UNIVERSITY OF MICHIGAN

REGENTS COMMUNICATION

Item for Information

Subject: Report of University Internal Audits

Attached is the report of activities completed by the Office of University Audits for the period **October through December 2, 2013**.

Included in the report are a:

- Summary of each audit report issued during the period, including Management's Corrective Action Plans. These audits were presented at the Regents' Finance, Audit, and Investment committee meeting in July.
- Summary of each follow-up review memo issued during the period, including the actions completed by management. Follow-up reviews are designed to provide assurance that Management's Corrective Action Plans have been implemented, are working as intended, and are sustainable.
- Table of open audit issues as of **December 2, 2013**, including estimated completion dates.

If you have any questions or would like additional information, please contact me at 647-7500 or by e-mail at jmoelich@umich.edu.

Respectfully submitted,

Jeff Moelich

Jeffrey M. Moelich, Executive Director
University Audits

Original Reports

ITS Implementation of M+Box 2013-310

Report issued October 2013

Executive Summary

1. **Overall Conclusion**

   M+Box is an important initiative to support the Productivity and Collaboration Service Portfolio of NextGen. Overall, ITS established an effective governance structure over M+Box and appropriate controls are in place to manage key risks. During development and deployment of M+Box, ITS identified and proactively addressed key risk exposures. In response to the audit, management has committed to strengthen the control environment through creation and review of daily audit reports to monitor user provisioning and actions of M+Box administrators, and to develop a de-provisioning process for accounts of users no longer affiliated with the University.

2. **Summary of High Risk Audit Issues**

   For this audit, University Audits did not identify any high-risk issues[1].

3. **Key Activities Audited and Conclusions by Sub-Activity**

   The scope of the audit was determined based on an assessment of the risks associated with the management and protection of data assets that reside in Box.com. This process included input from ITS management and interested parties from other University functions. The table below lists the key activities audited, along with the overall risks of the audit issues identified for each sub-activity.

Key Activities Audited / Conclusions by Sub-Activity

Governance	Auditing and Assessment	Monitoring	Contractual Agreements	Control of User Accounts	Incident Response
🟩 Operations	🟨 Audit Logs	🟩 Performance	🟩 Legal Requirements	🟨 Account Authorization	🟩 Notification
🟩 Security	🟩 Independent Audits	🟩 Security	🟩 Roles and Responsibilities	🟨 Account Provisioning	🟨 Escalation
	🟩 Accuracy of Audit Trails		🟩 Service Level Agreement	🟩 Account De-Provisioning	🟩 Response Time
	🟩 Protection of Audit Trail				🟩 Responsibilities
	Legend	🟥 High Risk Audit Findings	🟨 Medium Risk Audit Findings	🟩 No or Low Risk Audit Findings	

[1] University Audits categorizes each audit issue based on the risk it presents to the audited unit (in this case, M+Box), not to the University as a whole.

Note: Section B of this report (Audit Issues and Management Action Plans) provides details of the medium risk issues identified. Low risk issues were communicated to the unit management and are not included in the report.

B. Audit Issues and Management Action Plans

1. Review of Administrator Accounts — **Medium**

Issue: System administrators do not review administrator accounts.

Risk: Compromised or illegitimate administrative accounts could go undetected, which could enable unauthorized changes to user accounts or system configurations.

Support: Administrators have the access and tools necessary to run reports. Procedures have not been developed to identify what information should be extracted and how often the reports should be run indicating operational and security events. In addition, M+Box administrators have the ability to create, modify, and delete user's accounts and files.

Recommendation:

a) ITS should create reports to monitor the actions of M+Box administrators. These reports should be run and reviewed on a frequent basis.

Management Action Plan: Management will create and run reports showing the actions of M+Box administrator accounts. These reports will be scheduled to run and reviewed on the following schedule:

- automated daily email summary at midnight of all administrator activities sent to box.admins@umich.edu
- automated real-time alerts (cron job every 5 minutes) of administrator impersonations, deletes (and other critical activities as identified) sent to box.admins@umich.edu
- manual quarterly review of Box administrator activities by administrators to verify and validate the response to real-time alerts

Action Plan Owner: M+Box Service Owner

Expected Completion Date: December 31, 2013

2. De-Provisioning of User Accounts — **Medium**

Issue: Administrators do not always de-provision accounts when users leave the University.

Risk: Increased costs due to accounts for users no longer affiliated with the University.

Recommendation: ITS should continue to develop procedures for timely de-provisioning of M+Box accounts for users that are no longer affiliated with the University.

Management Action Plan: Management will

2. De-Provisioning of User Accounts **Medium**

Support: ITS is creating a process to de-provision M+Box accounts that no longer have an active University account. Users of these accounts would be able to retain all the data that resides in Box.com, but the data would no longer be accessed through U-M or count against the University's total storage space. As usage of the M+ Box services increases, the need for timely de-provisioning of accounts will also grow.

develop procedures to de-provision M+Box accounts of users no longer affiliated with the University. This work, which requires resources from MCommunity, has begun. As the project progresses, a better estimate of completion date will be possible.

Action Plan Owner: M+Box Service Owner

Expected Completion Date: December 31, 2013

College of Engineering Research Software Licensing 2013-310

Original report issued October 2013

A. Executive Summary

1. Overall Conclusion

Overall, College of Engineering Central Information Technology (CAEN) provides effective administration of centrally provisioned research software in the College of Engineering (College or CoE). However, actual research software use is not always consistent with terms of the licensing agreements. Violations of licensing agreements may constitute copyright infringement and could result in financial penalties or restrictions on future use.

Proper licensing of research software for the University environment is difficult because the same piece of research software may require different licenses based on who uses the software and how it is used. Licenses for teaching and learning purposes are often available on a fee free basis, while licenses for academic and commercial research purposes generally require payment of a licensing fee. Further, research software vendors vary greatly in how they define commercial research, which is generally dependent upon funding source, proprietary nature, or commercial viability of the research. Software providers are most concerned with fee-free academic software used in academic research and commercial research conducted without required licenses.

To enhance alignment of software use with the terms of licensing agreements, CAEN has committed to several actions. CAEN plans to review every title in the CoE research software catalog to determine whether the actual use of each piece of software is consistent with terms of the licensing. To increase awareness of software licensing requirements, CAEN will provide further user guidance, post research restriction signage in student labs, and update research software restrictions contained in user login banners. Although not feasible at this time, going-forward CAEN will periodically assess the implementation of a multi-tiered account access structure for logical access to research software that would allow users to have credentials (i.e., access to specific types of research software) based on their user category and job responsibilities.

