GEORGE MASON UNIVERSITY
BOARD OF VISITORS

Audit Committee
September 24, 2015
Merten Hall, Fairfax Campus

A G E N D A

 I. Call to Order

II. Approval of Audit Committee Minutes
A. Approval of Committee Minutes for May 6, 2015 (**ACTION ITEM**)

III. New Business
A. Appointment of Internal Audit Director (**ACTION ITEM**)

IV. Reports
A. Report of Internal Audit and Management Services

 V. Adjournment

(This page was left blank intentionally.)

AUDIT COMMITTEE
OF THE BOARD OF VISITORS

May 6, 2015
Merten Hall
1:05 p.m. – 1:35 p.m.

<u>MINUTES</u>

PRESENT: Chairman Sheikh; Vice Chair Pence; Visitors Beck, Brown (arrived late), Corley and Mendelsohn; Faculty Liaison Douthett; Senior Vice President Davis; Chief of Staff Neville; Assistant Director Rastogi; Mr. Strudgeon; and Secretary <u>pro</u> <u>tem</u> Thompson

ABSENT: Visitor Ahmed

  I. Chairman Sheikh called the meeting to order at 1:05 p.m.

 II. **Approval of Minutes**

A **MOTION** was made by Visitor Mendelsohn and **SECONDED** by Vice Chair Pence to approve the minutes for the meeting of March 26, 2015. **MOTION CARRIED UNANIMOUSLY BY VOICE VOTE.**

III. **New Business – Report from Auditor of Public Accounts (APA)**

George Strudgeon, Audit Director with the APA, briefed the Committee on their audit of the university's financial statements for the year ending June 30, 2014. Mr. Strudgeon stated that the APA had issued an unmodified opinion (the best opinion an institution can receive) and there were no material instances of noncompliance and no unusual transactions. Mr. Strudgeon also stated that a separate report on internal controls and compliance included two management recommendations. One recommendation pertained to maintaining consistent documentation for the myVRS Navigator reconciliation and the second recommendation related to strengthening of IT security policy.

New Business – Internal Audit Director Search Update

Chief of Staff Neville provided an update on the first Search Committee meeting for the position of the Director of Internal Audit. Mr. Neville stated that the search committee, represented by Visitors Corley and Brown had narrowed the pool down to 12 priority candidates and 10 back up candidates from which they will select 3 or 4 finalists to visit Fairfax and meet with the Board members individually. Mr. Neville also provided a general description of the professional backgrounds of the candidates, which includes the insurance industry, healthcare, government, and banking. Mr.

Neville stated that only a few candidates have experience in a university environment. Visitor Corley provided additional information regarding the interview process and stated that the committee members spent a lot of time talking about what the university can offer.

Visitor Mendelsohn asked whether or not the candidates were aware of the salary range. Mr. Neville stated that the candidates were in touch with Mason's Human Resources Department and that Mason is being as flexible as possible with regard to the compensation package.

IV.   **Reports**

Assistant Director Rastogi was thanked for her hard work by Committee Chair Sheikh. Ms. Rastogi then introduced the Internal Audit staff to the Committee; all 5 staff members were present. Ms. Rastogi was asked if any consideration was given to employing temporary audit help. Ms. Rastogi responded that at this point Internal Audit is continuing to work on the scheduled audit projects but conversations with senior management and the Board can take place for any items of concern. Assistant Director Rastogi stated that Internal Audit has had a very stable audit process and presence over the past 20 years, (although this past year has been quite challenging with all the disruptions in staffing).

The Committee had the opportunity to review handouts provided by the Assistant Director. Once reviewed, Ms. Rastogi was asked questions regarding selection of audits and the audit process. Ms. Rastogi responded that aside from risk several other factors are taken into consideration for selecting the audit units. The Assistant Director went on to explain the audit process including the audit follow up performed within a year on issues included in the audit report. In addition, she mentioned that there are times when audit issues are escalated to management level if the action plan remains outstanding. Mr. Neville then provided examples of audit escalations that were brought to his attention and how they were addressed by his office.

