

UNIVERSITY OF MICHIGAN

REGENTS COMMUNICATION

Item for Information

Received by the Regents

April 16, 2009

Subject: Report of University Internal Audits  
**February 2009**

Background:

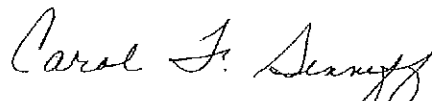
This is the report of the Office of University Audits activities for the period **February 1, 2009 through February 28, 2009**. The summaries of audits contained in this report were previously reported to members of the Regents' Finance, Audit and Investment Committee and included in discussions at Committee meetings.

Included in this report:

- Summaries of each audit report issued during the period, including Management's Plan to enhance specific control processes discussed with the audit client and presented in the report.
- Summaries of follow-up review reports issued during the period, including the actions taken by Management. Follow-up reviews are designed to give assurance that Management's Plan for corrective action has been implemented and controls are working appropriately.
- A report on the status of follow-up reviews as of **February 28, 2009**.

If you have any questions or would like additional information, please contact me at 647-7500 or by e-mail at [cseff@umich.edu](mailto:cseff@umich.edu).

Respectfully submitted,



Carol F. Senneff, Executive Director  
University Audits



## **ORIGINAL REPORTS**

Information Technology Central Services Active Directory UM ROOT Domain  
Issued February 16, 2009

# 2008-310

Active Directory is a Microsoft system for locating, connecting, and managing Windows servers, workstations, applications, and users. It is arranged in the form of “forests” consisting of one or more “domains”. The University of Michigan (U-M) operates several Microsoft Active Directory forests, including:

- Campus Forest
- Business and Finance
- Health System

University Audits completed an audit of the UMROOT Domain in the Microsoft Active Directory forest (Campus Forest) administered by Information Technology Central Services (ITCS).

The Campus Forest contains domains operated autonomously by five units:

- ITCS
- Ross School of Business
- College of Engineering
- College of Literature, Science, and the Arts (LSA)
- Housing

The largest domain in the Campus Forest is UMROOT. This domain organizes and controls access to not only ITCS resources, but also to the resources of many schools, colleges, and departments. UMROOT supports three major categories of IT systems or services:

- Central Microsoft Windows services including Central Accounts, Common Campus Exchange Service (e-mail and calendaring), and Windows Update Service
- Systems operated directly by schools, colleges, and departments
- Workstations in libraries, computing sites, and departments

These systems and services are necessary for the operation of administrative offices and academic computing sites throughout the University. If the security of the UMROOT Domain were compromised, these systems and services could be rendered unavailable, and sensitive data housed in them could be exposed.

University Audits’ primary objective was to determine whether the UMROOT Domain in the Campus Forest is being adequately safeguarded from security risks originating both inside and outside the University. To accomplish this, University Audits examined plans for corrective action that arose from two thorough risk assessments performed in 2006: one conducted by ITCS following the U-M RECON methodology, and the other by Microsoft following their Risk Assessment Program for Active Directory. We verified that corrections were made where required by these assessments, and evaluated the effectiveness of these changes. Auditors also evaluated high-risk controls recommended by the United States Defense Information Systems Agency (DISA) for Active Directory installations of all sensitivity levels.

University Audits reviewed change logs, system permissions, configuration parameters, and draft policies, and compared them to the recommendations of the risk assessments or DISA, as appropriate. Auditors also scanned the core UMROOT servers for all known security vulnerabilities.

This audit focused on UMROOT because of its pivotal role in Active Directory at U-M. In the larger context, however, there are broader Campus Forest concerns, including special challenges in trust relationships and governance.

- Risk by Association - The domains operated in the Campus Forest by the Business School, Engineering, LSA, and Housing pose risks to the UMROOT Domain that ITCS cannot control. Because of trust relationships designed into the Active Directory product, privileged access in one domain can be exploited to gain privileged access to another domain in the same forest. This means that UMROOT is only as secure as the weakest Campus Forest domain. If all domain operators can agree on a minimum set of security standards and enforce them equally across the Campus Forest, this challenge can be adequately addressed. However, the governance needed to make this happen is a challenge in itself.
- Governance - The centrality of the UMROOT Domain to Campus Forest operation means that while ITCS owns and administers the domain, policy decisions often require consultation with other IT providers and other domains in the Campus Forest.

