GEORGE MASON UNIVERSITY
BOARD OF VISITORS

Audit Committee
February 11, 2016
Merten Hall, Fairfax Campus

A G E N D A

I. Call to Order

II. Closed Session
A. Personnel Matters (Code of VA: 2.2-3711.A.1)

III. Approval of Audit Committee Minutes
A. Approval of Committee Minutes for December 8, 2015 (**ACTION ITEM**)
1. Minutes for December 8, 2015…….…….… **C-3**

IV. New Business
A. Auditor of Public Accounts Discussion…….. **C-7**
B. Approval of Internal Audit Department Plan (**ACTION ITEM**)
1. Proposed Internal Audit Department Plan……. **C-9**

V. Reports
A. Report of Internal Audit and Management Services
1. Report to the Audit Committee to the Board of Visitors…… **C-11**

VI. Adjournment

(This page was left blank intentionally.)

AUDIT COMMITTEE
OF THE BOARD OF VISITORS

December 8, 2015
Merten Hall
2:45 p.m. – 3:45 p.m.

MINUTES

PRESENT: Rector Davis; Chairman Sheikh; Visitors Corley and Gruner; Chief of Staff Neville; Senior Vice President Davis; Vice President Harber; University Counsel Moncure; Director Dittmeier; Interim Chief Ethics Officer Woodley; and Secretary pro tem Thompson

ABSENT: Vice Chair Pence; Visitors Peterson and Mendelsohn

I. Chairman Sheikh called the meeting to order at 2:45 p.m.

II. Approval of Minutes

Chairman Sheikh called for a motion to approve the minutes of the September 24, 2015 Audit Committee meeting. The motion was **MOVED** by Rector Davis and **SECONDED** by Visitor Corley. **MOTION CARRIED UNANIMOUSLY BY VOICE VOTE.**

III. New Business – Approval of Internal Audit Department Charter

At Chairman Sheikh's request, Rector Davis **MOVED** and Visitor Corley **SECONDED** a motion to approve the Internal Audit Department Charter.

Mr. Dittmeier reviewed proposed revisions to the Charter which better align the charter with current professional standards, add 'achievement of the university's strategic objectives" as a key objective of Internal Audit's risk-based assurance evaluations, removes the accountability for Internal Audit to provide oversight of other control and monitoring functions as this is a management responsibility, and makes clear the specific responsibility for Internal Audit to conduct investigations of matters referred by the Office of State Inspector General related to State Fraud, Waste, and Abuse Hotline case investigations. Mr. Dittmeier reported that the university president and management are fully supportive of the revised charter and committed to providing Internal Audit the necessary independence, stature, and access to university personnel and resources to accomplish its responsibilities to the Audit Committee. In discussion with the Committee, Mr. Dittmeier stated that appropriate management were fully aware of their responsibility to oversee control and monitoring functions and that this was not an Internal Audit responsibility.

MOTION CARRIED UNANIMOUSLY BY VOICE VOTE.

IV. Reports

Mr. Dittmeier reviewed with the Committee the Report of Internal Audit and Management Services. He stated that three audit reports had been issued since the prior Committee meeting; the Committee discussed business controls related to the Office of the Provost's information technology environment. Management continues to make progress to remediate 23 outstanding audit issues. He also reviewed the status of the internal audit plan; the progress of investigations of allegations of fraud, waste, and abuse; and the current internal audit staffing level. Since the prior Committee meeting, the Senior IT Auditor has resigned and the IT Audit Manager announced her retirement effective December 31, 2015. Recruiting efforts continue; a Senior Auditor candidate has accepted an offer to start in January 2016 and additional candidates are being interviewed. Internal Audit is working with Mason's Purchasing Department to establish one or more supplemental internal audit co-sourcing arrangements; a request for proposals is expected to be initiated in January 2016.

Ms. Woodley reviewed with the Committee the annual report of contractual conflict of interest waivers. In discussion with the Committee, Ms. Woodley stated that there was one waiver request which was not granted.

V. Closed Session

Rector Davis **MOVED** and Visitor Corley **SECONDED** that the Committee go into Closed Session under the provisions of Section 2.2-3711.A.1 to discuss Personnel Matters. There was no discussion. **MOTION CARRIED UNANIMOUSLY BY VOICE VOTE**.

Visitor Corley **MOVED** and Rector Davis **SECONDED** that the Committee go back into public session and it was further moved that by ROLL CALL VOTE 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 Session, and that only such business matters that were identified in the motion to go into Closed Session were heard, discussed, or considered in the Closed Session.

Roll call was taken with all present members responding in the affirmative.

VI. Adjournment

Chairman Sheikh declared the meeting adjourned at 3:45 p.m.

Respectfully submitted,

Karen Thompson

Karen Thompson
Secretary pro tem

(This page was left blank intentionally.)

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

PURPOSE OF ITEM: Brief the Audit Committee regarding the upcoming financial statement audit for the year ended June 30, 2015.

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.

Representing the Auditor of Public Accouts are:

- Zach Borgerding - Project Manager
- David Rasnic - Auditor In-Charge

ACTION: Receive briefing and discuss.

(This page was left blank intentionally.)

ITEM NUMBER: III.B. Approval of Proposed Internal Audit Department Plan

PURPOSE OF ITEM: This item requests Audit Committee approval of the proposed Internal Audit Department 3+6 Audit Plan.

NARRATIVE: Internal Audit uses a 'top-down' and a 'bottom-up' approach to develop its independent risk assessment used for determining priorities for providing assurance services.

- The 'top-down' approach seeks to identify macro-level areas of current and/or potentially emerging interest to stakeholders.
- The 'bottom-up' approach is used to develop a risk-based prioritized frequency of audit coverage across the university through the evaluation of Audit Risk Factors applied to Auditable Units.
    - The potential impact and likelihood of risks related to the following areas were considered: strategic; financial and financial reporting; regulatory compliance; operations; and hazards.

The proposed plan was reviewed with key members of university management, including the President, Provost, and Senior Vice President – Administration and Finance.

- Their input and feedback was considered and incorporated, where appropriate.