V.   **Adjournment**

Chairman Sheikh called for a motion to adjourn. It was **MOVED** by Vice Chair Pence and **SECONDED** by Visitor Brown. **MOTION CARRIED UNANIMOUSLY BY VOICE VOTE.**

Respectfully submitted,

Karen Thompson
Secretary pro tem

Edward R. Dittmeier – Biographical Information

Edward Dittmeier was named Director of Internal Audit and Management Services in July 2015. Ed has over thirty years of executive internal audit experience in the financial services industry prior to joining Mason. He was senior vice president and associate general auditor for BB&T Corporation for three years and, prior to that, served in multiple senior-level internal audit roles for American Express Company. Mr. Dittmeier earned bachelor's degrees in business administration (accounting) and statistics from the State University of New York at Buffalo. He is a Certified Public Accountant and Certified Internal Auditor.

Summary Resume:

State University of New York at Buffalo

BB&T Corporation, Winston-Salem, NC
- Senior Vice President & Associate General Auditor – Audit Governance and Practices (2011-14)

American Express Company, New York, NY
- Vice President & Audit Leader – Audit Committee Reporting, Network Businesses & Fraud (2006-09)
- Vice President & Audit Leader – Professional Practices (2003-06)
- Vice President & Audit Leader – Global Utilities (2000-02)
- Vice President & Audit Leader – Travel Related Services (1991-99)
- Audit Leadership Roles – American Express Bank (1982-91)

Marine Midland Bank, New York, NY
- Various internal audit positions (1978-1982)

State University of New York at Buffalo
- BS Accounting (1978)
- BA Statistics (1978)

Professional Certifications
- Certified Public Accountant (New Jersey)
- Certified Internal Auditor

(This page was left blank intentionally.)

**Internal Audit
and Management Services**

Report to the Audit Committee of the Board of Visitors

September 24, 2015

(This page was left blank intentionally.)

EXECUTIVE SUMMARY

- Two <u>audit reports</u> issued since last meeting; both with satisfactory results:
  - Office of Student Financial Aid: Decentralized IT Operations and IT Asset Management
  - Virginia Initiative for Science Teaching and Achievement (VISTA) Grant

- Remediation of 18 <u>audit issues</u> is in progress as of August 31, 2015:
  - Instituted enhanced follow-up management reporting process.
  - More than half of the issues relate to information technology.
  - Nearly all issues have current target remediation dates through mid-2016.

- <u>Audit Plan status:</u>
  - Original plan consisted of 13 projects
    - Two are complete.
    - Six are in progress and expected to be completed in Q4.
    - Five were postponed.

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

- The current <u>staffing level</u> is six audit professionals.
  - Recruiting efforts have been initiated to fill two open positions.

- <u>Additional plans</u> for the next two months:
  - Strengthen internal audit risk assessment processes and documentation.
  - Build new process for tracking, reporting, and following-up the status of management's remediation of audit issues.
  - Self-assess internal audit performance vs. professional standards.

(This page was left blank intentionally.)

TABLE OF CONTENTS

SUMMARY OF INTERNAL AUDIT REPORTS

- Office of Student Financial Aid: Decentralized IT Operations and IT Asset Management

- Virginia Initiative for Science Teaching and Achievement (VISTA) Grant

Report Title:	Office of Student Financial Aid: Decentralized IT Operations and IT Asset Management	**Report Date:**	May 18, 2015
Responsible Manager:	Heidi Granger, Director, Office of Student Financial Aid Marilyn Smith, Vice President/Chief Information Officer, Information Technology Services		

EXECUTIVE SUMMARY:

Background:

The Office of Student Financial Aid (OSFA) provides prospective students with information related to financing their education and assembles financial resource packages to assist students with reaching their educational goals. More than 50% of students receive financial aid, based on merit and/or need, from federal and state government, the university, and private organizations. More than $250 million in financial aid was disbursed to more than 18,500 students in academic year 2013-14.

OSFA uses the Banner Financial Aid Module to process more than 150,000 financial aid transactions and to help ensure compliance with applicable laws and regulations. This Module interfaces externally with the federal financial aid system and internally with systems related to General Accounting, Student Accounts, Account and Loan Management, and Registrar.

The audit evaluated the adequacy and effectiveness of the IT security programs governing OSFA's IT assets to ensure the sustainability of appropriate levels of confidentiality, integrity, and availability of data, information, and systems.

Audit Conclusion:

IT security programs governing OSFA's IT assets, including related controls and manual procedures, provide reasonable assurance of the accuracy, integrity, completeness, and validity of significant transactions under OSFA's control. OSFA has also completed appropriate actions to remediate matters identified in a 2013 security assessment completed by Accuvant, an external security consultant.