The Windows Core Working Group serves as the forum for discussion of policy and other shared interests affecting Windows services at U-M. This Working Group is made up of system administrators from each domain in the Campus Forest, large organizational units in the forest such as Libraries and Computing Sites, and other forests such as Business and Finance and the Institute for Social Research. Over the past year, ITCS has led the Working Group to address UMROOT security shortcomings, including lack of policy and security controls, identified in prior risk assessments.

To support the Working Group's efforts, technical leaders from ITCS and IT Security Services (ITSS) also meet regularly with IT Directors from the Business School, Engineering, LSA, Housing, ITCS, and MAIS (Michigan Administrative Information Services), as well as U-M's Chief IT Security Officer. By expanding the dialogue and fostering management buy-in, these meetings free the Working Group to focus on technical issues affecting Active Directory policy.

This multi-pronged, collaborative approach is generating security policy, but very slowly. The point of enforcing policy has not yet been reached.

These two forest-wide challenges have the greatest impact on the UMROOT Domain, which has the largest stake and is the linchpin of the Campus Forest. A more uniform approach to security would also encourage units with independent forests to join the Campus Forest. A unification of Active Directory would benefit the entire University by reducing costs while simplifying and increasing collaboration across campus.

Control Issues:

1. Exposed Telnet Services - "Fiber switches" connecting the Exchange Servers' Storage Area Network (SAN<sup>1</sup>) to the campus network and the Internet have a Telnet service that allows system

---

<sup>1</sup> Storage Area Network (SAN) is a high-speed subnetwork of shared storage devices. A storage device is a machine that contains nothing but a disk(s) for storing data.

administrators to connect to the switches and manage them remotely. Data transmitted through Telnet, including login IDs and passwords, is not encrypted and could be intercepted by unauthorized personnel. These Telnet services are accessible from campus and the Internet, where the chance of “eavesdropping” is greater. These switches also have SSH<sup>2</sup> service, which is a more secure equivalent to Telnet. This issue was reported to the client immediately.

Based on the security scans conducted by University Audits, all other access to network services on UMROOT infrastructure servers is limited as designed. ITCS follows a layered security approach, including network-based firewalls, built-in Windows firewalls, VPN requirements, a central Terminal Server, and isolation of mailbox servers.

**Management Plan** - The Telnet services are used exclusively by the Exchange Servers to communicate with the SAN. Older Exchange Servers positioned outside the UMROOT firewall require the Telnet services on the SAN to be exposed. ITCS Groupware Services is retiring these servers. Once they have been retired, the SAN will be repositioned so that Telnet services are protected by the firewall.

2. Depth of Security Scans - The UMROOT Domain is comprised of a complex array of Windows servers. The Windows operating system and Active Directory services possess many unique security considerations and challenges. Periodic security scans of UMROOT servers only check for the ten most common serious vulnerabilities. UMROOT servers could pass these scans and still be highly vulnerable. The Active Directory risk assessment performed for ITCS by Microsoft in 2006 also noted the risk of relying solely on these scans, and recommended particularly thorough security scans of the domain controllers.

Security scans of the UMROOT infrastructure should test for more types of serious security vulnerabilities specific to Windows and Active Directory. ITCS should either directly conduct more comprehensive security scans, or arrange with IT Security Services to expand the scope of their testing.

**Management Plan** - ITCS Groupware Services will consult with IT Security Services to determine their options for obtaining more comprehensive security scans of UMROOT infrastructure.

3. Inactive User Accounts - User accounts in Active Directory (AD) are generally not de-provisioned (deactivated or deleted) when they are no longer needed (e.g., when the user has left the University). However, departments can optionally request the de-provisioning of an account through the IT User Advocate Office if, for example, a user’s employment were terminated for cause.

Without de-provisioning, many of the user accounts in Active Directory are essentially abandoned. If one were to be compromised, no one would realize it. An attacker could use a compromised account to disable University systems and steal University data. It is also possible for the original account holder to continue using their account to access Active Directory resources, such as Campus Computing Sites workstations, without authorization or compensation to the University.

---

<sup>2</sup> SSH (Secure Shell) is a program to log into another computer over a network.

The AD user population is based on users listed in the U-M Online Directory (UMOD). Based on a comparison of user counts between the two directories, at least 8,000 AD user accounts could be eliminated today.

