices Framework, which are the Global Internal Audit Standards and Topical Requirements. To assess such conformance, the Office of University Audit maintains a quality assurance and improvement program that includes (i) internal self-assessments and (ii) external assessments performed by independent third-party assessors. The quality assurance and improvement program covers all aspects of internal audit activities. Results of the quality assurance and improvement program are communicated to management and the Audit, Risk, and Compliance Committee.

The OAC conducts work related to the university's institutional compliance program to achieve effective, risk-based implementation of legal and regulatory compliance program effectiveness requirements.

Effective Date:

This charter is effective November 19, 2024. The charter will be reviewed annually and revised when necessary.

GEORGE MASON UNIVERSITY

OFFICE OF AUDIT AND COMPLIANCE CHARTER

Adopted by the Audit, Risk, and Compliance Committee of the Board of Visitors

____ _________________________

Dolly Oberoi, Chairman,
Audit, Risk, and Compliance Committee

Date

University Management is fully supportive of the Office of Audit and Compliance in the accomplishment of its mission to assist the Board of Visitors and the Board's Audit, Risk, and Compliance Committee with fulfilling their oversight responsibilities through the provision of independent and objective risk-based assurance services; and planning and oversight of the university's institutional compliance and ethics program. Through its administrative reporting relationship, the Office of Audit and Compliance will have the necessary independence, stature, and access to university personnel and resources to accomplish its responsibilities to the Audit, Risk, and Compliance Committee.

____ _________________________

Gregory Washington, President

Date

~~Introduction~~Purpose:

The Office of Audit and Compliance (OAC) provides risk-based assurance services through independent and objective internal audits; advisory activities; and planning and oversight of the university's institutional compliance and ethics program. It is designed to assist George Mason University's Board of Visitors and the Board's Audit, Risk, and Compliance Committee with fulfilling their oversight responsibilities.

Mission and Mandate:

OAC's mission is to strengthen George Mason's ability to create, enhance, ~~and~~ protect, and sustain organizational value by providing risk-based assurance, advice, and insight as follows:

Audit:	Provides independent, objective, risk-based assurance and advisory services designed to add value and improve the university's operations. OAC utilizes a systematic, disciplined, and collaborative approach to evaluate and improve the effectiveness of university governance, risk management, control, and compliance processes.
Institutional Compliance:	Provide oversight of the university's institutional compliance program and the distributed processes that support compliance throughout the university by: • Planning, facilitating, and overseeing regular university-wide assessments of compliance risks, and ensuring management ownership for monitoring and managing compliance risks. • Advising risk owners in their design and implementation of risk-based distributed compliance programs, and evaluating the effectiveness of such risk-owner programs to monitor and manage compliance risks in consideration of legal and regulatory effectiveness requirements. • Ensuring the effectiveness of the institutional compliance program as well as significant compliance risks or exposures and the steps management has taken to monitor and control such risks are communicated to the President and the Audit, Risk, and Compliance Committee.
Ethics and Conflict of Interest Management:	Provide oversight of the university-wide processes that promote an ethical climate, including the university's code of ethics and policies for conflicts of interest and conflicts of commitment, and facilitating conflict evaluation and management processes.

Independence:

To provide for the independence of the OAC, the Chief Audit and Compliance Officer reports functionally to the Audit, Risk, and Compliance Committee of the Board of Visitors and administratively to the President.

The Audit, Risk, and Compliance Committee (i) approves the OAC Charter, and the appointment, replacement, performance, and compensation of the Chief Audit and Compliance Officer, and (ii) reviews the Chief Audit and Compliance Officer's confirmation of the organizational independence of the internal audit function; the internal audit process for establishing risk-based audit plans; the internal audit financial and staffing budget; and reports of significant findings and recommendations; among other things.

University management is responsible for, among other things, (i) the preparation, presentation, and integrity of the University's financial statements; (ii) the maintenance and implementation of effective policies, procedures, and controls designed to ensure compliance with generally accepted accounting principles and applicable laws and regulations; and (iii) the identification, assessment, monitoring, and management of significant enterprise-level risks to the University. OAC supports management by providing oversight, facilitation, coordination, advice, assurance, and reporting for the President and the Audit, Risk, and Compliance Committee. Accordingly, the OAC is prohibited from having management responsibility for any university operational areas and related management decisions. Administrative matters do not include, among other things, matters of audit risk assessments; audit selection and scheduling; audit scope, procedures, frequency, and timing; and audit reporting.

Authority:

The Chief Audit and Compliance Officer and OAC staff are authorized to:

- Have unrestricted access to all functions, data, records, information~~data~~, reports, property, and personnel.
- Have full and free access to the Audit, Risk, and Compliance Committee.
- Allocate resources, set frequencies, select subjects, determine scope of work, and apply the techniques required to accomplish audit and institutional compliance program objectives.
- Obtain the assistance of university personnel as well as other specialized services from within or outside the university.

The Chief Audit and Compliance Officer and OAC staff are not authorized to:

- Perform any operational duties for the university.
- Initiate or approve accounting transactions external to the OAC.
- Direct the activities of any university personnel not employed by the OAC.

Standards of Practice:

The OAC conducts its internal audit work to conform to (i) the directives of the Commonwealth of Virginia's Office of the State Inspector General and (ii) the mandatory elements ~~professional guidance~~ of the Institute of Internal Auditors' International Professional Practices Framework, which are the Global Internal Audit Standards and Topical Requirements.~~including: the Definition of Internal Auditing; Code of Ethics; and the Core Principles and the International Standards for the Professional Practice of Internal Auditing.~~ To assess such conformance, the Office of University Audit maintains a quality assurance and improvement program that includes (i) internal self-assessments and (ii) external assessments performed by independent third-party assessors. The quality assurance and improvement program covers all aspects of internal audit activities. Results of the quality assurance and improvement program are communicated to management and the Audit, Risk, and Compliance Committee.

The OAC conducts work related to the university's institutional compliance program to achieve effective, risk-based implementation of legal and regulatory compliance program effectiveness requirements.

Effective Date:

This charter is effective November 19, 2024~~September 28, 2023~~. The charter will be reviewed annually and revised when necessary.

OFFICE OF AUDIT AND COMPLIANCE
George Mason University

Office of Institutional Compliance
4400 University Drive, MS 1A2, Fairfax, Virginia 22030

MEMORANDUM

TO: Members of the Audit, Risk, and Compliance Committee of
George Mason University's Board of Visitors

FROM: George Mason University Office of Institutional Compliance
Elizabeth Woodley, University Ethics Officer and Outside Interests Manager

SUBJECT: Approved Contractual Conflict of Interest Waivers

DATE: November 1, 2024

Pursuant to the Board of Visitors Resolution adopted on August 1, 2014 (Appendix A) delegating to the President the authority to approve waivers of conflicts of interest arising from contracts pursuant to §2.2-3106 and §2.2-3110 of the Code of Virginia, the following is a report of existing approved contractual conflict of interest (COI) waivers at George Mason University (George Mason) as of October 1, 2023.

There are three categories of COI waivers at George Mason:

- Intellectual Property COI waivers: these are waivers of employee conflicts of interest in contracts for research and development or commercialization of intellectual property (§2.2-3106.C.8).
- Other Contractual COI waivers: these are waivers of conflicts of interest in other contracts, not relating to intellectual property (§2.2-3110).
- Immediate Family Waivers: these are waivers of employment of immediate family members at George Mason (§2.2-3106.C.2).

Intellectual Property COI waivers are reviewed and recommended for approval by the Conflict of Interest Committee[1], prior to being approved by the President and the Vice President for Research, Innovation, and Economic Impact. As a condition of each waiver, the employee will not participate, or has no authority to participate, in contract negotiations or oversight on behalf of George Mason or the outside entity. The employee will also follow the requirements of the Outside Employment Policy or Conflict of Commitment Policy, as applicable. All Intellectual Property COI waivers are monitored at least annually by the Office of Institutional Compliance to confirm the terms of the waivers are followed. Appendix B of this report lists the 20

[1] The Conflict of Interest Committee consists of 14 members: representatives of each College as well as Human Resources, Fiscal Services, Research, and Institutional Compliance.

Intellectual Property COI waivers existing as of October 1, 2023; there were 22 Research COI waivers existing as of November 1, 2023 (the prior report to the Committee).[2]

Other Contractual COI waivers are reviewed and recommended for approval by the Conflict of Interest Committee, prior to being approved by the President and the Executive Vice President for Finance and Administration. As a condition of each waiver, the employee will not participate, or has no authority to participate, in contract negotiations or oversight on behalf of George Mason or the outside entity. The employee will also follow the requirements of the Outside Employment Policy or Conflict of Commitment Policy, as applicable. All Contractual COI waivers are monitored at least annually by the Office of Institutional Compliance to confirm the terms of the waivers are followed. Appendix C of this report lists the 32 Other Contractual COI waivers existing as of October 1, 2024; there were 28 Non-Research COI waivers existing as of November 1, 2023.

Immediate Family Waivers are granted by the University Ethics Officer and Outside Interests Manager when, upon evaluation with the responsible supervisor, it is determined that the dual employment of the immediate family members is in the best interest of the University. The terms of all immediate family waivers require that both immediate family members are engaged in teaching, research, or administrative support positions; neither employee has the sole authority to supervise, evaluate, or make personnel decisions regarding the other, including decisions regarding initial appointment, retention, promotion, tenure, salary, leave of absence, and evaluation; and that the employment of the immediate family members is in the best interests of the institution and the Commonwealth. All immediate family waivers are monitored annually by the Office of Institutional Compliance to confirm the terms of the waivers are followed. Appendix D of this report lists the 139 immediate family waivers existing as of October 1, 2024; there were 134 immediate family waivers existing as of November 1, 2023. Of the 139 immediate family waivers existing on October 1, 2024:

- 51 waivers involve at least one tenured faculty member. In these cases, the other family member was a tenured faculty member (20), non-tenured instructional or research faculty member (20), or not a member of the instructional or research faculty (i.e., administrative or staff, 11).
- 35 waivers involved no tenured faculty and at least one family member being a non-tenured instructional or research faculty member. In these cases, the other family member was a non-tenured instructional or research faculty member (18), or not a member of the instructional or research faculty (i.e., administration or staff, 17).
- 53 waivers involved both family members being members of the administration or staff.

Highlighted Waivers: As of October 1, 2024, there were 6 Intellectual Property or Other Contractual COI waivers (Appended) where the contract giving rise to the COI has the following characteristics:

- the parties are George Mason and a for-profit company,
- the contract is potentially related to the conflicted employee's work at George Mason,
- the contract is negotiated (rather than routine or boilerplate),

[2] Virginia's Conflict of Interests and Ethics Advisory Council informed George Mason in 2024 that rather than all contracts relating to research, it was only contracts for research and development and commercialization of *intellectual property* which fall under §2.2-3106.C.8.

- the conflicted employee is Faculty or Classified Staff (i.e., not adjunct, or wage employee) with ownership in the for-profit company, and
- George Mason is paying over $5,000 to that company.

1. Paul Allvin, Vice President and Chief Brand Officer, Office of University Branding;
Brynmor Holdings, LLC;
waiver period: 2/1/2023–1/31/2025 ($14,800 paid by George Mason in FY 2024)
Personal interest: Allvin has 100% ownership in Brynmor Holdings, LLC through his spouse. Brynmor has been contracted to consult with George Mason on the provision of childcare services and to potentially support George Mason in the application for a federal grant. Allvin will have no authority over this contract and will recuse himself from any decisions or discussions which directly involve or affect Brynmor.

2. Vanessa Blair-Lewis, Head Coach Women's Basketball;
Shoot360;
waiver period: 7/20/2024–7/1/2025 ($4,950 paid by George Mason in FY 2024)
Personal interest: Blair-Lewis has 50% ownership in Shoot360 through her spouse. Shoot360 has been contracted to provide services, technologies and software to enhance the performance of student-athletes. Blair-Lewis will not participate in negotiations or oversee the contract on behalf of George Mason. The waiver specifies oversight and requirements in order to continue George Mason's contractual relationship with Shoot360.

3. Stephen Curtis, Head Coach Women's Tennis;
James (Jimmy) Davis, Head Coach Men's Tennis;
A Plus Sports, Burke Racquet & Swim Club;
waiver period: 3/16/2022–3/1/2025 ($24,279 paid by George Mason, $24,195 paid to George Mason in FY 2024)
Personal interest: Curtis and Davis have between 20% and 50% ownership and receive over $5,000 from A Plus Sports (BRSC). George Mason will utilize BRSC facilities for men's and women's tennis practice, as needed, depending on schedules and the weather, as George Mason does not have indoor tennis courts. A Plus Sports (BRSC) will utilize University facilities pursuant to the standard George Mason Recreation facilities use contract and operate a summer sports camp. The waiver specifies oversight and requirements in order to continue George Mason's contractual relationship with BRSC.

4. Andrew Gerard, Director, Men's and Women's Track and Field/Cross Country;
Andrew Gerard Coaching & Training, LLC;
waiver period: 3/21/2023–1/1/2025 ($9,500 paid by George Mason in FY 2024)
Personal interest: Gerard has 100% ownership of Andrew Gerard Coaching & Training. The LLC will provide timing and results reporting for Cross Country and Track & Field Events. Purchasing and Athletics were directly involved in the arrangement of this contract to confirm George Mason's Purchasing guidelines were followed. Gerard will not participate in negotiations or oversee the contract on behalf of George Mason. The waiver specifies oversight and requirements in order to continue George Mason's contractual relationship with the LLC beyond the current contract.

5. Yuntao Wu, Professor, Molecular and Microbiology, School of Systems Biology, College of Science;
Virongy Biosciences, Inc.;
waiver period: 8/19/2022–12/1/2024 ($325,000 paid by George Mason, $5,351 paid to George Mason in FY 2024)
Personal interest: Wu has over 50% but less than 100% ownership of Virongy. George Mason contracts with Virongy to buy research products, such as HIV indicator cells, peptides, etc. used by Wu's lab and other George Mason research labs. Virongy also sponsors research at George Mason. Wu's waiver details the requirements for purchasing oversight by the College of Science Associate Dean for Research, and for research management plans as a condition of granting the COI waiver.

6. Lap-Fai (Craig) Yu, Associate Professor, Computer Science, College of Engineering and Computing;
Great Victory Legends, Inc.;
waiver period: 4/22/2024–4/1/2025 ($32,000 paid by George Mason in FY 2024)
Personal interest: Yu has over 50% but less than 100% ownership of Great Victory Legends. George Mason has agreements with Great Victory Legends related to sponsored research. Yu will not participate in negotiations or oversee the contract on behalf of George Mason. Yu's waiver details the requirements for research management plans as a condition of granting the waiver.

Please feel free to contact me (at ewoodley@gmu.edu) should you like to discuss this report.

RESOLUTION OF THE BOARD OF VISITORS OF GEORGE MASON UNIVERSITY

Whereas: The State and Local Government Conflict of Interest Act prohibits certain conduct related to contracts, and

Whereas: The General Assembly has recognized the benefits provided to the citizens of Virginia by the scholarly and research activities of the Commonwealth's institutions of higher education, and

Whereas: To facilitate scholarship and research the General Assembly has created generous exceptions to otherwise prohibited conduct specifically for institutions of higher education, and

Whereas: It is the desire of the Board of Visitors to delegate the responsibility for approving waivers to the President in accord with his general authority to manage the affairs of the University, therefore

BE IT RESOLVED:

That the President or his designee is hereby authorized to approve waivers of conflicts of interest arising from contracts pursuant to §2.2-3106 and §2.2-3110.A.5.of the Code of Virginia, in the manner as set forth in the statutes, and,

BE IT FURTHER RESOLVED

That the President or his designee shall report to the Audit Committee of the Board annually, on or before December 1, all contract waivers approved.

Adopted: August 1, 2014

Tom Davis

Rector
Board of Visitors
George Mason University

August 1, 2014
Date

Appendix B: Research and Development of Intellectual Property COI Waivers as of 10/1/2024

I. Waivers of personal interests due to ownership and/or income from companies

#	Employee	Other Interest	Nature of COI	Waiver Period
1	Massimiliano Albanese, Associate Professor, IST Department, College of Engineering and Computing	The MITRE Corporation	• Albanese received over $5,000 annual income from outside consulting[1] for a MITRE project. • George Mason has sponsored research agreements with MITRE. • Albanese has no authority to participate in contract negotiations or oversee the contract on behalf of George Mason or MITRE. • In FY24, George Mason has paid $0 to MITRE. MITRE has paid $170,182 to George Mason.	4/1/2024 – 4/1/2025
2	Maureen Ashbrock, Research Integrity Project Manager, Office of Research Integrity and Assurance	The MITRE Corporation	• Ashbrock received over $5,000 annual income from spouse's employment by MITRE. • George Mason has agreements with MITRE related to sponsored research, but Ashbrock has no involvement in George Mason's contractual relationship with MITRE and will recuse herself from any decisions which involve or affect MITRE. • In FY24, George Mason has paid $0 to MITRE. MITRE has paid $170,182 to George Mason.	8/6/2024– 8/1/2025
3	Mary (Missy) Cummings, Professor, Mechanical Engineering, College of Engineering and Computing	Palantir	• Cummings received over $5,000 annual income from outside consulting, serving on Palantir's privacy and civil liberties advisory board. • George Mason has agreements with Palantir related to sponsored research. • Cummings' research is reviewed to determine whether her interest requires a Management Plan. Cummings does not currently have a Research Management Plan. • In FY24, George Mason has paid $5,986,823 to Palantir. Palantir has paid $0 to George Mason.	11/30/2024– 1/30/2025

[1] Note on Outside Employment and Consulting: Mason's Outside Employment Policy applies to Administrative/Professional Faculty and Classified Staff. Those employees require approval before engaging in Outside Employment (as defined by that Policy). Mason's Faculty Handbook and Conflict of Commitment Policy apply to Instructional/Research Faculty and require approval of certain Outside Professional Activities, including when they exceed one day per work week. Wage employees and Adjunct Faculty do not require approval for Outside Employment or Outside Professional Activities.

#	Employee	Other Interest	Nature of COI	Waiver Period
4	Robert Elder, Research Professor, Electrical and Computer Engineering, College of Engineering and Computing	Applied Research Associates, Inc. (ARA)	• Elder received over $5,000 annual income from ARA for outside consulting, serving as an NC3 subject matter expert to the Defense Threat Reduction Agency. • George Mason has sponsored research agreements with ARA. • Elder has no authority to participate in contract negotiations or oversee the contract on behalf of George Mason or ARA. • In FY24, George Mason has paid $0 to ARA. ARA has paid $180,815 to George Mason.	11/30/2023-11/30/2024
5	Maryam Sadat Farvid, Associate Professor, Nutrition and Food Studies, College of Public Health	Massachusetts General Hospital	• Farvid received over $5,000 annual income from statistical analysis and writing an article for MGH. • George Mason has agreements with Massachusetts General Hospital related to sponsored research, but Farvid has no involvement in Mason's contractual relationship with Massachusetts General Hospital. • In FY24, George Mason has paid $0 to Massachusetts General Hospital. Massachusetts General Hospital has paid $0 to George Mason.	8/19/2024–8/1/2025
6	Kenneth Griffin, Professor, Global and Community Health, College of Public Health	National Health Promotion Associates, Inc. (NHPA)	• Griffin received over $5,000 annual income from NHPA for outside consulting. • George Mason has subcontracted with NHPA on a sponsored research project. Griffin is Principal Investigator on this research project and has a Research Management Plan approved by the COI Committee. • Griffin's consulting work is unrelated to the subcontract and involves providing general advice and consultation to NHPA staff regarding evaluation design, survey development, and qualitative and quantitative data analysis. • In FY24, George Mason has paid $0 to NHPA. NHPA has paid $22,823 to George Mason.	4/30/2020–12/1/2024
7	Brett Hunter, Associate Professor, Statistics, College of Engineering and Computing	INOVA Health System	• Hunter received over $5,000 annual income from statistical consulting on a research project at INOVA. • George Mason has agreements with INOVA related to sponsored research, but Hunter has no involvement in George Mason's contractual relationship with INOVA. • In FY24, George Mason has paid $2,989 to INOVA. INOVA has paid $0 to George Mason.	9/4/2024–8/1/2025

#	Employee	Other Interest	Nature of COI	Waiver Period
8	Erin Maughan, Associate Professor, School of Nursing, College of Public Health	Center for School Health Innovation & Quality	• Maughan is the CEO of the Center and receives over $5,000 annual income for work on projects for the Center. • The Center for School Health Innovation & Quality (part of the Public Health Accreditation Board) will establish a research contract or contracts with George Mason. • Maughan has committed to following the procedures below to manage the conflict of interest: 1) In my role as a Mason employee, I will not have authority to approve the contract between Mason and the Center, and while I am a Mason employee I will not take part in negotiations between Mason and the Center. The CPH ADR (Dr. Alison Cuellar) will oversee contracts between Mason and the Center. 2) Each project will have a management plan, and public disclosure of the relationship will be made according to normal practice, or with greater disclosures as determined by that individualized management plan. 3) When a substantial change in situation occurs (such as a major new contract is proposed) or annually when the waiver is renewed, the CPH ADR and CPH Dean will meet with Dr. Chris DiTeresi, Associate Director, Research Integrity, to evaluate whether any changes are needed for the management of the COI. • In FY24, George Mason has paid $0 to the Center. The Center has paid $0 to George Mason.	4/7/2024–4/1/2025
9	Mikell Paige, Professor, Chemistry and Biochemistry, College of Science	Covenant Therapeutics, LLC	• Paige has 50% ownership of Covenant Therapeutics. • Covenant will establish a research contract or contracts with Mason. • Paige has committed to following the procedures below to manage the conflict of interest: 1) In my role as a Mason employee, I will not have authority to approve the contract between Mason and Covenant, and while I am a Mason employee I will not take part in negotiations between Mason and Covenant. The COS ADR (Dr. Pat Gillevet) will oversee Mason/Covenant contracts. 2) Each research project will have a management plan, and public disclosure of the relationship will be made according to normal practice, or with greater disclosures as determined by that individualized management plan. 3) When a substantial change in situation occurs (such as a major new contract is proposed) or annually when the waiver is renewed, the COS ADR and COS Dean	4/7/2024–2/1/2025

#	Employee	Other Interest	Nature of COI	Waiver Period
			will meet with Dr. Chris DiTeresi, Associate Director, Research Integrity, to evaluate whether any changes are needed for the management of the COI. • In FY24, George Mason has paid $0 to Covenant Therapeutics. Covenant Therapeutics has paid $0 to George Mason.	
10	Emanuel (Chip) Petricoin, Professor, Co-Director, Center for Applied Proteomics and Molecular Medicine, College of Science	Perthera, Inc.	• Petricoin is a co-founder of Perthera, Inc., is an equity interest holder (10%), serves as Chief Science Officer, and serves on the Board of Directors. • Perthera will establish a research contract or contracts with George Mason. • Petricoin has committed to following the procedures below to manage the conflict of interest: 1) In his role as a Mason employee, Dr. Petricoin will not have authority over the contract between Mason and Perthera, and while he is a Mason employees he will not take part in negotiations between Mason and Ambrosia. Dr. Pat Gillevet will oversee Mason/Perthera contracts. 2) Employees working in the lab must be informed of Dr. Petricoin's financial interest in Perthera and that they may contact Dr. Gillevet and/or the Department Chair if they have questions or concerns. 3) When a substantial change in situation occurs (such as a new contract is proposed) or annually when the waiver is renewed, Dr. Petricoin will inform ORIA and Institutional Compliance whether any changes are needed for the management of the COI. • In FY24, George Mason has paid $0 to Perthera. Perthera has paid $0 to George Mason.	10/16/2023–10/31/2024[2]
11	Yuntao Wu, Professor, Center for Infectious Disease Research, College of Science	Virongy Biosciences, Inc.	• Wu has over 50% but less than 100% ownership of Virongy. • Virongy is a company based in Virginia which produces research products, such as HIV indicator cells, peptides, etc. used by Dr. Wu's lab and other research labs at the University. Virongy will also sponsor research at George Mason. • Wu has committed to following the procedures below to manage the conflict of interest: (1) I will report any changes in my SFI to George Mason through the COI disclosure process within 30 days. (2) I will not be involved in any purchase decision that involves a Virongy product.	8/19/2022–12/1/2024

[2] This waiver is in active review, has been approved by the COI Committee, and/or is awaiting signature.

#	Employee	Other Interest	Nature of COI	Waiver Period
			(3) If my lab needs to purchase a unique product that is solely produced by Virongy, a sole source documentation of the product shall be submitted to the university's procurement office. Documentation of the fair market price of the product will be presented. Any requests for purchasing a unique product for my lab for any dollar amount will be first approved by Dr. Pat Gillevet. (4) If a Virongy product is not a sole-source product, at least three (3) quotations from three (3) different vendors will need to be independently acquired and compared, and a purchase decision will be made independently. Dr. Yuntao Wu will not be involved in the processes. Currently, Dr. Pat Gillevet is the purchase decision maker. Dr. Gillevet will monitor this process to ensure that he agrees with the scientific reasons this purchase is in George Mason's best interest. Documentation should be attached to orders submitted to Purchasing, showing this procedure was followed. (5) Any research results and their publications, presentations, and patent application disclosures from Dr. Yuntao Wu's lab will be promptly disclosed to George Mason. (6) Any employees or faculty in Dr. Wu's lab will not be involved in any research and commercialization activity in Virongy. • In addition to the above, any research project at George Mason sponsored by Virongy will be reviewed and subject to a Management Plan. • In FY24, George Mason has paid $325,000 to Virongy. Virongy has paid $5,351 to George Mason.	
12	Lap-Fai (Craig) Yu, Associate Professor, Computer Science, College of Engineering and Computing	Great Victory Legends, Inc.	• Yu is the CEO and has 55% equity ownership of Great Victory Legends. • George Mason has agreements with Great Victory Legends related to sponsored research. • Yu has committed to following the procedures below to manage the conflict of interest: 1) In my role as a Mason employee, I will not have authority to approve the contract between Mason and Great Victory Legends, and while I am a Mason employee I will not take part in negotiations between Mason and Great Victory Legends. The CEC ADR (Dr. Art Pyster) will oversee Mason/Great Victory Legends contracts.	4/22/2024–4/1/2025

#	Employee	Other Interest	Nature of COI	Waiver Period
			2) Each research project will have a management plan, and public disclosure of the relationship will be made according to normal practice, or with greater disclosures as determined by that individualized management plan. 3) When a substantial change in situation occurs (such as a major new contract is proposed) or annually when the waiver is renewed, the CEC ADR and CEC Dean will meet with Dr. Chris DiTeresi, Associate Director, Research Integrity, to evaluate whether any changes are needed for the management of the COI. • In FY24, George Mason has paid $32,000 to Great Victory Legends. Great Victory Legends has paid $0 to George Mason.	