The proposed 3+6 Audit Plan enables Internal Audit to be dynamic and flexible in addressing the changing nature of risks facing the university. It describes:

- Three months of audit work which is firmly planned to be conducted.
- The subsequent six months which is indicative of audit work likely to be conducted.

The proposed 3+6 Audit Plan will be updated each quarter for Audit Committee Chairman approval and Committee ratification.

ACTION: Approval of proposed Internal Audit Department Plan.

(This page was left blank intentionally.)

Internal Audit
and Management Services

Report to the Audit Committee of the Board of Visitors

February 11, 2016

(This page was left blank intentionally.)

EXECUTIVE SUMMARY

- Three audit reports issued since last meeting; with generally satisfactory or satisfactory results:
  - Laboratory Safety
  - Office of Admissions: Decentralized IT Operations and IT Asset Management
  - Analysis of Mason's Sexual Harassment and Misconduct Policy and Related Procedural Documents

- Remediation of 21 audit issues is in progress as of January 25, 2016:
  - More than half of the issues relate to information technology.
  - Nearly all issues have current target remediation dates through mid-2016.

- Audit Plan status:
  - Original plan consisted of 13 projects
    - Six are complete.
    - One audit is in reporting phase.
    - One audit remains in fieldwork and is likely to be completed in February 2016.
    - Five were postponed.

- Status of fraud, waste, and abuse investigations:
  - Three completed since last meeting.
  - Four are in progress.
  - All are isolated in nature and considered as having negligible impact to the University.

- The current staffing level is six audit professionals.
  - Changes since the last meeting include:
    - IT Audit Manager Carolyn Westbrook retired in December 2015.
    - Senior IT Auditor Michelle Workman left Mason in December 2015.
    - Senior Auditor Adam Herr joined January 4, 2016.
    - Senior IT Auditor Janatry Sanders joined January 25, 2016
  - Recruiting efforts continue. Search Committees are working to identify additional Senior IT Auditor candidates.
  - A Request for Proposals to establish one or more supplemental internal audit co-sourcing arrangements was issued in January. The timeline expects arrangements to be in place by April 2016.

- Additional plans:

• Strengthen internal audit risk assessment processes and documentation.	Underway.
• Build new process for tracking, reporting, and following-up the status of management's remediation of audit issues.	Underway.
• Self-assess internal audit performance vs. professional standards.	Completed.

(This page was left blank intentionally.)

TABLE OF CONTENTS

Topic

SUMMARY OF INTERNAL AUDIT REPORTS

- Laboratory Safety
- Office of Admissions: Decentralized IT Operations and IT Asset Management
- Analysis of Mason's Sexual Harassment and Misconduct Policy and Related Procedural Documents

Internal Audit
and Management Services

INTERNAL AUDIT REPORT

Report Title:	Laboratory Safety	**Report Date:**	December 17, 2015
Responsible Manager:	Julie Zobel Assistant Vice President, Safety, Emergency and Risk Management		

EXECUTIVE SUMMARY:

Background:

Maintaining a safe laboratory workplace is a collaborative effort between Principal Investigators (PI), academic departments, employees, and the Laboratory Safety Office of the Environmental Health and Safety Office (EHS). The Laboratory Safety Office administers the university's biological, chemical, laser, radiation, and x-ray safety programs and develops and maintains laboratory safety policies, provides training and guidance to research personnel to assist in compliance with regulations and industry standards, conducts laboratory inspections, assists with the design and renovation of laboratories, assists in the development of emergency procedures for laboratories, and manages laboratory waste streams.

Section 29 of the U.S. Code of Federal Regulations requires the university to provide a chemical hygiene plan that (i) establishes minimum safety standards for working with chemicals in laboratories and (ii) outlines procedures that minimize the risk of chemical exposure to laboratory personnel and the risk of chemical releases into the environment. The university's Laboratory Safety Manual serves as the university's chemical hygiene plan and provides general guidance for the university's 385 laboratories (located in various academic buildings) on laboratory safety practices, the safe handling of hazardous substances, and procedures for proper acquisition, use, storage, transfer, and disposal of chemicals.

This audit evaluated the university's oversight regarding laboratory safety in order to provide assurance that labs are operated safely and in compliance with the Laboratory Safety Manual.

Audit Conclusion:

The EHS lab safety inspection program infrastructure, consisting of the EHS Assistant system and appropriate process and inspection documentation, is well-designed to provide oversight and assurance regarding safe operations of university labs and compliance with the university's chemical hygiene plan (Laboratory Safety Manual). However, improvements are needed in (i) the deficiencies follow-up inspection process to ensure corrective action is implemented timely or is escalated to university management; (ii) documentation of inspection results in the EHS Assistant system; and, (iii) establishment of monitoring and review processes and controls as part of conducting the investigation and documenting the response to lab related accidents and incidents to ensure investigations and follow-up are performed, incident reports are prepared, and corrective action is implemented in a timely manner.

Internal Audit
and Management Services

INTERNAL AUDIT REPORT

Report Title:	Office of Admissions: Decentralized IT Operations and IT Asset Management	**Report Date:**	December 17, 2015
Responsible Manager:	Amy Takayama-Perez Dean of Admissions, Enrollment Management Marilyn Smith Vice President, Chief Information Officer		

EXECUTIVE SUMMARY:

Background:

The Office of Admissions recruits, admits, and enrolls students to fulfill university enrollment goals. Among other things, the Office handles over 350,000 sensitive documents to process over 50,000 applications annually; awards and notifies applicants of more than $2 million of academic scholarships; and enrolls more than 14,000 new students each academic year.

The six-person Admissions Technology Team manages a critical IT environment to support Admissions' processes outside the scope of Mason's centrally managed Information Technology Services (ITS). Although ITS hosts Admissions' IT assets so as to provide a secure and appropriately controlled physical environment, the Admissions Technology Team administers the Admissions module in Banner Student, the central administrative system, as well as several systems that feed critical data to Banner, including Hobson's customer relationship management system for student applications, secure transcript providers, and secure data-loading tools for student test scores.