However, this would not solve the problem. UMOD contains hundreds of thousands more users with no current need to access Active Directory resources. ITCS plans to address this overabundance of AD user accounts by basing them on the new MCommunity enterprise directory<sup>3</sup>. The clearer relationship data supplied by MCommunity will allow ITCS to reduce the number of AD user accounts over time by more than 280,000, by eliminating these users who do not have a current need to access resources in the Active Directory environment. This includes the 8,000 accounts noted above.

Investing resources to develop a UMOD-based de-provisioning process would not be a judicious use of resources at this point. ITCS should proceed with transitioning from UMOD to MCommunity as a source of user account data for UMROOT, including developing a process for removing users from AD. ITCS should also prepare a plan for reducing the remaining population of AD users to individuals with a current need for those resources.

**Management Plan** - When MCommunity is activated (anticipated Summer 2010), it will include checks to ensure old, unused accounts are not authorized for Active Directory access. In the interim, ITCS Groupware Services will document the criteria that will be used to determine whether a user should be granted Active Directory access, and a plan for communicating the policy change to holders of excluded accounts.

4. **Incomplete Host Hardening** - Servers are assigned to specific roles that may not require the wide variety of features and services that Windows installs by default. Disabling features and services that are not necessary to accomplish the server's designated function(s) increases security by eliminating potential sources of vulnerability. In addition, the configuration of required features and services can often be optimized for security. This process, collectively referred to as "host hardening," has been partially implemented within the UMROOT infrastructure. Hardening of servers and system administrators' workstations was a key recommendation of the 2006 RECON security assessment.

Host hardening involves enabling security features and disabling functionality that is not strictly necessary, to reduce a system's exposure to attack.

The Security Configuration Wizard is a tool that guides host hardening on Windows servers. It has been implemented on all domain controllers and all servers housed in the School of Education Building, but not on WINS (Windows Internet Name Service) or PKI (public key infrastructure) servers. PKI servers in particular are a crucial security component, issuing and validating security certificates used for encrypting web traffic, files, and folders. ITCS indicates the tool will be executed on the WINS and PKI servers when resources and priorities permit.

Internet Explorer Enhanced Security Configuration is another hardening tool designed to reduce the risk of web browsing. ITCS has not implemented the use of this tool. To compensate, they have written procedures warning administrators not to browse the web on servers. ITCS also

---

<sup>3</sup> MCommunity is U-M's new enterprise directory system. It will provide a means of exchanging information about the roles and privileges of campus community members (employees, students, alumni, retirees, emeritus faculty, and sponsored individuals), enabling more accurate and timely provisioning of IT resources.

plans to examine whether their Privileged Accounts Policy could be changed to proscribe most web browsing on servers.

Firewalls provide some compensating control by limiting access to these servers from the Internet. However, greater assurance of system security would be provided by a defense-in-depth strategy that includes across-the-board host hardening.

**Management Plan** - ITCS Groupware Services is planning to apply the Security Configuration Wizard (SCW) to all UMROOT servers while upgrading them to Windows Server 2008. The timetable for the upgrade cycle is now being determined. If servers where the SCW has not been run are scheduled late in the upgrade process, the SCW will be applied separately in the interim.

5. Justification of Privileged Accounts - Privileged accounts have generally unrestricted access to all programs, files, and resources on a computer system or network. A Privileged Account Policy for the UMROOT Domain is currently in draft. It requires periodic inspection and validation of privileged account groups, and real-time monitoring of changes. A separate policy details the specific mechanisms to be used for auditing and monitoring privileged accounts and groups. These mechanisms, which the Windows Core Working Group has not yet agreed upon, would substantially increase oversight opportunities.

The Privileged Account Policy does not specifically address role-based access. However, it lists and defines the privileged groups, describing what members are allowed to do and where they allow to do it. Many of these groups are purpose-specific (e.g., various types of Exchange email/calendaring administrators), and membership in them implies a role. The policy could be improved by specifying (when possible) which teams or job roles should belong to each group.

The Privileged Account Policy requires that privileges be limited to the minimum necessary. A separate implementation guideline outlines a tiered account structure. In this scenario, administrators are issued accounts with a range of privilege levels appropriate to their job duties, and choose the account with the least privilege necessary to accomplish the task at hand. This arrangement has not yet been approved by the Windows Core Working Group, and much work remains to be done in defining the privilege levels and assigning membership appropriately.

Privileged accounts in other domains besides UMROOT are outside the scope of this audit. However, as we noted at the outset of this audit, based on a number of sources, the privileges for these accounts can extend to the forest level, posing a risk to assets in UMROOT.