II. Waivers of personal interests due to income from private universities:

#	Employee	Other Interest	Nature of COI	Waiver Period
13	Paul Bubbosh, Professor, College of Science	Johns Hopkins University	• Bubbosh receives over $5,000 annual income from approved Outside Employment as an adjunct faculty member at Johns Hopkins. • Bubbosh's research is reviewed to determine whether his interest requires a Management Plan. Bubbosh does not currently have a Research Management Plan. • In FY24, George Mason has paid $45,712 to Johns Hopkins. Johns Hopkins has paid $313,228 to George Mason.	11/30/2024–1/31/2025
14	Lawrence Cheskin, Professor, Nutrition and Food Studies, College of Public Health	Johns Hopkins University	• Cheskin receives over $5,000 annual income from Outside Employment (less than one day per week) at Johns Hopkins. • George Mason has subcontracts with Johns Hopkins University related to sponsored research. • Cheskin is a part-time staff physician at a clinical and research center at Johns Hopkins University, and an adjunct faculty member. His research is reviewed to determine whether his interest requires a Management Plan. Cheskin does not currently have a Research Management Plan. • In FY24, George Mason has paid $45,712 to Johns Hopkins. Johns Hopkins has paid $313,228 to George Mason.	10/7/2021–3/12/2025
15	Annie Green, Data Governance Specialist, ITS	George Washington University	• Green receives over $5,000 annual income from approved Outside Employment as an adjunct faculty member at George Washington University.	1/6/2022–1/31/2025

#	Employee	Other Interest	Nature of COI	Waiver Period
			• George Mason has subcontracts with George Washington University related to sponsored research. • Green's role at Mason and at GW is not involved with sponsored research. • In FY24, George Mason has paid $37,644 to George Washington University. GW has paid $159,545 to George Mason.	
16	David Grossman, Senior Director, Tech Transfer, Office of Technology Transfer	American University	• Grossman received over $5,000 annual income from outside employment at American University, supervising students doing pro-bono patent work. • George Mason has agreements with American University related to sponsored research, but Grossman has no involvement in George Mason's contractual relationship with American and will recuse himself from any decisions which involve or affect American. • In FY24, George Mason has paid $216,983 to American University. American University has paid $0 to George Mason.	8/19/2024–8/1/2025
17	William Hahn, Program Director, GeorgeSquared Advanced Biomedical Sciences Programs, College of Science	Georgetown University	• Hahn receives over $5,000 annual income from approved Outside Employment as an adjunct faculty member at Georgetown. • George Mason has subcontracts with Georgetown related to sponsored research. • Hahn's research is reviewed to determine whether his interest requires a Management Plan. Hahn does not currently have a Research Management Plan. • In FY24, George Mason has paid $353,325 to Georgetown University. Georgetown has paid $265,969 to George Mason.	10/14/2022–8/31/2025
18	Kyung Hyeon Lee, Assistant Professor, Chemistry and Biochemistry, College of Science	Oak Ridge Associated Universities	• Lee received over $5,000 annual income from a fellowship at Walter Reed Army Institute of Research funded by Oak Ridge Associated Universities. • George Mason has agreements with Oak Ridge Associated Universities related to sponsored research, but Lee has no involvement in George Mason's contractual relationship with Oak Ridge Associated Universities. • In FY24, George Mason has paid $0 to Oak Ridge Associated Universities. Oak Ridge Associated Universities has paid $17,657 to George Mason.	6/21/2024–4/30/2025
19	Catherine Creighton Martin, Training and Technical Assistance Center (TTAC)	Marymount University	• Martin receives over $5,000 annual income from approved Outside Employment as an adjunct faculty member at Marymount. • George Mason has contracts with Marymount University related to sponsored research.	9/8/2021–7/1/2025

#	Employee	Other Interest	Nature of COI	Waiver Period
	Coordinator, College of Education and Human Development		• Martin's research is reviewed to determine whether her interest requires a Management Plan. Martin does have a Research Management Plan. • In FY24, George Mason has paid $0 to Marymount University. Marymount has paid $0 to George Mason.	
20	Pamela Patterson, Associate Vice President, University Life	Stanford University	• Patterson received over $5,000 annual income from Coaching/Consulting Activities at Stanford. • George Mason has agreements with Stanford related to sponsored research, but Patterson has no involvement in George Mason's contractual relationship with Stanford. • In FY24, George Mason has paid $29,289 to Stanford. Stanford has paid $249,132 to George Mason.	3/10/2024–1/30/2025

Appendix C: Other Contractual COI Waivers as of 10/1/2024

I. Waivers due to ownership of a contracting entity or income interest in a contracting entity related to Mason employment

#	Employee	Other Interest	Nature of COI	Waiver Period
1	Paul Allvin, Vice President and Chief Brand Officer, Office of University Branding	Brynmor Holdings, LLC	• Allvin has 100% ownership in Brynmor Holdings, LLC through his spouse. • Brynmor has been contracted to consult with George Mason on the provision of childcare services and to potentially support Mason in the application for a federal grant. • Allvin will have no authority over this contract and will recuse himself from any decisions or discussions which directly involve or affect Brynmor. • In FY24, George Mason has paid $14,800 to Brynmor.	2/1/2023–1/31/2025
2	Vanessa Blair-Lewis, Head Coach Women's Basketball	Shoot360	• Blair-Lewis' spouse has 50% ownership of Shoot360. • George Mason's Women's Basketball team uses Shoot360's services, technologies and software to enhance the performance of student-athletes. • Blair-Lewis will not participate in negotiations or oversee the contract on behalf of George Mason. The waiver specifies oversight and requirements in order to continue George Mason's contractual relationship with Shoot360 beyond the current contract. • In FY24, George Mason has paid $4,950 to Shoot360.	7/20/2024–7/1/2025
3	Mary (Missy) Cummings, Professor, Mechanical Engineering, College of Engineering and Computing	UC Berkeley	• Cummings received over $5,000 annual income from outside consulting[3] with the California Partners for Advanced Transportation Technology (PATH) at UC Berkeley. • George Mason has agreements with UC Berkeley related to sponsored research. • Cummings' research is reviewed to determine whether her interest requires a Management Plan. Cummings does not currently have a Research Management Plan. • In FY24, George Mason has paid $24,181 to UC Berkeley. UC Berkeley has paid $25,461 to George Mason.	11/30/2024–1/30/2025

[3] Note on Outside Employment and Consulting: Mason's Outside Employment Policy applies to Administrative/Professional Faculty and Classified Staff. Those employees require approval before engaging in Outside Employment (as defined by that Policy). Mason's Faculty Handbook and Conflict of Commitment Policy apply to Instructional/Research Faculty and require approval of certain Outside Professional Activities, including when they exceed one day per work week. Wage employees and Adjunct Faculty do not require approval for Outside Employment or Outside Professional Activities.

#	Employee	Other Interest	Nature of COI	Waiver Period
4	Megan DuBois, Assistant Professor, Global and Community Health, College of Public Health	Utah State University	• DuBois received over $5,000 annual income from outside consulting, serving as an Adjunct Professor at Utah State. • George Mason has agreements with Utah State related to sponsored research. • DuBois' research is reviewed to determine whether her interest requires a Management Plan. Dubois does not currently have a Research Management Plan. • In FY24, George Mason has paid $0 to Utah State. Utah State has paid $0 to George Mason.	1/30/2024–1/30/2025
5	Robert Elder, Research Professor, Electrical and Computer Engineering, College of Engineering and Computing	Georgia Tech Research Corporation (GTRC)	• Elder received over $5,000 annual income from GTRC for outside consulting, serving as Subject Matter Expert. • George Mason has agreements with GTRC related to sponsored research. • Elder has no authority to participate in contract negotiations or oversee the contract on behalf of George Mason or GTRC. • In FY24, George Mason has paid $177,773 to GTRC. GTRC has paid $0 to George Mason.	11/30/2023-11/30/2024
6	Boris Gafurov, Assistant Professor, Special Ed and disability Research, College of Education and Human Development	ATWare Solutions	• Gafurov has 100% ownership of ATWare Solutions. • ATWare Solutions was formed to submit free apps developed at George Mason's Training and Technical Assistance Center (TTAC) for people with disabilities to iTunes and Google Play. • TTAC is a George Mason Center that provides resources and technical assistance to educators. • In FY24, George Mason has paid $1,000 to ATWare Solutions.	9/8/2021-7/1/2025
7	Andrew Gerard, Director, Men's and Women's Track and Field/Cross Country	Andrew Gerard Coaching & Training, LLC	• Gerard has 100% ownership of Andrew Gerard Coaching & Training. • The LLC will provide timing and results reporting for Cross Country and Track & Field Events. Purchasing and Athletics were directly involved in the arrangement of this contract to confirm George Mason's Purchasing guidelines were followed. • Gerard will not participate in negotiations or oversee the contract on behalf of George Mason. The waiver specifies oversight and requirements in order to continue George Mason's contractual relationship with the LLC beyond the current contract. • In FY24, George Mason has paid $9,500 to Gerard Coaching & Training.	3/21/2023–1/1/2025

#	Employee	Other Interest	Nature of COI	Waiver Period
8	Gerald Matthews, Professor, Psychology, College of Humanities and Social Sciences	University of Central Florida	• Matthews received over $5,000 annual income from outside consulting, consulting on a research project at UCF sponsored by the Nuclear Regulatory Commission. • George Mason has agreements with UCF related to sponsored research. • Matthews' research is reviewed to determine whether his interest requires a Management Plan. Matthews does not currently have a Research Management Plan. • In FY24, George Mason has paid $292, 568 to UCF. UCF has paid $21,073 to George Mason.	11/30/2023–1/30/2025
9	Marybeth (MB) Mitcham, Dir MPH Online Program Global and Community Health, College of Public Health	Cornell University	• Mitcham receives over $5,000 annual income from approved outside consulting as an independent contractor facilitating non-credit-bearing certificate programs at Cornell. • George Mason has agreements with Cornell related to sponsored research. • Mitcham's research is reviewed to determine whether her interest requires a Management Plan. Mitcham does not currently have a Research Management Plan. • In FY24, George Mason has paid $15,000 to Cornell University. Cornell has paid $337,157 to George Mason.	2/6/2023–11/30/2024
10	Dieter Pfoser, Professor, Geography and Geoinformation Science Department, College of Science	Amazon.com, Inc.	• Pfoser is an Amazon Scholar (effort: one day per work week) and receives over $5,000 annual income from Amazon. • George Mason has business interactions with Amazon related to computing. • In Pfoser's role at George Mason, he has no authority to participate in contract negotiations or oversee George Mason's contract with Amazon. Similarly, in his role at Amazon, he has no authority over Amazon's work with George Mason. • In FY24, George Mason has paid $958 to Amazon.	4/30/2024-4/30/2025
11	Robert Simon, Professor, Computer Science, College of Engineering and Computing	Propensity	• Simon has 100% ownership in Propensity, LLC through his spouse. • George Mason's College of Health and Human Services (CHHS) has a contract with Propensity which involves assisting George Mason in placing opinion pieces with media outlets and otherwise gaining visibility for George Mason scholarship. • Simon no authority over this contract and will not negotiate with George Mason on behalf of Propensity. • In FY24, George Mason has paid $0 to Propensity.	2/1/2022-2/1/2025
12	Kun Sun, Professor, Information	Kryptowire, LLC	• Sun receives over $5,000 annual income from consulting for Kryptowire.	9/11/2024–8/1/2025

#	Employee	Other Interest	Nature of COI	Waiver Period
	Sciences and Technology, College of Engineering and Computing		• George Mason has agreements with Kryptowire related to sponsored research, but Sun has no involvement in George Mason's contractual relationship with Kryptowire. • Kun's research is reviewed to determine whether his interest requires a Management Plan. Kun does not currently have a Research Management Plan. • In FY24, George Mason has paid $72,043 to Kryptowire. Kryptowire has paid $398,608 to George Mason.	
13	Catherine Winkert, Associate Director Finance and Administration, College of Visual and Performing Arts	Monumental Sports & Entertainment	• Winkert receives over $5,000 annual income from her spouse's employment at Monumental Sports & Entertainment at the Capital One Arena. • Monumental Sports & Entertainment manages the Eagle Bank Arena and provides parking attendants during events hosted at the Eagle Bank Arena and for Center for the Arts (CfA). • Winkert does not have the authority to participate and will not participate in contract negotiations with Monumental on behalf of Mason. In addition, Winkert does not sign off on invoices from Monumental Sports & Entertainment. The Front of House Manager at CfA contacts Monumental to make arrangements, and the Finance and Budget Analyst at CfA reviews/approves invoices. • In FY23, George Mason has paid $818,278 to Centre Group LP/EagleBank Arena operated by Monumental Sports & Entertainment. Monumental Sports & Entertainment has paid $2,555,137 to George Mason.	1/25/2019–2/31/2025
14	Xiaokuan Zhang, Assistant Professor, Computer Science Department, College of Engineering and Computing	Ohio State University	• Zhang receives over $5,000 annual income from outside consulting for a sponsored research project at Ohio State. • George Mason has agreements with Ohio State related to sponsored research. • Zhang's research is reviewed to determine whether his interest requires a Management Plan. Zhang does not currently have a Research Management Plan. • In FY24, George Mason has paid $90,066 to Ohio State. Ohio State has paid $98,014 to George Mason.	11/30/2023-11/30/2024

II. Waivers due to Athletics facility contracts (e.g. athletic camps and clinics)

#	Employee	Other Interest	Nature of COI	Waiver Period
15	Frank Beasley, Head Coach, Wrestling	Beasley Training Systems	• Beasley has 100% ownership of Beasley Training Systems. • Beasley Training Systems will utilize University facilities pursuant to the standard facilities use contract and operate a summer wrestling camp. • In FY24, George Mason has paid $0 to Beasley Training Systems. Beasley Training Systems has paid $792 to George Mason.	9/27/2021–6/30/2024[4]
16	Vanessa Blair-Lewis, Head Coach Women's Basketball	Remedy Consulting, LLC	• Blair-Lewis has 100% ownership of Remedy Consulting. • Remedy Consulting will utilize University facilities pursuant to the standard Department of Intercollegiate Athletics sports camp facilities use contract and operate sports camps. • In FY24, George Mason has paid $0 to Remedy Consulting. Remedy Consulting has paid $3,506 to George Mason.	6/13/2022–7/1/2025
17	Shawn Camp, Head Coach Baseball	Shawn Camp Baseball Academy, LLC	• Camp has 100% Ownership of Shawn Camp Baseball Academy. • Shawn Camp Baseball Academy will utilize University facilities pursuant to the standard Department of Intercollegiate Athletics sports camp facilities use contract and operate clinics and a summer baseball camp. • In FY24, George Mason has paid $0 to Shawn Camp Baseball Academy. Shawn Camp Baseball Academy has paid $12,350 to George Mason.	9/27/2022–8/31/2025
18	Stephen Curtis, Head Coach Women's Tennis	A Plus Sports, Burke Racquet & Swim Club	• Curtis has over 20% but less than 50% ownership of and receives over $5,000 annual income from A Plus Sports (BRSC). • Mason will utilize A Plus Sports (BRSC) facilities for men's and women's tennis practice as needed depending on schedules and the weather, as Mason does not have indoor tennis courts. • A Plus Sports (BRSC) will utilize University facilities pursuant to the standard Mason Recreation facilities use contract and operate a summer sports camp. • The waiver specifies additional oversight and requirements in order to continue Mason's contractual relationship with BRSC. • In FY24, George Mason has paid $24,279 to A Plus Sports (BRSC). A Plus Sports (BRSC) has paid $24,195 to George Mason.	3/16/2022–3/1/2025

[4] This waiver is in active review, has been approved by the COI Committee, and/or is awaiting signature.

#	Employee	Other Interest	Nature of COI	Waiver Period
19	James Davis, Head Coach Men’s Tennis	A Plus Sports, Burke Racquet & Swim Club	• Davis has over 20% but less than 50% ownership of and receives over $5,000 annual income from A Plus Sports (BRSC). • Mason will utilize A Plus Sports (BRSC) facilities for men's and women's tennis practice as needed depending on schedules and the weather, as Mason does not have indoor tennis courts. • A Plus Sports (BRSC) will utilize University facilities pursuant to the standard Mason Recreation facilities use contract and operate a summer sports camp. • The waiver specifies additional oversight and requirements in order to continue Mason’s contractual relationship with BRSC. • In FY24, George Mason has paid $24,279 to A Plus Sports (BRSC). A Plus Sports (BRSC) has paid $24,195 to George Mason.	5/11/2022–7/1/2025
20	Jennifer Everett, Sr Associate AD for Finance and Administration, CFO, Athletics	HUSEL, Inc.	• Everett has 98% ownership of HUSEL. • HUSEL rents George Mason turf fields and indoor space to coach youth female field hockey athletes in the community. • In FY24, George Mason has paid $0 to HUSEL. HUSEL has paid $29,120 to Mason.	3/16/2022–1/31/2025
21	Nicholas Mata, Assistant Coach Women’s Volleyball	Gold Star Volleyball, LLC	• Mata received over $5,000 annual income from Gold Star Volleyball. • Gold Star Volleyball will utilize University facilities pursuant to the standard Department of Intercollegiate Athletics sports camp facilities use contract and operate clinics and a summer volleyball camp. • In FY24, George Mason has paid $0 to Gold Star Volleyball. Gold Star Volleyball has paid $19,115 to George Mason.	6/13/2022–6/1/2025
22	Kara Mupo, Head Coach Women’s Lacrosse	Surge Elite Lacrosse Academy	• Mupo has 100% ownership of Surge Elite Lacrosse Academy. • Surge Elite Lacrosse Academy will utilize University facilities pursuant to the standard Department of Intercollegiate Athletics sports camp facilities use contract and operate a summer sports camp as well as clinics. • In FY24, George Mason has paid $0 to Surge Elite Lacrosse Academy. Surge Elite Lacrosse Academy has paid $750 to George Mason.	8/20/2021–6/18/2025
23	Justin Ross-Walker, Head Coach Softball	Justin Walker Softball Camp	• Walker has 100% ownership and received over $5,000 annual income from Justin Walker Softball Camp. • Justin Walker Softball Camp will utilize University facilities pursuant to the standard Department of Intercollegiate Athletics sports camp facilities use contract and operate a summer sports camp.	8/20/2021–5/31/2025

#	Employee	Other Interest	Nature of COI	Waiver Period
			- In FY24, George Mason has paid $0 to Justin Walker Softball Camp. Justin Walker Softball Camp has paid $5,875 to George Mason.	

III. Waivers due to income from contracting entities unrelated to Mason employment

#	Employee	Other Interest	Nature of COI	Waiver Period
24	Susan Allen, Professor, Carter School	Apple, Inc.	• Allen received over $5,000 annual income from stock ownership in Apple. • Apple, Inc. is a vendor of goods to Mason, but Allen has no involvement in Mason's contractual relationship with Apple. (Note: If Allen were to request to purchase an Apple product at a uniform price available to the general public through Mason's ordinary purchasing process, this would be permissible under the terms of a COI waiver.) • In FY24, George Mason has paid $666,186 to Apple.	6/3/2021–5/18/2024[5]
25	Brian Benison, Director of Graduate Admissions and International Initiatives, Scalia Law School	Ernst & Young	• Benison received over $5,000 annual income from spouse's employment at Ernst & Young. • Ernst & Young has a contract with Mason for academic consulting services, but Benison has no involvement in Mason's contractual relationship with Ernst & Young. • In FY24, George Mason has paid $0 to Ernst & Young.	8/20/2021–7/30/2025
26	Brian Davern, Financial Specialist, Student Accounts	SP Plus Corporation (SP+)	• Davern received over $5,000 annual income from approved Outside Employment at SP+ as a parking enforcement technician. • SP+ contracts with Mason to oversee parking and transportation enforcement on campus, but Davern has no involvement in Mason's contractual relationship with SP+. • In FY24, George Mason has paid $2,819,504 to SP+.	3/16/2022–4/30/2025
27	Nancy Dunham, Grants Project Coordinator,	University of Pennsylvania The Wharton School	• Dunham received over $5,000 annual income from approved Outside Employment at the University of Pennsylvania as an auxiliary application reader for the Wharton MBA Admissions office.	10/11/2021–9/30/2024[5]

[5] This waiver is in active review, has been approved by the COI Committee, and/or is awaiting signature.

#	Employee	Other Interest	Nature of COI	Waiver Period
	University Accreditation		• Mason and the University of Pennsylvania have contracts and business interactions related to library database access. Dunham has no involvement in Mason's contractual relationship with the University of Pennsylvania. • In FY24, George Mason has paid $169,278 to the University of Pennsylvania. The University of Pennsylvania has paid $213,382 to George Mason.	
28	Jolie Gaspard, Transformation Manager, Office of the Provost	Gartner, Inc.	• Gaspard received over $5,000 annual income from spouse's employment at Gartner. • Mason has a contract with Gartner for access to their Higher Education Reference Library (Core Research), but Gaspard has no involvement in Mason's contractual relationship with Gartner. • In FY23, Mason has paid $268.949 to Gartner.	11/30/2022—8/30/2025[5]
29	Adrianne Jones, Performance Management and Engagement Specialist, HR	Amazon Web Services	• Jones received over $5,000 annual income from spouse's employment at Amazon Web Services. • George Mason has business interactions with Amazon Web Services related to computing, but Jones has no involvement in Mason's contractual relationship with AWS. • In FY24, George Mason has paid $958 to AWS.	12/13/2021–1/31/2025
30	Kenneth Turchi, Associate Dean for External Affairs, Scalia Law School	Indiana University	• Turchi received over $5,000 annual income from editing and design services for Indiana University. • George Mason has agreements with Indiana University related to sponsored research, but Turchi has no involvement in George Mason's contractual relationship with Indiana University. • In FY24, George Mason has paid $6,150 to Indiana University. Indiana University has paid $15,980 to George Mason.	8/19/2024–8/1/2025
31	Matthew Karush, Professor of History, College of Humanities and Social Sciences	University of Oxford, Oxford University Press	• Karush received over $5,000 annual income from Outside Employment as an Editor for OUP for under 1 day per week. • George Mason and OUP have contracts and business interactions related to the purchase of books and textbooks, but Karush has no involvement in Mason's contractual relationship with OUP. (Note: the Virginia COI Act in §2.2-3106(C)(5) exempts personal interests in contracts for textbooks or other educational materials for students, so if Karush were to assign OUP texts to his students that would not require a waiver.)	1/6/2022–10/31/2024

#	Employee	Other Interest	Nature of COI	Waiver Period
			• In FY24, George Mason has paid $259,263 to Oxford University. Oxford University has paid $43,030 to George Mason.	
32	Victoria (Tori) Unterberger, Front of House, Community Inclusion Manager College of Visual and Performing Arts	Ordway Conservatory of Classical Ballet	• Unterberger received over $5,000 annual income from outside employment as a dance instructor at the Conservatory. • George Mason has business interactions with the Ordway Conservatory related to dance education and performance, but Unterberger has no involvement in George Mason's contractual relationship with Ordway Conservatory. • In FY24, George Mason has paid $0 to Ordway Conservatory. Ordway Conservatory has paid $0 to George Mason.	8/19/2024–8/1/2025

Appendix D: Immediate Family Waivers

1. Jessica (Jessi) Adams, Assistant Director, Knowledge Management, Fiscal Services; and Robert (Wayne) Adams, Director Academic Admin, CPH
2. Eric G. Anderson, Associate Professor of English, CHSS; and E. Shelley Reid, Executive Dir of Engaged Teaching, Stearns Center
3. Md Tanvir Arafin, Assistant Professor, Cyber Security Engineering Dept, CEC; and Syeda Sanjidah, Grad Teaching Assistant, Cyber Security Engineering Dept, CEC
4. Roberto Arbieto, eVA PCard Customer Supp, Purchasing Office; and Nury Terrazas Sanchez, GMU Worker, Purchasing Office
5. Ann Ardis, Dean, CHSS; and Phillip Mink, Term Assistant Professor, Foundations Instruction, CCB
6. Deliah Arrington, PSC Site Coordinator, SciTech Campus Executive Office; and Amy Fowler, Associate Professor, Environ Sci & Policy Instruction, COS
7. Giorgio Ascoli, Professor, Bioengineering, CEC; and Rebecca Goldin, Professor, Mathematical Sciences, COS
8. Benjamin Ashworth, Sculpture and Foundations Manager, School of Art & Design, CVPA; and Jennifer Ashworth, GMU Worker, Fairfax Galleries, CVPA
9. Eric Auld, Instructor, English Instruction, CHSS; and Anastasia (Stasia) Kemp, Education Support Specialist, CEC Undergrad Student Services, CEC
10. Ivan Avramovic, Assistant Professor, Computer Science, CEC; and Sanja Avramovic, Associate Professor, Health Administration and Policy, PH
11. Pamela Baker, Director, Special Education and disAbility Research/Associate Professor, CEHD; and Robert Baker, Professor, Sport Recreation and Tourism Mgmt, CEHD
12. Sophia Balakian, Assistant Professor, School of Integrative Studies Instr, CHSS; and Michael Don, Assistant Professor, English Instruction, CHSS
13. Foteini Baldimtsi, Associate Professor, Computer Science, CEC; and Socrates Dimitriadis, Term Assistant Professor, Computer Science, CEC
14. Laura Balmaceda, Research Assistant Professor, Physics and Astronomy, COS; and Fernando Mut, GMU Worker, Bioengineering, CEC
15. Stephanie Barnett, Academic Advisor, Undergraduate Advising; and Thomas (Ryan) Barnett, Assoc Dir Military Services, Office of Military Services
16. Mariia Belaia, Assistant Professor, Computational and Data Scis Dept, COS; and Dale Rothman, Associate Professor, Computational and Data Scis Dept, COS
17. Stephanie Benassi, Assistant Professor, School of Art & Design, CVPA; and Jeffrey M. Kenney, Gallery Assistant, Arlington Galleries, CVPA
18. Lee Black, Assistant Professor, Health Administration & Policy, PH; and Heather Vough, Associate Professor, Management Instruction, Costello College of Business
19. Derek Borzi, Electrician II, Zone 6 Maintenance, Facilities; and Stacy Borzi, Contracts Specialist, Facilities Purchasing Fiscal Services, Facilities

20. RaShall Brackney, Dstg Prof of Practice, African and African AM Studies Ins, CHSS; and Stefan Wheelock, Associate Professor, English Instruction, CHSS
21. Kurt Brandhorst, Assistant Professor, Philosophy, CHSS; and Rachel Jones, Associate Professor, Philosophy, CHSS
22. Joan Bristol, Associate Professor, History and Art History, CHSS; and Randolph Scully, Associate Professor, History/M.A. History Program Director, History and Art History, CHSS
23. Amanda Bryan, Assistant Professor, English Instruction, CHSS; and Timothee (Tim) W Bryan, Assistant Professor, Mathematics Instruction, COS
24. Zofia Burr, Dean, Honors College; and Alok Yadav, Associate Professor of English, CHSS
25. Chris Burrell, Production Manager, Hylton Performing Arts Center, CVPA; and Diane Burrell, Operations Manager, Hylton Performing Arts Center, CVPA
26. Xiaomei Cai, Associate Professor, Department of Communication, CHSS; and Xiaoquan Zhao, Professor, Department of Communication, CHSS
27. Amanda Caswell, Professor, School of Kinesiology, CEHD; and Shane Caswell, Professor, School of Kinesiology, CEHD
28. Elena Chiru, Director Career Advising, Career Services; and John McShea, IT Project Manager, Project Management Office, ITS
29. Myunghwa Cho, Adjunct Faculty, CHSS; and Byunghwan (Ben) Son, Associate Professor, Global Affairs Program, CHSS
30. John Cicchetti, Director Behavioral Threat Assessment and Management, University Life; and Kaitlin Cicchetti, Director of Advancement, University Life
31. Caroline (Carrie) Cox, Technical Director, Arts Support Umbrella, CVPA; and Sean Cox, Assistant Director of Event Services, Student Centers
32. Arie Croitoru, Professor, Computational and Data Sciences, COS; and Natalie Lapidot-Croitoru, Finance and HR Analyst, Environ Sci & Policy Dept, COS
33. Christopher D'Amboise, Heritage Professor in Dance, School of Dance, CVPA; and Kelly D'Amboise, Adjunct Faculty, School of Dance, CVPA
34. Doran R Davis, Facilities Zone Supervisor, Zone 4 Maintenance, Facilities; and Doran Davis III, Electrical Apprentice, Zone 6 Maintenance, Facilities
35. Rick Davis, Dean, CVPA; and Julie Thompson, Executive Director, Center for the Arts
36. Mark DelVecchio, Research Manager Subcontractor and Program, CEC; and Mollie DelVecchio, Registered Nurse, Student Health Center, University Life
37. Desiree Desierto, Assistant Professor, Economics, CHSS; and Mark Koyama, Associate Professor, Economics, CHSS
38. Nikki Dinh, Senior Database Analyst, Database Middleware and ERP Support, ITS; and Robert Peraino, Advisory Systems Engineer, Enterprise Infrastructure Ops, ITS
39. Carlotta Domeniconi, Professor, Computer Science, CEC; and Sean Luke, Professor, Computer Science, CEC
40. Kevin Dunayer, Associate Professor, School of Theater, CVPA; and Laurel Dunayer, Costume Shop Supervisor, CFA

