GEORGE MASON UNIVERSITY
BOARD OF VISITORS

Audit Committee
May 5, 2016
Merten Hall, Fairfax Campus

AGENDA

I. Call to Order

II. Closed Session

A. Personnel Matters (Code of VA: 2.2-3711.A.1) and Consultation with Legal Counsel (Code of VA: 2.2-3711.A.7)

III. Approval of Audit Committee Minutes

A. Approval of Committee Minutes for March 31, 2016 Meeting (**ACTION**) .. **C-3**

IV. New Business

A. Review of Financial Statements for Year Ended June 30, 2015
(Joint Review with Finance and Land Use Committee)

B. Auditor of Public Accounts Examination Report
(Joint Review with Finance and Land Use Committee)

V. Reports

A.Report of Internal Audit and Management Services………………………….**C-5**

VI. Adjournment

(This page was left blank intentionally.)

AUDIT COMMITTEE
OF THE BOARD OF VISITORS

March 31, 2016
Merten Hall

MINUTES

PRESENT: Chairman Sheikh; Visitors Corley and Peterson; Senior Vice President Davis; Chief of Staff Neville; Vice President and Chief Information Officer Smith; Assistant Vice President Zobel; University Counsel Moncure; Chief Information Security Officer Landry; Director - IT Security McNay; Director Dittmeier; and Secretary pro tem Thompson

ABSENT: Vice Chair Pence and Visitor Mendelsohn

I. Chairman Sheikh called the meeting to order at 11:07 a.m.

II. Approval of Minutes

Chairman Sheikh called for a motion to approve the minutes of the February 11, 2016 Audit Committee meeting. The motion was **MOVED** by Visitor Peterson and **SECONDED** by Visitor Corley. **MOTION CARRIED UNANIMOUSLY BY VOICE VOTE.**

III. New Business

A. Enterprise Risk Management Update

Ms. Julie Zobel, Assistant Vice President, Safety, Emergency and Enterprise Risk Management, reviewed with the Committee the status of the university's Enterprise Risk Management program. She described the evolution of the program since 2013, including the establishment of the Enterprise Risk Management Council charged with implementing a comprehensive approach to enterprise risk management and monitoring programs and actions; and development of a core process for identifying, assessing, and overseeing management of significant enterprise risks. She updated the Committee on the highest priority enterprise risks identified by the Council; these risks are clustered on workforce sustainability, infrastructure, and compliance. The Committee discussed the Council's assessment of significant enterprise risks and management's process for considering risk appetite when monitoring and managing exposures associated with these risks.

B. Information Security Update

Ms. Marilyn Smith, Vice President and Chief Information Officer, introduced Mr. David Landry, Chief Information Security Officer, and Mr. Curtis McNay, Director - IT Security.

Mr. Landry described the nature of cyber threats being faced by the US higher education industry and the university. He discussed the size and extent of several information security breaches at comparable universities in the last three years and provided a context for relevant risk factors, including the speed of change and growth of technologies; the value higher education cultures place on openness and decentralization; and the extent of valuable information assets, such as personal data, financial data, research data, and intellectual property. He also described the frequency and extent of attempts by potential attackers to identify vulnerabilities within Mason's security infrastructure. Mr. McNay provided an update on the status of management's actions to manage exposures related to cyber threats, including, among others, increased systems hardening and further strengthening network security, privileged account management, and real-time monitoring and alerting.

IV. Reports

Mr. Dittmeier reviewed with the Committee the Report of Internal Audit and Management Services. He stated that one audit report, Enterprise Servers and Messaging: Operating Systems Security, was issued since the last meeting. Management continues to make progress to remediate 18 outstanding audit issues; three issues have been closed since the last meeting.

V. Adjournment

Chairman Sheikh declared the meeting adjourned at 11:39 a.m.

Respectfully submitted,

Karen Thompson

Karen Thompson
Secretary pro tem

GEORGE
MASON
UNIVERSITY

Internal Audit
and Management Services

Report to the Audit Committee of the Board of Visitors

May 5, 2016

(This page was left blank intentionally.)