This audit evaluated the Office of Admissions' IT-related policies and procedures designed to provide sustainable, risk-appropriate levels of confidentiality, integrity, and availability of data, information, and systems.

Audit Conclusion:

IT controls and associated procedures provide reasonable assurance of the overall security, confidentiality, availability, and integrity of the systems and applications controlled by the Admissions Technical Team. We confirmed that actions were completed to address issues reported in a 2012 IT security assessment performed by IBM.

Internal Audit
and Management Services

INTERNAL AUDIT REPORT

Report Title:	Analysis of Mason's Sexual Harassment and Misconduct Policy and Related Procedures	**Report Date:**	December 18, 2015
Responsible Manager:	Julian Williams Vice President, Compliance, Diversity, and Ethics		

EXECUTIVE SUMMARY:

Background:

Mason's Sexual Harassment and Misconduct Policy implements provisions of Title IX of the Education Amendments of 1972. The policy and the related Code of Student Conduct and Equal Opportunity/Affirmative Action Grievance Procedure require the university to provide an academic and work environment free from sexual harassment, encourages reports of sexual misconduct, and describes the university's responsibilities related to such reports.

In September 2015, the U.S. Department of Education Office for Civil Rights concluded that the University of Virginia's Title IX policies and procedures that address sexual misconduct complaints did not provide for prompt and equitable resolution of student and employee complaints. This resulted in the University of Virginia substantially revising its procedures for investigating and resolving reports of sexual harassment and violence against students, employees, and third parties, and entering into a Resolution Agreement with the Office for Civil Rights.

This audit compared Mason's policy and procedures with the University of Virginia's policy and procedures for investigating and resolving reports of prohibited conduct by students and employees. We did not evaluate any of Mason's actual practices in operation.

Audit Conclusion:

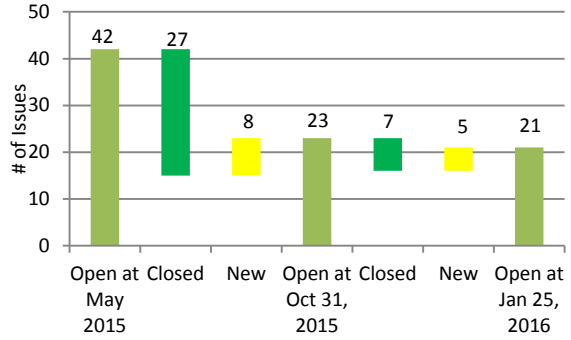
In our view, management with expertise in this field should conduct a thorough analysis and update of Mason's full set of sexual harassment and misconduct policies and procedures in light of changing expectations, the Office for Civil Rights review of the University of Virginia's policies and procedures, and recent changes in the Code of Virginia. We believe Mason's policies, procedures, and practices would benefit from consolidation and uniformity to strengthen consistency and coordination in the handling of complaints against students, employees, and third parties. Additional precision and detail in policy and procedural documentation would reduce potential ambiguity in expectations and requirements. Management should also consider investigating all complaints with impartial, dedicated staff investigators who complete ongoing specific training related to handling sexual misconduct investigations.

Management has a review committee in place charged with assessing and revising Mason's sexual harassment and misconduct policies, procedures, and practices; revisions are expected to be put forward for approval by May 2016.

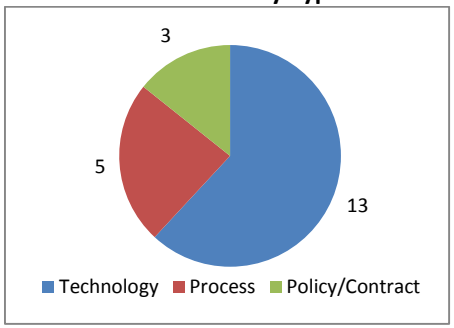
STATUS OF AUDIT ISSUES AS OF JANUARY 25, 2016

There were 21 open audit issues as of January 25, 2016. Remediation of seven audit issues was completed by management since October 2015.

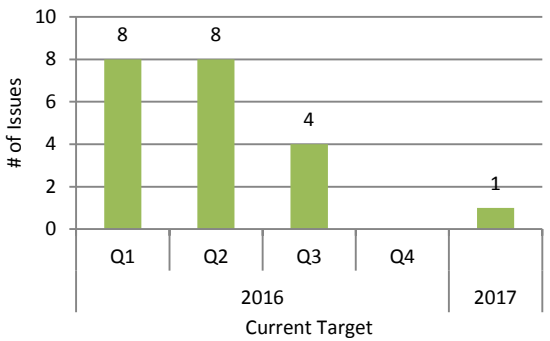
Audit Issue Inventory Movement



Audit Issues by Type



Audit Issues by Current Target



Audit Report	Report Date	May 2015	Closed	New	Oct 2015	Closed	New	Jan 2016
Analysis of Mason Sexual Harassment and Misconduct Policy and Procedures	12/18/15				0	-	1	1
Laboratory Safety	12/17/15				0	-	4	4
Decentralized IT Management and Security: Office of the Provost	10/23/15			5	5	-	-	5
Human Resources and Payroll – Employee Benefits	10/23/15			1	1	(1)	-	0
MESA Technical Point of Contact and Share Administration Account Management	9/10/15			2	2	-	-	2
Office of the University Registrar	3/5/15	3	(3)	-	0	-	-	0
Arlington Campus Parking Services	11/11/14	3	(3)	-	0	-	-	0
Aquatic and Fitness Center	8/21/14	1	(1)	-	0	-	-	0
Human and Animal Subjects Research	7/8/14	1		-	1	-	-	1
Facilities Service Contracts	4/22/14	2	(2)	-	0	-	-	0
Summer Camps and Enrichment Programs	4/22/14	4	(1)	-	3	(3)	-	0
Decentralized Servers: College of Humanities and Social Sciences	11/14/13	3	(2)	-	1	-	-	1
Intercollegiate Athletics: Student Athlete Financial Aid	11/5/13	4	(3)	-	1	(1)	-	0
Biomedical Research Laboratory: Physical Security	9/10/13	2	-	-	2	(1)	-	1
Information Security Management: Boundary Protection	9/9/13	3	(1)	-	2	(1)	-	1
Enterprise Project Management Framework and System	3/28/13	2	-	-	2	-	-	2
Housing and Residence Life	6/11/12	4	(4)	-	0	-	-	0
Applications and Security Audit: Housing and Residence Life Systems	12/21/11	5	(5)	-	0	-	-	0
Decentralized Servers: College of Science	8/18/11	3	(1)	-	2	-	-	2
SEC 501-01 IT Security Audits Prior to Level II Status (2008-2010)	8/30/10	2	(1)	-	1	-	-	1
		42	(27)	8	23	(7)	5	21