41. Nour El Meery, Admissions Counselor, Admissions; and Doaa Ibrahim, Sr Budget Analyst, Budget and Planning
42. Elisabeth Epstein, Associate Professor, Biology, COS; and Neil Epstein, Associate Professor, Mathematical Sciences, COS
43. Cory Faber, Telecom Technician, Telecom Admin, ITS; Elizabeth (Lee) Faber, IT Logistics Spc Mgmt Coord, ITS Finance; and Robert (Rob) B Faber, Fiscal Svcs Program Director, Finance
44. Alexandria Frisch Kinory, Assistant Professor, Religious Studies Instruction, CHSS; and Ethan Kinory, Assistant Professor, Accounting Instruction, Costello College of Business
45. Cindy Funes, GMU Worker, Academic Administration, Office of the Provost; and Corina Funes, Business Operations Specialist, Academic Administration, Office of the Provost
46. Boris Gafurov, Assistant Professor, Special Ed & disAbility Research, CEHD; and Anya Evmenova, Professor, Special Ed & disAbility Research, CEHD
47. Lei Gao, Associate Professor, Finance Instruction, Costello College of Business; and Lily Wang, Professor, Statistics, CEC
48. Christian Garcia, Program Support Specialist, Safety Emerg Ent Risk Mgmt Admin; and Lei An Ilan-Garcia, Industrial Hygiene Specialist, Environmnt Health and Safety Admin
49. Daniel Garrison, Assistant Professor, IST Department, CEC; and Victoria Garrison, Associate Professor, Student Health Center
50. Colby Grant, Director of Operations, SciTech Campus Executive Office; and Megan Grant, Fiscal and Administrative Specialist, Biomedical Research Lab, COS
51. Matthew Green, Assistant Director, Undergrad Student Svc, Schar School of Policy and Government; and Alice Magelssen-Green, Assoc Dir Watershed Lit, English Instruction, CHSS
52. Jesse Guessford, Director Curriculum Initiatives, Office of the Provost; and Jill Nelson, Associate Professor, Electrical and Computer Engineering, CEC
53. Mason Guilford, GMU Worker, ITS Finance; and Renate Guilford, Vice Provost Academic Admin, Academic Administration
54. John Hanks, Advisory Network Engineer, Enterprise Infrastructure Ops, ITS; and Tammy Hanks, Admin and Office Spec 3, Facilities Mgmt Admin
55. Nabiha Hasan, Senior IT Sec Ops Engineer, ITS Security; and Ubaidul Khan, Computer Systems Engineer, Cloud Compute & Storage Operations, ITS
56. Donald (Paul) Haspel, Associate Professor of English, CHSS; and Linda H. Mason, Professor and Director Helen A. Kellar Inst for Human disAbilities, CEHD
57. Barbara Helmick, Instr Designer Tech Spec, Global and Community Health, PH; and Greg Helmick, Adjunct Faculty (matrix), Computational and Data Scis Dept
58. John (Jay) Highsmith, Executive Assistant, Intercollegiate Athletics; and Shanelle Highsmith, Program Manager for Outreach and Partnerships, CHSS

59. Brittany Hupp, Assistant Professor, Atmosph Oceanic and Earth Sci Dept, COS; and Daniel Segessenman, Postdoctoral Research Fellow, Atmosph Oceanic and Earth Sci Dept, COS
60. Douglas Irvin-Erickson, Assistant Professor, Carter School; and Yasemin Irvin-Erickson, Assistant Professor, Criminology, Law & Society Department, CHSS
61. Farhana Islam, Acad Unit Admin Spec/Adm Asst, Sociology and Anthropology Instruction, CHSS; and Khondkar Islam, Professor, Information Sciences and Technology, CEC
62. Wassim Itani, Associate Professor, Computer Science Department, CEC; and Maha Shamseddine, Assistant Professor, Computer Science Department, CEC
63. Kristen V Jennette, Computer Systems Engineer, ITS-AE Support, ITS; and Shawn Jennette, Computer Systems Engineer; Cloud Compute & Storage Engineering, ITS
64. Weiwen Jiang, Assistant Professor, ECE Department, CEC; and Lei Yang, Assistant Professor, IST Department, CEC
65. Laurie A Juliana, Faculty RPT Ops Mgr, CEHD; and Hugh McIntosh, Adjunct Faculty, CEHD
66. Cing-Dao (Steve) Kan, Professor, Center for Collision Safety and Analysis, COS; and Chi Yang, Professor, Department of Physics and Astronomy, COS
67. Pilgyu Kang, Assistant Professor, Mechanical Engineering Dept, CEC; and Mirae Kim, Associate Professor, Schar School
68. Erdogan Kaya, Assistant Professor, Elem Lit and Sec Ed, CEHD; and Eter Mjavanadze, Graduate Research Assistant, CEHD
69. John Keady, Adjunct Faculty, Physics & Astronomy Instruction; and Kathleen (Kelly) Keady, Assist Dir Transfer Admissions, Admissions Operations
70. Sarah G Keith, Professor, English Instruction, CHSS; and Juana Medina Rosas, Assistant Professor, School of Art & Design, CVPA
71. Setarra Kennedy, Assistant Director, Arts Management, CVPA; and Charles Nicholson, Director of Brand Operations, Office of University Branding
72. David Kepplinger, Assistant Professor, Statistics, CEC; and Alexandra Patzak, Assistant Professor, Educational Psychology, CEHD
73. Maryam (Mary) Kheirollah, GMU Worker, Academic Administration; and Amir Tofighi, Sr Systems Analyst Devel Lead, Enterprise App Support & Develop, ITS
74. Dae Yong Kim, Term Instructor, Modern and Classical Lang Instr, CHSS; and Woomee Kim, Postdoctoral Research Fellow, CEE Teacher Enrichment Program, CEHD
75. Karen King, Assistant Professor, Business Foundations, Costello College of Business; and Michael (Mike) King, Assistant Professor, ISOM, Costello College of Business
76. Brenda Kling, Admin Assoc, Marketing Instruction, Costello College of Business; and Jeffrey L Kling, Assist Dir CaLT Class Support, Classroom Technologies, ITS
77. Christopher Koper, Professor, Criminology, Law and Society, CHSS; and Cynthia Lum, Professor, Criminology, Law and Society, CHSS
78. Evgenios Kornaropoulos, Assistant Professor, Computer Science Department, CEC; and Mary Righi, Clinical Operations Coord, School of Nursing

79. Davis Kuykendall, Associate Professor, Philosophy, CHSS; and Lauren Kuykendall, Associate Professor, Psychology, CHSS
80. Alison Landsberg, Professor, History Instruction, CHSS; and Matthew Karush, Professor and Department Chair, History and Art History, CHSS
81. Clare Laskofski, Assistant Controller Financial Operations, Finance; and Mike Laskofski, Associate Vice President of Research Services, Office of Sponsored Programs
82. Yi-Ching Lee, Associate Professor, Department of Psychology, CHSS; and Benoit Van Aken, Associate Professor, Department of Chemistry and Biochemistry, COS
83. Stephanie Lessard-Pilon, Associate Professor, Smithsonian-Mason School of Conservation; and James (Jim) McNeil, Associate Professor, Smithsonian-Mason School of Conservation
84. Fei Li, Associate Professor, Computer Science, CEC; and Qi Wei, Associate Professor, Bioengineering, CEC
85. Huwy-min Liu, Assistant Professor, Sociology and Anthropology, CHSS; and Matthew E West, Assistant Professor, Global Affairs Program, CHSS
86. Mingrui Liu, Assistant Professor, Computer Science Dept, CEC; and Jingya Yan, Instructor, Mathematical Sciences Department, COS
87. April Zoraida Lopez, Admin Asst to Dir, Special Ed & disAbility Research, CEHD; and Eduardo Lopez Atencio, Associate Professor, Comp & Data Sciences Instr, COS
88. Anton Lukyanenko, Associate Professor, Mathematical Sciences, COS; and Cynthia Lukyanenko, Assistant Professor, English Instruction, CHSS
89. Lannan (Lisa) Luo, Associate Professor, Computer Science Department, CEC; and Qiang Zeng, Associate Professor, Computer Science Department, CEC
90. Terrence Lyons, Professor, Carter School; and Agnieszka Paczynska, Professor, Carter School
91. Bonnie Madden, Microbiology Phage Lab Mgr, Biology Department, COS; and John Madden, GMU Worker, Biology Department, COS
92. Tamara Maddox, Professor, Computer Science, CEC; and John Otten, Senior Instructor, Computer Science, CEC
93. Gordon Maginness, HVAC Tech I, Zone 3 Maintenance, Facilities; and Karen Maginness, Lead Housekeeper, Facilities Custodial Services
94. Michael Malouf, Professor, English, CHSS; and Kristina Olson, Associate Professor of Italian, Modern and Classical Languages, CHSS
95. Brian Mark, Professor, Electrical and Computer Engineering, CEC; and Karen Sauer, Professor, Physics and Astronomy, COS
96. Wassim Masri, Professor, Computer Science Dept, CEC; and Rima Nakkash, Professor, Global & Community Health, PH
97. Robert Matz, Professor, English Instruction, CHSS; and Teresa Michals, Professor, English, CHSS
98. Joshua Maze, Grants and Programs Coord, English Instruction, CHSS; and Kimberly Maze, Reporting and Systems Admin, Sponsored Programs Admin

99. Daniel Meehan, Adjunct Faculty, CEHD; and Kelly Reid Meehan, Assoc Dir Comm Mktg Prgm Dev, Student Centers Admin
100. Anna Morgan, Administrative Assistant CCP, Ofc Community College Partnerships; and Carey Morgan, Lead Apple Technician, FFX Desktop Support, ITS
101. Janette Muir, Vice Provost Academic Affairs; and Star Muir, Associate Professor, Communication Department, CHSS
102. Clifton Murray, Director of Talent Acquisition, HR; and Monica Murray, Administrative Assistant ROTC, ROTC
103. Kelly Nam, Assistant Professor, School of Music, CVPA; and Sang Nam, Professor, Computer Game Design, CVPA
104. Vivek Narayanan, Associate Professor, English Instruction, CHSS; and Rashmi Sadana, Professor, Sociology and Anthropology Instruction, CHSS
105. Subodh Nayar, GMU Worker, SBDC; and Tracy Nayar, Associate Dir VA SBDC
106. Olivia O'Neill, Associate Professor, Management, Costello College of Business; and Tiago Requeijo, Assistant Professor, Finance, Costello College of Business
107. John Otten, Senior Instructor, Computer Science Department, CEC; and Joshua Otten, Grad Teaching Assistant, Computer Science Department, CEC
108. Diana Ottignon, Comp Resources Admin Spec, CEC Central IT Comp Lab Supp Team; and Lauren Ottignon, Student Wage Employee, MCAA Teaching, CVPA
109. Alpaslan Ozerdem, Dean, Carter School; and Ayce Bukulmeyen Ozerdem, Well Being Program Specialist, Center for Adv of Well Being, University Life
110. Audra Parker, Professor, Division of Elem, Lit, & Sec Ed, CEHD; and Kristien Zenkov, Professor, Division of Elem, Lit, & Sec Ed, CEHD
111. Cindy Parker, Associate Professor, Management Instruction, Costello College of Business; and Jack Parker, Student Support Specialist, Mason Autism Supp Initiative
112. Allison Ward Parsons, Associate Professor, Elem, Lit, & Sec Ed, School of Education, CEHD; and Seth Parsons, Professor, Elem, Lit, & Sec Ed, School of Education, CEHD
113. Gregory Pirog, Sr Application Analyst, Human Resources Technology Services; and Megan Pirog, Graduate Academic Affairs Coordinator, Graduate Education Administration
114. Alison Price, Dir of Operations LEC, Law and Economics Center, Antonin Scalia Law School; and Timothy Price, Adjunct Faculty, Antonin Scalia Law School
115. Hemant Purohit, Associate Professor, IST Department, CEC; and Apoorva Vyas, Fiscal Specialist, UL Finance, University Life
116. Ken Randall, Dean, Antonin Scalia Law School; and Susan Randall, Event Planner, Arlington Operations
117. Peter Rea, IT Project Manager CRM, Project Management Office; and Tammy Rogers, Executive Assistant, Library Administration
118. Ronald Resmini, Adjunct Faculty, Geography Geoinformation Sci Dept, COS; and Marilyn Ryan-Resmini, HR and Fiscal Specialist, Geography Geoinformation Sci Dept, COS
119. Claudia Rich, Mason Student Services Center Generalist, Mason Student Services Center; and Colleen Rich, Editorial Dir, Marketing, University Branding

120. Ellen Rodgers, Associate Professor, Sport, Recreation, and Tourism Mgmt, CEHD; and R.V. Pierre Rodgers, Associate Professor GSE, Sport, Recreation, and Tourism Mgmt, CEHD
121. Elsa Ronzier, Assistant Professor, Institute for Biohealth Innovation; and Remi Veneziano, Associate Professor, Bioengineering Department, CEC
122. James Russell, Director of Purchasing, Purchasing Office; and Rhett Russell, Application Analyst, Finance Technology Services
123. Amanda Sanchez, Assistant Professor, Psychology, CHSS; and Michael Ward, Assistant Director, Student Success Coaching, University Life
124. Evelyn Sander, Professor, Mathematical Sciences, COS; and Thomas Wanner, Professor, Mathematical Sciences, COS
125. Amber Saxton, Sustainability Program Manager, Campus Efficiency, University Sustainability; and Regis Saxton, Manager Pre-Award Administration, Office of Sponsored Programs
126. Laura Scott, Professor, English Department, CHSS; and Dean F. Taciuch, Professor, English Department, CHSS
127. John Sherman, Manager Sci Tech Library, Learning Research and Engagement; and Sarah Tomsyck, Events & Comm Coord, Ofc Community College Partnerships
128. Daniel (Dann) Sklarew, Professor, Environmental Science and Policy, COS; and Jennifer Sklarew, Assistant Professor, Environmental Science and Policy, COS
129. Charlie Spann, Asst VP Ent Svc Del Dep CIO, ITS; and Charles Spann Jr, (Will Spann), GMU Worker, GMU-TV
130. Kelly Hayward Stone, Facilities Billing Coordinator, Facilities; and Rebecca Hayward Stone, Project Coordinator, Learning Space Design, ITS
131. Heather Streckfus-Green, Assistant Professor, School of Art & Design, CVPA; and Peter Streckfus-Green, Associate Professor, English, CHSS
132. Erienne Sutherell, Adjunct Faculty, Scalia Law School; and Shaun Sutherell, Assoc Dean Strategic Initiativ, Law Strategic Initiatives, Scalia Law School
133. Alex Tabarrok, Professor, Economics, CHSS; and Monique van Hoek, Professor, School of Systems Biology, COS
134. Gail Therrien, Professor of Practice, IST; and Ronald Therrien, Adjunct Faculty, IST
135. Christopher Troiano, Historical Ensembles Prog Mgr, Pep Band, CVPA; and JennaMarie Warfield, GMU Worker, Pep Band, CVPA
136. Petrus J. van Oevelen, Professor of Practice, Atmosph Oceanic and Earth Sci Dept, COS; and Fernande P Vervoort, Research Manager, Atmosph Oceanic and Earth Sci Dept, COS
137. Ken Walsh, Vice President for Strategic Initiatives and Chief of Staff; and Tobi Walsh, Assistant Vice President, Capital Strategy and Planning, Office of the Senior Vice President
138. Fei Wang, Assistant Professor, Chemistry and Biochemistry Dept, COS; and Peiyu Yang, Assistant Professor, Modern and Classical Lang Instr, CHSS
139. Binqian Yin, Assistant Professor, Computer Science Department, CEC; and Keren Zhou, Assistant Professor, Computer Science Department, CEC

CAMPUSGUARD®

GLBA Assessment Report

October 11, 2024

Prepared for:

George Mason University
4400 University Drive
Fairfax, Virginia 22030

Prepared by:

Greg Lewis
Security Advisor
CampusGuard

GLewis@CampusGuard.com

This page is intentionally blank.

Contents

Executive Summary

A Gramm-Leach-Bliley Act (GLBA) program is implemented using an organization's information security and privacy programs together with administrative, technical, and physical controls applied in accordance with a risk assessment. The overall goal is to prevent data breaches by securing personal non-public information (NPI) and to minimize the impact of a breach by implementing these controls commensurate with an organization's own determination of relative risk.

Institutions are struggling to keep up with regulatory requirements, economic conditions, and risk management. Often, the role of information security is still not clearly defined in many organizations; some viewing it in isolation as someone else's responsibility, and in many cases, there is no collaborative effort to link the security program to the institution's goals. The need to comply with many regulations and standards such as GLBA, GDPR, HIPAA, FERPA, PCI, etc. has caused institutions to re-think their approach. While it is the intent of nearly all those affected by these regulations to comply, there are many challenges that complicate the overall process.

Due to this intrinsically complex nature of compliance, the difficulty in coordinating efforts across multiple departments, and the changing landscape of information security and privacy in general, George Mason University requested guidance from CampusGuard with the overall goal of leveraging best practices to establish and enhance components of the current information security program. In addition, protecting the sensitive information of current and former George Mason students, faculty, applicants, and friends while minimizing compliance risks and maximizing enterprise value.

The Assessment

A remote GLBA assessment including Federal Tax Information (FTI) was conducted between September 5th and September 19thth, 2024, by CampusGuard for George Mason University. During the review, CampusGuard met with Information Technology and department representatives with a variety of duties and responsibilities pertaining to the management and administration of the George Mason institutional data and infrastructure. We conducted interviews and reviewed documentation to understand the security controls currently in place and assess the maturity and completeness of those controls against the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 and general security best practices.

The following report consists of observations from the assessment at George Mason based on the NIST SP 800-171 standard that need addressing to help achieve the goal of compliance with GLBA, but taking various regulations into account (e.g., PCI DSS, GDPR, HIPAA, etc.). Within the NIST SP 800-171, there are a combined 110 Basic and Derived Security Requirements (Appendix F).

The George Mason staff demonstrated a deep understanding of protecting all types of sensitive data through the use of current practices, methodologies, and technologies to protect the George Mason environment. It was a pleasure to work with all personnel involved in the review.

Safeguards Rule Updates

The Federal Trade Commission (FTC) updated the Safeguards Rule under the Gramm-Leach-Bliley Act. in 2021 The revisions are meant to strengthen the data security safeguards to better protect customer financial information from data breaches and cyberattacks. The revised rule has a number of more specific requirements than the previous rule including access controls, data inventory and classification, vulnerability and penetration testing, authentication, encryption, data disposal, incident response, and risk assessments.

While the revised rule is more prescriptive, the Commission also emphasized that institutions still have the flexibility to implement an information security program that is appropriate to its size and complexity, the nature and scope of its activities, and the sensitivity of customer information.

The FTC summarized the modifications in the new rule as providing:

- More guidance on how to develop and implement specific aspects of an overall information security program.
- New provisions to improve the accountability of information security programs.
- Exemptions for financial institutions that collect less customer information.
- Inclusion of entities engaged in activities that are incidental to financial activities.
- New terms and examples.

The updated rule applies to nonbanking financial institutions including colleges and universities. Most of the more technical requirements took effect on June 9, 2023, eighteen months after the rule was published in the Federal Register. However, several of the new requirements became effective upon publishing on December 9, 2021, including regular testing and monitoring, service provider oversight, and additional risk assessments.

Another update to the Safeguards Rule occurred in May of 2024 which requires notification to the FTC upon discovery of a security event that involves the information of 500 or more individuals. The notification should be made as soon as possible and no more than 30 days after the discovery of the event. Notification can be performed on the FTC website at https://www.ftc.gov and must contain the following information:

- The name and contact information of the reporting financial institution;
- A description of the types of information that were involved in the notification event;
- If the information is possible to determine, the date or date range of the notification event;
- The number of consumers affected or potentially affected by the notification event;
- A general description of the notification event; and
- Whether any law enforcement official has provided you with a written determination that notifying the public of the breach would impede a criminal investigation or cause damage to national security, and a means for the Federal Trade Commission to contact the law enforcement official. A law enforcement official may request an initial delay of up to 30 days

> following the date when notice was provided to the Federal Trade Commission. The delay may be extended for an additional period of up to 60 days if the law enforcement official seeks such an extension in writing. Additional delay may be permitted only if the Commission staff determines that public disclosure of a security event continues to impede a criminal investigation or cause damage to national security.

As of the writing of this report, the FTC website did not have an obvious choice/link to use for this reporting requirement.

Assessment Contacts:

George Mason University:

Noor Aarohi
Director IT Risk and Compliance
naarohi@gmu.edu

CampusGuard:

Greg Lewis CISA, CMMC RPA, PCIP
Security Advisor
GLewis@CampusGuard.com

Laura Allison PCIP, PMP, MBA
Senior Customer Relationship Manager
LAllison@CampusGuard.com

---IMPORTANT---

Sections of this report have been redacted for containing 'Confidential – Restricted Data' which are excluded from disclosure under the Virginia Freedom of Information Act (Code of Virginia §2.2-3705.2.2 due to descriptions of security mechanisms and §2.2-3705.2.14b for vulnerability assessment information).

Risk Summary

The following observations have been identified as either having a greater impact on George Mason compliance efforts or on the risk of data compromise than other areas and are therefore presented first. It is recommended that these items be given priority for development, implementation, and remediation.

The observations are assessed considering their likelihood and impact. The likelihood is the probability that an observation might occur, and the impact reflects the anticipated size of the occurrence's effect. Both the likelihood and the impact are taken into consideration to determine the risk. Risks are rated as High, Medium, or Low.

Observations	Risk
1. [redacted]	High
2. [redacted]	High
3. [redacted]	High
4. The existing Information Technology Security Program (Policy 1311) does not contain all the elements for GLBA compliance.	Med
5. A Qualified Individual (QI) to manage and administer the Information Security Program is not formally identified.	Med
6. [redacted]	Med
7. [redacted]	Med
8. The roles, responsibilities and levels of decision making authority are not clearly identified in Incident Management Process.	Med
9. External communication actions and information sharing parameters are not identified in Incident Management Process.	Med
10. The criteria to confirm remediation of a cybersecurity incident are not clearly stated in the Incident Management Process.	Med

Assessment

Purpose

The purpose of this Gramm-Leach-Bliley Act (GLBA) Assessment is to evaluate the adequacy of George Mason University's security controls for storing, processing, and transmitting non-public personal information in scope for GLBA compliance and taking into consideration the use of Federal Tax Information. This risk analysis addresses threats, vulnerabilities, existing security controls, and the likelihood of confidential information exposure and impacts thereof. This assessment provides safeguards to mitigate threats and associated exploitable vulnerabilities.

Background

The Gramm-Leach-Bliley Act (GLBA) of 1999 requires that all financial institutions safeguard customer Non-public Personal Information (NPI). Colleges and universities that offer financial products or services, such as student loans, are considered financial institutions under the GLBA. Further, the Federal Student Aid (FSA) Department published a Dear Colleague Letter stating that colleges and universities must comply with GLBA as outlined in the Program Participation Agreement (PPA) for Title IV Federal student financial aid programs. The GLBA is enforced by the Federal Trade Commission (FTC). Activities that might trigger enforcement action by the FTC include student or employee complaints, press releases, or breach notifications. A data security breach that stems from a gap in GLBA compliance is a violation of federal law. It is worth noting that a college or university that is deemed compliant with the privacy provisions and regulations of the Family Education Rights and Privacy Act (FERPA) is also considered compliant with the privacy provisions and regulations of the GLBA for those student records which are subject to FERPA.

In order to evaluate compliance with the GLBA, organizations need to review the effectiveness of their security and privacy measures. The Gramm-Leach-Bliley Act was intended to be technology neutral and provides little guidance on controls or other implementation measures. The FSA recommends the National Institute of Science and Technology's Special Publication 800-171 controls, intended to protect Controlled Unclassified Information (CUI) as GLBA safeguards, and George Mason has accepted that recommendation for this review.

Scope

The scope of this risk analysis is the information infrastructure supporting financial services offered by George Mason University including confidential data that is created, received, transmitted, or stored; and the controls and resources used to eliminate and/or manage vulnerabilities exploitable by threats internal and external to the organization. If exploited, these vulnerabilities could result in:

- Unauthorized disclosure of data
- Unauthorized changes to the system, its data, or both
- Temporary or permanent loss or corruption of data
- Denial of service, access to data, or both to authorized end-users
- Loss of financial cash flow
- Loss of physical assets or resources
- Noticeable negative affect on the organization's mission, reputation, or interest

Throughout the process, a determination of risk to the ***confidentiality*** (protection from unauthorized disclosure of system and data information), ***integrity*** (protection from improper modification of information), and ***availability*** (loss of access) of the systems and data is made and documented. The recommended security safeguards in this report will allow management to make decisions about security-related initiatives to accept, reduce, or eliminate identified risks.

Departments interviewed and determined to be inside the scope of GLBA for this assessment are:

- Accounts Receivable
- Enrollment Management
- Enrollment Services
- Financial Aid
- Information Technology Services
- Institutional Effectiveness and Planning
- University Registrar

Departments interviewed and determined to be outside the scope of GLBA for this assessment are:

- Advancement
- Athletics
- Employee Services

Institution Level Guidance

Issues often affect several departments and align better with broader administrative or technical structures rather than individual departments. These issues are listed in this section so the leadership and technical teams can better focus on these higher-level challenges. Some observations might also appear in the discussion of a specific department to draw attention to issues within that department's direct control. Also, broad issues might be covered at a high level in the narrative discussion with more detail appearing in the individual observations.

Governance

Maintaining GLBA compliance requires a program that integrates into the regular activities of the organization and provides appropriate oversight, and ongoing compliance requires coordination of numerous resources, actions, projects, and people. To improve the accountability of institutions' information security programs, the Safeguards Rule requires George Mason to designate a single Qualified Individual to be responsible for overseeing and implementing the information security program (16 CFR 314.4(a)). It should be noted that the updated rule does not specify any particular level of education, experience, or certification providing the university with the flexibility to designate someone appropriate for the institution. Currently, George Mason has not formally designated an individual to oversee the information security plan as the Qualified Individual.

George Mason's designated Qualified Individual is required to regularly update the board of directors on the overall status of George Mason's Information Security Program, the status of compliance with the GLBA, any material events or decisions that impact the program, and any recommended changes to the program (16 CFR 314.4(i)).

The Safeguards Rule also requires George Mason to formally evaluate and adjust its Information Security Program taking into account the results of the risk assessments and testing required by the GLBA, material changes to operations and the institution, and any other changes that have had a material impact on the Information Security Program (16 CFR 314.4(g)).

Federal Tax Information (FTI)

FTI is a type of Controlled Unclassified Information (CUI) designated by the U.S. National Archives and Records Administration (NARA). The use of FTI is limited to purposes of administering financial aid programs, including determining eligibility for, and amounts of, funds under the Title IV, HEA programs and other financial aid programs offered by George Mason University. FTI may not be redisclosed or used for any other purpose, such as for research in promoting college attendance, persistence, and completion.

FTI originates from the Internal Revenue Service (IRS) and institutions that receive Institutional Student Information Records (ISIR) files from the Department of Education must protect the FTI provided to them by the IRS. ISIRs will include two FTI label fields which mark the beginning and end of the IRS data. The start and end of IRS data is designated as: 'CUI//SP-TAX' within the ISIR file. The FTI labels must be retained wherever the data is used and stored which primarily applies to the Student Information System(s).

Incident Response

The Safeguards Rule requires that relative to customer information, the written incident response plan must specifically address (1) the goals of the plan, (2) the process for responding to security events, (3) a clear definition of roles and responsibilities, (4) plans for communicating both internally and externally, (5) requirements for the remediation of weaknesses identified as part of a response, (6) how an incident response will be documented, and (7) how the incident response process will be reviewed both regularly and after an event. George Mason should review the components of its IRP to ensure it addresses the requirements of the updated GLBA rule, and that the plan is reviewed at least annually and after any event for which the plan is activated. George Mason should also consider conducting regular tabletop exercises and including incident response awareness in its training program to ensure the university community is aware of George Mason's policy and how to engage the response plan (16 CFR 314.4(h)).

Policies, Procedures, and Training

The Gramm-Leach-Bliley Act addresses a broad set of privacy and security parameters that involve people, processes, training, and technology. George Mason has many policies and standards published on their website which should be reviewed and updated as needed to reflect GLBA requirements, and then proactively communicated to all members of the campus community.

Departments handling NPI should assess their procedural documentation, and where necessary, develop and/or update procedures that augment institutional guidance to address the risks and needs specific to their environment. It is recommended that all formally published documents have a section documenting reviews and changes including the dates of those reviews, summaries of changes, and the names of the approvers.

The Safeguards Rule has multiple training requirements. While the requirements remain flexible, allowing institutions to adopt training programs appropriate to their needs, the Safeguards Rule requires personnel with information security responsibilities to receive training sufficient for their roles and/or necessary to address relevant risks. The rule also requires that training curriculum be regularly updated to address emerging threats and institutional changes. Steps must also be taken to regularly verify that information security personnel maintain their certifications or appropriate knowledge levels, and where service providers are utilized to meet information security needs, they should be required to regularly provide assurance to George Mason that GLBA training requirements are being met (16 CFR 314.4(e)).

To ensure that compliance obligations to protect sensitive information are understood by the entire university community, it is required that all personnel receive security awareness training when hired and at least annually thereafter. Anyone who handles or is involved in any way with non-public personal information should also receive specific training on their responsibility to protect sensitive information in general and GLBA related data in particular. George Mason should consider extending its awareness training curriculum to include awareness of university policies related to information security and privacy for the entire campus community including faculty (16 CFR 314.4(e)). The assessment revealed that George Mason gives cyber security awareness training, role-based training and role-based highly sensitive data training which are mandatory and required annually for the respective groups.

Personal Computers and Personal Smart Phones

George Mason allows employees to work from home and institutional issued devices (laptops) are used. If the use of personal devices is deemed necessary, the associated risks must be thoroughly assessed, and appropriate safeguards must be established. For example, personal computers accessing the George Mason network, should be segmented from the broader George Mason network, or technical measures should be employed to ensure the protection of customer data. (16 CFR 314.4(c)).