To improve security, the draft policies related to privileged accounts should be finalized. The draft policies on privileged accounts and monitoring of those accounts are generally sound. They could be improved by clarifying which teams or job roles should or do belong to each privileged group. Such a mapping could resemble the tiered administrative account structure that management proposes to help administrators use the least privileges necessary to perform a task.

**Management Plan** - The tiered administrative account structure has been implemented and is being used by Windows system administrators. ITCS Groupware Services will extract the memberships of the various privileged groups and document the precise makeup and the reasons for inclusion so that privileged access is clearly justified.

6. Caching of Domain Credentials - Windows uses "credential caching" to store an encrypted copy of the most recently used accounts and passwords to ensure these users can log on even if no domain controllers are available to authenticate them. This feature is especially important for

laptops, which may be used off-network. Caching of domain credentials is permitted on servers and workstations in the UMROOT domain. If a workstation containing cached credentials is compromised, the credentials can be obtained by using a number of tools. This poses the greatest risk to privileged accounts. The 2006 RECON assessment recommended this feature be deactivated.

University Audits recommends amending the Privileged Accounts Policy to require that privileged accounts not be used to log on directly to workstations – especially laptops. This would help mitigate the risk of highly sensitive account credentials being captured in the event of a workstation compromise or laptop loss. Communicate the new requirement to staff, and enforce it appropriately.

**Management Plan** - This requirement has been added to the Privileged Accounts Policy, and applies not only to desktop and laptop computers, but also to member servers (servers that are not Domain Controllers). The policy has been discussed within ITCS Groupware Services and with ITCOM Operations, the two most impacted teams. Groupware Services will issue a final announcement of the policy via email to ensure all affected system administrators are aware of it.

7. Absence of Operating Level Agreement - There is no operating level agreement (OLA) documenting the level of service the UMROOT Domain is expected to provide to members of the Campus Forest. OLAs typically document management's expectations of services to be delivered, performance tracking and reporting measures, problem management and dispute resolution procedures, customer duties and responsibilities, and security arrangements. The risk of inadequate controls in each of these areas is increased without sufficient documentation such as an approved, current OLA.

The Windows 2000 Infrastructure Policies lay out many of the parameters an OLA between ITCS and forest members would contain, including:

- ITCS commitments to provide Active Directory services to the campus 24 hours a day, 7 days a week; and monitoring and maintenance 24 hours a day, 365 days a year
- ITCS responsibilities for maintaining and administering the core directory service, DNS<sup>4</sup>, Exchange, and other services
- Maintenance windows and procedures for announcing maintenance
- Channels through which ITCS will communicate with UMROOT participating units
- ITCS responsibilities for supporting and administering users and services at the UMROOT level
- ITCS responsibilities for policing the forest, enforcing policies
- Unit responsibilities for supporting and administering users and servers in departmental OU (organizational units) and departmental domains
- Policies and procedures which any unit operating a domain in the forest (including ITCS) must follow

This document, however, has not been updated since 2001, and it does not appear to be binding. There is no space for official sign-off.

The Windows 2000 Infrastructure Policies should be updated and adapted to serve as an OLA between ITCS and members of the Campus Forest. Management from ITCS and member areas should approve and sign off on the agreement. Adjudication procedures for violations of the

---

<sup>4</sup> Data Source Name provides connectivity to a database.



OLA should be developed and included. In particular, security requirements should be expanded. The document should refer to more specific policies and procedures for change management, configuration standards, and security as needed.

**Management Plan** - The Windows Leadership Group recently agreed to collapse non-UMROOT domains into UMROOT organizational units (OUs), which will significantly alter the relationships and responsibilities documented in the Operating Level Agreement. ITCS Groupware Services will therefore develop an updated agreement reflecting the planned restructuring. A draft agreement will be drawn up based on existing OU customers, and will be revised substantially as the forest collapse takes shape, and technical and support processes change.

8. Informal Change Management - In practice, although changes affecting the entire UMROOT domain are communicated in advance, recorded, and tested before implementing in production, these practices are largely informal, not based in policy, and could be better integrated and documented.

Major changes, such as installation of the UMROOT firewall, are discussed and approved by the Windows Core Working Group. However, these discussions and approvals are recorded only in emails. Meeting minutes are not taken, and the practice is not documented.