Report Title:	Virginia Initiative for Science Teaching and Achievement (VISTA) Grant	Report Date:	August 28, 2015
Responsible Manager:	Mark Ginsberg, Dean, College of Education and Human Development		

EXECUTIVE SUMMARY:

Background:

In 2010, George Mason University received a $28.5 million, five year Virginia Initiative for Science Teaching and Achievement (VISTA) grant from the U.S. Department of Education with a $5.7 million private sector matching requirement to translate research-based best teaching practices into improved science teaching and student learning for all students at all levels. The VISTA program's overall objectives are to increase student learning in science; enhance quality of elementary science teaching; enhance quality of science teaching by new, underprepared secondary science teachers; increase the number of certified middle school and high school teachers; increase access for rural teachers to professional development; build state infrastructure to support effective science teaching and learning; and conduct research to determine what makes the most significant difference in helping teachers to help students learn.

VISTA is a statewide partnership among 87 Virginia school divisions, six Virginia universities, and the Virginia Department of Education. George Mason University's Center for Restructuring Education in Science and Technology (CREST) in the College of Education and Human Development (CEHD) hosts the program. All reimbursements and payments from the grant must be made by the grant's September 30, 2015 scheduled end date.

The audit evaluated controls related the appropriateness of charges to the grant, including salaries, wages, and Partner University expenditures, and wage employee hiring and recordkeeping.

Audit Conclusion:

The VISTA grant is administered in accordance with applicable university policies and procedures, and expenditures charged are for the intended purpose of the grant in accordance with sponsor requirements. Management is implementing minor improvements to strengthen maintenance of complete wage employee documentation and reconciliation of labor expenses.

STATUS OF AUDIT ISSUES AS OF AUGUST 31, 2015

There were 17 open audit issues as of August 31, 2015. Remediation of 25 audit issues was completed by management since May.

Audit Issue Inventory Movement

Audit Issues by Type

Audit Issues by Current Target
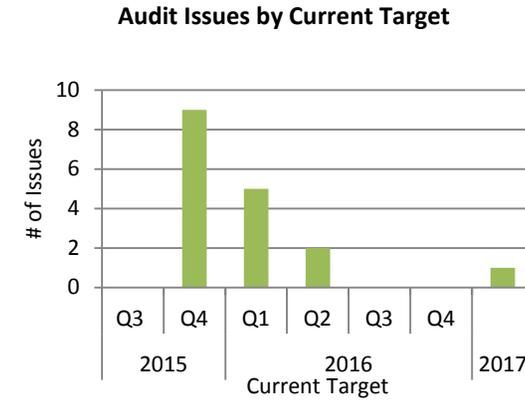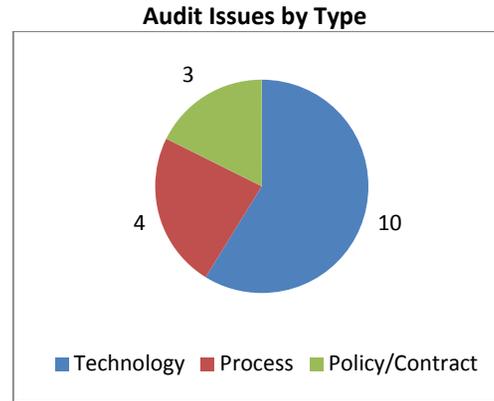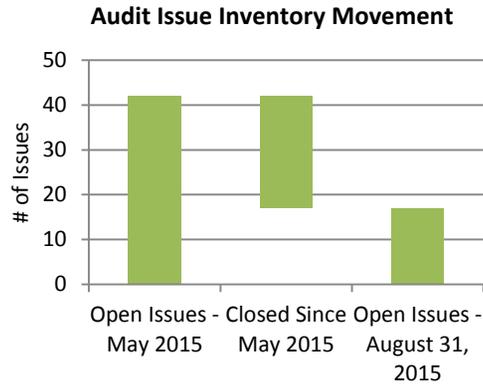
Audit Report	Report Date	Open at May 2015 Meeting	Closed Since May 2015	New	Open at Aug 31, 2015
Virginia Initiative for Science Teaching and Achievement (VISTA) Grant	8/1/15	-	-	0	0
Office of Student Financial Aid: Decentralized IT Operations and IT Asset Mgmt	5/18/15	-	-	0	0
Office of the University Registrar	3/5/15	3	2	-	1
Arlington Campus Parking Services	11/11/14	3	3	-	0
Aquatic and Fitness Center	8/21/14	1	1	-	0
Human and Animal Subjects Research	7/8/14	1	0	-	1
Facilities Service Contracts	4/22/14	2	2	-	0
Summer Camps and Enrichment Programs	4/22/14	4	1	-	3
Decentralized Servers: College of Humanities and Social Sciences	11/14/13	3	2	-	1
Intercollegiate Athletics: Student Athlete Financial Aid	11/5/13	4	3	-	1
Biomedical Research Laboratory: Physical Security	9/10/13	2	0	-	2
Information Security Management: Boundary Protection	9/9/13	3	1	-	2
Enterprise Project Management Framework and System	3/28/13	2	0	-	2
Housing and Residence Life	6/11/12	4	4	-	0
Applications and Security Audit: Housing and Residence Life Systems	12/21/11	5	5	-	0
Decentralized Servers: College of Science	8/18/11	3	1	-	2
SEC 501-01 IT Security Audits Prior to Level II Status (2008-2010)	8/30/10	2	0	-	2
		42	25		17