STATUS OF AUDIT PLAN AS OF JANUARY 25, 2016

The original 2014-15 Audit Plan consisted of 12 audits (adjusted to 13 audits with the separation of the IT security audits addressing Financial Aid and Admissions). Through January 25, 2016, six audits were completed with satisfactory results, fieldwork for one audit is completed and is now in the reporting phase, and fieldwork for one audit remains in progress and is expected to be completed in February 2016. As reviewed at the last meeting, five audits were postponed and will be considered in future audit planning. Follow-up audits to validate management's remediation of audit issues from prior audits were completed in six areas.

Audit	Type	Status	Remarks
Academic Areas			
Departmental IT Security Plan Implementation (Financial Aid)*	IT	Completed	Issued May 18, 2015. Satisfactory results.
Research: VISTA Grant	Operational	Completed	Issued August 28, 2015. Satisfactory results.
Departmental IT Security Plan Implementation (Admissions)*	IT	In Progress	*Issued November 6, 2015. Satisfactory results.*
Hylton Performing Arts Center	Operational	In Progress	Focus on box office and rental revenues; *completion expected in February 2016.*
Laboratory Safety	Operational	In Progress	*Issued December 17, 2015. Generally satisfactory results.*
Biomedical Research Laboratory: Physical Security	Follow-Up	Completed	Issued April 29, 2015. Five issues closed; one remains open with expected completion in March 2016.
Housing and Residence Life	Follow-Up	Completed	Issued June 25, 2015. Four issues closed.
Applications and Security Audit: Housing and Residence Life Systems	Follow-Up	Completed	Issued June 10, 2015. Management actions were delayed and have been re-initiated; follow-up planned for Spring 2016.
Tenured Faculty Teaching Loads	Operational	Postponed	Postponed.
Administrative Areas			
Enterprise Servers and Messaging: Operating Systems Security*	IT	In Progress	*Fieldwork completed, reporting phase. Satisfactory results.*
Human Resources: Employee Benefits*	Operational	Completed	Issued October 23, 2015. Satisfactory results.
MESA TPOC and Share Administrator Account Management	IT	Completed	Issued September 10, 2015. Satisfactory results.

Audit	Type	Status	Remarks
Summer Camps and Enrichment Programs	Follow-Up	Completed	Issued August 26, 2015.
Human and Animal Subjects Research	Follow-Up	In Progress	Issued September 8, 2015. One issue partially closed with remainder expected to be completed by March 2016.
Accounts Payable*	Operational	Postponed	Postponed.
Capital Projects	Operational	Postponed	Postponed.
Banner Student Access Management (BSO Layer)	IT	Postponed	Postponed.
Oracle Database Access Security Management (excludes) INB, SSB	IT	Postponed	Postponed.
Athletics			
Intercollegiate Athletics: Student Athlete Financial Aid	Follow-Up	Completed	Issued June 12, 2015.

* = Carry over from 2013-14 audit plan.

Note: Two additional audit projects have been completed:

- An Analysis of Mason's Sexual Harassment and Misconduct Policy and Related Procedural Documents was completed subsequent to the U.S. Department of Education Office for Civil Rights concluding that the University of Virginia's Title IX policies and procedures that address sexual misconduct complaints did not provide for prompt and equitable resolution of student and employee complaints. A summary of this audit is included in this Report to the Audit Committee.

- The Office of the Provost: Decentralized IT Management and Security audit was carried over from the 2012-13 audit plan and was completed in October 2015. A summary of this audit was reported to the Committee in December 2015.

STATUS OF INVESTIGATIONS AS OF JANUARY 25, 2016

Since the Committee's last meeting, three investigations were completed. Four investigations are in progress as of January 25, 2016. Completed investigations are isolated in nature and considered as having negligible impact to the University. Information as of January 25, 2016 indicates in-progress investigations also appear to be isolated in nature with negligible impact to the University.

Nature of Allegation	Type	Status	Remarks
Questionable Accounting Practices Related to Student Course Fees	Fraud	Completed	
Possible Timesheet Abuse and Irregularities	Fraud	Completed	Timekeeping practices needed to be more consistent.
Potential Falsification of Wage Employee Timesheets	Fraud	Completed	Supervision of wage employee timekeeping practices in one department needed strengthening.
Waste of State Funds	Waste	In Progress	
Employee on Grant Not Doing Work	Fraud	In Progress	
Falsification of Timesheet on Jobs/Inappropriate Destruction of Cell Phone	Fraud	In Progress	
Conference Expense Reimbursement	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

- Full accomplishment of the original 2014-15 Audit Plan required a staffing level totaling eight audit professionals.
- The actual staffing level has averaged 5.8 audit professionals.
- At December 31, 2015, there were four unfilled positions; two were filled in January.

	Plan	a/o Oct 2014	a/o Dec 2015	Plan vs Dec 2015
Director	1	1	1	-
Assistant Director	1	1	1	-
IT Audit	2	2	0	(2)
Operational Audit	3	2	1	(2)
Fraud Audit	1	1	1	-
Total Audit Professionals	**8**	**7**	**4**	**(4)**

- As discussed at the December meeting:
  - IT Audit Manager Carolyn Westbrook retired effective December 2015.
  - Senior IT Auditor Michelle Workman left Mason effective December 2015.