CAEN is also adopting other changes to enhance the licensing processes. These changes include improving control over software licensing agreements accepted directly by users (i.e., “click-through” licensing agreements for software downloaded directly by users) and potentially creating separate environments (i.e., labs) for use of specific types of research software. Annually, CAEN plans to review research software used in the College and included in Flux to make sure actual use continues to be consistent with the terms of the licensing agreements. Finally, management plans to require CoE departments to monitor and track each piece of software and maintain licenses in a central and secure location.

2. Summary of High Risk Audit Issues

For this audit, University Audits did not identify any high-risk issues.

3. Key Activities Audited and Conclusions by Sub-Activity

The scope of the audit was determined based on an assessment of the risks associated with research software licensing within the College of Engineering. This process included input from CoE Information Technology, CAEN management, and interested parties from other University functions. The table below lists the key activities audited, along with the overall risks of the audit issues identified for each sub-activity.

Key Activities Audited / Conclusions by Sub-Activity

License type and Use	Software Acquisition	Term./X-fer of licenses	Research Software	Training and Awareness	Vendor Monitoring
🟨 Teaching and Learning Licenses	🟨 License Compliance	🟩 End of Contract/Grant	🟨 Unanticipated Research Use	🟨 Knowing when to Use a License	🟩 Fines and Penalties
🟩 Contract and Grant Compliance	🟩 Requests for Software	🟩 Multi Project Software	🟨 Commercial Funding	🟩 Department Risk Assumption	🟨 End User Licensing Agreements
🟨 Use in Educational Venues	🟨 Purchase of Software (2)		🟩 Use in Work for Hire	🟩 Sharing of Media	
🟩 Research Software Use by Students	🟩 Licensing by Department		🟩 Use in Joint Ventures		

Legend	🟥 High Risk Audit Findings	🟨 Medium Risk Audit Findings	🟩 No or Low Risk Audit Findings

Note: Section B of this report (Audit Issues and Management Action Plans) provides details of the medium risk issues identified. Low risk issues were communicated to the unit management and are not included in the report.

4. Audit Objectives

- Software used for research is accurately identified, correctly licensed, and effectively tracked
- Acquisitions of research software are controlled and reviewed for appropriateness of licensing
- Research software is removed from hardware where it no longer belongs and licenses are disposed of as required
- Researchers and other stakeholders are being made aware of the licensing and use requirements for research software
- For existing research projects, research software is used only as licensed

5. Context and Key Considerations

Employing over 100 people in 11 groups, CAEN is responsible for providing IT resources to support teaching and learning in the College of Engineering. They have responsibility for 30 labs that house 210 research software applications licensed from 85 different vendors. These labs support a population of 9,500 students (including 1,500 PhD students), a total tenured track faculty of 367 and 123 researchers. The breadth and diversity of this support effort increases the complexity of licensing research software required to meet the College's needs. CAEN also serves individual departments in the College by helping to license research software required for specific departmental purposes.

Licensing research software is particularly complex. Licensing requirements are generally based on (1) who uses the software (e.g., educator or researcher), (2) how the software is used (e.g., teaching and learning, academic research, or research for commercial purposes), and (3) where the software is used (e.g., classroom or lab). A typical license grants certain end-users permission to use software for a specified purpose.

Just because a valid license for software is in place does not necessarily mean the software can be used for research. Further, research conducted by anyone other than undergraduate or master degree students requires a license that allows such research. There are three types of licenses for research software:

- Teaching and Learning
- Academic Research
- Commercial Research

Licensing fees generally increase as licenses move toward the commercial side, with commercial research typically acquired at full price. Restrictions also tend to diminish as licenses move toward commercial.

B. Audit Issues and Management Action Plans

1. Software Licensing and Usage — Medium

Issue: Research software is sometimes used for purposes that are inconsistent with terms of the underlying licensing agreements.

Risk: Vendors are proactively asserting their rights under software licensing agreements and may enforce consequences, such as monetary penalties or restricted use.

Support: Before using research software, users do not always understand what type of research license is required.

a) Some students, faculty, and staff use software licensed for teaching and learning purposes to conduct research.

b) Flux (Linus-based high-performance computing cluster) is an environment dedicated to research; however, the academic version of the EPD 6.2-2 software is installed and available to users. The EPD license explicitly excludes use of the software for commercial research.

c) PhD candidates, non-qualified faculty, staff, visiting scholars, and other researchers use student labs that contain software restricted to use for teaching and learning purposes. Student labs are provisioned by CAEN to include an array of engineering software, most of which is licensed for teaching and learning, and not research.

d) Visiting scholars, faculty, and PHD students do not have a venue where they can use software licensed for research.

Recommendation:

b) CAEN should provide guidance to students, staff, faculty, visiting scholars, and other research software users concerning the different types of licenses. In addition, CAEN should regularly monitor the use of research software for compliance with licensing requirements.

c) Flux management should replace the academic EPD license with a research version, examine the licenses for all other Flux offerings, and before installing software, review the license to verify the terms are consistent with the intended use.

d) Signage should be posted in student labs stating research is not to be conducted on lab computers. Further, a click-through agreement should be used specifying the labs are for teaching and learning, and computing resources are not to be used for research.

d) CAEN should provide an environment that could be used by PhD candidates, non-qualified faculty, staff, visiting scholars, and others who are actively performing research.

e) CAEN should consider implementing a multi-tiered account access structure to CAEN resources, so that users can access only software consistent with their credentials and job responsibilities.

Management Action Plan:

a) Web content that provides overall guidance about the use of software licensed for lab use by CAEN will be provided. Existing web content specific to each title will be updated to include license restrictions. Descriptions of typical appropriate use will

1. **Software Licensing and Usage** — **Medium**

be provided. CAEN will provide assistance and guidance for researchers who have requirements that cannot be supported with the license terms that apply to the titles that CAEN provides (e.g., COMSOL, ABACUS).

b) Developing an environment that supports un-restricted use of software, including what vendors consider to be commercial use is an important goal of CAEN.
All licenses in use on FLUX are being reviewed to verify that they accommodate non-commercial academic research use.

c) Signage will be provided in CAEN student computing labs. Login banners will also be updated. Click-through functionality as part of the login process will be assessed. MiLinc will be investigated as one option for supporting click-through agreements.
When possible, instruction-only licenses will be replaced with licenses that also allow non-commercial academic research. When that is not possible, computers will be identified in terms of which license(s) to which they provide access.

d) Depending on the demand and interest from faculty, a shared college-wide lab that supports licensing for broader research use will be established. An option is to support the work in departmental locations that obtain their own licenses.

e) Pending progress on graduated CAEN accounts, CAEN student computing labs will be accessible by only students and access to CAEN-licensed software will be limited to those locations. Access to titles outside of those settings, in departmental labs, for example, will be reviewed on a case-by-case basis starting this fall.

CAEN staff are investigating technology (application virtualization and access control

1. Software Licensing and Usage **Medium**

lists and group memberships). Institutional role and identity data will be reviewed for possible use.