Schema changes (a special subcategory of major change that affects the entire Campus Forest) are sent to the Windows 2000 Listserv for a two-week comment period, and implemented if there are no irreconcilable objections. This practice is documented in "ITCS Windows 2000 Infrastructure Policies at the University of Michigan" posted on the ITCS website. University Audits successfully traced back a schema change from May 2008 to verify that announcements and change records were made appropriately.

Smaller changes are discussed at daily meetings of the ITCS Groupware Services group. Approval is neither sought nor given. This practice is not documented.

All changes are recorded in the Windows Change Log, a shared calendar on the ITCS Exchange Server. Administrators search this log to determine what changes were made to Active Directory during a given time period. The change log is separate from the announcements and discussions, requiring extra documentation and making cross-referencing more difficult.

These change mechanisms work, but they rely on a large amount of free-form description and discussion, and do not provide much assurance that changes have actually been considered and accepted by UMROOT stakeholders. If a dispute were to arise over whether a change was properly vetted, the entire history of the change would need to be reviewed. This requires collecting the record of when a change was made, what it involved, the purpose, test results, authorizations, and discussion of concerns and potential issues. Under this system, those elements could be stored in emails, or calendar events, or even separate files, with no single identifier to link them together.

Risk and vulnerability assessment activities are not integrated with change management so they may not always be considered before a change is implemented. The 2006 RECON security assessment highlighted a need for post-install, pre-production vulnerability scans for new or changed applications. The client indicates that ITCOM has integrated these functions to some degree, making them a potential role model. Services taken over for management by ITCOM Operations, such as messaging servers, must fit their vulnerability and exposure guidelines.

**Management Plan** - ITCS Groupware Services will examine available options for unifying its change documentation and approval processes, including the Remedy system used by ITCOM and the FootPrints service offered elsewhere in ITCS. The selected process or system will simplify tracing the history of specific changes, and provide assurance that changes are suitably vetted, approved, and communicated.

9. Disaster Recovery Plan - The UMROOT Forest Disaster Recovery Procedures contain detailed technical steps for restoring Active Directory. The steps cover the type of backup needed, the options for restoring, and the configuration of services. Several types of recovery scenarios are covered, including loss of one or multiple domain controllers, or an entire domain. Special configurations applicable to domains other than UMROOT (e.g., Engineering or Business School) are noted.

As detailed as the disaster recovery procedures are, they do not address some of the broader operational issues that are typically covered in such plans, such as actual disaster scenarios, coordination of recovery efforts, communication methods, and how the plan will be tested and kept current. A disaster recovery plan needs to cover all of these areas to ensure timely and effective recovery including the following.

- Expand the UMROOT disaster recovery plan to address:
  - Who will lead Active Directory recovery efforts, who may be called on to assist with and support recovery, and how they will communicate (e.g., if U-M email is not functioning)
  - How and what types of information ITCS will communicate to stakeholders in subdomains and organizational units, and the user community
- Establish a periodic schedule (every one to two years) for reassessment and retesting of the recovery process, including documentation of lessons learned and any revisions to the plan.

Some scenarios, such as the loss of a data center, could be addressed in broader ITCS disaster recovery or business continuity plans. If so, those sources should be referenced appropriately.

**Management Plan** - ITCS Groupware Services will incorporate the recommended elements into the UMROOT disaster recovery plan as it is rewritten for Windows Server 2008.

Based on University Audits observations and testing, internal controls in the UMROOT Domain of the Campus Forest are partially adequate, and improving. Improvements in managing and ensuring the accuracy and timeliness of user access to UMROOT-supported resources hinge on the continuing deployment of the MCommunity enterprise directory project.

Current controls provide a moderate level of assurance that UMROOT is safeguarded from threats outside the University, due in large part to the addition of a network firewall to protect core UMROOT servers. Assurance of protection from internal threats can be improved by formalizing change control practices, tightening the issuance and expiration of user access, and issuing additional guidance to system administrators.

A follow-up to the outstanding issues will be conducted in the fourth quarter of fiscal year 2009.

Significant challenges in the areas of governance and trusted-system risk are gradually being addressed at a campus-wide level. Resolution of these issues will simplify collaboration across campus by permitting common calendaring, email, and file storage services, and may allow significant cost savings by eliminating servers and related maintenance. A verbal agreement reached in December 2008 to merge all Campus Forest domains into UMROOT is another step to achieve these goals.