STATUS OF AUDIT PLAN AS OF AUGUST 31, 2015

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 August 31, 2015, two audits were completed with satisfactory results, six are in progress and expected to be completed in Q4, and five were postponed. Follow-up audits to validate management's remediation of audit issues from prior audits were completed in five areas; an additional follow-up audit is underway. Actions related to the Housing and Residential Applications and Security audit were delayed and have been re-initiated.

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	Focus on IT security risks; completion expected in October 2015.
Hylton Performing Arts Center	Operational	In Progress	Focus on box office and rental revenues; completion expected in October 2015.
Laboratory Safety	Operational	In Progress	Focus on operation of laboratories in a safe manner and regulatory compliance: completion expected in September 2015.
Biomedical Research Laboratory: Physical Security	Follow-Up	Completed	Issued April 29, 2015. Four issues closed; two remain open with expected completion in December 2015.
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	Focus on management of Windows and Unix/Linux operating system security configurations and server-level account management; completion expected in October 2015.
Human Resources: Employee Benefits*	Operational	In Progress	Fieldwork completed, reporting phase. Satisfactory results.

Audit	Type	Status	Remarks
MESA TPOC and Share Administrator Account Management	IT	In Progress	Fieldwork completed, reporting phase. Satisfactory results.
Summer Camps and Enrichment Programs	Follow-Up	Completed	Issued August 26, 2015. One issue closed; three remain open with expected completion in November 2015 and May 2016.
Human and Animal Subjects Research	Follow-Up	In Progress	Expected completion in September 2015.
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. Three issues closed; one remains open with expected completion in October 2015.

* = Carry over from 2013-14 audit plan.

STATUS OF INVESTIGATIONS AS OF AUGUST 31, 2015

Since the Committee's last meeting, four investigations were completed. Six investigations are in progress as of August 31, 2015. These investigations are isolated in nature and considered as having negligible impact to the University.

Nature of Allegation	Type	Status	Remarks
Abuse of Power	Abuse	Completed	Reinforce certain University policies.
Misuse of Contractor Time	Abuse	Completed	Strengthen employee time card reviews.
Wage Employee Timesheet Abuse	Fraud	Completed	Strengthen wage employee time submission and approval.
Waste	Waste	Completed	Improve procedures for receiving goods.
Abuse of University and State Resources	Abuse	In Progress	
Employee Not Qualified for Position	Fraud	In Progress	
Employee on Grant Not Doing Work	Fraud	In Progress	
Employee Theft and Employee Working Outside University	Abuse	In Progress	
Possible Misuse of State Time and Equipment and Fraud	Abuse	In Progress	
Questionable Accounting Practices Related to Student Course Fees	Fraud	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

	Plan	**a/o Oct 2014**	**a/o Aug 2015**	**Plan vs Aug 2015**
Director	1	1	1	-
Assistant Director	1	1	1	-
IT Audit	2	2	2	-
Operational Audit	3	2	1	(2)
Fraud Audit	1	1	1	-
Total Audit Professionals	**8**	**7**	**6**	**(2)**

- Full accomplishment of the original 2014-15 Audit Plan required a staffing level totaling eight audit professionals.
- The actual staffing level has averaged 6.5 audit professionals.
- At August 31, 2015, there are two unfilled positions; recruiting efforts have been initiated.