EXECUTIVE SUMMARY

- One audit report issued since last meeting; with satisfactory results:
  - Hylton Performing Arts Center

- Remediation of 15 audit issues is in progress as of April 10, 2016:
  - Most issues relate to information technology.
  - All but one issue have current target remediation dates through October 2016.

- Audit Plan status:
  - Substantially on track with 3+6 Audit Plan approved at prior Committee meeting.

- Status of fraud, waste, and abuse investigations:
  - 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.
  - Recruiting efforts continue. Search Committee is working to identify additional Senior IT Auditor candidates.
  - Requests for Proposals to establish supplemental internal audit co-sourcing arrangements received from 11 providers were evaluated in March. Negotiations are underway with two providers and are expected to be completed in April 2016.

- Additional plans:

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

(This page was left blank intentionally.)

TABLE OF CONTENTS

Topic

SUMMARY OF INTERNAL AUDIT REPORTS

- Hylton Performing Arts Center

Internal Audit
and Management Services

INTERNAL AUDIT REPORT

Report Title:	Hylton Performing Arts Center	**Report Date:**	April 11, 2016
Responsible Manager:	Rick Davis Dean, College of Visual and Performing Arts and Executive Director, Hylton Performing Arts Center		

EXECUTIVE SUMMARY:

Background:

Opened in May 2010, the Hylton Performing Arts Center (HPAC) operates under the umbrella of the College of Visual and Performing Arts on Mason's Science & Technology (formerly Prince William) campus. HPAC is the result of a Tripartite Agreement between Prince William County, the City of Manassas, and Mason. While the university owns and operates the Performing Arts Center, all three parties provide governance through a Board, provide funding, and service debt in accordance with the Agreement.

HPAC consists of 85,000 square feet of space that comprises the following facilities: Merchant Hall (a 1,100+ seat opera house), Gregory Family Theater (a black box space with 4,900 square feet of open space and seating for 350), Didlake Grand Foyer, Buchannan Partners Art Gallery, Lovey Hammel Lounge, and Novant Rehearsal Room. All facilities are available for rental and HPAC's Ticket Office is responsible for ticket and subscription sales for events and performances. Under contract, Tickets.com (TDC) provides ticketing services, including use of its ProVenue Ticketing system used for selling, delivering, and controlling the sale of event tickets; TDC also sells tickets via its retail outlets, by telephone call centers, and over the internet. Fiscal year 2015 operations resulted in a $461,000 deficit (excluding debt service funded by the Tripartite Agreement parties); an improvement of more than $200,000 from fiscal year 2014.

This audit evaluated the adequacy and effectiveness of internal controls over HPAC Ticket Office operations and Facility Rental activity, including ticket sale processing and settlement.

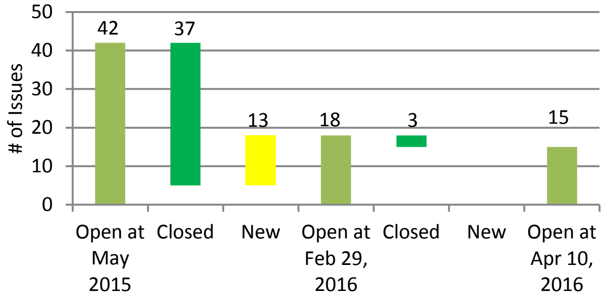
Audit Conclusion:

HPAC Ticket Office operations are well designed and established with an organized framework of processes that provide assurance that access to the Ticket Office and the money safe inside is controlled; ticket sales and other payments are processed accurately and timely; cash receipts are properly accounted and reconciled with TDC system reports and Banner Finance; individual performances and events are settled accurately and timely; weekly settlement with TDC results in accurate remittance of funds; and facility rental estimated charges are accurately accounted and settled with the clients.