George Mason permits its employees to use personal smartphones for university business, The university should assess the necessity of this practice for its operations. If the use of personal smartphones is deemed essential, they must be subjected to the same risk evaluation and security standards as devices managed by the institution (16 CFR 314.4(c)). Alternatively, George Mason could implement policies and procedures to ensure that only fully managed devices are utilized for storing, processing, or transmitting sensitive data.

Risk Assessment

IT risk assessments that account for the risks associated with the handling of sensitive personal information are regularly performed. Generally, Information Technology Services would conduct the risk assessment of the IT infrastructure; responsible departments would conduct or participate in assessments of their environments; the administration would contribute through its involvement with the risk management team which is responsible for the overall assessment that pulls the individual assessments into a cohesive whole. George Mason has extended its risk management program to include regular IT risk assessments and ensure the risks associated with handling GLBA related data are addressed (16 CFR 314.4(b)).

The Safeguards Rule requires risk assessments be conducted periodically. In addition, George Mason is required to perform more frequent risk assessments that specifically review the material risks identified by the primary risk assessment along with the effectiveness of any controls put in place to control those risks. Like the primary risk assessment, these additional assessments should update the regular evaluation of the information security program. George Mason should review its risk management program to assure it takes the specifically identified risks associated with handling GLBA related data into account, and that the program itself is reviewed at least annually (16 CFR 314.4(b)(2)).

Storage of Sensitive Data and Encryption

Currently, sensitive data is being stored electronically at George Mason. However, data retention is not consistent. The storage of sensitive data, the standards, processes, and procedures governing the lifecycle of that data will need to be reviewed and developed and/or updated as appropriate. The retention period must be formally documented, and that period must be based upon either a legal requirement or a reasonable business need. Processes must be developed and implemented to regularly review all stored sensitive data to assure the retention period is not exceeded and expired data is securely destroyed. George Mason should also evaluate its business and legal need to store sensitive data and, if appropriate, redesign its business processes to eliminate the need to store that data (16 CFR 314.4(c)(6)).

The Safeguards Rule also requires encryption of customer information both in transit and at rest. This requirement has flexibility to secure customer information with alterative equivalent controls that have been reviewed and approved by the designated Qualified Individual. George Mason should review all systems where customer information is stored to ensure that information is either encrypted or adequately protected. Additionally, George Mason should review its policies to ensure sensitive information is encrypted both in transit and at rest (16 CFR 314.4(c)(3)).

Service Providers

George Mason uses third-party service providers to handle aspects of their data processing environment. All third parties used in the processing of sensitive information must provide evidence to George Mason of their privacy and security programs effectiveness. George Mason should review its vendor management program to ensure it includes a process that documents the responsibilities of each of its service providers, as well as their associated attestations of GLBA compliance. The GLBA Safeguards Rule requires George Mason to oversee its service providers and also requires those providers be periodically reviewed. All third parties used in the processing of sensitive information must provide evidence to George Mason of the effectiveness of their privacy and security programs at least annually. Both the program and the compliance status of George Mason's service providers must be reviewed at least annually (16 CFR 314.4(f)).

Shared Services

The impact of services like Active Directory that can be shared between the systems servicing sensitive data and the broader campus environment should be reviewed. Any system that stores, processes, or transmits GLBA data, or that can affect the security of that data could be in the scope of GLBA requirements. Typically, these services include (but are not limited to) account management and authentication, patch management, antivirus, time synchronization, and DNS. The Risk and Compliance Team should evaluate and define both the current scope and alternatives for scope reduction.

User Accounts and Access Control

George Mason leverages user accounts and groups to manage access to systems and applications. The standards governing these accounts and groups provide security and accountability across the information environment. Creating, managing, and monitoring accounts is a cornerstone to the information security strategy. Also, the need for assigned access privileges changes over time reflecting changes in organization, operations, and threats. George Mason has formal policies and procedures that manage the creation, modification, and deletion of user accounts and group membership address the requirements of managing access to customer information.

In many cases the responsibility to manage group memberships and other measures that control access to NPI is distributed to departments and custodians. It is recommended that the process be reviewed to confirm that the approval and review workflows are in-place, documented, and operating correctly (16 CFR 314.4(c)).

George Mason uses a Banner Administrative Systems Account Request form and has Banner Security Officers to document and control access to the Banner student information system. Access to Banner is periodically reviewed to ensure only authorized users are allowed access to Banner.

System Monitoring

The Safeguards Rule requires George Mason to monitor systems for unauthorized access of customer information. The rule offers two paths to compliance: periodic penetration testing or continuous monitoring and vulnerability assessments. Continuous monitoring is real-time, ongoing monitoring of security threats, configuration changes, and other identified vulnerabilities. Alternatively, George Mason can perform both annual penetration testing and vulnerability assessments. Currently, George Mason performs continuous monitoring, vulnerability scanning and is in the process of performing penetration testing. The university should review these programs to ensure they include all in-scope systems. Additionally George Mason should review its current systems and vulnerability management programs to determine the most appropriate way to address the requirements and ensure its practices are reflected in its policies and procedures (16 CFR 314.4(d)). Currently, George Mason uses Splunk as their SIEM for monitoring and alerting.

Multi-factor Authentication(MFA)

The Safeguards Rule requires institutions to implement MFA to control access to customer information for both systems and networks that contain GLBA in scope data. It should be noted that the rule provides George Mason some flexibility on the requirement allowing the use of alternative and equivalent access controls with the written approval of the designated Qualified Individual (16 CFR 314.4(c)(5)). The university should implement a process to regularly verify that all access to in-scope GLBA data requires the use of MFA.

General Guidance/Recommendations

Assessments often lead to observations that are not categorized into specific regulatory requirements, but should be reviewed and addresses, or whose risks should be evaluated.

- Retain the CUI labeling of FTI wherever ISIR data is stored and used within the student information system(s).
- Consider developing a diagram of data flows for GLBA data.
- Confirm GLBA training clearly defines in-scope GLBA data.
- Recommend the use of data sharing agreements for financial aid data.
- Review HR processes to ensure access reviews are included for internal transfers.
- Confirm data retention policy addresses email containing NPI.
- Review data repository data retention practices (imaging, shared storage, etc.)
- Ensure data classification-based controls account for GLBA.
- Ensure all systems/servers in GLBA scope are sending logs to Splunk.
- Consider developing a formal “Clean Desk” policy for departments that handle sensitive data.
- Consider using a FACTA Red Flags training program. FACTA Red Flags: Program Checklist - CampusGuard
- Ensure separation of duties occurs in Financial Aid office when granting access or sharing data. Recommend Director Student Financial Aid only approve requests and Assistant Director only implements the requests.

Understanding the GLBA Assessment Tables in the Report

This GLBA assessment report is divided into two sections of observations. The first section, *Institutional Observations*, details those observations of risk that were found across multiple or all departments. The second section, *Departmental Observations*, breaks down observations for each department so that a more focused approach may be applied where necessary. The observations and mitigations, along with assumed risk and relevant NIST 800-171 controls, are presented in the following table format:

Observation #	***Threat Evaluation***			***Mitigation Effort***
	Likelihood	**Impact**	**Risk**	
Description of the risk to systems, processes, or information.	Low /Med/ High	Low /Med/ High	Low /Med/ High	Low /Med/ High
Recommendation(s)				
• Suggested action(s) to take for mitigation of risk.				
GLBA Safeguards Rule Reference(s)				
• **§314.3** Standards for safeguarding customer information.				
NIST SP 800-171 Reference(s)				
• **3.1** Access Control(s)				

Observation – Description of the risk to systems, processes, or information.

Threat Evaluation – Indicates the likelihood of occurrence of the threat, potential impact due to a failure to mitigate the threat, and overall risk to the organization that is posed by the threat. See *Appendix B: Risk Scale and Necessary Actions* for explanation of Low/Med/High ratings.

Mitigation Effort – Indicates the level of difficulty or cost associated with mitigating the threat as recommended.

Recommendation(s) – Suggested action(s) to take for mitigation of risk.

Institutional Observations

Issues identified that align better with broader administrative or technical structures, rather than individual departments, are listed in this section so the leadership and technical teams can provide an organizationally higher level of focus to these challenges. There may be some crossover between these issues and those found in individual departments and the effort to mitigate or reduce the risks may also be shared with those departments.

Observation 1	***Threat Evaluation***			***Mitigation Effort***
	Likelihood	**Impact**	**Risk**	
The existing Information Technology Security Program (Policy 1311) does not contain all the elements for GLBA compliance.	Med	Med	Med	Med

Recommendation(s)

- Develop a Written Information Security Program (WISP) for the purposes of GLBA compliance or expand policy 1311. At a minimum, the WISP must address the 9 required elements outlined by the FTC.
- https://fsapartners.ed.gov/knowledge-center/library/electronic-announcements/2023-02-09/updates-gramm-leach-bliley-act-cybersecurity-requirements
- Communicate George Mason's GLBA compliance on GMU.edu website and direct compliance inquiries/requests to the appropriate George Mason individual/role (QI).
- Optionally, provide mechanism for WISP to be downloaded for audit purposes.

GLBA Safeguards Rule Reference(s)

- **§314.3(a)** Information security program. You shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue. The information security program shall include the elements set forth in § 314.4 and shall be reasonably designed to achieve the objectives of this part, as set forth in paragraph (b) of this section.

NIST SP 800-171 Reference(s)

- **Not Applicable**

Observation 2	***Threat Evaluation***			***Mitigation Effort***
	Likelihood	**Impact**	**Risk**	
A Qualified Individual (QI) to manage and administer the Information Security Program is not formally identified.	Low	Low	Med	Med

Recommendation(s)

- Formally designate in writing the role or individual who is responsible for managing and administering the Information Security Program for George Mason University.
- Alternatively, the role can be outsourced which adds additional requirements. See CFR 314.4(a)(1), 314.4(a)(2) & 314.4(a)(3).

GLBA Safeguards Rule Reference(s)

- **§314.4(a)** Designate a qualified individual responsible for overseeing and implementing your information security program and enforcing your information security program (for purposes of this part, "Qualified Individual"). The Qualified Individual may be employed by you, an affiliate, or a service provider. To the extent the requirement in this paragraph (a) is met using a service provider or an affiliate, you shall:
- **§314.4(a)(1)** Retain responsibility for compliance with this part;
- **§314.4(a)(2)** Designate a senior member of your personnel responsible for direction and oversight of the Qualified Individual; and
- **§314.4(a)(3)** Require the service provider or affiliate to maintain an information security program that protects you in accordance with the requirements of this part.

NIST SP 800-171 Reference(s)

- **Not Applicable**

Departmental Observations

During the assessment, CampusGuard met with multiple departments to discuss their business practices and technical processes. Several issues were identified ranging from simple items such as a lack of written procedures to more complex items such as the use of unsecured email for the transmission of NPI. Those identified issues are covered below. There may be some crossover in observations both between departments and the institution. Also, the controls to mitigate or reduce the risks may be shared.

Accounts Receivable

Interviewees:	Clare Laskofski Bill Cunningham

Upon completion of interview, it was determined that Accounts Receivable falls inside of GLBA scope but no concerns around GLBA compliance were found.

See General Guidance/Recommendations and Institutional Observations for additional consideration.

Advancement

Interviewees:	John Smilde

Upon completion of interview, it was determined that Advancement is outside of GLBA scope.

See General Guidance/Recommendations and Institutional Observations for additional consideration.

Athletics

Interviewees:	Robert Smith Malcolm Grace

Upon completion of interview, it was determined that Athletics is outside of GLBA scope.

See General Guidance/Recommendations and Institutional Observations for additional consideration.

Employee Services

Interviewees:

Andrew Lane
Clifton Murray
Michelle Lim
Patricia Coray
Robyn Madar

Upon completion of interview, it was determined that Employee Services is outside of GLBA scope.

See General Guidance/Recommendations and Institutional Observations for additional consideration.

Enrollment Management

Interviewees: Dan Fisher

Observation 1	*Threat Evaluation*			*Mitigation Effort*
	Likelihood	**Impact**	**Risk**	
GLBA training being offered/completed is unconfirmed.	Low	Low	Low	Low
Recommendation(s)				
• Ensure all in-scope GLBA departments complete GLBA training annually.				
GLBA Safeguards Rule Reference(s)				
• **§314.4(e)(1)** Providing your personnel with security awareness training that is updated as necessary to reflect risks identified by the risk assessment.				
NIST SP 800-171 Reference(s)				
• **3.2.1** Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems. • **3.2.2** Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.				

Enrollment Services

Interviewees:	Andrew Bunting Kathy Zimmerman

Upon completion of interview, it was determined that Enrollment Services falls inside of GLBA scope but no concerns around GLBA compliance were found.

See General Guidance/Recommendations and Institutional Observations for additional consideration.

Financial Aid

Interviewees:	Alethia Shipman Cassandra Thomas

Observation 1	***Threat Evaluation***			***Mitigation Effort***
	Likelihood	**Impact**	**Risk**	
[redacted]	Low	Low	Low	Low
Note: [redacted]				
Recommendation(s)				
• [redacted] • [redacted]				
GLBA Safeguards Rule Reference(s)				
• **§314.4(c)(6)(i)** Develop, implement, and maintain procedures for the secure disposal of customer information in any format no later than two years after the last date the information is used in connection with the provision of a product or service to the customer to which it relates, unless such information is necessary for business operations or for other legitimate business purposes, is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained. • **§314.4(c)(6)(ii)** Periodically review your data retention policy to minimize the unnecessary retention of data.				
NIST SP 800-171 Reference(s)				
• **Not Applicable**				

Information Technology Services (ITS)

Interviewees:	Allen Santora Casey Campbell Haoxin Song Lori Polnow Nico Clemente

Observation 1	***Threat Evaluation***			***Mitigation Effort***
	Likelihood	**Impact**	**Risk**	
[redacted]	Med	Med	High	Med

Recommendation(s)

- [redacted]

GLBA Safeguards Rule Reference(s)

- **§314.4(c)(3)** Protect by encryption all customer information held or transmitted by you both in transit over external networks and at rest. To the extent you determine that encryption of customer information, either in transit over external networks or at rest, is infeasible, you may instead secure such customer information using effective alternative compensating controls reviewed and approved by your Qualified Individual.

NIST SP 800-171 Reference(s)

- **3.13.16** Protect the confidentiality of CUI at rest.

Observation 2	***Threat Evaluation***			***Mitigation Effort***
	Likelihood	**Impact**	**Risk**	
[redacted]	Med	Med	High	Low

Recommendation(s)

- [redacted]

GLBA Safeguards Rule Reference(s)

- **§314.4(c)(3)** Protect by encryption all customer information held or transmitted by you both in transit over external networks and at rest. To the extent you determine that encryption of customer information, either in transit over external networks or at rest, is infeasible, you may instead secure such customer information using effective alternative compensating controls reviewed and approved by your Qualified Individual.

NIST SP 800-171 Reference(s)

- **3.13.16** Protect the confidentiality of CUI at rest.

Observation 3	***Threat Evaluation***			***Mitigation Effort***
	Likelihood	**Impact**	**Risk**	
[redacted]	Med	Med	Med	Med

Recommendation(s)

- [redacted]

GLBA Safeguards Rule Reference(s)

- **§314.4(c)(8)** Implement policies, procedures, and controls designed to monitor and log the activity of authorized users and detect unauthorized access or use of, or tampering with, customer information by such users.

NIST SP 800-171 Reference(s)

- **3.14.3** Monitor system security alerts and advisories and take action in response.
- **3.14.7** Identify unauthorized use of organizational systems.

Observation 4	***Threat Evaluation***			***Mitigation Effort***
	Likelihood	**Impact**	**Risk**	
[redacted]	Med	Med	Med	Low

Recommendation(s)

- [redacted]
- [redacted]

GLBA Safeguards Rule Reference(s)

- **§314.4(c)(6)(i)** Develop, implement, and maintain procedures for the secure disposal of customer information in any format no later than two years after the last date the information is used in connection with the provision of a product or service to the customer to which it relates, unless such information is necessary for business operations or for other legitimate business purposes, is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained; and
- **§314.4(c)(6)(ii)** Periodically review your data retention policy to minimize the unnecessary retention of data.

NIST SP 800-171 Reference(s)

- **Not Applicable**

Observation 5	***Threat Evaluation***			***Mitigation Effort***
	Likelihood	**Impact**	**Risk**	
The roles, responsibilities and levels of decision-making authority are not clearly identified in Incident Management Process.	Med	Med	Med	Med

Recommendation(s)

- Update ITS.ESD-PRS004 Incident Management Process v3.0final_Level 3.pdf to include a RACI chart of Responsibilities, Accountability, Consulted and Informed.

GLBA Safeguards Rule Reference(s)

- **§314.4(h)(3)** The definition of clear roles, responsibilities, and levels of decision-making authority;

NIST SP 800-171 Reference(s)

- **3.6.1** Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.

Observation 6	***Threat Evaluation***			***Mitigation Effort***
	Likelihood	**Impact**	**Risk**	
External communication actions and information sharing parameters are not identified in Incident Management Process.	Med	Med	Med	Med

Recommendation(s)

- Update ITS.ESD-PRS004 Incident Management Process v3.0final_Level 3.pdf to include a RACI chart of Responsibilities, Accountability, Consulted and Informed.

GLBA Safeguards Rule Reference(s)

- **§314.4(h)(4)** External and internal communications and information sharing.

NIST SP 800-171 Reference(s)

- **3.6.2** Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.

Observation 7	***Threat Evaluation***			***Mitigation Effort***
	Likelihood	**Impact**	**Risk**	
The criteria to confirm remediation of a cybersecurity incident are not clearly stated in the Incident Management Process.	Low	Med	Med	Low

Recommendation(s)

- Update ITS.ESD-PRS004 Incident Management Process v3.0final_Level 3.pdf to include the parameters/conditions of a successful recovery from a cybersecurity event/incident.

GLBA Safeguards Rule Reference(s)

- **§314.4(h)(5)** Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;

NIST SP 800-171 Reference(s)

- **3.6.1** Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.
- **3.6.3** Test the organizational incident response capability.

Observation 8	***Threat Evaluation***			***Mitigation Effort***
	Likelihood	**Impact**	**Risk**	
Existing inventories do not identify in-scope GLBA systems and data.	Low	Med	Med	Med
Recommendation(s)				
• Improve inventories to distinguish in-scope GLBA systems and whether the systems process, store or transmit Non-public Personal Information.				
GLBA Safeguards Rule Reference(s)				
• **§314.4(c)(2)** Identify and manage the data, personnel, devices, systems, and facilities that enable you to achieve business purposes in accordance with their relative importance to business objectives and your risk strategy.				
NIST SP 800-171 Reference(s)				
• **3.4.1** Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.				

Observation 9	***Threat Evaluation***			***Mitigation Effort***
	Likelihood	**Impact**	**Risk**	
There are no data flow diagrams that show the flow of sensitive data from Banner to other interconnected systems.	Low	Med	Med	Med
Recommendation(s)				
• Identify and document all in-scope GLBA data contained in Banner and the subsequent systems that Banner feeds.				
GLBA Safeguards Rule Reference(s)				
• **§314.4(c)(2)** Identify and manage the data, personnel, devices, systems, and facilities that enable you to achieve business purposes in accordance with their relative importance to business objectives and your risk strategy.				
NIST SP 800-171 Reference(s)				
• **3.12.4** Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.				

Observation 10	***Threat Evaluation***			***Mitigation Effort***
	Likelihood	**Impact**	**Risk**	
[redacted]	Med	Med	Med	Low

Recommendation(s)

- [redacted]
- Consider update to https://its.gmu.edu/working-with-its/it-security-office/it-security-standards/password-complexity-standard/ to include a section for GLBA compliance that is similar to the section *For PCI Compliance*.

GLBA Safeguards Rule Reference(s)

- **§314.3(b)(3)** Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

NIST SP 800-171 Reference(s)

- **3.5.5** Prevent reuse of identifiers for a defined period.

Institutional Effectiveness and Planning

Interviewees:

Gesele Durham
Patrick Kimball
Lisa Anh Nguyen
Yi Yuan

<table>
<tr><th><em>Observation 1</em></th><th colspan="3"><em>Threat Evaluation</em></th><th><em>Mitigation Effort</em></th></tr>
<tr><td rowspan="2">[redacted]</td><th>Likelihood</th><th>Impact</th><th>Risk</th><td rowspan="2">Low</td></tr>
<tr><td>Low</td><td>Med</td><td>Med</td></tr>
<tr><th colspan="5"><em>Recommendation(s)</em></th></tr>
<tr><td colspan="5">• [redacted]
• [redacted]
• [redacted]</td></tr>
<tr><th colspan="5"><em>GLBA Safeguards Rule Reference(s)</em></th></tr>
<tr><td colspan="5">• <strong>§314.4(c)(1)(i)</strong> Authenticate and permit access only to authorized users to protect against the unauthorized acquisition of customer information.</td></tr>
<tr><th colspan="5"><em>NIST SP 800-171 Reference(s)</em></th></tr>
<tr><td colspan="5">• <strong>3.5.3</strong> Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.</td></tr>
</table>

Observation 2	***Threat Evaluation***			***Mitigation Effort***
	Likelihood	**Impact**	**Risk**	
[redacted]	Med	Med	High	Low

Recommendation(s)

- Follow secure disposal guidance from University Records Management office. In lieu of institutional guidance, follow state of Virginia guidance.
- Document process and perform secure disposal of data on a periodic basis or annual frequency at minimum unless a business justification exists. If extended data retention is necessary, ensure QI approves documented process in writing.

GLBA Safeguards Rule Reference(s)

- **§314.4(c)(6)(i)** Develop, implement, and maintain procedures for the secure disposal of customer information in any format no later than two years after the last date the information is used in connection with the provision of a product or service to the customer to which it relates, unless such information is necessary for business operations or for other legitimate business purposes, is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.
- **§314.4(c)(6)(ii)** Periodically review your data retention policy to minimize the unnecessary retention of data.

NIST SP 800-171 Reference(s)

- **3.8.1** Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.
- **3.8.9** Protect the confidentiality of backup CUI at storage locations.

University Registrar

Interviewees: Doug McKenna

Observation 1	***Threat Evaluation***			***Mitigation Effort***
	Likelihood	**Impact**	**Risk**	
[redacted]	Low	Med	Med	Low

Recommendation(s)

- Follow secure disposal guidance from University Records Management office. In lieu of institutional guidance, follow state of Virginia guidance.
- Document process and perform secure disposal of data on a periodic basis or annual frequency at minimum unless a business justification exists. If extended data retention is necessary, ensure QI approves documented process in writing.

GLBA Safeguards Rule Reference(s)

- **§314.4(c)(6)(i)** Develop, implement, and maintain procedures for the secure disposal of customer information in any format no later than two years after the last date the information is used in connection with the provision of a product or service to the customer to which it relates, unless such information is necessary for business operations or for other legitimate business purposes, is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.
- **§314.4(c)(6)(ii)** Periodically review your data retention policy to minimize the unnecessary retention of data.

NIST SP 800-171 Reference(s)

- **Not Applicable**

Closing

Protection of data for regulatory purposes requires the cooperative synergy of an organization's information security and privacy programs along with administrative, technical, and physical controls applied in accordance with a risk assessment. The overall goal is to prevent and minimize the impact of a breach by implementing technical and administrative controls commensurate with the relative risk to sensitive information.

Observations in this report should improve management awareness of actions needed to continue critical efforts to comply with the Gramm-Leach-Bliley Act and reduce the likelihood of data being compromised. Some of the risks that require management action include training for those with information security responsibilities; the review and updating of policies, plans, and procedures that govern data access; and investment of time and resources to procure, install, maintain, and operate systems that provide and monitor the security of customer information.

Once the report is reviewed, it is recommended the university leverage the report to enhance the ongoing efforts of reducing risk by guiding staff through remediation and implementation of recommendations. The observations in this report can be used to develop a project plan for managing and prioritizing remediation. Because information security presents ever-evolving challenges, George Mason University will need to keep the plan current by staying abreast of industry and regulatory changes and regularly assessing risk.

It should be mentioned that some of the recommendations that are given may already have been implemented by the time the report is reviewed. Many of the staff were willing to address what is necessary to protect customer information and may have already acted on some recommendations discussed during the interview process.

CampusGuard thanks the George Mason University team for their assistance and involvement during the remote interview process. We look forward to a continued partnership and your ongoing information security and GLBA compliance efforts.

Greg Lewis
Security Advisor
CampusGuard

Appendix A: Threat Identification Overview

This information was taken directly from the NIST SP 800-30

Threat Identification Overview

NIST SP 800-30 describes the identification of the threat, the threat source and threat action for use in the assessment process. The following is a definition for each:

1. **Threat –** The potential for a particular threat-source to successfully exercise a particular vulnerability. *(A **vulnerability** is a flaw or weakness that can be accidentally triggered or intentionally exploited and result in a security breach or violation of policy)*.
2. **Threat Source –** Any circumstance or event with the potential to cause harm to an IT system. The common threat sources can be natural, human, or environmental which can impact the organization's ability to protect confidential or sensitive data.
3. **Threat Action –** The method by which an attack might be carried out (e.g., hacking, system intrusion).

Threat Sources

A threat-source is any circumstance or event with the potential to cause harm to an information technology system and its processing environment. Common threat-sources are natural, human, and environmental. Threat sources can threaten the facilities, systems, data, personnel, utilities, and physical operations and how they function, their ability to perform their responsibilities/duties, or exposes them to disruption and/or harm.

Level	Likelihood Definitions
Threat	The potential for a particular threat-source to successfully exercise a particular vulnerability. *(A **vulnerability** is a flaw or weakness that can be accidentally triggered or intentionally exploited and result in a security breach or violation of policy)*.
Threat Source	Any circumstance or event with the potential to cause harm to an IT system. The common threat sources can be natural, human, or environmental which can impact the organization's ability to protect confidential or sensitive data.
Threat Action	The method by which an attack might be carried out (e.g., hacking, system intrusion).

Appendix B: Risk Scale and Necessary Actions

This information was taken directly from the NIST SP 800-30

The following Risk Scale and Necessary Actions table presents actions that NIST SP 800-30 recommends senior management (the mission owners) must take for each risk level. George Mason University to determine if this will be used, or another methodology.

Risk Level	Risk Description and Necessary Actions
High	If an observation or observation or is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Medium	If an observation or observation is rated as medium risk, corrective actions are needed, and a plan must be developed to incorporate these actions within a reasonable period of time.
Low	If an observation or observation is described as low risk, the system's Designated Approving Authority (DAA) must determine whether corrective actions are still required or decide to accept the risk.

Appendix C: Risk Likelihood, Risk Impact, and Risk Level Definitions

This information was taken directly from the NIST SP 800-30

Level	Likelihood Definitions
High	The threat source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Moderate	The threat source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low	The threat source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

Impact Analysis: The adverse impact of a security event in terms of loss or degradation of any, or a combination of any, of the following three security goals, resulting from successful exploitation of a vulnerability:

- Loss of Confidentiality – Impact of unauthorized disclosure of confidential information (ex. Privacy Act). Unauthorized, unanticipated, or unintentional disclosure could result in loss of public confidence, embarrassment, or legal action against the organization.
- Loss of Integrity – Impact if system or data integrity is compromised by intentional or accidental changes to the data or system.
- Loss of Availability – Impact to system functionality and operational effectiveness should systems be unavailable to end users.

Magnitude of Impact	Impact Definitions
High	Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury.
Medium	Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm or impeded an organization's mission, reputation, or interest; or (3) may result in human injury.
Low	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources; (2) may noticeably affect an organization's mission, reputation, or interest.

Risk Level Determination: These levels represent the degree or level of risk to which an IT system, facility, or procedure might be exposed if a given vulnerability were exercised:

- The likelihood of a given threat source's attempting to exercise a given vulnerability.
- The magnitude of the impact should a threat-source successfully exercise the vulnerability.
- The adequacy of planned or existing security controls for reducing or eliminating risk.

Magnitude of Impact	Risk Level Definitions
High	There is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Medium	Corrective actions are needed, and a plan must be developed to incorporate these actions within a reasonable period of time.
Low	The system's Authorizing Official must determine whether corrective actions are still required or decide to accept the risk.