Name	Title	GMU Audit (Years)	Prior Audit (Years)	Prior Experience	Education	Prof Certs
Edward Dittmeier	Director	0	34	• BB&T Corporation (3) • American Express Company (27) • Marine Midland Bank (4)	• BS Accounting • BA Statistics	CIA CPA
Alka Rastogi	Assistant Director	18	10	• Marriott Employees Federal Credit Union (2) • Perpetual Savings Bank / Crestar Bank (5) • State Street Bank (3)	• BBA	CIA CFE CICA
Carol Westbrook	IT Audit Manager	21	3	• Pierce Butler & Co (2) • MCI (1)	• MA English • BA English • BS Accounting	CPA CISA
Jacqueline Curtis	Senior Auditor / Fraud Examiner	6	24	• DC Water (1) • AARP (7) • Washington Metropolitan Area Transit Authority (11) • Coopers and Lybrand (1) • Touche Ross (4)	• MBA Finance • BBA Accounting	CPA
Richard Cheney	Senior Auditor	11	10	• First Virginia Bank (10)	• BS Accounting	CICA
Michelle Workman	Senior IT Auditor	8	6.5	• Deloitte (5) • Universal Service Administrative Company (1.5)	• BS Accounting Information Systems	CISA
	Average =	10.7	14.6			
	Avg ex Director =	12.8	10.7			

Legend of Professional Certifications: CIA = Certified Internal Auditor; CPA = Certified Public Accountant; CISA = Certified Information Systems Auditor; CFE = Certified Fraud Examiner; CICA = Certified Internal Controls Auditor

#	Audit Report	Audit Issue	Status of Management Action	Original Target	Current Target
1	**Report Name:** Office of the University Registrar **Report Date:** 03/05/2015 **Management:** Eve Dauer, University Registrar, Registrar	**Consortium Course Registration and Reconciliation:** Mason is a cooperating member of the Consortium of Universities of the Washington Metropolitan Area (Consortium); and the Consortium's cross-registration arrangement allows students enrolled in eligible degree programs at one member institution to take a course at another member institution. Consortium students require proper academic approvals from both institutions and are manually registered in the Banner system. • The Consortium Coordinator collects all documentation and approvals, registers students, attaches consortium documentation to the student's account, and performs the semester end reconciliation. These duties should be segregated. • E-mail approvals by Mason academic units for incoming visiting students and visiting institution approvals for Mason outgoing students are not always attached to the student's account. Instead, they are stored in the Consortium Coordinator's personal e-mail account. This practice was remediated during the audit. • Consortium procedures do not cover registration and processing of Reserve Officer Training Corps (ROTC) students in Banner nor their billing for the end of semester reconciliation.	Beginning fall 2014, the Associate Registrar for Operations will conduct a second review and approval of reconciliation reports received from the Washington Consortium before the reports are returned to the Consortium. After the final reconciliation report is received, the Consortium Coordinator will, in writing, verify for Third Party Billing the total amount due prior to Mason sending fees due to the Washington Consortium. This will be implemented by October 2016 when the submission is due to the Washington Consortium.	Aug 2015	Oct 2015
2	**Report Name:** Human and Animal Subjects Research Compliance	**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	ORIA successfully filled the IRB Manager position with an internal candidate; however, backfilling the vacated position has been delayed.	Jan 2015	Mar 2016

#	Audit Report	Audit Issue	Status of Management Action	Original Target	Current Target
	Report Date: 07/08/2014 **Management:** Aurali Dade Assistant Vice President for Research Compliance, Office of Research Integrity and Assurance	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. Ten of the 50 procedures requiring update have been completed; updating of the remaining procedures is underway with priority being given to procedures with federally mandated elements. Implementation of a post-approval monitoring program has been delayed due to extended staff recruiting delays.		
3	**Report Name:** Summer Camps and Enrichment Programs **Report Date:** 04/22/2014 **Management:** Jennifer Wagner Davis Senior Vice President for Administration and Finance	**University Policy:** The inherent risks and liabilities associated with hosting and operating summer camps and enrichment programs on campus are not governed by a university policy and are not overseen by a central office responsible for these activities and for ensuring that these programs are consistent with the university's mission. There is no written guidance related to operational, financial, safety and security, incident response, health emergency/administration of medication, drop off/pick up, and staff training requirements specific for these programs. The ORM and OEHS have provided relevant risk management advisory and emergency preparedness information on their websites; however, there is no requirement for the summer camps and enrichment programs to	A Summer Camps Coordinating Office was established within Auxiliary Enterprises to oversee all administrative and operational aspects of summer camps and enrichment programs in June 2015. A cross-functional advisory group has drafted an appropriate policy and related procedures; the draft is undergoing final review and is expected to be published in Q4.	Jul 2014	Nov 2015