- Additions:
  - Adam Herr joined January 4, 2016. He has nine years of experience with CGI Federal and Kearney and Company conducting financial, compliance, and information security audits primarily at federal government agencies. He has a bachelor's degree in accounting from Susquehanna University and is a Certified Public Accountant, Certified Information Systems Auditor, and Certified Fraud Examiner.
  - Janatry Sanders joined January 25, 2016. He has ten years of risk advisory, information technology, and information security consulting experience with several firms, most recently PricewaterhouseCoopers and KPMG. He has a bachelor's degree in business administration and computer information systems from James Madison University and is a Certified Information Systems Security Professional.

- Recruiting efforts continue. Search Committees are working to identify additional Senior IT Auditor candidates.

- A Request for Proposals to establish one or more supplemental internal audit co-sourcing arrangements was issued in January. The arrangements will provide supplemental staffing capability as well as access to specific knowledge, expertise, and industry practices. The timeline expects arrangements to be in place by April 2016.

APPENDIX: AUDIT ISSUE DETAILS AS OF JANUARY 20, 2016

#	Audit Report	Audit Issue	Status of Management Action	Original Target	Current Target
1	**Report Name:** SEC501-01 IT Security Audits Prior to Level II Status (2008-2010) **Report Date:** 8/30/12 **Management:** John Kettlewell, Interim Executive Director, Information Technology Services	**Current Documentation for Back-Up and Restore, Data Replication:** Although Information Technology Services has some formal documented policies and procedures regarding backups performed in the Data Center, documentation is inconsistent, unclear, and incomplete related to critical systems and sub-systems identified in the IT Disaster Recovery documents. There should be adequate, centralized back-up information on each system and sub-system in the Disaster Recovery documents, including back-up schedules, media, location, and responsible person(s) for each system and sub-system.	Information Technology Services will use the agreed-upon system prioritizations developed by Environmental Health and Safety (EHS) to align the ITS Disaster Recovery / Continuity of Operations Plan with those priorities. Based on the expected timing of EHS' work, management estimates the Disaster Recovery site plans will be aligned and documented by February 2016, depending on other project workloads and university priorities.	3/31/11	2/29/16
2	**Report Name:** MoU and Agreement with American Type Culture Collection (ATCC) **Report Date:** 12/17/15 **Management:** Julie Zobel, Assistant Vice President, Safety, Emergency and Enterprise Risk Management	**Safety Management in Labs Leased by ATCC:** Mason leases 25 laboratories on the Science and Technology campus to ATCC for its exclusive use in promotion of research, education, training, and service in the biosciences essential to biotechnological knowledge acquisition and application. The current agreement with ATCC, dated 1995 and amended in 1998, does not include safety provisions that: • Require ATCC to comply with applicable Mason safety policies and/or laws and regulations. • Provide Mason safety personnel full and complete access to the university labs and facilities used by ATCC upon reasonable notice, to inspect and to enforce Mason safety policies and procedures regarding laboratory activities. • Give Mason full authority to require corrective action in the event of ATCC's non-compliance with the Mason's safety policies and procedures, and/or applicable laws and regulations affecting the university.	Environmental Health and Safety will meet with Legal, Facilities, and the Provost's Office to develop a workable solution under existing legal arrangement. An update regarding the university's plan to address safe operation and potential health and safety risks in ATCC leased labs will be provided.	2/29/16	2/29/16

#	Audit Report	Audit Issue	Status of Management Action	Original Target	Current Target
		As a result, Mason Lab Safety personnel do not inspect these labs for safe operation, potential health and safety risks, and compliance with policies. Although we have seen improvement in safety-related contract language in contracts executed with some other organizations, the ATCC arrangement should be strengthened to address the current situation and the contracting process for future arrangements could be tightened.			
3	**Report Name:** Biomedical Research Laboratory: Physical Security **Report Date:** 9/10/13 **Management:** Charles Bailey, Executive Director, National Center for Biodefense and Infectious Diseases	**Physical Access System:** Physical access to the Biomedical Research Laboratory (BRL) facility and the BSL-3 containment suite is administered and managed utilizing an electronic system designed for implementing various control measures. Our review determined that requests for access are appropriately authorized; however, there were numerous differences between access requested and access actually granted. Causes included: • Vendor defined and other developed profiles are not tailored to the BRL's needs. • Profiles are not clearly defined as to the access included. • Access request forms have been continuously developing with changing information requirements. • No review to ensure that access granted is what was requested.	User access forms have been developed and are being tailored to address the BRL's needs. This process, which ensures that access granted is actually requested, is in place for new requests for access. Existing access already granted is being re-assessed using the revised process and forms; this review is expected to be completed by March 2016, a two month delay due to personnel changes. BRL management will confirm at least annually the appropriateness of all individuals with access to the BRL facility and containment suite.	8/31/14	3/1/16
4	**Report Name:** Enterprise Project Management Framework and System **Report Date:** 3/28/13	**Project and Portfolio Management:** In 2007, the university established IT governance initiatives to help provide a more mature environment for the management of the university's IT asset portfolio and alignment of IT investments with university priorities. These initiatives included the Portfolio Evaluation Committee (PEC) who is responsible for prioritizing large and medium project	The IT Governance Group (ITGG) approved the proposed prioritization process. The PEC will follow the same process. ITS will coordinate communications between the PEC and the ITGG, and expects the process to be fully operational by March 2016.	6/30/13	3/31/16