Non-student access to labs will be granted on a case-by-case basis as well. Software use requirements for other users will be gathered when requests for access are received by CAEN.

Action Plan Owners:
a), c), d) and e) Associate Director Software Application Services and Faculty Liaison
b) Director of High Performance Computing

Expected Completion Date:
a), c), d) and e) December 2013
b) June 2014

2. Software for Commercial Research **Medium**

Issue: CAEN has not identified labs that require software licensed for commercial research.

Risk: Using teaching and learning or non-commercial research software for commercial research purposes may result in liability for the University, monetary penalties, or restrictions on future use.

Support: Research software vendors vary greatly in how they define non-academic (commercial) research. However, the characterization of research as commercial is generally based upon its funding source, proprietary nature, or commercial viability. When commercial research is conducted in College of Engineering labs, a higher level of licensing is required.
We examined the software inventory on computers in 12 Mechanical Engineering

Recommendation: CAEN should work with the departments in the College of Engineering to identify those labs where the commercial nature of research conducted requires commercial research licenses and work with researchers to upgrade their licenses.

Management Action Plan: For those researchers with significant commercial funding, licensing in their labs will be reviewed and licenses will be upgraded, if necessary.

Action Plan Owner: Associate Director Software Application Services and Faculty Liaison

Expected Completion Date: June 2014

2. Software for Commercial Research

Medium

research labs and determined six had research contracts with commercial funding sources. However, commercial software licenses were not in place. Although no specific license violations were noted, risks of licensing violations exist.

3. Acceptance of "Click-Through" Licenses

Medium

Issue: Users sometimes directly download software to fulfill U-M responsibilities, which often requires acceptance of third-party "click-through" licensing agreements.

Risk: The University may be bound to unfavorable terms and conditions contained in software licenses accepted by users.

Support: "Click-through" licenses are agreements that appear as one of the first screens of a software installation program. The installation is allowed to continue if the user clicks "I Agree," "I Accept," or something similar; otherwise the software cannot be installed.
Users are able to download and install software that has not been reviewed or licensed by CAEN or the College of Engineering. The licenses for such software may restrict use to personal or non-research purposes.

Recommendation: CAEN should examine software loaded on lab machines to verify that is licensed correctly and that the terms of the licenses do not subject the College to an unacceptable level of risk. CAEN should work with Procurement Services and the Office of the General Counsel to define procedures and create training to respond to click-through requests when loading software.

Management Action Plan: CAEN staff will meet with Procurement Services and Office of General Counsel representatives to review and document appropriate review and acceptance of click-through licensing agreements for software used in research. Material will be provided on the web and shared in meetings with applicable groups in the College of Engineering.

Action Plan Owner: Executive Director of Information Technology and CAEN

Expected Completion Date: December 2013

4. Tracking of Software Licenses in Nanotechnology Labs

Medium

Issue: Licenses could not be located for all software installed in the Nanotechnology Labs.

Risk: The College may be unaware of licenses held and be unable to comply with contractual terms and conditions, which could lead to monetary penalties or restricted use by

Recommendation: Any software for which a valid license cannot be found needs to be relicensed or removed from College computers. Management should develop a tracking system that will account for all software licenses held by the College. All licenses should also be stored in a centralized and secure location.

4. Tracking of Software Licenses in Nanotechnology Labs

Medium

software vendors. Further, untracked software may not be licensed.

Support: Licenses for software in the Nanotechnology Lab is not tracked and licenses for three pieces of software could not be located:

- Concorda PSLF
- ViewMate
- Eagle Layout Editor

No central asset management tool exists in the College of Engineering to track software. The inability to produce a valid license is tantamount to not licensing the software at all.

Management Action Plan: The license for the Eagle Layout Editor was found subsequent to the audit. For the other pieces of software, Nanotechnology will be instructed to relicense or remove the software. The importance of managing licensing records will be reviewed with College of Engineering departmental and research administrators in one of their respective standing meetings. This will be included in an agenda for an annual IT update that is given to these groups. In addition, a central repository for licenses will be created.

Action Plan Owner: Associate Director Software Application Services and Faculty Liaison

Expected Completion Date: December 2013

5. Creation of a Research Lab

Medium

Issue: Visiting scholars, faculty, and PhD students do not have a venue where they can use software licensed for research.

Risk: Lack of dedicated facilities where these special users can use licensed research software may lead to licensing violations and subsequent fines and penalties.

Support: Faculty, PhD candidates, visiting scholars, and other researchers do not have a dedicated environment to conduct research and often use student computer labs.

Recommendation: CAEN should provide a dedicated environment for College of Engineering personnel and affiliated users actively performing research.

Management Action Plan: When possible, instruction-only licenses will be replaced with licenses that also allow non-commercial academic research. When that is not possible, computers will be identified in terms of which license(s) to which they provide access. Depending on the demand and interest from faculty, a shared college-wide lab that supports licensing for broader research use will be established. An option is to support the work in departmental locations that obtain their own licenses.

Action Plan Owner: Executive Director of Information Technology and CAEN

5. Creation of a Research Lab

Medium

Expected Completion Date: June 2014

6. Definition of PhD Students

Medium

Issue: PhD candidates are not defined as students in research software licenses.

Risk: Exclusion of PhD candidates from the definition of students may force the College of Engineering to purchase more expensive research-oriented licenses and may increase the likelihood of licensing violations.

Support: Software vendors are becoming increasingly stringent in terms of who can use academically licensed software. Engineering software is often provided to institutions of higher learning at deeply discounted prices, provided the software is used for teaching and learning, and not research.

Recommendation: CAEN should work with Procurement Services and the Office of General Counsel to clarify the definition of a student for licensing research software. Purchasing templates and current and future licenses should be revised to include provisions defining PhD candidates as students when necessary.

Management Action Plan: CAEN will work with Procurement Services and the Office of the General Council to define PhD candidates as students for the purpose of research software licensing and reflect this definition in contracts.

Action Plan Owner: Executive Director of Information Technology and CAEN

Expected Completion Date: June 2014

7. Recording Software Purchases to Program Codes

Medium

Issue: The College of Engineering is using invalid program codes to record software purchases.

Risk: Misclassification of software purchases could result in incorrect account monitoring and analytics, and potentially effect management decisions.

Support: The University has a valid set of program codes for coding purchases, all of which are alphabetic. Over 950 software purchases in 2012 were coded as '10000,' which is actually a fund code indicating an unrestricted fund.

Recommendation: Record software purchases to the correct University program codes.

Management Action Plan: CAEN will review guidelines from both Financial Operations and Procurement Services and develop web content and training material for use in the College of Engineering.

Action Plan Owner: Associate Director Software Application Services and Faculty Liaison

Expected Completion Date: December 2013

8. Software Purchases Classified as Professional Licenses

Medium

Issue: Software purchases are sometimes coded as professional licenses.