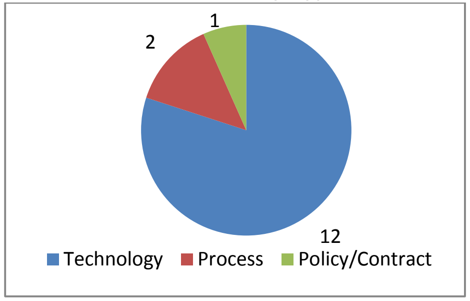
STATUS OF AUDIT ISSUES AS OF APRIL 10, 2016

There were 15 open audit issues as of April 10, 2016. Remediation of two audit issues was completed by management since February 2016.

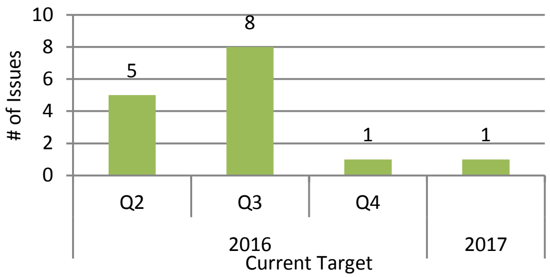
Audit Issue Inventory Movement



Audit Issues by Type



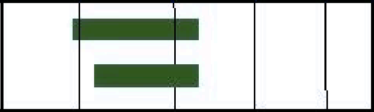
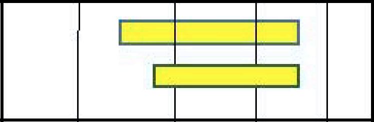
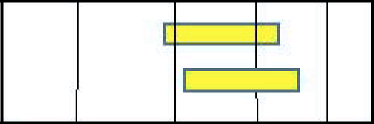
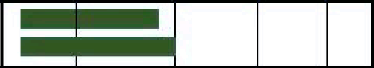
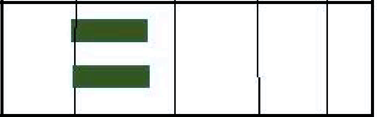
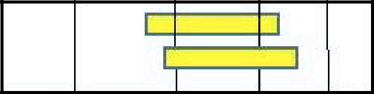
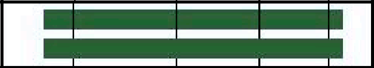
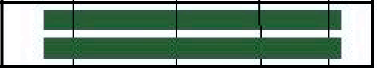
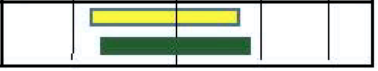
Audit Issues by Current Target



Audit Report	Report Date	May 2015	New	Closed	Feb 2016	New	Closed	Apr 2016
Hylton Performing Arts Center	4/11/16		-	-	0	-	-	0
Enterprise Servers and Messaging: Operating Systems Security	2/2/16		-	-	0	-	-	0
Analysis of Mason Sexual Harassment and Misconduct Policy and Procedures	12/18/15		1	-	1	-	-	1
Laboratory Safety	12/17/15		4	(1)	3	-	(1)	2
Decentralized IT Operations and IT Asset Management: Office of Admissions	12/17/15		-	-	0	-	-	0
Decentralized IT Management and Security: Office of the Provost	10/23/15		5	-	5	-	(1)	4
Human Resources and Payroll – Employee Benefits	10/23/15		1	(1)	0	-	-	0
MESA Technical Point of Contact and Share Administration Account Mgmt	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)	0	-	-	0
Facilities Service Contracts	4/22/14	2	-	(2)	0	-	-	0
Summer Camps and Enrichment Programs	4/22/14	4	-	(4)	0	-	-	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	-	(4)	0	-	-	0
Biomedical Research Laboratory: Physical Security	9/10/13	2	-	(2)	0	-	-	0
Information Security Management: Boundary Protection	9/9/13	3	-	(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	-	(1)	1
SEC 501-01 IT Security Audits Prior to Level II Status (2008-2010)	8/30/10	2	-	(1)	1	-	-	1
		42	13	(37)	18	0	(3)	15

STATUS OF AUDIT PLAN AS OF APRIL 10, 2016

The 3+6 Audit Plan as of April 10, 2016 (bottom bars) is compared with the status as of the prior Committee meeting (top bars). (Note: Work underway is shown in green bars; planned work is shown in yellow bars.)