Appendix D: NIST Risk Mitigation Methodology Activities

This information was taken directly from the NIST SP 800-30

Input	**Risk Mitigation Activities**	**Output**
Risk levels from the risk assessment report	**Step 1.** Prioritize Actions	Actions ranking from high to low
Risk assessment report	**Step 2.** Evaluate Recommended Control Options • Feasibility • Effectiveness	List of possible controls
	Step 3. Conduct Cost-Benefit Analysis • Impact of implementing • Impact of not implementing • Associated costs	Cost-benefit analysis
	Step 4: Select Controls	Selected controls
	Step 5: Assign Responsibility	List of responsible persons
	Step 6: Develop Safeguard Implementation Plan • Risks and Associated Risk Levels • Prioritized Actions • Recommended Controls • Selected Planned Controls • Responsible Persons • Start Date • Target Completion Date • Maintenance Requirements	Safeguard implementation plan
	Step 7: Implement Selected Controls	Residual risks

Appendix E: Risk Analysis and Management

Risk Analysis Approach

Methodology

The risk analysis was conducted using guidelines in NIST SP 800-30, *Risk Management Guide for Information Technology Systems*. There are three main segments of control that are evaluated during the assessment:

- ***Management Controls:*** Management of the information technology security system and the acceptance of risk.
- ***Operational Controls:*** Security methods focusing on mechanisms implemented and executed primarily by people (as opposed to systems or technology), including all aspects of physical security, media safeguards, and inventory controls.
- ***Technical Controls:*** Hardware and software controls providing automated protection to the systems or applications (technical controls operate within the IT system and applications).

Data Collection Phase

The data collection and assessment phase included identifying and interviewing key personnel within the organization and conducting document reviews. Interviews were focused on the operating environment, process, and procedures. Documents were reviewed to provide a base on which to evaluate compliance with security policies and procedures.

The interview process was also used to identify system and location-specific threats and vulnerabilities (Appendix B), and associated controls. An understanding of the technical and non-technical security controls in place at an organization helps identify opportunities to reduce the list of vulnerabilities, as well as the probability of a threat being exploited and compromising confidential information.

Risks to systems were ranked based on risk tolerance and operational objectives important to the organization. Vulnerabilities may be identified as individual risks or may be combined into a single risk based upon likelihood and impact (Appendix C).

Risk Likelihood, Impact Analysis, & Determination

The goal of this step is to determine an overall likelihood rating that indicates the probability that a vulnerability could be exploited by a threat-source given the existing or planned security controls, as well as the level of adverse impact that would result from a threat successfully exploiting a vulnerability.

The likelihood that a potential vulnerability may happen, the impact that would result from a successful threat exploiting a vulnerability, and the risk determination (level of risk) were determined by using the NIST SP 800-30 Risk Likelihood, Risk Impact, and Risk Level Definitions (Appendix D).

Risk Management Approach

Risk Mitigation

Risk mitigation involves evaluating, prioritizing, and implementing appropriate safeguards to reduce identified risks during the risk analysis process. The goal is to ensure the confidentiality, integrity, and availability of George Mason's systems.

Because the elimination of all risk is impractical, senior management, risk managers, and business managers will assess control recommendations, determine the acceptable level of residual risk, perform cost-benefit analyses, and approve implementation of those controls that have the greatest risk reduction impact in the most cost-effective manner to meet security regulation requirements.

Refer to Appendix E for NIST Risk Mitigation Activities, and to NIST SP 800-30 for additional methods to mitigate known and potential risks.

Evaluate and Prioritize Risks

Safeguarding recommendations are the results of the risk analysis process and provide a basis by which the authorizing official can evaluate and prioritize the identified risks and their associated controls.

The project team will work across the organization to develop a Risk Mitigation Implementation Plan if necessary, including recommended controls. At this point, the system contacts can collaborate to either accept the control recommendations, provide alternative suggestions, or reject the control recommendations and accept the risk.

The Risk Mitigation Implementation Plan should include risks identified as medium to high priority levels. Low risk priority levels are not generally included as they are assumed to currently be organizationally accepted risks but should be evaluated once the medium to high priority risks are addressed.

Identify Controls to Mitigate or Eliminate Risks

Controls, safeguarding recommendations, and/or actions that could reduce or eliminate the likelihood and/or impact of the associated risks that are identified should be documented in the Risk Mitigation Implementation Plan.

The Security Advisor considered all of the following factors when recommending controls and solutions to minimize or eliminate risks (note: these are not in any particular order):

- Sensitivity of the data and the system
- Previous security incidents
- Safety, reliability, and/or effectiveness of controls
- System compatibility and dependencies
- Incompatibilities with other controls
- Legislation and regulations
- Organizational policies and procedures
- Operational impact
- Budgetary constraints

- Other resource constraints

Implement Safeguards Based on NIST SP 800-171 Controls

- Implement the controls that have been approved and budgeted by senior management, in order of priority (e.g., greatest impact first).
- Wherever possible, objectively measure the effective reduction in risk as a result of the control and document this result.
- Identify and resolve unintended problems associated with the control implementation.

Ongoing Monitoring

- Ongoing monitoring will be done to determine if new risks have developed.
- Ongoing monitoring includes, but is not limited to, the following:
    - Conduct periodic reviews/mini risk assessment of security controls to measure their ongoing effectiveness and document the results.
    - Perform periodic system audits/mini risk assessment, such as before upgrading and purchasing new systems, with significant personnel changes, implementing new security policies, etc. When a new or upgraded system is introduced to the organization, a review must be done in order to determine if a new risk analysis must be conducted due to the introduction of new assets in the organization.
    - After conducting ongoing risk evaluation mitigate new risks identified.
- Complete a Risk Analysis/Assessment on a scheduled basis (e.g., every year or as needed to meet the organization's risk needs, regulatory requirements, other applicable Standards, etc.).

Results Documentation and Reporting to Management

- Provide an annual summary of the risk analysis to management to:
    - Help management understand the risks.
    - Help make decisions on policy, procedure, budget, and system operational and management changes.
    - Help make resource allocation decisions to reduce and correct potential and known risks.
- Fully document risk mitigation strategies and processes including those that:
    - Have been approved, budgeted, and implemented.
    - Have been approved and budgeted, but not yet implemented.
    - Have been approved but are not yet budgeted.
    - Have not been approved (including the reason).
    - The above documentation will be maintained for a period of time commensurate with the documented retention policy.

Appendix F: NIST SP 800-171 Requirements

This information was taken directly from the NIST SP 800-171

3.1 ACCESS CONTROL

Basic Security Requirements

3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).

3.1.2 Limit system access to the types of transactions and functions that authorized users are permitted to execute.

Derived Security Requirements

3.1.3 Control the flow of CUI in accordance with approved authorizations.

3.1.4 Separate the duties of individuals to reduce the risk of malevolent activity without collusion.

3.1.5 Employ the principle of least privilege, including for specific security functions and privileged accounts.

3.1.6 Use non-privileged accounts or roles when accessing non-security functions.

3.1.7 Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.

3.1.8 Limit unsuccessful logon attempts.

3.1.9 Provide privacy and security notices consistent with applicable CUI rules.

3.1.10 Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.

3.1.11 Terminate (automatically) a user session after a defined condition.

3.1.12 Monitor and control remote access sessions.

3.1.13 Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.

3.1.14 Route remote access via managed access control points.

3.1.15 Authorize remote execution of privileged commands and remote access to security-relevant information.

3.1.16 Authorize wireless access prior to allowing such connections.

3.1.17 Protect wireless access using authentication and encryption.

3.1.18 Control connection of mobile devices.

3.1.19 Encrypt CUI on mobile devices and mobile computing platforms.21

3.1.20 Verify and control/limit connections to and use of external systems.

3.1.21 Limit use of portable storage devices on external systems.

3.1.22 Control CUI posted or processed on publicly accessible systems.

3.2 AWARENESS AND TRAINING

Basic Security Requirements

3.2.1 Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.

3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.

Derived Security Requirements

3.2.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat.

3.3 AUDIT AND ACCOUNTABILITY

Basic Security Requirements

3.3.1 Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.

3.3.2 Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.

Derived Security Requirements

3.3.3 Review and update logged events.

3.3.4 Alert in the event of an audit logging process failure.

3.3.5 Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.

3.3.6 Provide audit record reduction and report generation to support on-demand analysis and reporting.

3.3.7 Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.

3.3.8 Protect audit information and audit logging tools from unauthorized access, modification, and deletion.

3.3.9 Limit management of audit logging functionality to a subset of privileged users.

3.4 CONFIGURATION MANAGEMENT

Basic Security Requirements

3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational systems.

Derived Security Requirements

3.4.3 Track, review, approve or disapprove, and log changes to organizational systems.

3.4.4 Analyze the security impact of changes prior to implementation.

3.4.5 Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.

3.4.6 Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.

3.4.7 Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.

3.4.8 Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.

3.4.9 Control and monitor user-installed software.

3.5 IDENTIFICATION AND AUTHENTICATION

Basic Security Requirements

3.5.1 Identify system users, processes acting on behalf of users, and devices.

3.5.2 Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.

Derived Security Requirements

3.5.3 Use multifactor authentication22 for local and network access23 to privileged accounts and for network access to non-privileged accounts.

3.5.4 Employ replay-resistant authentication mechanisms for network access to privileged and non- privileged accounts.

3.5.5 Prevent reuse of identifiers for a defined period.

3.5.6 Disable identifiers after a defined period of inactivity.

3.5.7 Enforce a minimum password complexity and change of characters when new passwords are created.

3.5.8 Prohibit password reuse for a specified number of generations.

3.5.9 Allow temporary password use for system logons with an immediate change to a permanent password.

3.5.10 Store and transmit only cryptographically-protected passwords.

3.5.11 Obscure feedback of authentication information.

3.6 INCIDENT RESPONSE

Basic Security Requirements

3.6.1 Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.

3.6.2 Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.

Derived Security Requirements

3.6.3 Test the organizational incident response capability.

3.7 MAINTENANCE

Basic Security Requirements

3.7.1 Perform maintenance on organizational systems.

3.7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.

Derived Security Requirements

3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI.

3.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.

3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.

3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization.

3.8 MEDIA PROTECTION

Basic Security Requirements

3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.

3.8.2 Limit access to CUI on system media to authorized users.

3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse.

Derived Security Requirements

3.8.4 Mark media with necessary CUI markings and distribution limitations.

3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.

3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.

3.8.7 Control the use of removable media on system components.

3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner.

3.8.9 Protect the confidentiality of backup CUI at storage locations.

3.9 PERSONNEL SECURITY

Basic Security Requirements

3.9.1 Screen individuals prior to authorizing access to organizational systems containing CUI.

3.9.2 Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.

3.10 PHYSICAL PROTECTION

Basic Security Requirements

3.10.1 Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.

3.10.2 Protect and monitor the physical facility and support infrastructure for organizational systems.

Derived Security Requirements

3.10.3 Escort visitors and monitor visitor activity.

3.10.4 Maintain audit logs of physical access.

3.10.5 Control and manage physical access devices.

3.10.6 Enforce safeguarding measures for CUI at alternate work sites.

3.11 RISK ASSESSMENT

Basic Security Requirements

3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.

Derived Security Requirements

3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.

3.11.3 Remediate vulnerabilities in accordance with risk assessments.

3.12 SECURITY ASSESSMENT

Basic Security Requirements

3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.

3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.

3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.

3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

3.13 SYSTEM AND COMMUNICATIONS PROTECTION

Basic Security Requirements

3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.

3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.

Derived Security Requirements

3.13.3 Separate user functionality from system management functionality.

3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.

3.13.5 Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

3.13.6 Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

3.13.7 Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).

3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.

3.13.9 Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.

3.13.10 Establish and manage cryptographic keys for cryptography employed in organizational systems.

3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.

3.13.12 Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.

3.13.13 Control and monitor the use of mobile code.

3.13.14 Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.

3.13.15 Protect the authenticity of communications sessions.

3.13.16 Protect the confidentiality of CUI at rest.

3.14 SYSTEM AND INFORMATION INTEGRITY

Basic Security Requirements

3.14.1 Identify, report, and correct system flaws in a timely manner.

3.14.2 Provide protection from malicious code at designated locations within organizational systems.

3.14.3 Monitor system security alerts and advisories and take action in response.

Derived Security Requirements

3.14.4 Update malicious code protection mechanisms when new releases are available.

3.14.5 Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.

3.14.6 Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.
3.14.7 Identify unauthorized use of organizational systems.

Appendix G: GLBA controls without Observations

This section identifies GLBA Safeguards Rule controls that did not present significant observations during the assessment. While observations were not discovered during this year's assessment, continued vigilance is necessary in today's ever-changing information security threat landscape. These controls should still be reviewed year-over-year to ensure George Mason compliance with the GLBA Safeguards Rule.

CFR #	CFR Description
§314.3(b)	Objectives. The objectives of section 501(b) of the Act, and of this part, are to:
§314.3(b)(1)	Insure the security and confidentiality of customer information;
§314.3(b)(2)	Protect against any anticipated threats or hazards to the security or integrity of such information.
§314.4(b)	Base your 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.
§314.4(b)(1)	The risk assessment shall be written and shall include:
§314.4(b)(1)(i)	Criteria for the evaluation and categorization of identified security risks or threats you face;
§314.4(b)(1)(ii)	Criteria for the assessment of the confidentiality, integrity, and availability of your information systems and customer information, including the adequacy of the existing controls in the context of the identified risks or threats you face; and
§314.4(b)(1)(iii)	Requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the information security program will address the risks.
§314.4(b)(2)	You shall periodically perform additional risk assessments that reexamine the 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 reassess the sufficiency of any safeguards in place to control these risks.
§314.4(c)	Design and implement safeguards to control the risks you identity through risk assessment, including by:
§314.4(c)(1)	Implementing and periodically reviewing access controls, including technical and, as appropriate, physical controls
§314.4(c)(1)(i)	Authenticate and permit access only to authorized users to protect against the unauthorized acquisition of customer information; and
§314.4(c)(4)	Adopt secure development practices for in-house developed applications utilized by you for transmitting, accessing, or storing customer information and procedures for evaluating, assessing, or testing the security of externally developed applications you utilize to transmit, access, or store customer information;
§314.4(c)(6)	Intentionally left blank
§314.4(c)(7)	Adopt procedures for change management; and
§314.4(d)	Intentionally left blank
§314.4(d)(1)	Regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures, including those to detect actual and attempted attacks on, or intrusions into, information systems.

§314.4(d)(2)	For information systems, the monitoring and testing shall include continuous monitoring or periodic penetration testing and vulnerability assessments. Absent effective continuous monitoring or other systems to detect, on an ongoing basis, changes in information systems that may create vulnerabilities, you shall conduct:
§314.4(d)(2)(i)	Annual penetration testing of your information systems determined each given year based on relevant identified risks in accordance with the risk assessment; and
§314.4(d)(2)(ii)	Vulnerability assessments, including any systemic scans or reviews of information systems reasonably designed to identify publicly known security vulnerabilities in your information systems based on the risk assessment, at least every six months; and whenever there are material changes to your operations or business arrangements; and whenever there are circumstances you know or have reason to know may have a material impact on your information security program.
§314.4(e)	Implement policies and procedures to ensure that personnel are able to enact your information security program
§314.4(e)(2)	Utilizing qualified information security personnel employed by you or an affiliate or service provider sufficient to manage your information security risks and to perform or oversee the information security program;
§314.4(e)(3)	Providing information security personnel with security updates and training sufficient to address relevant security risks; and
§314.4(e)(4)	Verifying that key information security personnel take steps to maintain current knowledge of changing information security threats and countermeasures.
§314.4(f)	Oversee service providers, by:
§314.4(f)(1)	Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue;
§314.4(f)(2)	Requiring your service providers by contract to implement and maintain such safeguards; and
§314.4(f)(3)	Periodically assessing your service providers based on the risk they present and the continued adequacy of their safeguards.
§314.4(g)	Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (d) of this section; any material changes to your operations or business arrangements; the results of risk assessments performed under paragraph (b)(2) of this section; or any other circumstances that you know or have reason to know may have a material impact on your information security program.
§314.4(h)	Establish a written incident response plan designed to promptly respond to, and recover from, any security event materially affecting the confidentiality, integrity, or availability of customer information in your control. Such incident response plan shall address the following areas:
§314.4(h)(1)	The goals of the incident response plan;
§314.4(h)(2)	The internal processes for responding to a security event;
§314.4(h)(3)	The definition of clear roles, responsibilities, and levels of decision-making authority;
§314.4(h)(4)	External and internal communications and information sharing;
§314.4(h)(5)	Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;
§314.4(h)(6)	Documentation and reporting regarding security events and related incident response activities; and
§314.4(h)(7)	The evaluation and revision as necessary of the incident response plan following a security event.

§314.4(i)	Require your Qualified Individual to report in writing, regularly and at least annually, to your board of directors or equivalent governing body. If no such board of directors or equivalent governing body exists, such report shall be timely presented to a senior officer responsible for your information security program. The report shall include the following information:
§314.4(i)(1)	The overall status of the information security program and your compliance with this part; and
§314.4(i)(2)	Material matters related to the information security program, addressing issues such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security events or violations and management's responses thereto, and recommendations for changes in the information security program.

GEORGE MASON UNIVERSITY Office of University Audit

Report to the Audit, Risk, and Compliance Committee of the Board of Visitors

November 19, 2024

EXECUTIVE SUMMARY

- Audit Staffing:
  - We continue to utilize our hybrid organizational model to provide assurance services for George Mason. The model blends full time professional staff with co-sourced professionals from national and local accounting firms that bring specialized expertise to execute specific audit engagements. As of November 1, 2024, the full-time staff consists of four professionals. Seeking the right balance of audit professionals who are George Mason employees and those who are co-sourced professionals is being managed continuously by University Audit leadership.

  - Co-sourced resources are being utilized to complete the following audit engagements:
    - Information technology process infrastructure monitoring.
    - Information technology configuration and change management.
    - Information technology project management office (PMO) methodology.
    - Accounts Payable.
    - Housing and Residence Life.

- Four audit memos were issued since the last meeting including:
  - Banner Core Physical Access,
  - Student Bar Association (SBA) – Governance and Oversight,
  - Two memos related to Biomedical Research Laboratory (BRL) employee timekeeping practices impacting controls in payroll and grant allocation.

- Remediation of six audit issues is in progress as of November 1, 2024.

- Audit Plan status:
  - Planned audit work remains consistent with the 3+6 Audit Plan reviewed at the prior meeting. However, the timing of planned audit work continues to be reevaluated in consideration of the use of co-sourced audit resources.

- Status of fraud, waste, and abuse investigations:
  - Five investigations were completed since the prior meeting; they are isolated in nature with negligible impact to the University.
  - There are three investigations in progress.

TABLE OF CONTENTS

Topic

SUMMARY OF AUDIT REPORTS

- Audit Memos:
  - Banner Core Physical Access Controls (Aquia Data Center)
  - Student Bar Association – Governance and Oversight
  - Biomedical Research Laboratory Employee Timekeeping Practices (Payroll Controls)
  - Biomedical Research Laboratory Employee Timekeeping Practices (Compensation Time Review and Grant Allocation)

Summary of Audit Memos:

Audit Memos are communications which provide assurance related to a narrow, targeted topic or provide interim updates on longer-term assurance activities.

Banner Core Physical Access Controls (Aquia Data Center):

- Confidential – Restricted Data: Critical Infrastructure Vulnerability Assessment Information (Code of VA: 2.2-3705.2.4).

Student Bar Association – Governance and Oversight

- University Policy 6000 (Student Organizations and Fiscal Policy) defines the various types of student organizations and prescribes the procedures for registration and governance, and funding from university and non-university sources. This review assessed certain governance and oversight practices related to Student Bar Association activities. Management is reviewing, clarifying, and establishing appropriate protocols and communications to strengthen oversight of Student Bar Association activities, including the use and handling of university-provided funding for Student Bar Association activities, in the areas of student organization independence from the university, governance and oversight for Student Organizations, the administration and use of self-generated revenues, and the consumption of alcohol at student events funded by university-provided funds or on university properties.

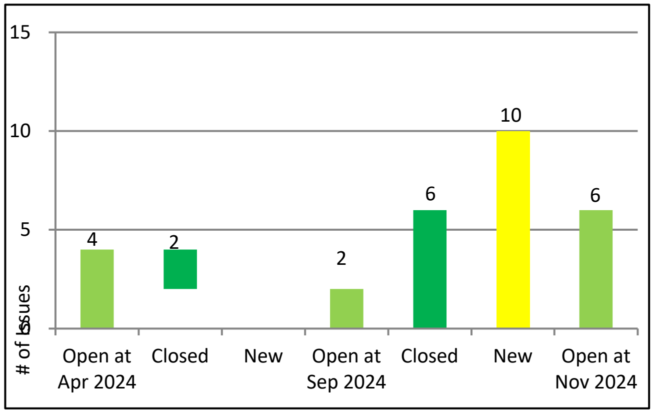
Biomedical Research Laboratory Employee Timekeeping Practices

- This review of BRL Employee Timekeeping practices recommended actions to strengthen timesheet review and approval, accurate reporting of time, review of certain positions, review of the earning and use of compensatory time, and review of the allocation of expenses to a research award.
- The review also recommended enhancements to Payroll controls for monitoring of compensatory time charged and providing guidance and training for employees and supervisors in certain positions.

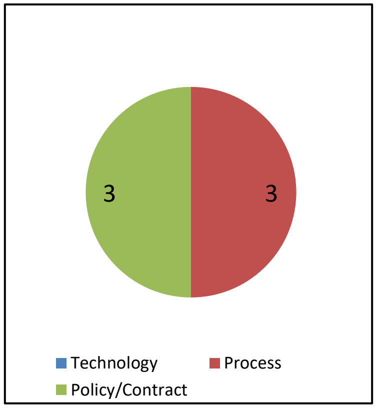
Summary Status of Audit Issues as of November 1, 2024

Six audit issues were closed since the last meeting. There were six open audit issues as of November 1, 2024.

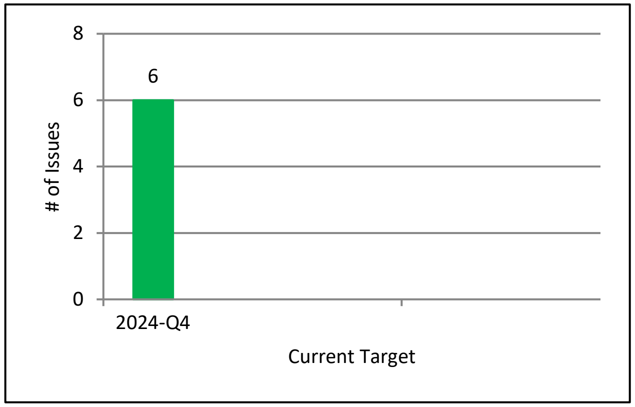
Audit Issue Inventory Movement



Audit Issues by Type



Audit Issues by Current Target



Audit Report	Report Date	Open at Apr 2024	New	Closed	Open at Sep 2024	New	Closed	Open at Nov 2024
Biomedical Research Laboratory Employee Timekeeping Practices	11/1/24	0	-	-	0	6	(5)	1
Student Bar Association Governance and Oversight	10/8/24	0	-	-	0	4	-	4
IT Third Party Service Providers	9/13/23	1	-	(1)	0	-	-	0
Background Investigations	4/20/23	2	-	-	2	-	(1)	1
Academic Integrity	8/29/22	1	-	(1)	0	-	-	0
		4	0	(2)	2	10	(6)	6

STATUS OF AUDIT PLAN AS OF NOVEMBER 1, 2024

The 3+6 Audit Plan as of November 1, 2024 (bottom bars) is compared with the status as of the prior report to the Committee (top bars). (Note: The status of work is shown as follows: completed = orange bars, in progress = green bars, and planned = yellow bars)

Topic	Description	9 30	12 31	3 31	6 30
Aligned with University-Level Risk Areas					
IT Risk and Control Infrastructure Program	• Monitor ITS program workstreams to strengthen the risk and control infrastructure and improve technology service delivery.	🟩 🟩	🟩 🟩	🟩 🟩	🟩 🟩
Information Security Program	• Monitor projects to further strengthen security of George Mason's entire technology environment.	🟩 🟩	🟩 🟩	🟩 🟩	🟩 🟩
Research Security	• Monitor cybersecurity assessments of research computing environments, including NSPM-33 expectations.		🟨	🟨	
Housing and Residence Life	• Assess business and compliance processes relevant to student housing and residence life.	🟩 🟩	🟩 🟩		
Business Continuity and Disaster Recovery Planning	• Assess business continuity, disaster recovery, and continuity of operations planning.		🟨	🟨	
Compliance with TTIP MOUs	• Assess progress in achieving obligations under Tech Talent Investment Program memoranda of understanding and related reporting.		🟨		
Construction Payments and Change Orders	• Monitor and assess payments related to planned campus construction projects.			🟨	🟨
Additional Areas					
Accounts Payable Processing	• Assess processes for ensuring authorized, accurate, and timely payment transactions.	🟩 🟩			
Issue Validation Procedures	• Validate management has remediated audit issues in a comprehensive and sustainable manner.	🟩 🟩	🟩 🟩	🟩 🟩	🟩 🟩
Hotline Investigations Referred by OSIG	• Investigate allegations of fraud, waste, or abuse received from the Commonwealth's Office of the State Inspector General.	🟩 🟩	🟩 🟩	🟩 🟩	🟩 🟩

STATUS OF INVESTIGATIONS AS OF NOVEMBER 1, 2024

Nature of Allegation	Type	Status	Remarks
Potential falsification of timesheets	Fraud	Completed	*Certain time sheet review and approval controls and payroll monitoring controls were strengthened.*
Potential falsification of timesheets	Fraud	Completed	
Potential mismanagement of research funds	Abuse	Completed	*Minor adjustment of expenses charged to research award was made.*
Potential mismanagement of student fee monies	Abuse	Completed	*Management is reviewing, clarifying, and establishing appropriate protocols and communications to strengthen oversight in various areas.*
Potential abuse of procurement/P-Card policies	Abuse	Completed	
Potential noncompliance with development policies	Abuse	In Progress	
Potential time abuse and conflict of interest	Fraud	In Progress	
Potential non-compliance with conflict of interest policy	Abuse	In Progress	

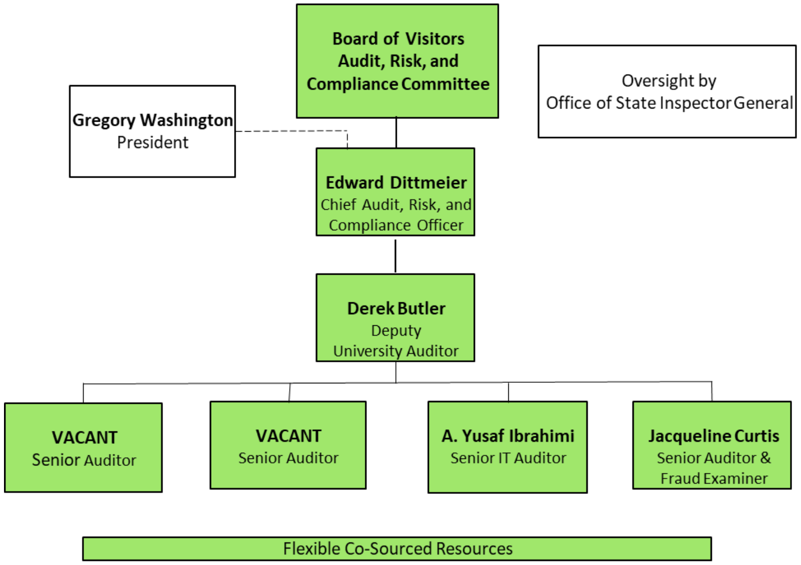
Summary of Types:

- Fraud = Intentional deception which could result in a benefit to the perpetrator, others, or the Commonwealth or could cause detriment to others or the Commonwealth. Fraud includes a false representation of a matter of fact, whether by words or by conduct, by false or misleading statements, or by concealment of that which should have been disclosed, which deceives or is intended to deceive. E.g., falsifying financial records to cover up theft.
- Waste = Careless expenditure, mismanagement, use, or squandering of Commonwealth resources to the actual or potential detriment of the Commonwealth. Includes unnecessary costs due to inefficient or ineffective practices, systems, or controls. E.g., unnecessary spending of state funds for no business purpose.
- Abuse = Excessive or improper use of something contrary to natural or legal rules for its use. Intentional destruction, diversion, manipulation, misapplication, mistreatment, or misuse of Commonwealth resources. Excessive use as to abuse one’s position or authority. E.g., use of state assets for non-state business.

STAFFING

University Audit utilizes a hybrid organizational model to provide assurance services for George Mason. The model is designed to blend full time professional staff with co-sourced professionals from national and local accounting firms that bring specialized expertise to execute specific audit engagements under the Deputy University Auditor's direction and supervision. As of November 1, 2024, the full-time staff consists of four professionals.