Recommendation: CAEN should examine purchases classified as licenses and reclassify

8. Software Purchases Classified as Professional Licenses	Medium
Risk: Misclassification of software purchases could result in improper analytical results and incorrect management decisions **Support**: Not all coding is done centrally, resulting in variations in the coding of purchases: • Detailed review of the College of Engineering Statement of Account (SOA) for 2012 revealed numerous instances where software purchases were charged to an account called licenses. The software licenses should be charged to computer software. • 'Licenses' code is only used for professional licensure such as that of Notary Publics.	those that refer to software purchases. Going-forward, the 'Licenses' classification should be periodically reexamined, and software purchases should be reclassified. **Management Action Plan**: CAEN will review guidelines from both Financial Operations and Procurement Services and develop web content and training material for use in the College of Engineering. **Action Plan Owner**: Associate Director Software Application Services and Faculty Liaison **Expected Completion Date**: December 2013

Donor & Alumni Relationship Tool (DART) 2012-103

Original report issued October 2013

A. Executive Summary

1. **Overall Conclusion**

The University of Michigan and vendor, Blackbaud, collaborated to co-develop an enterprise development system to meet University of Michigan requirements. The process is a long-term project that will take five to seven years for full implementation. The first phase of the project, which focused on deployment of a functional system, is complete. The Office of University Development (OUD) and Information and Technology Services (ITS) are in the process of implementing an upgrade, scheduled for Spring 2014. The upgrade will focus on streamlining processes and enhancing functionality. The first phase was very complex, and OUD and ITS effectively brought the system online and DART is functioning in a reasonable manner. While the system is functioning adequately, University Audits identified several opportunities for improvement:

Security: OUD and ITS have demonstrated that protection of sensitive data and the security of DART information systems are high priorities. While vulnerabilities exist in the infrastructure, some mitigating controls reduce the overall risk. OUD and ITS have agreed to prioritize the remaining risks as indicated in their management action plans (see section B of the report).

Effectiveness and Efficiencies: System effectiveness and efficiency should continue to improve as additional modules come online and upgrades are implemented. During this process, it is important for OUD and ITS to continue to clarify user expectations. Additionally, they should address concerns of the users that may not have rated as high priority prior to stabilizing the system and preparing for the upgrade.

2. Summary of High Risk Audit Issues

For this audit, University Audits did not identify any high-risk issues.

3. Audit Objectives

- Management of DART development and implementation was in accordance with the Master Agreement and Statement of Work.
- OUD and ITS responded to requests for assistance in a timely manner.
- Training programs were effective and there are processes in place to handle post go-live training needs. Alternatives to formal training programs are effective.
- Users have access to reports necessary to monitor their business processes and ability to customize reports specific to their needs.
- Users understand the system and expectations, and are able to use DART to effectively complete their business activities.
- Performance is effectively monitored and feedback provided to the users.
- DART networks and ancillary web applications are adequately protected from vulnerabilities.
- Adequate security exists over private personal information (PPI).
- Systems and sensitive data are encrypted.
- Systems management is effective for production processes.
- Accounts are provisioned and de-provisioned timely and based on proper authority.
- Migration from test environments to production is adequately controlled.

4. Key Activities Audited and Conclusions by Sub-Activity

The scope of the audit was determined based on an assessment of the risks associated with the development, implementation, and operation of DART. This process included input from ITS, OUD, Unit Development Offices, and interested parties from other University functions. The table below lists the key activities audited, along with the overall risks of the audit issues identified for each sub-activity.

Key Activities Audited/Conclusions by Sub-Activity

IT Security	IT Security (continued)	IT Operations	Migration	Training	Contract Management
🟨 Network Vulnerability	🟨 Encryption of PPI	🟩 Documentation	🟩 Roll Back	🟩 Training Process	🟩 Vendor Commitments & Performance
🟨 DART Vulnerability	🟩 Segregation of Duties	🟩 Audit Logging	🟩 De-identification of PPI	🟨 Training Resources	🟩 Payment Reconciliation
🟨 DevWeb Vulnerability	🟨 Access Revocation	🟩 Failover	🟩 Change Management	🟩 DART Upgrades	🟩 Dispute Resolution
🟩 Penetration Test	🟩 Force SSL	🟩 Performance Monitoring	🟩 System Configuration		🟩 Vendor (Blackbaud) Deliverables

Customer Service	Reporting	System Management	Oversight
🟩 Performance Standards	🟩 Walkthrough	🟨 Policies, Procedures, and Standards	🟩 Communication
🟨 Help Desk	🟩 Documentation	🟨 User Feedback	🟨 System Utilization
🟩 Donor Feedback	🟩 Accuracy	🟩 Project Completion	🟩 Campaign Oversight
	🟩 Blackbaud Support	🟩 Gift Reporting	🟩 Upgrades and Work-Arounds
		🟩 Stewardship, Project Management	

Legend		
🟥 High Risk Audit Issues	🟨 Medium Risk Audit Issues	🟩 No or Low Risk Audit Issues

Note: Section B of this report (Audit Issues and Management Action Plans) provides details of the medium risk issues identified during the audit. Low risk issues were communicated separately to the unit management and are not included in the report.

5. Context and Key Considerations

When the University of Michigan decided to replace the Donor, Alumni, and Constituent Database (DAC), a business case was developed with input from detailed discussions with development stakeholders across the University to determine what functionality the new system should provide. After reviewing proposals from several vendors, the University selected Blackbaud to collaborate and co-develop an enterprise-wide donor management and fundraising tool. The contract with Blackbaud was signed in August 2009. The

University and vendor completed a FitGap review to determine the significant risks and best approaches to mitigate the identified risks.

The partnership with the vendor had obstacles to overcome. The initial go-live date of April 2011 was delayed because the design process took longer than anticipated. Blackbaud missed the target implementation date and was assessed a delay penalty. When finally launched, the University had to expend resources to stabilize the system and fix revenue recognition issues. Blackbaud had to finish the events module and provide a tool to migrate computer code. Despite the difficulties, the system has been successful at providing development units with a more complete fundraising tool and the relationship with Blackbaud has matured into a solid partnership.

When fully implemented, DART is expected to provide substantial benefits: improved efficiency of managing the donor base, better integration with the University's financial systems, enable the Office of University Development (OUD) and unit development offices track and serve donors, and meet University compliance requirements.