#	Audit Report	Audit Issue	Status of Management Action	Original Target	Current Target
	Management: Robert Nakles, Executive Director, Information Technology Services	portfolio requests impacting the Banner suite and related administrative applications. Although the PEC reviews such project requests, they are not being prioritized by the PEC. As a result, IT resources may be prioritized and allocated inappropriately. Furthermore, the effort to integrate Banner governance and the procedures recommended in the university's Project Management Framework was never completed. Certain requests need to be assessed by both the Banner governance structure and the Project Management Framework; however, these structures are disconnected.			
5	**Report Name:** Decentralized Servers: College of Science **Report Date:** 08/18/11 **Management:** Peggy Agouris, Dean, College of Science	**IT System Hardening:** College of Science does not require system administrators to harden systems according to accepted standards such as the National Institute of Standards and Technology. The College should establish and enforce policy to require system administrators to configure systems, based on risk, to appropriate security baselines.	College of Science implemented a configuration assessment to address hardening of new systems. This process will be automated using the university's centralized governance, risk management, and compliance product. The gathering of system information, including baseline assessments, is underway. Existing systems will be assessed through this automated process by March 2016.	12/31/13	3/31/16
6	**Report Name:** Decentralized Servers: College of Science **Report Date:** 8/18/11 **Management:** Peggy Agouris, Dean, College of Science	**Logical Access Controls:** College of Science does not have documented policies for account management, password management, or remote access requirements. At the time of this audit (2011), the university was developing a new policy for all academic and operational departments on remote access.	College of Science implemented policy and procedures that delegates account, password, and remote access management duties to specific individuals within their respective areas of responsibility. This included conformance to College of Science-defined minimum authentication, authorization, access request, account review, and password parameter requirements and to the University's remote access requirements. College of Science implemented a configuration assessment workflow to address account management and password management for new servers. This workflow will be automated using the university's	12/31/13	3/31/16

#	Audit Report	Audit Issue	Status of Management Action	Original Target	Current Target
			centralized governance, risk management, and compliance product. The gathering of system information, including baseline assessments, is underway. Existing servers will be assessed through this automated workflow by March 2016.		
7	**Report Name:** Human and Animal Subjects Research Compliance **Report Date:** 7/08/14 **Management:** Aurali Dade Assistant Vice President for Research Compliance, Office of Research Integrity and Assurance	**ORIA Staffing Levels:** Office of Research Integrity and Assurance (ORIA) staffing levels present non-compliance risks since the department does not have staffing redundancies to help ensure that compliance activities can be performed when the individual with primary responsibility is absent. (The need for additional support is especially crucial in the areas of COI, research misconduct, and RCR). Limited staffing resources has precluded ORIA management from: 1. Providing in-person Responsible Conduct of Research (RCR) training for specified NIH projects in accordance with Notice NOT-OD-10-19. 2. Updating Institutional Review Board (IRB) policies and procedures which were last revised in May 2006 and do not reflect current terminology, procedures, and requirements. 3. Implementing post approval monitoring (i.e., examination of research facilities and study documents to assure that investigators are in compliance with university and federal regulations.) IA review determined IRB consent forms were not always retained or current.	Mandated in-person RCR training for specified NIH projects was held in 2014. The revised IRB Policy was approved in October 2014. All procedures requiring update are in place; a process for ongoing updates has been established. A new employee has filled the vacated position, has been trained, and is now performing job functions independently. Post approval monitoring procedures are expected to be reviewed at the February 2016 IRB meeting; implementation remains on target for March 2016.	1/31/15	3/31/16
8	**Report Name:** MESA Technical Point of Contact and Share Administration Account Management **Report Date:** 9/10/15	**Employee Role Definitions:** MESA is the IT infrastructure that provides networked file services and storage, and desktop management and security. Credentials are provisioned based on an individual's Banner Human Resources (HR) record. Individuals are generally set to "inactive" when no longer actively employed; however, HR purposes require individuals within the	The ITS project build a replacement provisioning system is actively underway. Parallel operations with the legacy system are expected to occur in early March 2016 with the new system assuming current production services later in March 2016. This first phase of the project will implement existing functionality and provide the	3/31/16	3/31/16

#	Audit Report	Audit Issue	Status of Management Action	Original Target	Current Target
	Management: John Kettlewell, Interim Executive Director, Information Technology Services (ITS)	"GMU Retirees" class be set to "active" status. As a result, their MESA accounts are not deprovisioned, even though access to specific MESA shares may have been removed by the local share administrators. Such dormant but active accounts allow access to Mason's MESA network and to services not restricted by other access controls. Audit identified 104 retirees with an active MESA account and access to at least one MESA share. Since no retirees were identified within the six MESA shares that had completed annual access reviews, Audit believes that the newly instituted ITS annual audit process when fully deployed will limit the length of time retirees' MESA shares access remains active inappropriately.	capability to address "GMU Retiree" individuals in the second phase. The status of the plan for implementing second phase changes will be reported by March 31, 2016.		
9	**Report Name:** Office of the Provost: Decentralized IT Management and Security **Report Date:** 10/23/15 **Management:** Renate Guilford, Associate Provost, Academic Administration	**Design and Document Configuration and Change Management Controls:** The Provost IT Team has not yet developed and documented structured configuration management and change control (CM) policies and procedures to manage and control configurations and changes to its IT environment. Because there is significant web application development, CM procedures are critical to ensure that local development and changes to deployed software are made according to management's intentions, authorized, and in compliance with both security and software development standards.	The Provost IT Team is working to: • Develop and employ a configuration and change management system and templates. • Monitor ongoing compliance with design document requirements and the change management system. • Maintain relevant documents on the MESA shared drive and provide access to relevant authorized users.	4/30/16	4/30/16
10	**Report Name:** Office of the Provost: Decentralized IT Management and Security **Report Date:** 10/23/15 **Management:** Renate Guilford, Associate	**Formalize Periodic IT Security Risk Management Activities:** The Provost IT Team has not yet developed a standard set of IT security risk assessment activities, consisting of evaluating assets to prioritize their significance according to a structured business impact analysis process; performing a documented risk and vulnerability analysis on the assets to identify issues needing remediation; and executing the remediation. Risk assessments should be	The Provost IT Team is working to: • Develop and document standard risk assessment plans and procedures for platforms as well as for individual applications. • Perform the standard risk assessment activities and document results, repeating every three years or whenever a major change in systems or applications takes place.	4/30/16	4/30/16