TOPIC	DESCRIPTION	LIKELY TIMING Jan Mar Jun Sep
ALIGNED WITH UNIVERSITY-LEVEL RISK AREAS		
Construction Procurement and Change Order Processes – Peterson Family Health and Human Services Building	• Assess construction procurement and change management processes related to $71 million in-progress building project.	
Information Security Program	• Assess the university's ability to protect large volumes of personally identifiable and classified information in a globally connected, decentralized technology environment. • Assess cybersecurity readiness.	
College of Health and Human Services	• Evaluate a college's governance, risk management, and control processes to ensure alignment with Mason's strategic objectives and best serve students, the community, and society. • Address governance of centers, institutes, and public/private partnerships.	
ADDITIONAL AREAS		
Hylton Performing Arts Center	• Complete in-progress audit from prior audit plan.	
Reconciliation Policy Compliance – Sponsored Programs	• Assess compliance with policies requiring (i) research grant financial records be reconciled with supporting records and (ii) records support certifications that expenditures are made for the intended purpose of the grant or contract in accordance with sponsor requirements.	
ARMICS as Second Line of Defense	• Mason's Agency Risk Management and Internal Control Standards (ARMICS) function is part of Fiscal Services. ARMICS implements and assesses annually university internal control systems primarily related to fiscal processes.	
Issue Validation Procedures	• Validate management has remediated audit issues in a comprehensive and sustainable manner.	
Hotline Investigations Referred by OSIG	• Investigate allegations of fraud, waste, or abuse received from the Commonwealth's Office of the State Inspector General.	
Fraud Risk Assessment	• Develop a university-wide assessment of fraud risks; align with ERM.	

STATUS OF INVESTIGATIONS AS OF APRIL 10, 2016

Four investigations are in progress as of April 10, 2016. These in-progress investigations appear to be isolated in nature with negligible impact to the University.

Nature of Allegation	Type	Status	Remarks
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	
Allegations of Mismanagement and Misconduct	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 April 10, 2016, there were two unfilled positions.

	Plan	**a/o Oct 2014**	**a/o Mar 2016**	**Plan vs Mar 2016**
Director	1	1	1	-
Assistant Director	1	1	1	-
IT Audit	2	2	1	(1)
Operational Audit	3	2	2	(1)
Fraud Audit	1	1	1	-
Total Audit Professionals	**8**	**7**	**6**	**(2)**

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

- Work is underway to establish supplemental internal audit co-sourcing arrangements. The arrangements will provide supplemental staffing capability as well as access to specific knowledge, expertise, and industry practices. Requests for Proposal from 11 potential service providers were evaluated. Negotiations are underway with two service providers to establish contractual arrangements; these are expected to be in place by April 2016.

APPENDIX: AUDIT ISSUE DETAILS AS OF APRIL 10, 2016

#	Audit Report	Audit Issue	Status of Management Action	Original Target	Current Target
1	**Report Name:** Analysis of Mason’s Sexual Harassment and Misconduct Policy and Related Procedures **Report Date:** 12/18/15 **Management:** Julian Williams, Vice President, Compliance, Diversity and Ethics	**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 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’s review committee expects to submit revisions of Mason’s sexual harassment and misconduct policies, procedures, and practices for approval in May 2016.	5/31/16	5/31/16
2	**Report Name:** Enterprise Project Management Framework and System **Report Date:** 3/28/13 **Management:** Charles Spann, 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	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 June 2016.	6/30/13	6/30/16