B. Audit Issues and Management Action Plans

1. **Changes to the Default Master Encryption Password**	**Medium**
Issue: The default master encryption password provided by the vendor was not changed by ITS. **Risk:** Attackers can obtain default passwords with little effort and use them to gain access to sensitive PPI. Over 700,000 PPI records are maintained in DART. **Support:** During installation sensitive PPI was encrypted with a vendor supplied default password; however, the password was never changed. Multiple security layers reduce overall risk.	**Recommendation:** ITS immediately changed the default master encryption password after the issue was brought to their attention. In addition, a procedure (standard) should be established requiring the password to be changed at least annually. **Management Action Plan:** ITS will work with University Audits to determine the process and plan for changing the encryption key by November 2013. **Action Plan Owner:** DART Technical Manager **Expected Completion Date:** Plan executed by January 2014

2. **OUD Dev/Net Web Application Security**	**Medium**
Issue: The Dev/Net web application is outdated and needs to be retired or upgraded. **Risk:** The OUD site is accessible to anyone with a self-created friend account (also known as	**Recommendation:** The current OUD Intranet should be retired or repaired to mitigate known threats. **Management Action Plan:** OUD recognizes the

2. OUD Dev/Net Web Application Security

Medium

guest accounts). Friend accounts can be created by anyone on demand without approval, which could enable unauthorized access to confidential donor information.

Support: The OUD Intranet web site is used to store and share sensitive data about donors and constituents. OUD has limited resources to address the vulnerable site and have been unable to make retiring the site a priority.
The DevNet site:

- Contains constituent data
- Is at risk to easily exploitable vulnerabilities
- Can be accessed by creating self-created friend accounts
- Could be used to further exploit other systems and collect credentials
- Is an older, less secure application, it is still necessary as an internal system to collaborate and share information.

vulnerability associated with use of older technology; however, will not assign resources to rebuilding DevNet with new software until fiscal year 2015. In the interim, OUD will completely shut down Guest access to DevNet.

Action Plan Owner: Senior Director of Development Services

Expected Completion Date: Shut down DevNet Guest site by November 2013. During fiscal year 2014, begin Google site structure for replacement of DevNet; complete transition to Google sites by end of fiscal year 2015.

3. DART Web Application Security

Medium

Issue: Known security issues in the DART system, specifically DART Blackbaud Internet Service (BBIS), and Blackbaud Enterprise CRM (BBEC), have not been fully resolved by OUD and ITS.

Risk: Known security vulnerabilities could potentially lead to a compromise of sensitive and confidential donor information.

Support: Information and Infrastructure Assurance (IIA) conducted a penetration test and issued a report to OUD and ITS in December 2011. The report listed several findings; however, not all of the findings had been addressed at the time of our audit.

A web application vulnerability scan conducted by University Audits also identified several

Recommendation: ITS, IIA, OUD, and Blackbaud should address the identified vulnerabilities that are present in the BBEC and BBIS web applications. Going-forward, the DART applications should undergo a web application vulnerability scan during the change process and at least annually. Results of the scan should be used to prioritize issues and create action plans to address critical and high-risk issues within a maximum time of 30 days after discovery.

Management Action Plan: ITS, IIA, OUD and University Audits are currently meeting to determine the context of items reported in the recent vulnerability scan and set a plan of action.

Action Plan Owner: Senior Director of Development Services and DART Technical

3. DART Web Application Security

Medium

potential high-risk vulnerabilities in BBIS and BBEC, which were not identified in the IIA penetration test. DART web applications are protected by two-factor authentication (2FA) that allow the severity of some risks to be reduced, but not eliminated.

Manager

Expected Completion Date: Plan determined by November 2013 with targeted dates for implementation.

4. Network Vulnerabilities

Medium

Issue: OUD did not address high and critical Common Vulnerability Scoring System (CVSS) vulnerabilities within a reasonable time.

Risk: A remote attacker could leverage identified vulnerabilities to install malicious code that could run with elevated privileges. This could allow malicious automated programs such as worms to propagate and compromise other systems.

Support: Management was aware of some of the vulnerabilities identified in the audit. They had planned to address some of them during the MiWorkspace transition; however, management immediately addressed others when they were notified.

CVSS provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. Its quantitative model ensures repeatable accurate measurement while enabling users to see the underlying vulnerability characteristics that were used to generate the scores.

Recommendation: In the future, critical and high-risk vulnerabilities should be resolved immediately. ITS and OUD should work with IIA to conduct regular security checks and address critical and high level risks within 30 days of discovery. Resource management controls should be improved to prioritize vulnerabilities as they are detected.

Management Action Plan: Vulnerabilities were resolved as planned during the MiWorkspace transition. OUD, ITS, IIA, and University Audits will define a plan for regular monitoring, identification and addressing of network vulnerabilities.

Action Plan Owners: Senior Director of Development Services and University Chief Security Officer

Expected Completion Date: Issues identified in the initial scan have been addressed. Move forward plan will be determined and implemented by June 2014.

5. Terminations and Periodic Review of User Access

Medium

Issue: User access to DART is not always promptly revoked upon termination of employment or when access to DART is no longer required when job responsibilities change. In addition, access roles based on job responsibilities are not reviewed regularly.

Recommendation: User access accounts for terminated employees and employees who no longer have development responsibilities should be deactivated immediately. User access and role assignments should be reviewed by OUD semi-annually. The procedural breakdown that led to the oversight of removing access roles

5. Terminations and Periodic Review of User Access

Medium

Risk: Data loss, theft, destruction, or unapproved modification could potentially occur.

Support: Management indicated that a procedural breakdown of the account de-provisioning process allowed for the oversight.

- Over 30 active DART user accounts for terminated employees existed. Some accounts had access roles that management believed were removed.
- Two active users with roles that could create a conflict by allowing the users to disable application auditing were identified.

should be investigated and corrected. Permissions to modify audit functions in DART should be granted as needed and access requests should be tracked.

Management Action Plan: Current processes to change passwords and get back MTokens for terminated employees address access issues. OUD and ITS are working together to determine ways to correct the procedural breakdown to allow for quick revocation of user roles when employees are terminated. OUD already reviews recent access requests granted on a biweekly basis; however, a comprehensive review of all access levels will be implemented on a semi-annual basis. ITS and OUD will investigate the feasibility of a separate security role solely for audit table functions and will follow-up with University Audits on an implementation plan.

Action Plan Owners: Senior Director of Development Services and Assistant Director University Development Systems

Expected Completion Date: Develop a plan by October 2013. Explore feasibility of separate security role for audit table functions by December 2013.

6. Organization of Key Information

Medium

Issue: OUD and ITS have not effectively organized key information to facilitate efficient and full use of DART.

Risk: Users may not easily find policies and procedures or understand the standards and expectations. As a result, they may not use DART to its full capabilities.

Support:

- Information helpful to users is not easily

Recommendation:

- Organize information so DART users can retrieve it when needed. A possible solution may include a central repository and users training to search this primary location to address questions. Include relevant quick tips and FAQs, and training reference materials that support policy and procedures.
- Document standards and expectations for key processes. Clarify for units what they

6. Organization of Key Information — Medium

located and searching can be time consuming due to multiple locations for information, including the Standard Practice Guide, DevNet, and the Business Practice Library on the Education and Training Intranet site.