#	Audit Report	Audit Issue	Status of Management Action	Original Target	Current Target
		implement the guidance and no enforcement of procedures.			
4	**Report Name:** Summer Camps and Enrichment Programs **Report Date:** 04/22/2014 **Management:** Jennifer Wagner Davis Senior Vice President for Administration and Finance	**Background Investigations:** Within the seven university affiliated camps and programs evaluated for compliance with University Policy 2221, Background Investigations, there was one camp director who did not have background investigations performed for camp staff members. In addition, background investigations were not always conducted on camp staffers hired directly by university affiliated program camp administrators because the staffer's name was not included on the list forwarded to HR or because the staffer did not return the signed form permitting the check. Also, space utilization contracts with non-university affiliated camp and program sponsors do not consistently require background investigations and, when it does, there is no validation of the sponsor's compliance.	The Summer Camps Coordinating Office, established within Auxiliary Enterprises in June 2015, ensures that Program Administrators are clearly required to verify completion of background investigations prior to hiring program, event, and camp personnel. A standard summer camp facility use contract for external clients has been drafted for use in 2016. All summer camp contracts will be required to be reviewed and signed by the SVP or designee.	Jul 2014	May 2016
5	**Report Name:** Summer Camps and Enrichment Programs **Report Date:** 04/22/2014 **Management:** Jennifer Wagner Davis Senior Vice President for Administration and Finance	**Other Miscellaneous Risks and Liability:** The majority of sponsors/directors of seven university affiliated summer camps and enrichment programs in our test sample were not aware of ORM's Risk Advisory which requires certain actions to assure coverage by the Commonwealth's Risk Management Plan. Most programs had some part of the requirements in place but no program had comprehensive compliance documentation. Facilities usage contracts for non-university affiliated programs did not consistently address ORM's Risk Advisory actions.	A cross-functional advisory group has drafted an appropriate policy and related procedures; the draft is undergoing final review and is expected to be published in Q4. Once finalized, the new Camps and Programs Administrator, established in June 2015, will begin monitoring compliance.	Jul 2014	Nov 2015
6	**Report Name:** Decentralized Servers:	**Considerations Over Use of Cloud Services:** Individuals in some departments have independently	Central CHSS IT staff continues to encourage individual CHSS units to utilize	Fall 2014	Aug 2017

#	Audit Report	Audit Issue	Status of Management Action	Original Target	Current Target
	College of Humanities and Social Sciences **Report Date:** 11/14/13 **Management:** Deborah Boehm-Davis, Dean, College of Humanities and Social Sciences	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.	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.		
7	**Report Name:** Intercollegiate Athletics: Student Athlete Financial Aid **Report Date:** 11/05/2013 **Management:** Brad Edwards Assistant Vice President/Director, Intercollegiate Athletics	**Scholarship Awards With Cash Option:** Typically, athletic scholarship awards determined by individual coaches are disbursed to student athletes by the Office of Student Financial Aid (OSFA) initiating the award in the Banner Financial Aid system for crediting to the student account. With coach approval, student athletes can opt for the room and/or board only portion of the award to be paid via check (rather than student account credit). For academic year 2012-2013, these payments totaled approximately $313,000. The Assistant Athletic Director administering the athletic scholarship award process and monitoring	Procedures were revised, effective October 2015, to require student athlete to pick up checks for room and/or board only portions of their awards directly from Accounts Payable.	Oct 2014	Oct 2015

#	Audit Report	Audit Issue	Status of Management Action	Original Target	Current Target
		the status of awards is also responsible for (i) requesting and collecting student athlete checks from the Accounts Payable for the room and/or board cash option payments, (ii) distributing checks to the student athletes, and (iii) accounting and maintaining the supporting documentation. These duties should be segregated.			
8	**Report Name:** Biomedical Research Laboratory: Physical Security **Report Date:** 09/10/2013 **Management:** Charles Bailey, Executive Director, National Center for Biodefense and Infectious Diseases	**IT Security Risk Assessment:** Security standards followed by the university require a risk assessment be completed on sensitive systems at least once every three years and whenever major changes in systems or personnel occur. Mason's Information Technology Security Office (ITSO) performed an IT security risk assessment on BRL's systems in 2010. Since then, there were no formal follow-ups performed to determine the status of corrective actions taken on the findings from the risk assessment.	In October 2014, ITSO completed a risk assessment which identified five areas of vulnerability. Management is developing and implementing remediation action plans.	Jul 2014	Dec 2015
9	**Report Name:** Biomedical Research Laboratory: Physical Security **Report Date:** 09/10/2013 **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.	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 December 2015. BRL management will confirm at least annually the appropriateness of all individuals with access to the BRL facility and containment suite.	Aug 2014	Dec 2015