#	Audit Report	Audit Issue	Status of Management Action	Original Target	Current Target
		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.			
3	**Report Name:** Enterprise Project Management Framework and System **Report Date:** 3/28/13 **Management:** Charles Spann, 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 management re-designing certain processes. As part of this, management is working to re-assess the appropriate process for making decisions regarding sizing and undertaking IT projects, including the appropriate level of consideration for time and cost, and tracking and reporting actual performance. A conceptual design for this process with a plan for beginning implementation is expected by June 2016.	9/30/13	6/30/16
4	**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
5	**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;	The ITS project to build a replacement provisioning system is actively underway. The new system is running parallel with the legacy account management system and is expected to assume production services after several weeks of operation. Once implemented, management will plan to	3/31/16	6/30/16

#	Audit Report	Audit Issue	Status of Management Action	Original Target	Current Target
	Management: John Kettlewell, Interim Executive Director, Information Technology Services (ITS)	however, HR purposes require individuals within the "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.	implement changes to address "GMU Retiree" individuals, among other things; this planning is expected to be completed by June 2016.		
6	**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.	A configuration assessment was implemented to address hardening of new systems. This process will be automated using the university's IT Security Office-managed 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 July 2016.	12/31/13	7/31/16
7	**Report Name:** Office of the Provost: Decentralized IT Management and Security **Report Date:** 10/23/15 **Management:** Renate Guilford, Associate Provost, Academic Administration	**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 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	The Provost IT Team continues to work to: • Develop and document COOP contingency plans and procedures for the platform as well as for individual 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	7/31/16	7/31/16

#	Audit Report	Audit Issue	Status of Management Action	Original Target	Current Target
		cooperation among their office, ITS, and the Provost IT users.	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.		
8	**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. • 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.	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
		- 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.			
9	**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.	After research and evaluation, management has identified EHS Assistant system hardware and process improvements to strengthen documentation of positive compliance. These are on track for implementation prior to the FY17 inspection cycle.	7/31/16	7/31/16
10	**Report Name:** Office of the Provost: Decentralized IT Management and Security **Report Date:** 10/23/15 **Management:** Renate Guilford, Associate Provost, Academic Administration	**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 performed every three years or earlier, whenever material changes are made to systems.	The Provost IT Team had begun to develop their own solutions to effective IT security risk assessment activities. In March 2016, Provost IT Team determined that use of the university's IT Security Office-managed centralized governance, risk management, and compliance product would be a more effective solution and began working to gather appropriate system information. Working with the IT Security Office's schedule, results of the initial assessments are expected by September 2016.	4/30/16	9/30/16
11	**Report Name:** Office of the Provost: Decentralized IT Management and Security **Report Date:** 10/23/15	**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	The Provost IT Team's original intent was to leverage Information Technology Services' design documentation and methodology. However, the focus of this material was determined to be too centered on Banner and required substantial update to meet Provost IT Team's needs. The Provost IT Team and ITS's Enterprise Applications team are working together to develop and document	4/30/16	9/30/16

#	Audit Report	Audit Issue	Status of Management Action	Original Target	Current Target
	Management: Renate Guilford, Associate Provost, Academic Administration	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.	system design documentation reflective of the design methodologies currently in use; this is expected to be completed by September 2016.		
12	**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. EHS completed their work in March 2016 and, as a result, ITS management estimates the Disaster Recovery site plans will be aligned and documented by September 2016, depending on other project workloads and university priorities.	3/31/11	9/30/16
13	**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 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	1/31/14	9/30/16

#	Audit Report	Audit Issue	Status of Management Action	Original Target	Current Target
			expected to be in production by September 2016.		
14	**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 training and documentation, and post-development maintenance.	Completion of Provost IT Team standard operating procedures is dependent on remediation of other audit issues, among other things. These other issues are expected to be completed by September 2016, with full standard operating procedures completed in October 2016.	4/30/16	10/30/16
15	**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).	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	10/31/14	8/31/17

#	Audit Report	Audit Issue	Status of Management Action	Original Target	Current Target
		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.	university's project team is holding monthly project status meetings.		