- Users find the Education and Training website difficult to use and information does not address all current issues and concerns.
- DART users struggle to locate policy and procedure documents, understand what is expected, and find training and reference information.

must do and what is best practice.

- Revise the Education and Training website to be more user-friendly and improve search ability. Revise the site regularly so information is relevant and current.

Management Action Plan: Management concurs with the recommendation. Meetings will be held to determine best options for addressing the issue. Once the evaluation is complete, a resolution will be developed and implemented.

Action Plan Owners: Senior Executive Director, Campaign, Development Services and Strategic Solutions, OUD and Performance Support Manager, ITS

Expected Completion Date: Evaluation will be complete by December 2013. Once the evaluation is complete, a resolution will be developed and implemented.

7. Assignment and Completion of Project Tasks — Medium

Issue: The University assumed responsibility for completing work initially assigned to the vendor without having resources available to complete the project.

Risk: Unfinished project steps may negatively affect user efficiency.

Support: Blackbaud was responsible for providing a data dictionary as part of the agreement with the University. Management indicated that the University's expectations were higher than what Blackbaud provided, so the University accepted the responsibility for providing the data dictionary. However, the data dictionary has not been completed because higher priority issues took precedence. The delay affected the ability to customize reports for both Development's Reporting

Recommendation: Version 3.0 of DART will be released in spring 2014. OUD and ITS should review the data dictionary prior to the new version's release to determine if it meets expectations. If the revision is acceptable, it should be released as soon as possible. If the revision is not sufficient, developing a data dictionary should be a priority for completion. For future projects or phases, documentation of changes to the recorded statement of work should exist and detail the following:

- Reasons why the Statement of Work was changed
- Timeframe for completing the work and resources assigned

Management Action Plan: Management agrees that changes to project Statement of Work should be recorded, when applicable.

7. Assignment and Completion of Project Tasks

Medium

team and users of DART.

Management agrees with the recommendation to get a useable data dictionary into the hands of the end users. As part of the Phase II project, U-M will evaluate whether the delivered data dictionary meets our needs or whether U-M staff needs to be assigned to complete the project.

Action Plan Owner: Assistant Director University Development Systems

Expected Completion Date: The assessment of the version 3.0 data dictionary will be completed prior to the completion of the upgrade, scheduled for March 2014.

8. Ongoing User Training

Medium

Issue: Although online training courses are available, OUD does not offer refresher training or users are unaware of options available.

Risk: Users may not be aware of the full system capabilities, which may lead to inefficient and ineffective use.

Support: DART users interviewed were consistent in their desire for refresher training programs. OUD expressed reservations because interest in training does not always equate to attendance and the benefits of additional training may not be cost effective.

Communities of Practice are groups of U-M employees with similar job responsibilities. Members share tips, best practices, and help new employees better understand the system.

Recommendation:

- Survey users to gauge interest. Provide training for only those areas where interest warrants the additional expense.
- Expand Communities of Practice groups to augment training. Include smaller academic and non-academic units in the Communities of Practice.
- Update the Education and Training website to communicate more effectively with users to address their needs such as expanding supplemental training aids like the quick reference guides and FAQs.

Management Action Plan: Management has implemented a number of the recommendations, but agrees that improvements can always be made. OUD and ITS have held several conversations around implementing a new communications plan that will target communications across various segmented user groups. As part of the Phase II capital project plan, a Performance Support Analyst was recently hired to help carry out this new communications approach, as well as to help further develop Communities of Practice and assess additional training needs of the Development community.

Action Plan Owners: Senior Executive Director, Campaign, Development Services and Strategic Solutions and Performance Support Manager

Expected Completion Date: Communications Plan in place fall 2013. Training aides will be reassessed as part of the upgrade, scheduled for spring 2014, and will be iteratively developed as the needs are defined.

9. Use of Help Desk Questions

Medium

Issue: ITS and OUD do not leverage help desk questions and user complaint trends to proactively address and prevent similar problems.

Risk: Efficient use of OUD and ITS resources and the DART system can be negatively affected by failing to proactively address DART users' current issues and concerns.

Support: Users request assistance by formally contacting the Help Desk or informally during conversations at training sessions, meetings, or conference calls. A process does not exist to capture, analyze, and use the requests to proactively address common issues and trends.

Recommendation: Implement a process to analyze help desk tickets and other requests for assistance. Provide the analysis to OUD departments like communications, training, and the website design team who can help the DART user community.

Management Action Plan: Management agrees. The new ServiceLink project will allow both ITS and OUD the opportunity to simplify and consolidate ticket tracking. This will allow us to more easily analyze tickets to identify problem areas that could benefit from additional training or attention. OUD has been working to develop a more comprehensive set of ticket reports to be drawn out of Footprints, OUD's current ticketing tool. The new reports will allow OUD to analyze the categories of ticket types to better focus training opportunities and reference guides.

Action Plan Owners: Senior Executive Director, Campaign, Development Services and Strategic Solutions and Assistant Director University Development Systems

Expected Completion Date: ServiceLink is already in place for ITS ticket tracking. Analysis

9. Use of Help Desk Questions — Medium

and problem management phases will be scheduled to coincide with the ServiceLink implementation plan.

10. System Utilization Metrics — Medium

Issue: OUD has not provided system utilization metrics and reporting to enable monitoring of performance by unit development offices.

Risk: DART cannot reach its full effectiveness if users are not using the system as expected.

Support: Individuals responsible for supervising unit development offices may lack sufficient information to assess performance. OUD indicated that they are reluctant to issue system utilization metrics because they lack the ability to enforce standards and do not want to damage collaborative relationships with unit development offices.

Recommendation: Determine what information should be shared, provide tools and training for units to self-monitor and aggregate the data, and provide reporting to assess progress. There are resources that can share lessons learned and best practices for formalizing the process including ITS Security, Office of Internal Controls, and Human Resources. The first step is to provide standards and expectations and build the self-monitoring tools. Once that process is complete, OUD should disseminate the information, consulting with Development Units as necessary.

Management Action Plan: Management agrees that system utilization metrics are crucial to improving performance. The timing for implementing additional metrics is more conducive to success now. With the recent Tableau Consortium initiative well underway, there will be an enterprise data visualization tool available to OUD that would allow for deep levels of system utilization metric reporting in fiscal year 2014.

Action Plan Owner: Senior Director of Development Services

Expected Completion Date: By end of fiscal year 2014

A. Alfred Taubman Medical Research Institute 2013-310

Original report issued October 2013

A. Executive Summary

1. Overall Conclusion

In just a few years, the A. Alfred Taubman Medical Research Institute (the Institute) has fostered significant medical research advances by providing resources for the pursuit of discoveries unrestrained by conventional grant funding mechanisms. Since the funding model is new and is not part of the Office of Research oversight and infrastructure, the Institute needs to develop internal control structures for effective stewardship and legal protection. The following report outlines these gaps, and recommends some practical solutions to improve oversight and monitoring and limit legal liability. Institute management has responded to the audit recommendations and has taken significant steps to reduce risk without impeding scientific progress.