#	Audit Report	Audit Issue	Status of Management Action	Original Target	Current Target
	Provost, Academic Administration	performed every three years or earlier, whenever material changes are made to systems.	• Maintain relevant documents on the MESA shared drive and provide access to the relevant authorized users.		
11	**Report Name:** Office of the Provost: Decentralized IT Management and Security **Report Date:** 10/23/15 **Management:** Renate Guilford, Associate Provost, Academic Administration	**Design and Document Development Methodologies and Procedures:** The Provost IT Team has only recently begun to develop a framework of activities, documentation, and project management for system or software acquisition or development on behalf of Provost area units requesting their services. Project development life cycle or project management techniques have been executed *ad hoc* using informally communicated expectations of standards. While there are numerous development methodologies and none are one size fits all, good development and project management standards is the strongest control to help avoid primary causes of project failures.	The Provost IT Team is working to: • Develop project templates and documents based on industry best practices. • Document the development methodology used for each application and project, and the related documentation. • Ensure compliance with methodology requirements through the use of templates provided during the development phase. • Maintain relevant documents on the MESA shared drive and provide access to the relevant authorized users.	4/30/16	4/30/16
12	**Report Name:** Office of the Provost: Decentralized IT Management and Security **Report Date:** 10/23/15 **Management:** Renate Guilford, Associate Provost, Academic Administration	**Document Standard Operating Procedures:** The Provost IT Team is just beginning to develop documented standard operating procedures and documented workflow procedures that will enable its entire staff to establish consistent practices. Procedures and templates are needed to: • Ensure compliance with University Policy 1312 regarding logical access. • Establish configuration management and change controls over systems and applications. • Document service level agreements with units for which they provide web or application hosting services. • Manage and prioritize development projects. • Document web and application development services to be provided for all phases, including templates, such as formal agreement with client as to scope of work, initiation, specs, design, coding, testing, various points of review by supervisor and approvals, separation of duties for migration to production, client testing and approval, client	The Provost IT Team will continue to: • Develop standard operating procedures for Provost IT team. • Develop service level agreement templates to be used to document formal agreement with system end-users for each application and system. • Document compliance with standard operating procedures for each individual application. • Maintain relevant documents on the MESA shared drive and provide access to the relevant authorized users.	4/30/16	4/30/16

#	Audit Report	Audit Issue	Status of Management Action	Original Target	Current Target
		training and documentation, and post-development maintenance.			
13	**Report Name:** Laboratory Safety **Report Date:** 12/17/15 **Management:** Julie Zobel, Assistant Vice President, Safety, Emergency and Enterprise Risk Management	**Establish Comprehensive Processes for Accident and Incident Reporting Follow-Up:** Lab accidents and incidents are reported to the Laboratory Safety group; Lab Safety inspectors conduct and document incident investigations and assessments of safety controls following the accident (injury, illness, property damage), exposure (needle stick, chemical or biological exposure), or a physical response to provide assistance (spill cleanup, assist third party responders, etc.). Although such accidents and incidents are investigated adequately, requirements are needed for the following: • Communication of corrective action to responsible party. • Timeline of follow-up to be performed. • Tracking and monitoring of outstanding corrective action. Additionally, Lab Safety supervisory personnel should complete independent reviews to ensure that safety controls were properly assessed, corrective actions were appropriately identified, investigation and follow-up information was documented completely, and corrective action(s) implemented timely.	Standard operating procedures and documentation requirements will be modified to provide for tracking and documentation of corrective actions and supervisory review. These changes will be coordinated with other EHS programs (Occupational Safety, Fire Safety, and Emergency Management) and the Office of Risk Management.	4/30/16	4/30/16
14	**Report Name:** Analysis of Mason's Sexual Harassment and Misconduct Policy and Related Procedures **Report Date:** 12/18/15 **Management:** Julian Williams, Vice	**Assess and Revise Mason's Sexual Harassment and Misconduct Policies and Procedures:** Management with expertise in this field should conduct a thorough analysis and update of Mason's full set of sexual harassment and misconduct policies and procedures in light of changing expectations, the Office for Civil Rights review of the University of Virginia's policies and procedures, and recent changes in the Code of Virginia. Mason's policies, procedures, and practices would	Management has a review committee in place charged with assessing and revising Mason's sexual harassment and misconduct policies, procedures, and practices; revisions are expected to be put forward for approval by May 2016.	5/31/16	5/31/16

#	Audit Report	Audit Issue	Status of Management Action	Original Target	Current Target
	President, Compliance, Diversity and Ethics	benefit from consolidation and uniformity to strengthen consistency and coordination in the handling of complaints against students, employees, and third parties. Additional precision and detail in policy and procedural documentation would reduce potential ambiguity in expectations and requirements. Management should also consider investigating all complaints with impartial, dedicated staff investigators who complete ongoing specific training related to handling sexual misconduct investigations.			
15	**Report Name:** Enterprise Project Management Framework and System **Report Date:** 3/28/13 **Management:** Robert Nakles, Executive Director, Information Technology Services	**Metrics Based Project Management:** A cost estimation and tracking mechanism is not in place to determine and track time and costs to complete IT projects. Such a mechanism can support improved comparative analysis, decision making about future projects, and project monitoring and control.	The Information Technology Services organizational restructuring and the creation of the IT Governance Group have resulted in a "restart" in the remediation for this issue. Current project management portfolio tools do not include a structure to capture the level of detail to cost labor resources. Management continues to work to create a resource reporting structure and provide related training by June 2016.	9/30/13	6/30/16
16	**Report Name:** MESA Technical Point of Contact and Share Administration Account Management **Report Date:** 9/10/15 **Management:** John Kettlewell, Interim Executive Director, Information Technology Services (ITS)	**MESA Desktop Security:** MESA is the IT infrastructure that provides networked file services and storage, and desktop management and security. Access to unattended MESA workstations is not limited by an enforced password-enabled screensaver. Unattended, logged-in workstations provide opportunities for unauthorized access all information displayed on the screen, stored on the computer's hard drive, and accessible from the computer of the signed-on user.	An ITS project is underway to implement a password-enabled screensaver after 15 minutes of inactivity to all desktop computers. The screensaver has been implemented successfully in the Technology Support Services area and is being implemented in phases across the university. All managed desktops are expected to be running a screensaver by June 30, 2016.	2/29/16	6/30/16
17	**Report Name:** Office of the Provost: Decentralized IT	**Develop and Document Continuity of Operations Plan (COOP) and Disaster Recovery (DR) Plan:** Because the Provost IT Team's environment is hosted on ITS VMWare equipment, they are	The Provost IT Team is working to: • Develop and document COOP contingency plans and procedures for the platform as well as for individual	7/31/16	7/31/16