Staffing



		Actual		
Core Audit Team	Plan	a/o July 2024	Avg to Oct 2024	Frct
Audit Leadership	2.0	2.0	2.0	2.0
Auditors by Expertise:				
Operational Audit	1.5	0.5	0.5	0.5
IT Audit	1.0	1.0	1.0	1.0
Fraud Audit	0.5	0.5	0.5	0.5
Total Audit Professional Employees	5.0	4.0	4.0	4.0
Co-sourced FTE* Supported by Permanent Budget	1.7		0.7	2.9
Total Audit Professionals Supported by Permanent Budget	6.7	4.0	4.7	6.9

Note: * = Co-sourced FTE are estimated based on actual hours provided by co-sourced resources and a 1,500 hour/FTE rate.

APPENDIX: AUDIT ISSUE DETAILS AS OF NOVEMBER 1, 2024

#	Audit Report	Audit Issue	Status of Management Action	Original Target	Current Target
1	**Report Name:** Background Investigations **Report Date:** 4/19/23 **Management:** Michelle Lim, Interim Vice President and Chief Human Resources Officer	**Ensure All Employees Have Completed Required Background Investigations:** Central HR should ensure all current and prospective employees have completed background investigations prior to beginning work; establish communication mechanisms to inform hiring departments of the status of a prospective employee's background investigation; develop automated procedures for ensuring regular integration of Truescreen background investigation data into Banner; implement a continuous monitoring program; and create a central repository of all completed background investigations.	All current employees hired on or after July 1, 2016 have a background investigation on file. Since George Mason's policy prior to this date did not require all employees to have a background investigation, the Executive Vice President of Finance and Administration decided to focus efforts on ensuring background investigations are on file for all employees hired on or after July 1, 2016. IT enhancements now halt the employee onboarding process if there is no background investigation on file. A dashboard now assists the Background Specialist with monitoring background investigations status/data. Banner and the background investigation vendor have been fully integrated to ensure near real time updates of background investigation status. The establishment of processes and procedures to ensure timely background investigations for adjunct faculty, a population which may not maintain consistent employment, has been delayed due to departures of senior human resources leaders.	9/30/23	12/31/24
2	**Report Name:** Student Bar Association-Governance and Oversight **Report Date:** 10/8/24 **Management:** Rose Pascarell, Vice President, University Life	**Student Organization Independence from the University:** The SBA and related LSSOs are not registered student organizations and are not subject to the policies or procedures of the Student Involvement Office. It is not clear whether any of these student organizations are 'independent' given the requirements to adhere to university policies and procedures, and dependency on funds from university sources. Given that student organizations are considered by the University to be independent, Leadership in the Law School believe they do not have the authority to control how university	The Vice President, University Life will work with University Counsel and university management (including representation from the Law School) to clarify whether student organizations are independent from the university and document the authority provided to management. The Vice President, University Life will also convene the appropriate parties and stakeholders to assess the current governance, oversight, policies, and procedures used across student organizations, including the SBA and LSSOs.	12/31/24	12/31/24

#	Audit Report	Audit Issue	Status of Management Action	Original Target	Current Target
		funds were being used by the SBA and the related LSSOs.			
3	**Report Name:** Student Bar Association-Governance and Oversight **Report Date:** 10/8/24 **Management:** Rose Pascarell, Vice President, University Life	**Governance and Oversight for Student Organizations:** A review of the SBA and LSSO expenditures between January 1, 2023 and April 18, 2024 noted items that are not typically approved expenditures by the SFB for RSOs or by the university. These items include: events that are not free, open and accessible to all students (formals/banquets closed or designed specifically for the group, i.e., Barrister's Ball), bartending services at on-campus events; and branded/non-branded apparel ($4,005 for embroidered sweat shirts). On the other hand, the SBA does not reimburse for student organization travel to and from the airport or train station to minimize expenses; whereas the RSOs are permitted to request reimbursement for these items, and are reimbursable per the university's travel policy.	The Vice President, University Life will work with University Counsel and university management (including representation from the Law School) to clarify whether student organizations are independent from the university and document the authority provided to management. The Vice President, University Life will also convene the appropriate parties and stakeholders to assess the current governance, oversight, policies, and procedures used across student organizations, including the SBA and LSSOs.	12/31/24	12/31/24
4	**Report Name:** Student Bar Association-Governance and Oversight **Report Date:** 10/8/24 **Management:** Rose Pascarell, Vice President, University Life	**Self-Generated Revenues:** Per UP 6000, self-generated revenue is money raised by an organization through various activities, such as the collection of dues from its members, charging admission to its events, fundraising, advertising, submission fees, and sales. These funds are kept in an off-campus bank account and managed by the student organizations (SBA, LSSOs and RSOs). Since these funds are not held in a university account, the university has no visibility into the account activity or say into how the funds are spent. The SBA charges admission to certain university funded events (Barrister's Ball, Casino Night). These funds have been used to cover the cost of alcohol which cannot be paid for using funds from university sources. Funds from the university account are used to cover the cost of the venue, food and entertainment.	The Vice President, University Life will work with University Counsel and university management (including representation from the Law School) to clarify whether student organizations are independent from the university and document the authority provided to management. The Vice President, University Life will also convene the appropriate parties and stakeholders to assess the current governance, oversight, policies, and procedures used across student organizations, including the SBA and LSSOs.	12/31/24	12/31/24

#	Audit Report	Audit Issue	Status of Management Action	Original Target	Current Target
5	**Report Name:** Student Bar Association-Governance and Oversight **Report Date:** 10/8/24 **Management:** Rose Pascarell, Vice President, University Life	**Alcohol at University Funded Events:** Alcohol is provided and consumed at various SBA events funded by university sources. These events can occur on the Arlington campus (Casino Night) or off campus (Barrister's Ball). While admission fees (self-generated revenue) and Foundation monies cover the cost of the alcohol for such events, funds from the university are used to pay the cost of the venue, food and entertainment	Enhanced requirements will be established that ensure consistent execution of university policies across student organizations, with specific attention on guidelines that govern the use of alcohol at student events funded by the university whether held on or off university properties.	12/31/24	12/31/24
6	**Report Name:** Biomedical Research Laboratory (BRL) Employee Timekeeping Practices Report Date: 11/1/24 **Management:** Sonya Howell, Director Payroll, Fiscal Services	Payroll should issue additional guidance or resources to educate impacted employees and supervisors on eligibility criteria for earning compensatory time, procedures for recording such time, and procedures for recording compensatory time taken (similar to previous timesheet guidelines which were published on University Policy #2205).	Payroll will coordinate with Fiscal Learning & Engagement to publish additional timesheet resources to the Fiscal Services website to assist impacted employees and supervisors with recording and approving compensatory time earned and taken. In addition, Payroll will partner with Human Resources (who administers leave) to include a notice in the HR Liaisons Newsletter at least annually outlining eligibility criteria for earning compensatory time and a link to procedures for recording such time earned and taken.	12/31/24	12/31/24

GEORGE MASON UNIVERSITY

Office of University Audit

Office of University Audit:
Review of Audit Planning - Risk Assessment

Report to Audit, Risk and Compliance Committee
November 19, 2024

Internal Audit Planning Process

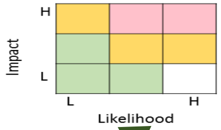
Audit priorities are determined in a dynamic, flexible, risk-based manner using a frequently refreshed audit risk assessment. Planning is governed by an Audit Policy originally endorsed by the Committee in 2016; essential elements are:

Top-Down Analysis

- University-level risk brainstorming and monitoring
- Cross-cutting / programmatic risks
- Governance focused
- Environmental scanning basis
- Collaborative, yet independent and objective

Bottom-Up Analysis

- Audit Universe
- Assess risk to determine frequency
  - Impact/Likelihood
  - Factors aligned w/ERM
    - Strategic
    - Regulatory compliance
    - Financial and Financial Reporting
    - Operations
    - Hazards



Monitoring

- Environmental Scanning
- Relationships; Management Call Program
- Benchmarking
- Adjust risk assessments and audit plans based on changes in risk

Key Stakeholder Input

- Executives
- University risk leaders
- Audit, Risk and Compliance Committee

Proposed 3+6 Audit Plan

- Engagement risk assessment determines depth (nature, extent and timing) at time of audit
- Use work of others (2LOD) where relevant and appropriate
- Hour budgets are estimates; adjust at time of audit based on engagement risk assessment
- Seek to design audit work across organizations where possible to increase value

Evaluate Resources

- Resource levels
- Skill needs

Seek Review

- Chairman review
- Committee review

GEORGE MASON UNIVERSITY

Office of University Audit

University-Level Risk Areas

Consistent with our most recent view formed in June 2024, university-level risk areas include:

Risk Area	Description	Potential Internal Audit Work
Enrollment Changes	Student enrollment processes drive the quality and diversity of the university community while sourcing ~ 50% of revenues through net tuition, fee, housing, and dining revenues. Success is dependent on achieving an balanced student size, mix, diversity, and financial capability while managing to limit the impacts of potential changes in enrollment due to competitiveness, relevance, demographics, economics, or other reasons.	• **Evaluate academic integrity processes.** • **Evaluate university registrar processes.** • Monitor APA student financial aid testing (fall 2024); consider supplemental procedures. • Monitor ADVANCE program with NOVA and other community colleges. • Monitor pricing/competition as other universities expand offerings in Northern Virginia.
Research Enterprise Growth	The university is continuing to expand research substantially to strengthen research impact and sustain a Carnegie Very High Research Activity (R1) classification. Growth in research faculty and scalable support, including infrastructure capabilities (people, facilities, computing, funding, and processes), need to support planned growth.	• **Assess research proposal development process.** • **Evaluate financial administration of sponsored programs.** • **Monitor cyber security assessment of research computing environments.** Continue. • Monitor strengthening of research security process enhancements related to federal requirements.
Financial Stewardship and Funding Uncertainty	Legislative processes, inflationary impacts on costs, expiration of pandemic-era relief actions, and overall volatility in higher education are challenging available resources. Financial planning, analysis, reporting, and governance processes are being adjusted to better align resource allocation with achieving strategic goals and the university's instructional and research missions while protecting the university's creditworthiness and balancing current needs with longer-term investments.	• **Evaluate student billing processes.** • Evaluate accounts payable processing. • Monitor budget model redesign initiative. • Monitor processes for managing reserve levels. • Monitor compliance with Tech Talent Investment Program agreements. • Monitor investment planning processes.
Campus Safety, Security, Health and Well Being	Providing a safe, secure, and healthy environment for students, employees, and other community members is essential to the accomplishment of the university's instructional, research, and public service missions.	• Monitor self-assessment of emergency management program. • Evaluate compliance with Commonwealth violence prevention requirements, including recent threat assessment legislation. • Monitor active threat-related training completion rates by students and employees. • Monitor status of mental health programs with selected comparable peers.

Potential indicative Work: **Bold** = recently completed; Red = included in 3+6 audit plan

University-Level Risk Areas

Consistent with our most recent view formed in June 2024, university-level risk areas include:

Risk Area	Description	Potential Internal Audit Work
Operating Infrastructure Robustness	Mason's workforce and important core processes, technology, and facilities are likely to require further strengthening and investment to appropriately support scalable growth and innovation while ensuring core processing is effective and efficient.	• **Evaluate university registrar processes.** • **Monitor actions to improve IT governance and process infrastructure projects.** • **Evaluate student billing processes.** • **Evaluate financial administration of sponsored programs.** • Evaluate Housing and Residence Life processes. • Evaluate accounts payable processing. • Continue to monitor implementation of IT governance and process infrastructure projects. • Evaluate IT configuration and change management processes. • Monitor strengthening of intercollegiate athletics compliance processes. • Evaluate processes to manage Banner Access authorization, management, and termination. • Evaluate disaster recovery and continuity of operations planning and capabilities. • Monitor selected construction projects.
Information Protection (Cyber Threats)	The university holds large volumes of protected (personally identifiable, classified, and controlled unclassified) information in a globally connected, decentralized technology environment.	• **Monitor actions to improve IT governance and process infrastructure projects.** • **Monitor cyber security assessment of research computing environments.** Continue. • Continue to monitor implementation of IT governance and process infrastructure projects. • Monitor IT vulnerability and patch management processes. • Evaluate disaster recovery and continuity of operations planning and capabilities.
Key Role Succession	Turnover in certain leadership positions and key roles has been experienced recently and is expected in the near future (due to planned retirements). The orderly filling and acclimation of strong individuals for these positions is important to sustaining strategic momentum.	• **Monitor recruitment searches, on-boarding, and assimilation for certain roles.** Continue.

Potential indicative Work: **Bold** = recently completed; Red = included in 3+6 audit plan

GEORGE MASON UNIVERSITY Office of University Audit

ERM to Audit Risks Crosswalk

Our view of university-level risk areas maps well to management's enterprise risk areas.

	Funding Resources	Competition	Cybersecurity	Governance Volatility	Campus Safety & Security	Physical & Technology Infrastructure	Global Volatility	Compliance and Ethics	Business Practices	Student Success
Enrollment Changes	🟥	🟥		🟧			🟨		🟩	🟩
Research Enterprise Growth	🟥	🟥	🟥		🟧	🟧		🟨		
Financial Stewardship & Funding Uncertainty	🟥	🟥	🟥	🟧		🟧			🟩	
Campus Safety, Security, Health, and Well Being				🟧	🟧		🟨			🟩
Operating Infrastructure Robustness			🟥			🟧		🟨	🟩	
Information Protection (Cyber)	🟥		🟥			🟧			🟩	
Key Role Succession		🟥		🟧					🟩	

Risk assessment results highlight areas with potentially high impact.

RISK FACTOR	DESCRIPTION	DISTRIBUTION OF AUDITABLE UNITS
STRATEGIC	The risk of this auditable unit to GMU's people, reputation, or financial position, and to the achievement of GMU's Mission, Values, and Strategic Plan objectives arising from ineffective business strategies and tactics; adverse business decisions; insufficient resources, funding, or management focus; ineffective implementation of decisions; or lack of responsiveness to changes in business environment.	Impact H 12 8 0 M 26 17 0 L 16 1 0 L M H Likelihood
FINANCIAL and FINANCIAL REPORTING	The risk of this auditable unit to GMU's people, reputation, or financial position arising from inadequate or ineffective management of financial-related processes and reporting or external events, including processes upstream from those normally associated with financial aspects of the university. Among other things, this includes risks associated with credit, investments, financings, currencies, financial models, markets, and related transaction processing, accounting, and reporting activities.	Impact H 3 3 1 M 7 11 0 L 47 8 0 L M H Likelihood
REGULATORY COMPLIANCE	The risk of this auditable unit to GMU's people, reputation, or financial position arising from violations of, or non-compliance with, current and changing laws, regulations, supervisory guidance, or regulatory expectations.	Impact H 8 9 0 M 6 20 0 L 36 1 0 L M H Likelihood
OPERATIONS	The risk of this auditable unit to GMU's people, reputation, or financial position arising from inadequate or failed internal processes, people, and systems or from external events. This includes the following types of risk: technology-related risk, which is the risk arising from the University's overall use of technology (whether centralized or decentralized) and includes, among other things, its governance, processes, infrastructure, applications, security, and reliability; and legal risk, which is the risk arising from defective transactions, litigation or claims made, or the failure to protect university assets.	Impact H 3 6 2 M 6 40 2 L 14 6 1 L M H Likelihood
HAZARD	The risk of this auditable unit to GMU's people, reputation, or financial position arising from inadequate or failed internal processes, people, and systems or from external events. This includes the following types of risk: (i) health, safety, and environmental risks, which is the risk arising from processes or events that potentially cause damage, harm, or adverse effects to someone (e.g., health) or something (e.g., property).	Impact H 0 1 0 M 7 11 0 L 60 1 0 L M H Likelihood

Appendix: Risk Assessment Details

The risk-assessed Audit Universe, sorted by Executive:

#	Executive	Group	Area	Str	Fin	Comp	Opns	Haz	Audit Work: FY 2020 (7/1/19) to Present
1	Provost	Antonin Scalia School of Law		Mod	Low	Mod	Mod	Low	
2	Provost	College of Education & Human Development (CEHD)		Mod	Low	Mod	Mod	Low	10/27/22 – IT Risk Self-Assessment 4/8/22 – Research Proposal Process Review 10/1/20 - Confucius Institute Financial Review

3	Provost	College of Engineering & Computing		High	Low	High	Mod	Low	5/6/24 - RPRC CMMC and SPRS Scoring Validation;
									9/6/22 - RPRC SSP and POA&M Assessment;
									4/8/22 – Research Proposal Process Review;

4	Provost	College of Humanities & Social Sciences (CHSS)		Mod	Low	Mod	Mod	Low	4/8/22 – Research Proposal Process Review
5	Provost	College of Public Health		Mod	Low	Mod	Mod	Low	8/10/2022 - IT Risk Self-Assessment

6	Provost	College of Science (CoS)		High	Low	Mod	Mod	Mod	5/24/24 - IT Risk Self-Assessment;
									4/8/22 – Research Proposal Process Review
									2/27/20 – IT Security Self-Assessment
									12/16/19 – Validation of IT Security Self-Assessment Results;

7	Provost	College of Visual & Performing Arts (CVPA)		Low	Low	Mod	Mod	Low	10/26/20 – CVPA Wage Employee Charges 6/17/20 - Assessment of Interest and Other Matters 11/25/19 - Computer Game Design Scholarship Program 8/7/19 – Validation of IT Security Self-Assessment Results
8	Provost	Costello College of Business		Mod	Low	Mod	Mod	Low	2/27/23 - IT Risk Self-Assessment Results: School of Business
9	Provost	Honors College		Low	Low	Mod	Low	Low	
10	Provost	Jimmy and Rosalynn Carter School of Peace and Conflict Resolution		Low	Low	Mod	Low	Low	
11	Provost	Schar School of Policy & Government		Mod	Low	Mod	Mod	Low	
12	Provost	Cross-functional (formerly Research & Innovation Initiatives)	Smithsonian Mason School of Conservation	Low	Low	Low	Low	Low	
13	Provost	Entrepreneurship Programming	Mason Enterprise	Mod	Low	Low	Low	Low	

The risk-assessed Audit Universe, sorted by Executive:

#	Executive	Group	Area	Str	Fin	Comp	Opns	Haz	Audit Work: FY 2020 (7/1/19) to Present
14	Provost	Research & Innovation Initiatives	Research Development and Computing	Mod	Low	Mod	Mod	Low	5/6/24 - SRC CMMC and SPRS Scoring Validation; 8/29/22 - SRC CUI SSP and POA&M Assessment
15	Provost	Research & Innovation Initiatives	University Institutes and Centers	High	Low	Low	Mod	High	

16	Provost	Research Services	Research Services - Integrity & Assurance	Mod	Low	High	Mod	Low	5/6/24 - RPRC CMMC and SPRS Scoring Validation;
									5/6/24 - SRC CMMC and SPRS Scoring Validation;
									9/6/22 - RPRC SSP and POA&M Assessment
									8/29/22 - SRC CUI SSP and POA&M Assessment

17	Provost	Research Services	Research Services - Sponsored Programs Administration	Mod	High	Mod	High	Low	2/8/24 - GMU Research and Development Testing Results 4/8/22 – Research Proposal Process Review 5/1/20 - Continuance Audit of Federally Sponsored Fund Reconciliations
18	Provost	Academic Administration		Low	Low	Low	Low	Low	
19	Provost	Enrollment Management	Admissions and Enrollment Planning	High	Low	Mod	Mod	Low	11/4/21 - Office of Admissions
20	Provost	Enrollment Management	Student Financial Aid	Low	Mod	Mod	Mod	Low	12/12/23 - Review of Satisfactory Academic Progress; 11/10/21 - Student Financial Aid 1/25/21 - Use and Distribution of GEERF 12/18/20 - Use and Distribution of CARES Act Funding
21	Provost	Institutional Effectiveness and Planning		Mod	Low	Mod	Mod	Low	
22	Provost	Academic Affairs	Registrar	Low	Low	High	Mod	Low	12/8/22 - Office of University Registrar Audit
23	Provost	Academic Affairs	Undergraduate Education	Low	Low	Low	Mod	Low	
24	Provost	Academic Affairs	Graduate Education	Low	Low	Low	Mod	Low	
25	Provost	Academic Affairs	Accreditation	Mod	Low	High	Mod	Low	
26	Provost	Academic Affairs	Global Education Office	Low	Low	Low	Low	Mod	
27	Provost	Academic Affairs	INTO Mason	Low	Low	Low	Low	Low	
28	Provost	Academic Affairs	Mason Continuing and Professional Education	Low	Low	Low	Low	Low	

The risk-assessed Audit Universe, sorted by Executive:

#	Executive	Group	Area	Str	Fin	Comp	Opns	Haz	Audit Work: FY 2020 (7/1/19) to Present
29	Provost	Academic Affairs	ADVANCE and Other Community College Partnerships	Mod	Low	Low	Low	Low	
30	Provost	Academic Affairs	Provost Activities (incl Mercatus Center)	Mod	Low	Low	Mod	Low	
31	Provost	Faculty Affairs		Low	Low	Low	Low	Low	8/26/2020 - Online Graduate Learning Arrangement Wiley
32	Provost	Mason Korea		Mod	Low	Low	Low	Low	
33	Provost	University Life	Access and Holistic Student Support Services	Low	Low	High	Mod	Mod	8/29/22 - Academic Integrity 12/18/20 - Use and Distribution of CARES Act Funding 12/16/19 - Drug and Alcohol Prevention Program
34	Provost	University Life - Student Engagement	Housing and Residential Life	Mod	Low	Low	Mod	Mod	
35	Provost	University Life - Student Engagement	Recreations	Low	Low	Low	Low	Low	
36	Provost	University Life - Student Engagement	Student Organizations	Low	Low	Low	Low	Mod	7/10/24 - Campus Ministry Association (CMA) Affiliate Review;
37	Provost	University Libraries		Low	Low	Low	Low	Low	8/7/19 – Validation of IT Security Self-Assessment Results
38	Administration	Fiscal Services	Accounts Payable	Low	Mod	Mod	Mod	Low	
39	Administration	Fiscal Services	General Accounting (and Financial Reporting & ARMICS)	Low	High	Mod	Mod	Low	9/3/21 - Clearing Accounts 6/17/21 - Bank Accounts 4/15/21 - Foreign Gifts and Contracts 2/5/21 - Enhanced ARMICS IT Assurance Control Assessment
40	Administration	Fiscal Services	Payroll Processing	Mod	Mod	Mod	Mod	Low	4/23/20- Wage Employee Time Entry and Annual Leave Usage for Administrative Faculty
41	Administration	Fiscal Services	Purchasing and Central Receiving	Low	Mod	Mod	Low	Low	
42	Administration	Fiscal Services	Strategic Planning and Budget	High	Mod	Mod	Mod	Low	

The risk-assessed Audit Universe, sorted by Executive:

#	Executive	Group	Area	Str	Fin	Comp	Opns	Haz	Audit Work: FY 2020 (7/1/19) to Present
43	Administration	Fiscal Services	Student Fiscal Services	Low	Mod	Mod	Mod	Low	10/12/23 - Student Accounts Office 7/19/19 – Student Fiscal Services
44	Administration	Fiscal Services	Treasury and Debt Management	Mod	Mod	Mod	Mod	Low	
45	Administration	Human Resources and Benefits	Human Resources	Mod	Low	Mod	High	Low	4/20/23 - Background Investigations 7/23/19 – Recruiting Processes
46	Administration	Information Technology Services	Enterprise Applications / Banner Support	Low	Mod	Low	High	Low	2/2/24 - Review Facilitated Banner Core Control Self-Assessment Results; 5/9/24 – Feedback on Banner Core SSP and POA&M; 3/8/24 – Facilitated Banner Core Self-Assessment; 4/9/21 - IAM Identity Management 6/11/21 - IAM Access Management 10/5/20 - Security Over Highly Privileged Banner Account 7/22/19 - Assessment of Banner 9 Upgrade System testing
47	Administration	Information Technology Services	Enterprise Applications / Banner Development, Change Management, and Operations (SDLC)	Low	Low	Low	Mod	Low	2/2/24 - Review Facilitated Banner Core Control Self-Assessment Results;
48	Administration	Information Technology Services	Enterprise Applications / Database, Middleware, and ERP Support	Low	Mod	Low	High	Low	2/2/24 - Review Facilitated Banner Core Control Self-Assessment Results;

49	Administration	Information Technology Services	Cloud Computing and Storage	Low	Mod	Low	High	Low	2/2/24 - Review Facilitated Banner Core Control Self-Assessment Results;
									9/14/23 – IT Third Party Service Providers;
									10/30/18 – Monitoring Server Configuration Benchmarks and Implementations

50	Administration	Information Technology Services	Enterprise Service Delivery / Business Continuity & Recovery	Mod	Low	Low	Mod	Low	2/2/24 - Review Facilitated Banner Core Control Self-Assessment Results; 1/3/23 - ITS Disaster Recovery Exercise - Banner
51	Administration	Information Technology Services	Enterprise Service Delivery / Technology Support Services	Low	Low	Low	Low	Low	

The risk-assessed Audit Universe, sorted by Executive:

#	Executive	Group	Area	Str	Fin	Comp	Opns	Haz	Audit Work: FY 2020 (7/1/19) to Present
52	Administration	Information Technology Services	IT Security	Mod	Low	Mod	High	Low	5/9/24 - Feedback on Updated Banner Core System Security Plan (SSP) and Plan of Action and Milestones (POA&M); 5/9/24 - Updated IT Security Standard; 2/2/24 - Review Facilitated Banner Core Control Self-Assessment Results; 1/29/24 - University-Wide Incident Response Policies and Procedures; 5/10/23 - Feedback on ITS Security Awareness Training Updates 1/18/23 - IT Risk Self-Assessment Results: Enterprise-wide Guidance 11/4/22 - Feedback on Proposed University-wide Information Security Control Baselines 8/26/22 - IT Risk and Control Infrastructure Program Monitoring 9/17/21 - Compare Mason's IT Security Program with NIST Controls Framework 9/15/21 - Remediation of 3rd Party Service Provider Oversight 3/25/20 - Validation of Management's Remediation of APA's Firewall security issues 12/16/19 – Enterprise CUI Environment Assessment of Certain Control Requirements & CUI Project Intake Process Design
53	Administration	Information Technology Services	Learning Support Services / Online Learning Resources	Mod	Low	Low	Mod	Low	
54	Administration	Information Technology Services	Network IT Infrastructure	Mod	Mod	Low	High	Low	2/2/24 - Review Facilitated Banner Core Control Self-Assessment Results;
55	Administration	Information Technology Services	Physical IT Infrastructure (+ physical server management)	Low	High	Low	Mod	Low	2/2/24 - Review Facilitated Banner Core Control Self-Assessment Results;
56	Administration	Information Technology Services	Strategic Business Operations / Process and Planning	Mod	Low	Low	High	Low	3/14/23 - Feedback on ITS Portfolio and Project Management Updates 9/17/20 - IT Portfolio Management
57	Administration	Capital Strategy and Planning		High	Low	Low	Low	Low	
58	Administration	Facilities	Facilities Management Maintenance & Utilities	Low	Low	Low	Mod	Low	
59	Administration	Facilities	Planning, Design and Construction (including University Building Official)	High	High	High	Mod	Mod	11/15/22 - Life Sciences and Engineering Building Pre-Construction GMP 2 Proposal 9/21/22 - GMU Design Manual: Suggested Areas to Clarify 5/8/20 - Construction Contract Payment Processing - Robinson Hall Replacement Project 7/2/19 - Construction Contract Payment Processing - Core Campus Project

The risk-assessed Audit Universe, sorted by Executive:

#	Executive	Group	Area	Str	Fin	Comp	Opns	Haz	Audit Work: FY 2020 (7/1/19) to Present
60	Administration	Risk, Safety, and Resilience	Enterprise Risk Management	High	Low	Low	Mod	Low	
61	Administration	Risk, Safety, and Resilience	Public Health Management	Low	Low	Mod	Low	Mod	
62	Administration	Risk, Safety, and Resilience	Risk Management (Insurance)	Low	Low	Low	Low	Low	
63	Administration	Risk, Safety, and Resilience	Safety and Emergency Services	Low	Low	Mod	Low	Mod	
64	Administration	Auxiliary Operations & Services	Eagle Bank Arena	Low	Low	Low	Mod	Low	
65	Administration	Auxiliary Operations & Services	Food-Related Services; including related facilities and maintenance (& Independent Food)	Low	Low	Low	Mod	Mod	
66	Administration	Auxiliary Operations & Services	Mason Card	Low	Low	Low	Low	Low	
67	Administration	Auxiliary Operations & Services	Parking, Shuttles, and Transportation	Low	Low	Low	Mod	Low	
68	Administration	Auxiliary Operations & Services	Print and Mail Services	Low	Low	Low	Low	Low	
69	Administration	Auxiliary Operations & Services	Retail-Related Services (& Independent Retail)	Low	Low	Low	Mod	Low	
70	Administration	Real Estate	Real Estate Administration (Lease Properties)	Low	Mod	Low	Low	Low	
71	Advancement	University Advancement and Alumni Relations	University Advancement	Mod	Low	Low	Low	Low	6/22/20 - Gift Acceptance Policy Implementation
72	Athletics	Intercollegiate Athletics	External Affairs, Fund Raising and Funds Management	Low	Mod	Low	Mod	Low	7/25/24 - Intercollegiate Athletics Certain Compliance Areas; 2/10/20 - Intercollegiate Audit: reopening of audit issues
73	Athletics	Intercollegiate Athletics	Student-Athlete Processes	Low	Mod	High	Mod	Mod	2/10/20 - Intercollegiate Audit: reopening of audit issues
74	Branding	Strategic Communications and Marketing		Mod	Low	Low	Mod	Low	4/24/23 - Noncompliance with Hiring Practices

The risk-assessed Audit Universe, sorted by Executive:

#	Executive	Group	Area	Str	Fin	Comp	Opns	Haz	Audit Work: FY 2020 (7/1/19) to Present
75	Diversity, Equity and Inclusion	Diversity, Equity and Inclusion		Mod	Low	High	Mod	Low	12/14/20 - Handling Investigations of Allegations of Discrimination 6/11/20 - Possible conflict of personal interest and misuse of Mason resources for private business 12/13/19 - Employee Disclosures and evaluation of Personal Interest 11/19/19 - Possible misuse of 3D Printer
76	Govt & Comm Relations	Government and Community Relations		Mod	Low	Mod	Low	Low	
77	Police and Public Safety	Police and Public Safety		Low	Low	Low	Mod	Mod	9/19/19 - Separation of Purchasing and Inventory Responsibilities
78	President	Audit and Compliance	Institutional Compliance Program	Low	Low	Mod	Mod	Low	6/15/22 - Ethics Program Initial Assessment
79	President	University Counsel		Low	Low	High	Mod	Low	
80	President	President's Office		Mod	Low	Low	Low	Low	1/21/20 - Noticing of December 2019 Presidential Search Committee Meeting

Enterprise Risk Management Update
Audit, Risk, and Compliance Committee of the Board of Visitors
November 19, 2024

The following information is an update to the reports provided to the Board in FY24 and September 2024. It is important to note that enterprise risk management is a continuous improvement process and therefore the assessment provided herein may continue to change as the risk landscape and conditions change both internally and externally. At this time, the highest priority risks are Funding Resources, Competition, and Cybersecurity. A summary of the mitigation actions for these three highest priority risks are shown in Figure 2.