2. Summary of High Risk Audit Issues

For this audit, University Audits identified the following high-risk issues.

Ref.	Issue	Risk	Action Plan Owner	Expected Completion
B.1.	In some instances, gift funds are used as discretionary funds to cover cost overruns on Scholar's sponsored research projects. There is no Institute approval and oversight of Scholar award transfer activity.	High	Director of the Institute	Completed
B.2.	The Institute made Scholar award payments to a recipient outside U-M without a contractual arrangement.	High	Managing Director of the Institute	Completed

3. Key Activities Audited and Conclusions by Sub-Activity

The scope of the audit was determined based on an assessment of the risks associated with the key activities of the Institute. This process included input from Institute management and interested parties from other University functions. The table below lists the key activities audited, along with the overall risks of the audit issues identified for each sub-activity.

Key Activities Audited / Conclusions by Sub-Activity

General Controls	Research Awards	Gift Agreement	Procurement	Fiscal Responsibility	Payroll
🟩 Annual Gap Analysis	🟩 Grants and Donor Intent	🟩 Agreement Authorization	🟩 Travel and Hosting	🟩 Annual Budget Process	🟨 Time Reporting
🟩 Policies and Procedures	🟩 Compliance with U-M Policy		🟩 Non-PO Activity	🟩 Budget Variance Analysis	🟩 Review and Approval
🟩 Compliance Hotline	🟩 Annual Progress Reports		🟩 Approval Process	🟩 Statement of Activity Reconciliation	🟩 Policies and Procedures
🟩 Funding Mechanism	🟥 **Financial Oversight**		🟩 Vendor Purchases	🟩 Review and Approval	🟩 Gross Pay Register
🟩 Information Technology	🟥 **External Award Reciepients**		🟩 P-Cards		🟨 Temporary Employees
🟨 Governance and Leadership	🟩 Research Compliance				
🟩 COI/COC	🟨 Fiscal Responsibility (2)				

Legend		
🟥 **High Risk**	🟨 Medium Risk	🟩 No or Low Risk

Note: Section B of this report (Audit Issues and Management Action Plans) provides details of the high and medium risk issues identified during the audit. We communicated low risk issues to unit management and they are not included in the report.

4. Audit Objectives

- Institute Charter and Bylaws are followed by Oversight Council
- Mission statement of Institute exists and is communicated
- Institute has comprehensive policies and procedures, and complies with applicable University policies and procedures
- Assets are adequately protected
- Scholar awards are managed in accordance with donor intent and U-M policy
- Controls are adequate for awarding funds outside U-M
- Controls are adequate over Institute fiscal responsibilities

5. Context and Key Considerations

In 2007, Michigan businessman and philanthropist A. Alfred Taubman provided funds to establish the A. Alfred Taubman Medical Research Institute at the University of Michigan Medical School. The mission of the Institute is to provide the University's finest medical scientists the freedom, resources, and collaborative environment they need to push the boundaries of medical discovery to produce breakthroughs in cures to speed the development of effective treatment for some of the most devastating illnesses.

One of the core requirements of the Institute is to fund high-risk, high-reward research not typically available through traditional sources of funding. At the time of our audit, 19 Scholars were conducting research with the assistance of grants from the Institute, examples include:

Award Type	Description	Amount	Frequency
Emerging Scholar	Support and encourage early career physician scientist	$50,000	Annually for 3 years
Taubman Scholar	Senior level scientists who are doing discovery-driven research	$150,000	Annually for 3 years
Senior Scholar	Former Taubman scholars with continued funding	$50,000	Annually for 3 years
Director's Fund	Determined by Oversight Council	$300,000	Annual
Taubman Prize	Awarded to a non-U-M researcher	$100,000	Annual

Consistent with the Institute charter, an Oversight Council provides stewardship, oversight, and guidance to Institute leadership. A Scientific Advisory Board is also in place to evaluate the progress of currently funded research and other scientific matters, conduct scientific review of grant applications, and advise Taubman Scholar nominations. The Institute also has a Leadership Advisory Board, which provides a sense of vision for the organization; monitors the progress toward fulfillment of the Institutes missions and objectives; and provides support, advice, and counsel.

In addition to the Taubman family, other generous donors support the Institute with gifts for both expendable purposes and endowment. The Institute Director and Oversight Council direct the use of expendable gifts and proceeds from the endowment. The Office of the Executive Vice President for Medical Affairs provides additional funds. Fiscal year 2013 operating expenditure was $702,876, which includes the $100,000 annual Taubman Prize. In fiscal year 2013, the Institute awarded $1.3 million of endowed funds to Scholars. An additional $325,000 was awarded to Emerging Scholars from other private donors.

B. Audit Issues and Management Action Plans

1. **Gift Funds** **High**

Issue: In some instances, gift funds are used as discretionary funds to cover cost overruns on Scholar's sponsored research projects. There is no Institute approval and oversight of Scholar award transfer activity.

Risk: Funds may not be spent in accordance with Institute mission and gift intent to support high-risk high-reward research that traditional sources often do not fund.

Support: Since November 2010, Scholars have spent $207,000 of their Institute award to cover overruns on 13 other research projects. Transfers ranged from $1,186 to $48,187. Standard Practice Guide Section 501.01, *Fiscal Responsibility* requires management to put in place sufficient controls to ensure that funds are spent in compliance with University policy, as well as sponsor, donor, or federal guidelines. These controls will streamline oversight and support the efforts of the Principle Investigator (PI).

Recommendation: Require the Scholars to obtain preauthorization from a designated Institute manager for any transfer of funds to other project grants or departments, including the use of funds to cover sponsored project cost overruns. Verify transfers are in line with the gift agreement. Along with the annual scientific progress reports, direct the Scholars to provide the Oversight Council with annual financial reports with sufficient detail on how expenditures support the research progress and are in accordance with the Institute's core requirements. To streamline the process, develop a template or format for the Scholars to use for periodic financial reporting.

Management Action Plan: The Taubman Institute will require Scholars to obtain pre-authorization from the Institute Director for any transfer of funds to other project grants or departments, including the use of funds to cover sponsored project cost overruns. Any such transfer of funds cannot exceed 20 percent of the total grant. The Taubman Institute has updated its Standard Operating Procedures to that effect and will communicate those changes to all current Scholars. That language will also be incorporated into the letters of appointment of new Scholars. However, now that the project grants reside in the home departments of the Scholars, the departmental chairs and their administrators are in the best position to assure that the grant money is spent properly. The Scholars should submit financial statements according to their departmental policy for their department to review. The Institute Director will communicate that responsibility to each department chair and ask for a letter of confirmation.