#	Audit Report	Audit Issue	Status of Management Action	Original Target	Current Target
	Management and Security **Report Date:** 10/23/15 **Management:** Renate Guilford, Associate Provost, Academic Administration	afforded access to backups prepared by ITS' Server Support Group which image and store VMWare contents on separate media. However, the Provost IT Team has not yet completed a fully operational plan and procedures for accessing the backups and restoring service. Additionally, COOP/DR requirements have not been formalized and restorations have not been tested with the combined cooperation among their office, ITS, and the Provost IT users.	applications with detailed steps required to perform the necessary tasks, including manual procedures, to compensate for lack of immediate system restoration. These documents will be developed in cooperation with end-users. COOP documents will be made available to the users in the event the system is unavailable for extended period. • Develop detailed DR plan documents which specify the procedures and steps required to restore system functionality and access to authorized users; and test such plans. • Maintain relevant documents on the MESA shared drive and provide access to the relevant authorized users.		
18	**Report Name:** Laboratory Safety **Report Date:** 12/17/15 **Management:** Julie Zobel, Assistant Vice President, Safety, Emergency and Enterprise Risk Management	**Strengthen Lab Safety Inspection and Follow-Up Process:** Lab Safety inspectors perform general and chemical safety inspections of all labs at least once each fiscal year; additional biological safety and radiation safety inspection steps are performed for those labs. Inspectors ensure that all critical issues are addressed immediately, while other deficiencies are assigned to the Principal Investigator/Lab Supervisor or a Lab Safety staff member for correction within 30 days. Issues corrected by Principal Investigators are re-inspected; issues not corrected are communicated on 45-day delinquent letter to the department Chair and/or Director. • Lab Safety processes do not follow-up remediation of deficiencies included in 45-day delinquent letters and do not require escalation to more senior levels of university management for instances where corrective action remains outstanding.	Management will modify standard operating procedures to provide for additional follow-up on 45-day deficiency letter items, including escalation and documentation of final remediation. Appropriate supervision of remediation of deficiencies assigned to EHS personnel will be put in place.	7/31/16	7/31/16

#	Audit Report	Audit Issue	Status of Management Action	Original Target	Current Target
		• Due to personnel changes in the Lab Safety office, 45-day delinquent letters were not sent to department Chairs and/or Directors during fiscal year 2015. • There is no supervisory review of deficiencies assigned to Lab Safety personnel to ensure they are corrected timely and/or escalated. • The corrective action for deficiencies assigned to Lab Safety personnel is occasionally delegated to another Lab Safety staff member. This re-assignment causes the EHS Assistant system to inappropriately close-out the issue, impairing the monitoring of these actions to ensure they are completed timely.			
19	**Report Name:** Laboratory Safety **Report Date:** 12/17/15 **Management:** Julie Zobel, Assistant Vice President, Safety, Emergency and Enterprise Risk Management	**Enhance Inspection Documentation in EHS Assistant System:** Lab Safety inspectors conduct inspections using a mobile checklist that is uploaded to the EHS Assistant system. The EHS Assistant system has limits regarding recording positive compliance evidence (i.e., "no violation" responses) and only observed violations are documented, rather than answering each checklist item. As a result, an item may be missed during am the inspection.	Management will research and evaluate the EHS Assistant system architecture related to documenting positive compliance and develop appropriate solutions before the FY17 inspection cycle.	7/31/16	7/31/16
20	**Report Name:** Information Security Management: Boundary Protection **Report Date:** 9/09/13 **Management:** Marilyn Smith Vice President/Chief Information Officer, Information Technology Services	**Review of Firewall Configurations:** Firewall configurations are currently not being reviewed and re-authorized on a cyclic basis. Without a formal process to periodically review and re-authorize firewall configurations, the university cannot ensure that rule bases are adequate and/or still required.	The IT Security Office and Network Engineering and Technology have determined that existing firewall rule procedures include many undocumented rules and that inventorying and evaluating these rules is likely not to be effective or efficient. Instead, ITS will build a new server zone architecture and firewall framework for ITS servers. The new, zone-based architecture will (i) dramatically reduce the number of rules specific to servers as well as the total number of rules, (ii) create a more stable and supportable firewall rule set, (iii) provide for rule set	1/31/14	9/30/16

#	Audit Report	Audit Issue	Status of Management Action	Original Target	Current Target
			documentation and maintenance, and (iv) provide for assessment of firewall rule adequacy and lifecycle management. Although these actions are delayed from original plans, they are more holistic at addressing root causes. The framework is expected to be in production by September 2016.		
21	**Report Name:** Decentralized Servers: College of Humanities and Social Sciences **Report Date:** 11/14/13 **Management:** Deborah Boehm-Davis, Dean, College of Humanities and Social Sciences	**Considerations Over Use of Cloud Services:** Individuals in some departments have independently contracted for varying levels of internet "cloud" services for their programs' web sites. These services ranged from: • Fully hosted websites (such as GoDaddy or Wordpress which include domain name registration, content management application, infrastructure or "middleware", and physical server on which all of this resides). • Arrangements for middleware and server (such as Engine Yard) • Physical server only (such as Amazon EC2). Use of certain services can involve subcontracting of services to additional vendors with little or no transparency of terms. While such services may provide users with low cost, high immediacy advantages, they may also present vulnerabilities to known and frequently exploited security flaws, contract obligations contrary to Virginia procurement law, and responsibilities and related costs for full compliance with university's security and architectural standards.	Central CHSS IT staff continues to encourage individual CHSS units to utilize Information Technology Services rather than host systems separately and to follow university standards and procedures. The commercially-hosted CHSSWeb's highest risk, the lack of security surrounding user logins, has been mitigated by the use of Mason's Central Authentication Service. CHSSWeb will be migrated to Mason's new centralized content management system within the next two years, according to the project's university-wide schedule. The university's project team is holding monthly project status meetings.	10/31/14	8/31/17