#	Audit Report	Audit Issue	Status of Management Action	Original Target	Current Target
		• Access request forms have been continuously developing with changing information requirements. • No review to ensure that access granted is what was requested.			
10	**Report Name:** Information Security Management: Boundary Protection **Report Date:** 09/09/2013 **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 are working on a Firewall Architecture Project to mitigate risks resulting from existing firewall rule procedures. This project is contained within the IT Project Prioritization process; updates of the status of this process, including milestones and related timing, will be available in November 2015.	Jan 2014	Nov 2015
11	**Report Name:** Information Security Management: Boundary Protection **Report Date:** 09/09/2013 **Management:** Marilyn Smith, Vice President/Chief Information Officer, Information Technology Services	**Network Assignment Requests:** Network assignment requests (e.g., serve, point of sale, etc.) authorizations are not being reviewed and re-authorized on a cyclic basis since they are serviced through ITS's trouble ticket system and stored as a virtual email rather than as a database record. As a result, the university cannot ensure that the assignment is still required and the validity of system information on file.	Workflow to facilitate annual network assignment re-certifications is part of the design of IT Security Office's (ITSO) IT Governance, Risk, and Compliance system. The pilot phase is beginning; implementation is expected by November 2015.	Aug 2014	Nov 2015

#	Audit Report	Audit Issue	Status of Management Action	Original Target	Current Target
12	**Report Name:** Enterprise Project Management Framework and System **Report Date:** 03/28/13 **Management:** Robert Nakles, Executive Director, Information Technology Services	**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 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.	The IT Governance Group (ITGG) is a strategic level team chartered in December 2014 to provide prioritization guidance. Information Technology Services developing a prioritization process for the ITGG's review and approval in October 2015. The PEC has agreed to use the same process, once approved by the ITGG. Information Technology Services will coordinate communications between the PEC and the ITGG, and expects the process to be fully operational by March 2016.	Jun 2013	Mar 2016
13	**Report Name:** Enterprise Project Management Framework and System **Report Date:** 03/28/13 **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 plans to create a resource reporting structure and provide related training by June 2016.	Sep 2013	Jun 2016

#	Audit Report	Audit Issue	Status of Management Action	Original Target	Current Target
14	**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. Existing systems will be assessed through this automated process by March 2016.	Dec 2013	Mar 2016
15	**Report Name:** Decentralized Servers: College of Science **Report Date:** 08/18/11 **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 centralized governance, risk management, and compliance product. Existing servers will be assessed through this automated workflow by March 2016.	Dec 2013	Mar 2016
16	**Report Name:** SEC501-01 IT Security Audits Prior to Level II Status (2008-2010) **Report Date:** 08/30/12	**Consistency of Business Impact Analysis, University and IT Continuity of Operations Plan, and Disaster Recovery Plan Documents:** There were some inconsistencies among various university Continuity of Operations Plan (COOP) and disaster recovery documents, particularly in the identification	The Environmental Health and Safety Office has continued its detailed work with individual units to identify essential IT systems for primary business functions to be continued during an emergency event. The Executive Council will review in October 2015 and the prioritization will be	Apr 2011	Dec 2015

#	Audit Report	Audit Issue	Status of Management Action	Original Target	Current Target
	Management: John Kettlewell, Interim Executive Director, Information Technology Services	of some systems and sub-systems supporting essential functions.	ready for Information Technology Services by December 2015.		
17	**Report Name:** SEC501-01 IT Security Audits Prior to Level II Status (2008-2010) **Report Date:** 08/30/12 **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 to align the ITS Disaster Recovery / Continuity of Operations Plan with those priorities. Management estimates the Disaster Recovery site plans will be aligned and documented by February 2016, depending on other project workloads and university priorities.	Mar 2011	Feb 2016