## FOLLOW-UP REPORTS

University of Michigan Health System Emergency Department

# 2008-112

Original Report issued May 9, 2008

Follow-up Report Issued February 18, 2009

Management has taken appropriate corrective action or plans are well underway on all audit recommendations, as indicated below. **This audit is closed.**

### *Discharge Process Opportunity*

Plans are underway to equip the Emergency Department with a formal check-out location in fiscal year 2010. The redesigned area will provide a private and secure location to handle post visit patient counseling, including financial matters such as insurance and cash collection.

### *Medical Documentation*

Emergency Department management provided additional training and now regularly monitors to ensure completion of transfer documentation.

**Open Audits Follow-up Table  
February 28, 2009**

Audit Title	Report Date	Issues	Expected Completion
Physical Security at Harlan Hatcher Graduate Library 2008-303	9/2/08	Emergency exits; alarms and monitoring systems; fire safety; safety of patrons and staff; storage; deferred maintenance; procedures	March 2009
University Health Service HIPAA IT Security 2008-309	9/2/08	Practice management system; verification of internet access; intranet tools server; data access procedures; security policy	June 2009
College of Engineering Research Computing 2008-302	10/29/08	Vulnerable systems; unnecessary services; unknown ports and services; unknown systems; unsupported devices; users with system administrator privileges; updating firewalls; procedural documentation	May 2009
Institute of Continuing Legal Education 2008-202	11/24/08	Removal of access for terminated employees; role-based access; website usage monitoring; backup power testing; security assessment	March 2009
Michigan Administrative Information Services Grade System: Web-based Grade Changes 2008-114	12/23/08	Role assignments; customization; two-factor authentication	July 2009
Intercollegiate Athletics Paciolan Ticket System 2009-302	01/09/09	System administrator documentation; system scan for PCI/DSS compliance	March 2009
Information Technology Central Services Active Directory UMROOT Domain 2008-310	02/16/2009	Telnet services; security scans; user accounts; host hardening; privileged accounts; caching of domain credentials; operating level agreement; change management; disaster recovery plan	June 2009
Medical School Pulmonary and Critical Care Medicine Operational Review 2008-207	9/26/08	Grant key personnel; travel and hosting	March 2009
University of Michigan Hospitals and Health Centers Cashier's Office 2008-206	10/17/08	Segregation of duties; bank statement reconciliation and check writing practices; follow-up of outstanding vouchers; duplicate facility refunds	June 2009
UMHHC Payroll and Timekeeping 2008-110	1/30/09	Human Resource Management System access; systematic data integrity; payroll expenditure analysis; roles and responsibilities	October 2009
Medical School Administrative Internal Control Review 2008-208	1/30/09	IT strategic planning; reconciliations; gift fund usage; IT security; fire drill regulations	September 2009

Resident Duty Hours 2008-102	1/30/09	Duty hours compliance	September 2009
University Human Resources Family and Medical Leave Act 2007-403	12/17/07	Training; update relevant SPG sections; written notifications	First follow-up was completed August 2008
			Second follow-up March 2009
Transportation Services 2007-101	1/28/08	Controls over physical access; system user access levels; commercial driver's license testing; vehicle inventory monitoring; fuel inspection upon delivery; gross pay register review; imprest cash fund; formal policies and procedures	March 2009
I-9 Employment Verification Process 2007-823	1/29/08	Filing timeliness; automation; training	March 2009
University of Michigan – Flint Chancellor's Office 2008-205	9/30/08	Roles and responsibilities; conflict of interest; disaster recovery; reconciliations; segregation of duties; procedures	March 2009
Plant Operations Construction Services 2008-602	11/4/08	Project management reporting	June 2009
Sponsored Programs Subrecipient Monitoring 2008-501	11/21/08	Written guidance for PIs; subcontract template	June 2009
School of Music, Theatre & Dance Fiscal Responsibilities 2008-815	11/26/08	Financial oversight and monitoring; several procurement and payroll observations; documented procedures; written delegation of authority; imprest cash management;	July 2009
Intercollegiate Athletics Business Office Fiscal Responsibility 2008-210	12/23/08	Reconciliations; procurement; cash controls; overtime; check writing; mobile devices; equipment disposition; hiring and termination procedures	April 2009
William L. Clements Library 2008-212	1/26/09	Grant compliance; endowment agreements; collection management; insurance coverage; physical safety and security; reconciliations; recharge rates	September 2009
University Press Inventory and Receivables 2008-203	1/30/09	Accounting checklists; inventory analysis	September 2009