Since the last report provided to the Board, Executive Risk Owners (ERO) and Action Plan Risk Owners (APRO) have continued to implement the action plans aligned with the mitigation strategies for all 10 enterprise risks. These strategies will continue to be refined and implemented as appropriate until the risks are reduced to an acceptable level. The Chief Risk Officer is working with ERO on financial analyses to ensure limited resources are appropriated prudently for action plans that require additional funding.

Some action plan highlights pertaining to the highest priority risks from recent months:

- As part of the mitigation strategy addressing **Funding Resources**:
  - Advocacy for Commonwealth funding resulted in receiving ~$7.9m for FY25 for the VMSDEP program, with a similar amount expected in FY26.
  - The Budget Model Redesign project is underway, with an expected timeline allowing its use in FY26 budget development.
- As part of the mitigation strategy addressing **Competition**:
  - Human Resources has automated a host of recruitment sites (LinkedIn, HigherEd Jobs, etc.) to enable more streamlined recruitment processes.
  - Gallup engagement survey results were shared with the university, and reports are available to unit leaders.
  - The Office of University Branding continues to support the university’s competitiveness through marketing strategies; for instance, brand advertising featuring top faculty and national rankings continues regionally and digitally, generating millions of impressions.
  - Improved access and affordability are being achieved via an extension of the Mason Virginia Promise Grant to all full Pell recipients starting with the fall 2025 semester, as well as an expected expansion of the ADVANCE-Mason Virginia Promise program to two new institutions.
- As part of the mitigation strategy addressing **Cybersecurity**:
  - The university continues to make progress towards establishing an identity and access management solution.
  - George Mason is creating an Office of Research Security within the Office of Research Integrity and Assurance to ensure the effective implementation of research security measures, including National Security Presidential Memo-33.

Lastly, the environment is continually scanned for internal and external factors that impact enterprise risks, to ensure risk response efforts are focused in the most critical areas. The trend assessment for each of the 10 enterprise risks is shown in Table 1.

Figure 1. FY24/25 Enterprise Risk Heat Map

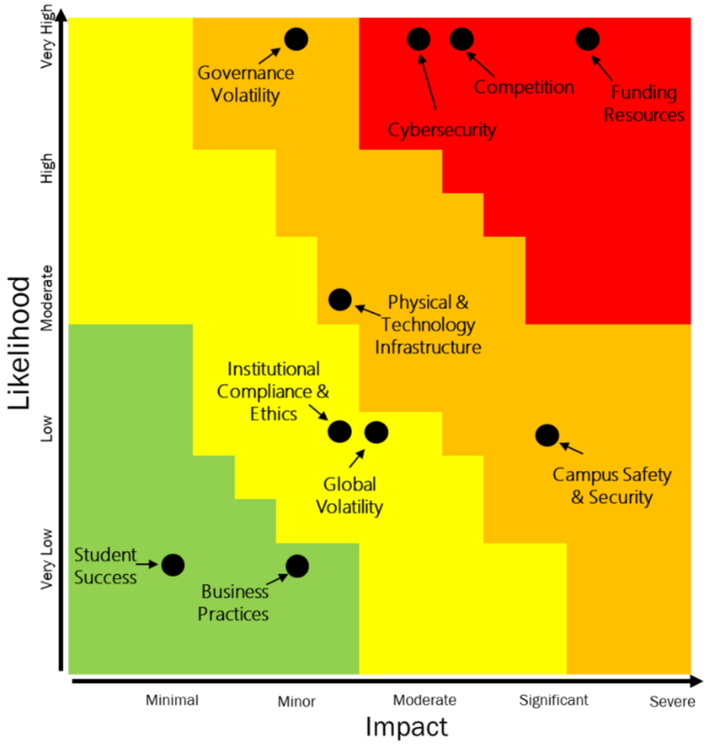


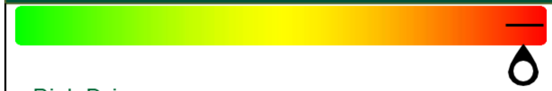
Table 1. FY24/25 Ranked Enterprise Risks

Risk Name	Priority/ Rank	Risk Level	Risk Trend*
Funding Resources	1	🟥	Neutral
Competition	2	🟥	Increasing
Cybersecurity	3	🟥	Neutral
Governance Volatility	4	🟧	Increasing
Campus Safety & Security	5	🟧	Increasing
Physical & Technology Infrastructure	6	🟧	Increasing
Global Volatility	7	🟨	Decreasing
Institutional Compliance & Ethics	8	🟨	Decreasing
Business Practices	9	🟩	Neutral
Student Success	10	🟩	Neutral

**Compared to September 2024 BOV Report*

Figure 2. Highest Priority Enterprise Risks

Funding Resources



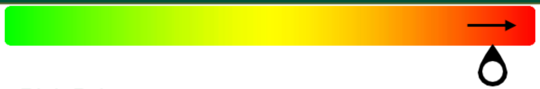
Risk Drivers

- Funding (State and Federal support) and financial aid
- Economic environment
- Reduced revenue/enrollments
- Tuition funding directives and unfunded mandates from state
- Historic underinvestment in systems and infrastructure
- Workforce shortages/Skill gaps in critical areas

Mitigation Actions

- Advocate for Commonwealth funding
- Manage tuition, room and board rates
- Meet enrollment targets in the SCHEV Six-Year plan
- Execute unit budget reductions & cost containment
- Continue revenue diversification
- Align service models and organization
- Continue to enhance operational efficiency and effectiveness
- Propose and implement retirement incentives
- Manage enrollment revenue through deliberate student aid practices
- Catalyze early-stage and large-scale research activity
- Leverage congressionally directed funding
- Scale Research, Innovation, and Entrepreneurship infrastructure through external support
- Launch and execute billion-dollar comprehensive campaign

Competition



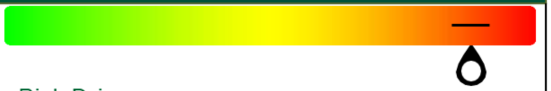
Risk Drivers

- Increased competition for student enrollment from a growing number of institutions
- Stagnant/declining number of high school graduates from key markets
- Changing value proposition associated with higher education
- Student/faculty/staff recruitment, retention, engagement and inclusivity
- Faculty/staff total compensation

Mitigation Actions

- Enhance student/faculty/staff recruitment technology and process
- Upgrade performance management system
- Continually assess market compensation
- Expand employee engagement
- Expand professional development offerings
- Provide recruitment central support
- Provide research support and training
- Provide graduate and postdoctoral fellow student support
- Increase competitiveness through marketing strategies
- Improve access and affordability through expanded financial assistance and partnerships

Cybersecurity



Risk Drivers

- Network, Application, Information, and Operational Security
- Disaster recovery and business continuity
- Increased sophistication in threat actor activity; (i.e., ransomware attacks)
- Third party applications
- End-user behavior

Mitigation Actions

- Apply IT Security Standard
- Establish identity and access management program
- Exercise change and configuration management
- Enhance IT Security end-user education frequency and modality
- Improve disaster recovery infrastructure leveraging cloud services
- Enhance risk assessment and remediation program
- Launch MIDAS (Mason Insights – Data to Analytics Solutions) project
- Enhance data loss prevention capabilities in Microsoft365 service
- Implement Cloud Access Security Broker
- Assess research cybersecurity

GEORGE MASON UNIVERSITY

Office of Institutional Compliance

Report to the Audit, Risk, and Compliance Committee of the Board of Visitors

November 19, 2024

EXECUTIVE SUMMARY

This report summarizes Institutional Compliance activities since the prior Committee meeting:

- Compliance assessment activity:
  - Inventory: 458 laws and regulations applicable to George Mason tracked, up from 454.
    - Risk ownership has been identified and confirmed for 444 laws and regulations, up from 439 (97%).
  - Guided, granular regulatory risk assessments for priority risk areas continue:
    - In Progress: FAR/DFARS, award management and costing
  - Guided, program maturity self-assessments of distributed compliance programs continue:
    - Completed: Counseling and Psychological Services, Center for Community Mental Health Records Management
    - In Progress: FAR/DFARS, Award Management and Costing, Athletics Privacy
  - External reviews: One new external review was announced since the last meeting and is in progress. One review remains in progress since the last meeting and two were completed.

- Status of reported compliance matters:
  - One potential compliance matter was reported to Institutional Compliance since the prior meeting, and was referred to another unit for investigation. Two matters investigated directly by Institutional Compliance were closed since the last meeting and one remains in progress. None of the matters appear significant to George Mason.
  - Coordination of investigations and investigative protocols continues to occur with units such as Research Integrity and Assurance; Diversity, Equity, and Inclusion; Human Resources; Information Technology Services; and the Office of the Registrar

- Additional institutional compliance activities:
  - Institutional Compliance continues to work with the Enterprise Risk Management Program and other groups to refine action plans to address the Institutional Compliance and Ethics enterprise risk and to strengthen George Mason's culture of integrity, ethics, and compliance; the action plans will be reviewed with senior leaders in early 2025.
  - Institutional Compliance continues to support substantial university-wide efforts to strengthen conflict of interest and related disclosure and management processes. Ongoing work includes: improving workflows, participating in the new review committee for organizational conflict of interests, ongoing development of an organizational conflict of interest policy and process, and additional communications and training.
  - Institutional Compliance benchmarked peer institution anonymous reporting capabilities, and has begun socializing such a capability for George Mason prior to implementation.

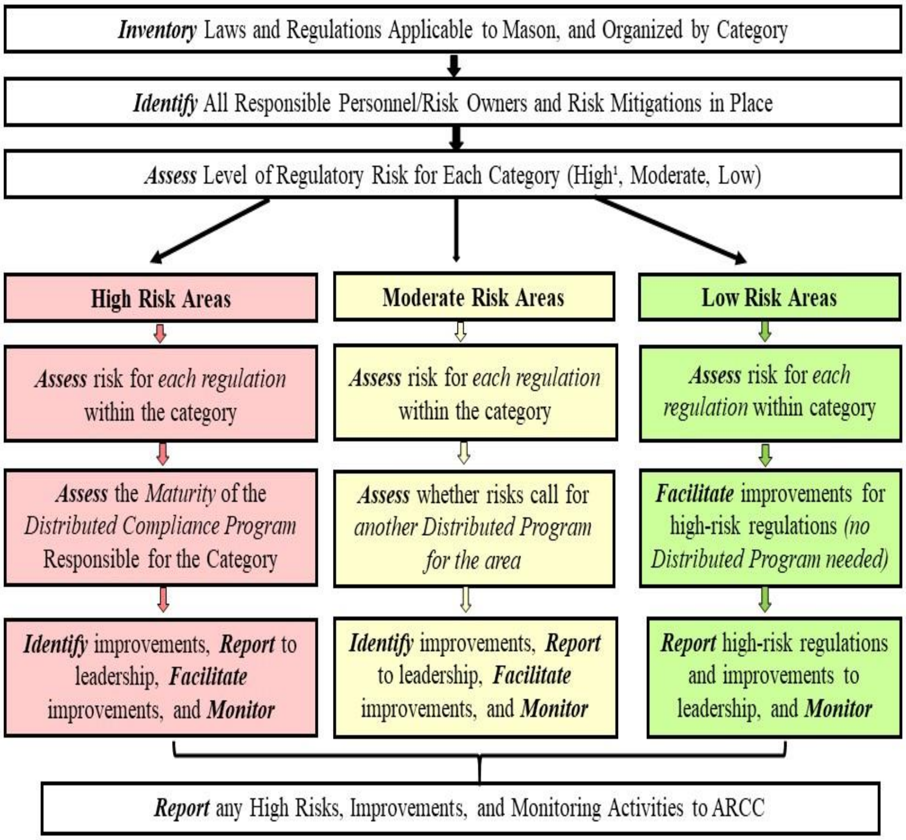
TABLE OF CONTENTS

Topic

Summary of Assessment and Monitoring Activity

Approach:

The Audit, Risk, and Compliance Committee of the Board has a Charter responsibility to oversee the effectiveness of institutional compliance processes for monitoring compliance with laws and regulations, including policies and processes related to ethics and conflicts of interest. Institutional Compliance supports the Committee's accomplishment of this responsibility through planning, facilitating, and overseeing regular university-wide assessments of compliance risks guided by the elements of effective compliance programs in the *US Federal Sentencing Guidelines for Organizations* and related guidance from the Department of Justice; ensuring management ownership for monitoring and managing compliance risks; evaluating the effectiveness of risk-owner programs to monitor and manage compliance risks; and ensuring communication to leadership and the Committee. The assessment and monitoring approach are depicted in the chart below.


Inventory Laws and Regulations Applicable to Mason, and Organized by Category
Identify All Responsible Personnel/Risk Owners and Risk Mitigations in Place
Assess Level of Regulatory Risk for Each Category (High[1], Moderate, Low)
High Risk Areas
Moderate Risk Areas
Low Risk Areas
Assess risk for *each regulation* within the category
Assess risk for *each regulation* within the category
Assess risk for *each regulation* within category
Assess the *Maturity* of the *Distributed Compliance Program* Responsible for the Category
Assess whether risks call for *another Distributed Program for the area*
Facilitate improvements for high-risk regulations *(no Distributed Program needed)*
Identify improvements, *Report* to leadership, *Facilitate* improvements, and *Monitor*
Identify improvements, *Report* to leadership, *Facilitate* improvements, and *Monitor*
Report high-risk regulations and improvements to leadership, and *Monitor*
Report any High Risks, Improvements, and Monitoring Activities to ARCC

Factors considered in assessing the level of regulatory risk include the potential for adverse regulatory action or critical interest by legislative or investigative entities which could result in governmental penalties, disruption or suspension of operations, programs, accreditation, or licensure, loss or reduction of funding, or sustained adverse public attention. The assessment of the level of regulatory risk indicates the expected robustness of the associated mitigation activities, including the formality and maturity of the related distributed risk-area compliance program.

INVENTORY OF LAWS AND REGULATIONS AND ACCOUNTABLE PERSONNEL:

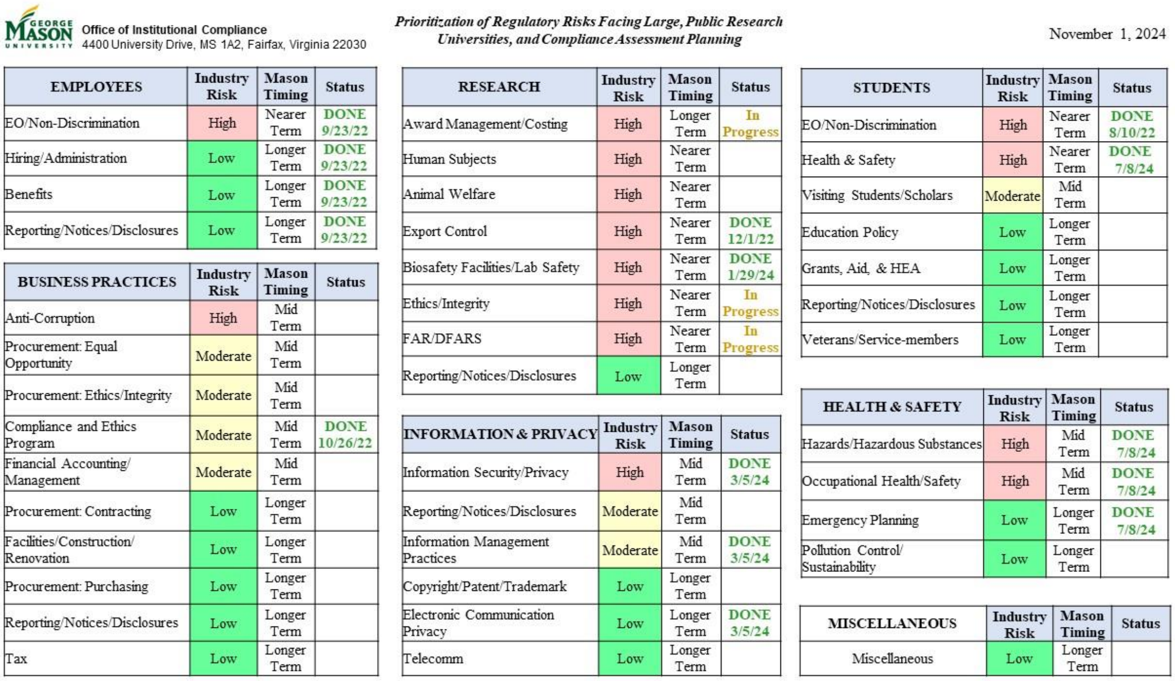
As of November 1, 2024, an inventory of 458 laws and regulations applicable to George Mason has been compiled and was reviewed with the Office of University Counsel for completeness and applicability. Risk owners have been identified and confirmed for 444 (97%) of the 458 laws and regulations; these owners have confirmed and accepted their responsibilities related to the 444 laws and regulations. Ownership and identification work is ongoing. The table below summarizes the inventory of laws and regulations by category together with those laws and regulations where ownership has been confirmed and accepted.

	Regulatory Category	**Number of Laws and Regulations Tracked**			**Number of Laws and Regulations for which Ownership Confirmed**		
		9/13/24	**11/1/24**	**Change**	**9/13/24**	**11/1/24**	**Change**
1	Compliance and Ethics Program	3	4	+1	3	4	+1
2	Copyright and Intellectual Property	9	-	-	9	9	-
3	Employment	93	94	+1	92	93	+1
4	Environmental Health and Safety and Occupational Health & Safety	53	53	-	53	53	-
5	Facilities, Construction, and Renovation	4	4	-	3	4	+1
6	Finance and Tax	45	45	-	45	45	-
7	Information Management and Security, and Privacy	50	50	-	43	43	-
8	Procurement and Contracting	21	21	-	20	20	-
9	Research	69	71	+2	69	71	+2
10	Students and Academic Policy	104	104	-	102	102	-
11	Miscellaneous	3	3	-	-		-
	Totals	**454**	**458**	**+5**	**439**	**444**	**+5**

ASSESSMENT PRIORITIZATION AND STATUS:

Institutional Compliance, in coordination with University Counsel, compiled a preliminary assessment of regulatory risks facing large, public research universities that are similar to George Mason. The assessment was completed using the inventory of laws and regulations by category and subcategory. It does not represent an assessment of specific risks or risk levels at George Mason; it is solely intended to provide a basis for identifying and prioritizing future George Mason-specific assessment activities. The preliminary assessment, summarized below, was shared with senior leaders and their input was used to prioritize further assessment work.

In coordination with Counsel, the Enterprise Risk Management Program, and leadership, the prioritization will be reviewed and modified as necessary in 2025.



Office of Institutional Compliance
4400 University Drive, MS 1A2, Fairfax, Virginia 22030

Prioritization of Regulatory Risks Facing Large, Public Research Universities, and Compliance Assessment Planning

November 1, 2024

EMPLOYEES	Industry Risk	Mason Timing	Status
EO/Non-Discrimination	High	Nearer Term	DONE 9/23/22
Hiring/Administration	Low	Longer Term	DONE 9/23/22
Benefits	Low	Longer Term	DONE 9/23/22
Reporting/Notices/Disclosures	Low	Longer Term	DONE 9/23/22

BUSINESS PRACTICES	Industry Risk	Mason Timing	Status
Anti-Corruption	High	Mid Term	
Procurement: Equal Opportunity	Moderate	Mid Term	
Procurement: Ethics/Integrity	Moderate	Mid Term	
Compliance and Ethics Program	Moderate	Mid Term	DONE 10/26/22
Financial Accounting/ Management	Moderate	Mid Term	
Procurement: Contracting	Low	Longer Term	
Facilities/Construction/ Renovation	Low	Longer Term	
Procurement: Purchasing	Low	Longer Term	
Reporting/Notices/Disclosures	Low	Longer Term	
Tax	Low	Longer Term	

RESEARCH	Industry Risk	Mason Timing	Status
Award Management/Costing	High	Longer Term	In Progress
Human Subjects	High	Nearer Term	
Animal Welfare	High	Nearer Term	
Export Control	High	Nearer Term	DONE 12/1/22
Biosafety Facilities/Lab Safety	High	Nearer Term	DONE 1/29/24
Ethics/Integrity	High	Nearer Term	In Progress
FAR/DFARS	High	Nearer Term	In Progress
Reporting/Notices/Disclosures	Low	Longer Term	

INFORMATION & PRIVACY	Industry Risk	Mason Timing	Status
Information Security/Privacy	High	Mid Term	DONE 3/5/24
Reporting/Notices/Disclosures	Moderate	Mid Term	
Information Management Practices	Moderate	Mid Term	DONE 3/5/24
Copyright/Patent/Trademark	Low	Longer Term	
Electronic Communication Privacy	Low	Longer Term	DONE 3/5/24
Telecomm	Low	Longer Term	

STUDENTS	Industry Risk	Mason Timing	Status
EO/Non-Discrimination	High	Nearer Term	DONE 8/10/22
Health & Safety	High	Nearer Term	DONE 7/8/24
Visiting Students/Scholars	Moderate	Mid Term	
Education Policy	Low	Longer Term	
Grants, Aid, & HEA	Low	Longer Term	
Reporting/Notices/Disclosures	Low	Longer Term	
Veterans/Service-members	Low	Longer Term	

HEALTH & SAFETY	Industry Risk	Mason Timing	Status
Hazards/Hazardous Substances	High	Mid Term	DONE 7/8/24
Occupational Health/Safety	High	Mid Term	DONE 7/8/24
Emergency Planning	Low	Longer Term	DONE 7/8/24
Pollution Control/ Sustainability	Low	Longer Term	

MISCELLANEOUS	Industry Risk	Mason Timing	Status
Miscellaneous	Low	Longer Term	

IN-PROGRESS ASSESSMENTS:

Assessments of distributed, risk-specific programs are planned and facilitated based upon the prioritization of risk areas, as well as upon request by distributed program owners. The assessment of the level of regulatory risk in a given category indicates the expected robustness of the associated mitigation activities, including the formality and maturity of the related distributed risk-area compliance program. Assessment activities completed, in progress, and planned are summarized in the following chart:

Summary of Assessment Activity	As of 9/13/24	As of 11/1/24
Regulatory Risk Assessments:		
Federal Contracting (FAR/DFARS)	IP	IP
Program Maturity Guided Self-Assessments:		
Counseling and Psychological Services – Privacy	Draft	DONE
Center for Community Mental Health – Privacy	Draft	DONE
Records Management	Draft	DONE
Research – Award Management and Costing	Draft	Draft
Athletics – Privacy	Draft	Draft
Research – Ethics, Conflict of Interest and Commitment, Foreign Influence, Organizational Conflict of Interest	IP	IP
Federal Contracting (FAR/DFARS)	IP	IP

(Legend: DONE=completed; Draft = report draft; IP=in progress; NS=not started.)

Summary Status of External Reviews:

The Committee has a Charter responsibility to "review and discuss with management the results of significant reviews by regulatory agencies or other external entities, or summaries thereof, and management's responses." University policy requires that all notices of any external review be reported to the Institutional Compliance Leader for tracking, reporting, and follow-up. One new external review was announced since the prior meeting and is in progress. One remains in progress since the last meeting and two were completed. The table below summarizes external review activity since the prior meeting.

Reviewing Entity	As of 9/26/24	As of 11/1/24	Remarks
Auditor of Public Accounts (APA)	Not Announced	In Progress	Statewide Financial Aid Audit, including evaluation of GLBA compliance.
Virginia Joint Legislative Audit & Review Commission (JLARC)	In Progress	In Progress	Statutory review of George Mason's tier 3 management authority; scheduled for review with Commission in November 2024.
Office of Naval Research (ONR)	In Progress	Complete	Annual desk review of George Mason's property management system. Review completed with no findings.
Office of the State Inspector General (OSIG)	In Progress	Complete	Performance review related to higher education institution security programs for responding to cyber-attacks. Includes all Commonwealth universities and VCCS. Review complete and report received.

SUMMARY OF REPORTING MECHANISMS AND MATTERS

Institutional Compliance conducts, oversees, coordinates, and/or monitors investigations of allegations of non-compliance or ethical misconduct. The office utilizes up-to-date, detailed guidelines for conducting compliance investigations, which are incorporated into the Institutional Compliance and Ethics Program operating manual. A process also was implemented for tracking the disposition of reported matters investigated by Institutional Compliance; additional processes are being developed to monitor the disposition of certain reported matters referred to other units.

To encourage reporting, a landing website is maintained by Institutional Compliance that links to reporting mechanisms for various constituencies and issue types across campus. To further encourage reporting, and to reduce risk and to meet accepted standards for effective compliance and ethics programs, Institutional Compliance benchmarked anonymous reporting capabilities at numerous peer institutions, and has begun the process of socializing and implementing the addition of such a mechanism for George Mason.

Institutional Compliance received one new allegation of non-compliance or ethical misconduct since the last Committee report, which matter was referred to other units. Two matters under investigation by Institutional Compliance and/or University Audit as of the last report were closed, and one remains in progress. None of the matters reported appear significant to George Mason. The table below shows the status of matters reported to Institutional Compliance, and whether referred to other units for handling or handled directly by Institutional Compliance and/or University Audit.

Status	**6/12/24 to 9/13/24**	**9/13/24 to 11/1/24**	**Total**
Matters Reported to Institutional Compliance in Period	4	1	5
Matters Referred to Other Units for Handling in Period	2	1	3
Matters Reported in Period Investigated by Institutional Compliance or University Audit	2	-	2
In Progress of Investigation	1	1	2
Closed - Non-Compliance Not Substantiated	1	2	3
Closed where Non-Compliance Substantiated	-	-	-
Closed where Non-Compliance was Significant	-	-	-

The table below lists the reported matters since the last meeting by topic area.

Topic Area	**#**
Research	1
Total	1

SUMMARY OF ADDITIONAL COMPLIANCE ACTIVITIES

INSTITUTIONAL COMPLIANCE ENTERPRISE RISK MITIGATION STRATEGY:

Since the prior meeting, Institutional Compliance has worked with Risk, Safety, and Resilience and other groups to refine action plans to address the Institutional Compliance and Ethics enterprise risk and to strengthen George Mason's culture of integrity, ethics, and compliance. The action plans provide a roadmap for further build-out of George Mason's institutional compliance and ethics program; they will be reviewed with senior leaders in 2025.

The table below summarizes each area of focus within the draft strategy, and the status of each. Institutional Compliance will update the Committee when the strategy has been finalized, and will provide updates regarding each focus area.

1. Design and implement processes to increase compliance with mandated trainings	IP
2. Review Core Values and Code of Ethics; update if needed	IP
3. Build consensus for and implement a university-wide process for surfacing concerns about integrity, ethics, and compliance matters	IP
4. Improve the institutional policy development, review, and communication process	IP
5. Develop and implement compliance escalation matrix	IP

(Legend: DONE=completed; IP=in progress; NS=not started.)

TRAINING AND COMMUNICATION ACTIVITIES:

The following activities advance the preliminary institutional compliance and ethics risk management action plans described above.

- Additional George Mason-specific compliance awareness training content has been developed and is undergoing stakeholder review. The training is anticipated to also be used for new employee and new faculty orientations. Implementation is anticipated for 2025.

- Conflict of Interest/Conflict of Commitment guides, training, and other resources were added and improved and made available to users through the RAMP platform on George Mason's COI website. Institutional Compliance is evaluating whether and where additional conflict of interest training might be needed.

- In order to improve tracking and enforcement of all training required for all employees (e.g., ethics, information security, student privacy, Title IX, violence prevention, and others), Institutional Compliance worked with Human Resources to obtain access to training completion data, and has developed preliminary metrics for providing training data to leadership. A process for sending automated reminders for all training modules is anticipated to be implemented in 2025.

- The draft compliance communications calendar, setting forth key compliance deadlines and information about common compliance risks, continues to be refined and expanded. Once implemented, the calendar will assist George Mason in meeting compliance communication expectations, as well as socialize Institutional Compliance resources with the campus community.

INSTITUTIONAL COMPLIANCE STAFFING

There have been no changes to Institutional Compliance staffing since the last Committee report. Below are professional biographies for the two team members.

Vin Lacovara, Associate Vice President for Institutional Compliance
vlacovar@gmu.edu

Vin Lacovara joined George Mason to establish and lead the Institutional Compliance function in February 2021. His responsibilities are to implement and manage an effective, institution-wide compliance and ethics program for George Mason; oversee and coordinate the efforts of numerous distributed, area-specific compliance programs across campus; and provide senior leadership and the Committee with information to fulfill their oversight of compliance processes.

Prior to joining George Mason, Vin implemented and managed the compliance and ethics program for Catholic University for ten years. For seven years prior to joining Catholic, he worked alongside George Washington University's compliance officer in managing all aspects of its compliance and ethics program, and was in the private practice of law for seven years prior to becoming a compliance professional. Vin earned bachelor's degrees in English and political science from Duke University, and a law degree from Catholic University's Columbus School of Law. He is also a Certified Compliance and Ethics Professional$^{©}$, and has presented at national industry conferences on the topics of compliance program implementation, compliance assessment frameworks, and compliance investigations.

Elizabeth Woodley, University Ethics Officer and Outside Interests Manager
ewoodley@gmu.edu

Elizabeth Woodley joined Institutional Compliance in March 2021 to assist in establishing a more robust ethics program for George Mason; oversee George Mason's Conflict of Interest policies, disclosures, and waiver processes; investigate complaints related to ethical conduct; and develop and track ongoing communications, training, and education activities.

After serving as a Robert F. Kennedy Public Service Fellow with the University Counsel's Office, Elizabeth joined George Mason's Compliance, Diversity, and Ethics office in 2013 as the University Policy Manager. She later added responsibilities as the FOIA Compliance Officer in 2014 and the Ethics Officer in 2016. Elizabeth earned a bachelor's degree in history and art history from the University of Virginia, and a law degree from the University of Virginia School of Law. She is also a Certified Compliance and Ethics Professional$^{©}$.

APPENDIX

- Reports
  - Counseling and Psychological Services Privacy Program Maturity Assessment Report
  - Center for Community Publish Health Privacy Program Maturity Assessment Report
- Schedule of Assessments Completed Since 2021

Office of Institutional Compliance

ASSESSMENT REPORT

Report Title:	Counseling and Psychological Services Privacy Program Maturity Self-Assessment	**Report Date:**	October 1, 2024
Responsible Manager:	Dr. Jennifer Kahler Director, Counseling and Psychological Services		

EXECUTIVE SUMMARY:

Background

Distributed Compliance Programs should evaluate regularly whether their design is tailored to Mason's operations and level of risk, and whether they are working effectively in practice. In May 2024, the Office of Institutional Compliance facilitated a self-assessment of the maturity of Mason's Office of Counseling and Psychological Services. The self-assessment evaluated the design adequacy and operating effectiveness of each of the elements necessary for an effective program.

The Family Educational Rights and Privacy Act (FERPA) protects student "treatment records," which are records made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in their professional or paraprofessional capacity, and which are made, maintained, or used only in connection with the provision of treatment to the student. Per FERPA, treatment records may only be shared with other treatment providers except with the student's consent[1].

Counseling and Psychological Services (CAPS) seeks to cultivate a thriving George Mason community through inclusive, innovative, and compassionate student care. Its mission is to support students through ethical and responsive care and prevention, and fostering the well-being of the diverse George Mason community through psychological, outreach, and consultation services. CAPS is committed to excellence in psychological services by promoting student safety, enhancing emotional growth, and supporting academic success. The Director of CAPS reports to the Associate Dean and Chief Mental Health Officer and is composed of 35 staff members at two campus locations.

Conclusion

The overall self-assessment concluded that the CAPS Privacy Program is **well defined** and **trending toward mature**, and working well in practice. The Program has a designated leader with a clearly documented role and authority, skilled staff and clinicians, engaged and effective oversight, detailed and current policies and procedures, required and current training, and a culture of risk-based

[1] NOTE: If the university engages in electronic transactions with respect to the student's treatment, particularly in the area of billing, the Health Insurance Portability and Accountability Act (HIPAA) would then apply. CAPS does not bill electronically for services provided, and thus only FERPA applies.

assessment and continuous improvement. Collaboration with relevant units (e.g., Student Health Services; Diversity, Equity, and Inclusion; International Programs and Services, INTO Mason, and Institutional Compliance) is effective.

Assessment

CAPS has a designated Program leader (the Director) who is appropriately skilled and credentialed, and who has a clearly documented role and authority as set forth in her position description. The Program leader reports to the Associate Dean and Chief Mental Health Officer (CMHO), who oversees and is knowledgeable and supportive of the Program. The Associate Vice President (AVP) for University Life and the Vice President (VP) for University Life also are knowledgeable about and support the Program. The Program leader provides weekly briefings to the CMHO about the Program, and twice per month reports to the CMHO on Program changes. Reports are forwarded to the AVP University Life and to the VP University Life who provides such reports to the Provost. This reporting and oversight process is a particular strength.

Required background investigations are administered centrally by Human Resources, and the Program confirms that prospective staff are licensed and have not been subject to disciplinary action by credentialing authorities. Extensive ethics questions are asked during the interview process, and upon extending a conditional offer of employment, the Program conducts extensive record checks (including two prior supervisor references and a non-supervisor reference). These are Program strengths.

George Mason maintains a central FERPA Compliance Policy that clearly defines "treatment records" as distinct from other forms of student records, and includes the specific limitations on sharing treatment records as set forth in the law. CAPS maintains a Policy and Procedures (P&P) Manual that contains all key policies, such as those addressing physical access, access to the electronic medical records system, appropriate electronic communications, and accurate and confidential recordkeeping. The Manual is organized and clear, current, tailored to the Program, and is reviewed every other year. Per P&P 1004, Ethical Principles and Codes of Conduct, staff must follow George Mason policies as well as ethical principles and codes specific to their discipline, and when there is a difference in standards, the more stringent will apply. The Program website is clear and easy to navigate, and also includes FAQs with a link to the students' rights as clients, including the right to confidentiality, to review and release records, and to share concerns and present a complaint. To improve Program maturity further, consider adding a table of contents to the P&P Manual, and consider adding the last date the Manual was reviewed and/or revised.

CAPS uses the secure Titanium electronic medical records system , managed on premises by Information Technology Services, to store treatment records. CAPS also requires that all clinicians sign a Confidentiality Agreement with respect to secure and appropriate treatment of records. A student Release of Information Form that is specific and detailed also is utilized to prevent against unauthorized disclosure of records. These are all program strengths.

All Program staff complete university FERPA training, which is clear and current. Staff also complete initial and annual refresher privacy training specific to CAPS operations. The initial and refresher modules are reviewed annually and revised as necessary to include new and revised requirements and resources, which are also communicated on an ongoing basis. Orientation training materials also are in place for new staff, and address confidential data and its limits, guidelines for safeguarding such data, student consent and record requests, confidential storage areas, secure communications, computer security, and breach procedures. All new staff must acknowledge that they have reviewed the orientation training material. In addition, a senior clinician is assigned to each junior clinician to serve as a consultant and mentor, a particular Program strength. Training completion is tracked and, where appropriate, non-compliance is escalated and system access may be revoked. However, tracking does not occur formally or regularly. To improve Program maturity, consider implementing a mechanism to regularly track, enforce, and document training completion by all staff, and to reinforce consequences for non-completion.

The Program has a culture of continuous assessment and improvement. Program staff assess risks and trends in real-time, and promptly implement improvements. Formal, regular Program assessments occur annually. For example, a formal chart audit is conducted annually whereby medical charts are randomly reviewed for compliance with requirements regarding notice and informed consent. No significant issues were identified with respect to the assessments conducted. The Program also undergoes regular external audits by the International Association of Counseling Services (IACS), which reviews licensure, administrative staffing, reasons for clinicians leaving George Mason employment, supervision and training, changes to the reporting structure, and any larger changes that could affect clinical work. The Program should confirm that annual assessments and audits are documented.

Per P&P 1008 Client Feedback About Services, students have the opportunity to raise concerns or complaints with the Program. The Program website also includes FAQs with a link to the students' rights as clients, including the right to share concerns and present a complaint. The Associate Director is listed by title and telephone as the point of contact for concerns and complaints. Specific investigative and disciplinary steps are in place, including coordination with Human Resources on employee relations and performance matters. A consistent investigative rubric is utilized, though tailored as needed for specific circumstances. To improve Program maturity, confirm that the investigative steps and disciplinary rubric are documented. Also, consider comparing investigative protocols against those maintained and utilized by Institutional Compliance.

Office of Institutional Compliance

ASSESSMENT REPORT

Report Title:	Center for Community Mental Health Privacy Program Maturity Self-Assessment	**Report Date:**	October 1, 2024
Responsible Manager:	Dr. Robyn Mehlenbeck Director, Center for Community Mental Health		

EXECUTIVE SUMMARY:

Background

Distributed Compliance Programs should evaluate regularly whether their design is tailored to Mason's operations and level of risk, and whether they are working effectively in practice. In July 2024, the Office of Institutional Compliance facilitated a self-assessment of the maturity of Mason's Center for Community Mental Health (CCMH) Privacy Program. The self-assessment evaluated the design adequacy and operating effectiveness of each of the elements necessary for an effective program.

The Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, and the Virginia Health Records Act, impose privacy and security requirements on institutions that collect, use, store, and/or share Protected Health Information[1]. Such requirements include privacy notices to consumers and a right to access their records, data encryption, a formal security plan with administrative, physical, and technical safeguards, and breach notification protocols. These requirements can overlap with certain Family Educational Rights and Privacy Act (FERPA) privacy provisions. Fines and penalties for non-compliance with HIPAA and HITECH can reach $4 million per year, and the Acts provide for private rights of action for individuals.

The Center for Community Mental Health (CCMH) is a multidisciplinary training facility for students in behavioral health, which serves the wider community. Its mission is to provide culturally responsive evidence-based clinical training in assessment, consultation, and intervention, as well as to provide accessible, culturally sensitive, state-of-the-art mental health services to the community. CCMH also participates in clinical research to help improve the quality of existing interventions and contribute to the scientific community. The Director of CCMH reports to the Chair of the Department of Psychology in the College of Humanities and Social Sciences, and CCMH is composed of approximately 17 staff members and faculty advisors at one campus location.

Conclusion

The overall self-assessment concluded that the CCMH Privacy Program is **well defined** and **trending toward mature**, and working well in practice. The Program has a designated leader with a clearly documented role and authority, skilled staff and clinicians, oversight by the Department of Psychology in the College of Humanities and Social Sciences and support and engagement from the Department, Dean, and Provost. The Program also has detailed and current policies and procedures, required and current training, and a culture of risk-based assessment and continuous improvement. Collaboration with relevant units (e.g., Counseling and Psychological Services; Student Health Services, Mason and Partners Clinic; University Counsel, and Institutional Compliance) is effective.

Assessment

CCMH has a designated Program leader (the Director) who is appropriately skilled and credentialed, and who has a clearly documented role and authority as set forth in her position description, which also includes responsibility for responding to concerns. The Program leader reports to the Chair of the Department of Psychology in the College of Humanities and Social Sciences, who oversees and is knowledgeable and supportive of the Program, and who receives the Program's annual report. The Dean and the previous Provost was also both aware and supportive of the Program. The Program should seek continued awareness and support from the new Provost. The Director affirmatively fosters a culture of collaboration within the unit, as well as with other key units as described above. The Program also is part of the institutional Mental Health Task Force, which fosters further collaboration and provides additional ongoing information to leadership about the Program. Reporting, oversight and collaboration processes are particular Program strengths.

Required background investigations for staff are administered centrally by Human Resources, and the Program confirms that prospective staff have the appropriate psychological or counseling licenses. Background investigations also are conducted for student trainees who work with minors. Licensed staff complete appropriate continuing education and are required to meet certification requirements, which is monitored by Program staff. To improve Program maturity, consider more formal tracking that psychological and counseling licenses are current and that continuing education and certification requirements have been met.

George Mason maintains an institutional HIPAA compliance policy that clearly defines regulatory requirements and is current. HIPAA data also is defined as Protected-Highly Sensitive in George Mason's institutional Data Stewardship Policy. CCMH maintains a *Center Training Book* for students that contains provisions pertaining to confidentiality, and references HIPAA requirements extensively and clearly. The *Center Training Book* is comprehensive and complete, is reviewed annually prior to each academic year, and includes contact information for pertinent staff and encourages students to raise questions. As the *Center Training Book* also acts as an operational document for student trainees, CCMH might consider renaming the document to reflect its ongoing operational nature.

CCMH also maintains a *Supervisor Handbook* for staff who oversee student trainees, and which contains provisions regarding orientation, supervisor oversight responsibilities, confidentiality, physical and technological security requirements, ongoing assessment responsibilities, and contact information for key personnel. The *Supervisor Handbook* is clear and comprehensible and is reviewed annually prior to the start of the academic year. Standards and policies as described are a program strength. To improve Program maturity, CCMH should consider stating more directly in the *Center Training Book* and the *Supervisor Handbook* that reports and concerns should be directed to Director, and include contact information for the director. Consider also providing clear information to the public regarding Center policies, procedures and information on how to share any concerns, and how to follow up on any concerns, potentially through FAQs on the website.

Program staff are skilled at reviewing instances of potential HIPAA non-compliance, though formal protocols are not currently documented. While consequences for non-compliance with Program standards are applied, when necessary, such consequences are not documented. To improve Program maturity, consider including statements in the *Center Training Book* and *Supervisor Handbook* regarding consequences for non-compliance with privacy requirements. Consider also working with Institutional Compliance to develop more formal processes for prompt and thorough triage and review of concerns raised.

The Program website clearly describes CCMH and its role and approach, as well as fee and insurance information. The Director, staff, clinicians, and supervisors are listed by title, though only general contact information for the unit is provided. To improve Program maturity, consider adding additional contact information for personnel to both the Handbooks and TEAMS folders accessible by everyone working at the Center, and consider adding language and contact information for reporting concerns. As noted above, consider also making a more detailed FAQ on the website for the public.

CCMH uses the secure Titanium electronic medical records system to store treatment records, and requires that all clinicians and students sign a Confidentiality Agreement with respect to secure and appropriate treatment of records. A current and complete Notice of Privacy Practices is provided to all who utilize the center, and Release of Information (ROI) Forms are used to obtain authorization to release information.

All Program staff complete required institutional Information Technology Services Security and FERPA training, which are clear and current. Institutional training is tracked, and access to the electronic medical records system is denied or suspended if both modules are not completed. Staff and student trainees also complete initial and annual refresher training that addresses HIPAA and Protected Health Information (PHI), as well as confidentiality requirements. Training is tailored to the particular audience (i.e., clinicians, student trainees, staff), is tracked, and student trainees are not permitted to see clients until training is completed. During annual and refresher training staff and students are provided with the *Center Training Book* or the *Supervisor Handbook*, as applicable. The initial and refresher modules are reviewed annually and revised as necessary to include new and revised requirements and resources, which are also communicated on an ongoing basis. These are program strengths.

The Program uses an ongoing, risk-based approach to assessing HIPAA compliance. Several layers of supervision for student trainees are in place so that such trainees always have an avenue for support and client safety. This approach is incorporated into ongoing in-person communication and supervision of trainees, through targeted reviews of trainee cohort performance, and into annual training revisions. Root causes analyses of trends are conducted, and modifications and improvements to the Program are made in real time as part of the culture of continuous assessment, a Program strength.

SCHEDULE OF COMPLETED COMPLIANCE ASSESSMENTS SINCE 2021

This Appendix provides a schedule of regulatory risk assessments and program maturity guided self-assessments completed since the Program's inception in 2021.

Summary of Assessment Activity	Date Completed
Regulatory Risk Assessments:	
Equal Opportunity and Title IX (DEI)	12/8/2021
Equal Opportunity (HR)	3/30/2022
Human Resources Benefits	3/30/2022
Human Resources Hiring and Administration	3/30/2022
Office of the Registrar	10/12/2022
Laboratory Safety	5/1/2023
Institutional Privacy	3/5/2024
Health, Safety, and Emergency Planning and Response	2/27/2024
Research Award Management and Costing	3/14/2024
Program Maturity Guided Self-Assessments:	
Equal Opportunity and Title IX (DEI)	8/12/2022
Research: Export Control	12/9/2022
Office of the Registrar	10/10/2023
Student Health Services Privacy	12/7/2023
Laboratory Safety	1/29/2024
Health, Safety, and Emergency Planning and Response	7/8/2024
Mason and Partners Clinics and Population Health Center Privacy	8/26/2024
Counseling and Psychological Services Privacy Program	10/1/2024
Center for Community Mental Health Privacy Program	10/1/2024
Records Management Program	10/3/2024

INFORMATION
TECHNOLOGY SERVICES
George Mason University®

Information Technology Risk and Control Infrastructure Program
Update for the Board of Visitors
Audit, Risk, and Compliance Committee

October 2024

Prepared by

Dr. Charmaine Madison, Vice President and Chief Information Officer

Charlie Spann, Assistant Vice President, Enterprise Service Delivery and Deputy CIO

Noor Aarohi, Director - IT Risk and Compliance

Curtis McNay, Director - IT Security Office

Executive Summary

The following update provides a report of activities and accomplishments for September and October of Fiscal Year (FY) 25. This summarizes activities for maturing technical capabilities and controls focusing on specific program areas.

Since December 2021, with the input of the Office of University Audit (OUA), Information Technology Services (ITS) has established a multi-year program to strengthen the risk and control infrastructure at George Mason University and improve the quality of technology services delivered. The purpose of this report is to update the Audit, Risk, and Compliance Committee on the status of these efforts.

October 2024: George Mason's Cyber Security Strategy Published

Key Pillars:

- Data Protection & Privacy
- Security Awareness & Training
- Cutting-edge Cybersecurity Research
- Technology & Infrastructure
- Collaboration & Partnerships

The program is comprised of six areas of focus designed to guide the adoption and implementation of a set of controls derived from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 moderate baseline, scoped and tailored to the context of institutions of higher education as well as to help support the academic and research efforts while maintaining a strong information security posture. This will strengthen policies, standards, processes, and procedures related to George Mason's quality management and Information Security Management programs to improve IT service quality, reliability, and security. The overall program includes the following focus areas:

- George Mason Scoped and Tailored NIST 800-53-Based Security Compliance Framework
- Portfolio and Project Management
- Information Security Program Management
- Risk Assessment and Remediation
- Change and Configuration Management
- Identity Management and Access Control

Each area is comprised of activities tied to projects and assigned priority and ownership. This report outlines the status in each of the areas. Please note that these projects are only a subset of the technology investments currently being made at the university. All ITS-managed and administered information technology projects (including those related to these focus areas) are available for review at https://its.gmu.edu/working-with-its/ppmo/projects-dashboard/.

Since the prior report submitted covered activities through August 31, 2024, this report is pertinent to activities that occurred from September (partial FY25 Q1) through October 31, 2024 (partial FY25 Q2).

FY25 Q1 (September) & Q2 (October) Accomplishments, and FY25 Q2 (Nov-Dec) Planned Activities

George Mason Scoped and Tailored NIST 800-53-Based Security Compliance Framework

Adoption of a NIST 800-53 controls set that has been scoped and tailored to the context of institutions of higher education and to help support the academic and research efforts while maintaining a strong information security posture. Supporting policy and standards underpin our internal quality management for central ITS and our distributed partners.

FY25 September-October Accomplishments:

- Project #853: George Mason Scoped and Tailored NIST 800-53 Security Baselines Rollout - Project closeout activities have been initiated. Processes and documentation that have been put in place will continue to be socialized through the System Administrator Leadership Team (SALT) monthly meetings and training sessions.
- Security configurations based on Center for Internet Security (CIS) Level 1 recommendations for Windows 11 and Mac OS were reviewed and formalized, and consensus baselines have been deployed to all centrally managed macOS and Windows 11 endpoint machines. CIS benchmarks are configuration baselines and best practices for securely configuring a system. They are developed by the CIS and provide guidelines to enhance an organization's ability to prevent, detect, and respond to cyber threats.
- After Action Report (AAR) from the annual Disaster Recovery (DR) exercise was published to the stakeholders including the Risk, Safety, and Resilience team.

FY25 Q2 (November-December) Planned Activities:

- Initiate security consensus baselines based on the Center for Internet Security's (CIS) or equivalent benchmarks for at least one additional technology i.e., a server or network component.
- Continue work to update the Continuity of Operations (COOP) plans and create a new disaster recovery (DR) plan template that can be used across various applications and systems that are hosted on-premises within the George Mason primary data center.

Portfolio and Project Management

Enhancements to the Portfolio and Project Management processes to align with the investment lifecycle and towards better program/project artifact management.

FY25 September-October Accomplishments:

- The Enterprise and the Provost Administration Domain Councils have been scheduled to launch in November. The Domain Councils govern phase transitions and establish the portfolio structure aligned with client area domains. Each council is accountable for project activation approval, prioritization, and progress monitoring for their area and jurisdiction. The Domain Councils fall under a new Executive Administration Committee (EAC) created by the Senior Vice President to provide senior leadership insight into Facilities, Space, and IT project requests.
- Work is underway to establish the support structure for the Executive Administration Committee.

- Additional data fields have been configured in TeamDynamix and Power Business Intelligence (BI) dashboard such as Lifecycle Documents have been updated to report Domain Council status.

FY25 Q2 (November-December) Planned Activities:

- Work towards operationalizing Enterprise and the Provost Administration Domain Councils by FY25 Q3.
- Prepare to launch the Schools & Colleges Domain Council (SCDC) by FY25 Q3.
- Align processes of Facilities, Space, and IT project requests to support Executive Administration Committee (EAC)
- Roll out TeamDynamix automation to support DC1 and DC2 of the Domain Council process to streamline intake and review of requests

Information Security Program Management

Program enhancements for maturing the information security program at George Mason University, including protecting the confidentiality, integrity, and availability of data and systems while balancing access and productivity for the George Mason community.

FY25 September-October Accomplishments:

- Project #854: Enforcing Mandatory Trainings Compliance Through NetID Password Reset Page – This project has been closed out. Enforcement through the automated process is now operational.
- Project #861: Microsoft 365 (M365) Security, Optimization, Assessment, and Remediation (SOAR) – The team continued to work through the planned tasks list to bolster the control enhancements in the M365 environment, completing 18 remediation tasks out of 44, with 5 items currently in progress. Note that from the previous update, the total tasks decreased from 46 to 44. One item was an administrative correction from the deferred tasks list, and another was moved to Phase 4, which are items needing to be a large project on their own.
- Project #758: Migrate MESA M: drive data to Microsoft 365 services – As part of the migration the project team implemented data labels and tags in Teams SharePoint libraries for inventorying Protected categories of data and monitoring. The data from M: Drive was successfully migrated to newer secure repositories.
- The ITS Support Center services were moved to Anthology (vendor) who will now provide 24/7 support to the George Mason community. System accesses, data, and support processes were reviewed for security context and workflows were designed to manage potential risks associated with outsourcing.
- Cybersecurity Awareness Month activities: Multiple activities were organized, and articles were published to raise awareness around cybersecurity-related topics. Additionally, an "Ask Me Anything" Reddit thread was hosted by the IT Security Office to answer questions from the George Mason community.
- George Mason is a founding member and a member of the Virginia Alliance for Secure Computing and Networking (VASCAN) steering committee. The VASCAN annual conference was hosted by William & Mary this year and George Mason conducted sessions on 'Securing the Future: Navigating Microsoft Purview for Information Protection' and on 'Linux Forensics'.

FY25 Q2 (November-December) Planned Activities:

- Finalize the scope and the statement of work for the penetration test. This is to help George Mason align with industry best practices in this area, augment existing continuous monitoring as well as risk reduction efforts, and meet specific regulatory requirements.

Risk Assessment and Remediation

Program enhancements to mature the risk assessment and remediation processes at George Mason, including a Governance, Risk, and Compliance (GRC) program.

FY25 September-October Accomplishments:

- ITS has begun conducting risk assessments using the workflows now available in the Archer Integrated Risk Management (IRM) tool.
- The cybersecurity review by the Office of State Inspector General has concluded. George Mason was able to close out 80% of the findings and has action plans to address the rest by FY26 Q1.
- George Mason commissioned and completed a Gramm–Leach–Bliley Act (GLBA) and Federal Tax Information (FTI) assessment. Periodic assessments for compliance and associated reporting to the Board are required under GLBA.

FY25 Q2 (November-December) Planned Activities:

- Continue to configure and operationalize the issues, action plans, and exceptions management functionality in the Archer IRM application.
- Publish and socialize the new Risk Assessment procedure.
- MP01 remediation activities for the finding issued by the Virginia Auditor of Accounts (APA), continue to be prioritized with help from contract personnel in addition to ITS staff supporting the remediation tasks. These activities include conducting system risk assessments, creating System Security Plans (SSPs), and documenting Recovery Point Objectives (RPOs) for systems that meet the categorization criteria.

Change and Configuration Management

Establish a Quality Management Program to improve the delivery of IT services at George Mason, with a first area of focus on asset management and change/configuration management across the service portfolio.

FY25 September-October Accomplishments:

- Project #617: Implement TeamDynamix Asset and Change Management (Phase 2) – The project was closed out in March 2024. As part of maturing the operational process, the operations team is finishing moving IT asset listings into TeamDynamix and by December 2024 plans to have the process fully operationalized.
- Project #864: DevOps practice implementation and technology acquisition & operationalization - This project remains in the approval pipeline pending funding and resource prioritization decisions.
- The effort to update the Service Catalog by incorporating TeamDynamix is underway and should be complete by December 2024. The Service Catalog will then be able to search ITS.gmu.edu across TeamDynamix and WordPress catalogs providing better results and user experience.

FY25 Q2 Planned Activities:

- Continue work to improve the search options within the new TeamDynamix Service Catalog for a better user experience and functionality.

Identity Management and Access Control

Continuously improve and mature the processes that support identity and access management (IAM) at George Mason.

FY25 September-October Accomplishments:

- Project #867: Selection and implementation of an Identity Access Governance tool – No change in status. The project is on hold for funding and resource prioritization approvals.
- Project #866: Establish an IAM program as recommended by the Identity Access Management current state review and maturity consulting engagements. The proposed scope for this project includes staffing for support personnel, engaging functional partners, and establishing governance. This project is currently also on hold pending funding and prioritization decisions.

  The purpose of both these projects is to establish and mature IAM capability at George Mason.

FY25 Q2 Planned Activities:

- There are no specific activities planned for this program area for the FY25 Q2. Both projects associated with this program area are currently on hold for funding and resource prioritization approvals.

All ITS-managed/administered information technology projects (including those related to these focus areas) are available for review online at https://its.gmu.edu/working-with-its/ppmo/projects-dashboard/. Questions regarding projects in the portfolio can be addressed to Charmaine Madison (cmadiso@gmu.edu).