1. Gift Funds

High

Action Plan Owner: Director of the Institute

Expected Completion Date: October 1, 2013

2. Award Recipients Outside U-M

High

Issue: The Institute made Scholar award payments to a recipient outside U-M without a contractual arrangement.

Risk: The Scholar awards support high-risk high-reward translational research that involves highly regulated activities such as embryonic stem cell and animal and human subject research. Transferring funds to other institutions and individuals without sufficient contractual framework puts the University and Institute potentially liable for high-risk research activities outside U-M's control and monitoring processes.

Support: Since fiscal year 2012, an award was made to Emory University each year for $150,000 to support a Taubman Scholar who is conducting research at Emory. The payments were made on a non-PO voucher, which is similar to a check request and is not a legally binding contract.

Recommendation: Work with U-M Office of General Counsel, Procurement Services, and Contract Administration to determine the contractual arrangements and payment method between U-M and any outside recipient of a Scholar award. The correct structure will support ongoing control and monitoring.

Management Action Plan: The Office of Contract Administration has drafted a purchase order for the Taubman Institute to use for the next installment of funds to be transferred to Taubman Scholar at Emory University. The Taubman Institute will employ that as a template for all future awards to recipients outside the University of Michigan. A Standard Operating Procedure addresses this procedure, and it will be the responsibility of the Managing Director to monitor such grants in the future.

Action Plan Owner: Managing Director of the A. Alfred Taubman Medical Research Institute

Expected Completion Date: Completed

3. Scholar Award Accountability

Medium

Issue: Scholar award accountability has not been defined and documented. The Scholars and their home department administrators do not have a clear understanding of who is responsible for Scholar award monitoring and fiscal responsibility.

Risk: Responsibility for regular internal control processes, such as monthly Statement of Activity reconciliation and financial monitoring is fragmented. The Institute runs the risk of

Recommendation: The Institute Managing Director should move all Scholar project accounts to the Scholar's home department to promote clear fiscal accountability and monitoring.

Management Action Plan: The Scholar project accounts have been moved to the Scholars' home departments.

Action Plan Owner: Managing Director of the

3. Scholar Award Accountability

Medium

award misspending and overspending.

Support: Each Institute award is set up with a unique project grant number. The funds for the Taubman Scholars and the Senior Scholar award projects remain within the Institute department accounting structure, but financial expenditures are processed within the Scholar's home department.

A. Alfred Taubman Medical Research Institute

Expected Completion Date: Completed

4. Establishment of Project/Grant in University Systems

Medium

Issue: At project set-up, University of Michigan Health System (UMHS) Finance did not establish end dates for the majority of Scholar award project/grants. In addition, on most of the Institute project awards, an accounting manager in UMHS Finance is named as the project PI instead of the Research Scholar.

Risk: Research administrators in the Scholar's home department interpret the project as open ended and are assuming they have longer than the three years to spend the funds. An accounting manager in UMHS Finance is not close enough to the project activity to be named as PI.

Support: All Institute projects are typically a three-year commitment. All projects were established with an end date beyond that of the three-year commitment. Of 18 U-M Scholar projects, 15 have an end date 2030 or later. Standard Practice Guide Section 500.01, *Fiscal Responsibilities* requires the PI to be responsible to review the work of others, including oversight of financial matters, in order to provide a reasonable level of assurance that the work is performed properly and on a timely basis. These are duties performed by the Scholar. The duties of the accounting manager and accounting staff are to

Recommendation: The Institute Managing Director should request that existing project information be corrected to accurately record the Scholar as PI. Record accurate information on all future Scholar awards. Institute management should review project/grant information at set up to verify accuracy.

Management Action Plan: Current Scholars have been established as the PI's of their Taubman Institute grants. Standard Operating Procedures have been updated to assure this happens in the future, and the Managing Director will review all project/grant information in the future to verify accuracy.

Action Plan Owner: Managing Director of the A. Alfred Taubman Medical Research Institute

Expected Completion Date: Completed

prepare accounting entries and adjustments.

5. Unspent Funds

Medium

Issue: The Institute has not developed or communicated written guidance for unspent Scholar awards including reversion of funds if a Scholar leaves the university.

Risk: There is misunderstanding and confusion on the part of the Scholars and their home department whether the funds are still available after the award ends or when a Scholar leaves the university.

Support: In February 2013, a Taubman Scholar left U-M after receiving the second year of funding from the Institute. Department staff was unclear as to the disposition of the remaining funds.

Recommendation: Develop a written policy on disposition of unspent funds at award end date and when a Scholar leaves the university. The policy should not conflict with the U-M Faculty Handbook. Policy should include:

- Circumstances and process for requesting time extension (if allowed)
- How long and for what purpose charges can be made to the project account after a Scholar departs
- How the policy will be communicated to the Scholar and home department

Academic Human Resources should review the policy before finalization and approval by the Oversight Council.

Management Action Plan: Standard Operating Procedures have been established for the disposition of unspent funds at the award end date and when a Scholar leaves the university. These procedures will be sent to Academic Human Resources for review, after which they will be submitted to the Oversight Council for approval. When approved, they will be incorporated into the letters of appointment and communicated to the Scholars and their home departments by the Taubman Institute Director.

Action Plan Owner: Managing Director of the A. Alfred Taubman Medical Research Institute

Expected Completion Date: November 1, 2013

6. Scientific Advisory Board (SAB)	**Medium**
Issue: On-going Institute funding of Scholar award is occurring without periodic outside scientific evaluation and review by the SAB, as required in the gift agreement. **Risk:** The Institute is not following the terms of the gift agreement. **Support:** The University has named two of the five members of the SAB. The donor is responsible for naming the other three, which has not occurred. The gift agreement charges the SAB with monitoring the progress of research currently funded by the Institute, conducting scientific review of applications for funding under Institute programs, and making recommendations about the funding to the Institute Executive Committee.	**Recommendation:** Work with the donor to name the three remaining members to the SAB. When fully staffed, standardize and document processes for the initial award application scientific review and on-going annual progress review. Going forward, maintain the SAB role in the annual review processes. **Management Action Plan:** The Taubman Family has appointed a chair of the SAB. He is working with the Taubman Institute Director to name the remaining members. When fully staffed, the SAB, in conjunction with the Director, will standardize and document processes for the initial award application scientific review and ongoing annual progress review. From now on, the SAB will maintain its role in the annual review processes. **Action Plan Owner:** Director of the A. Alfred Taubman Medical Research Institute **Expected Completion Date:** February 1, 2014

University of Michigan-Flint Banner System 2013-310

Original report issued October 2013

A. Executive Summary

1. Overall Conclusion

University of Michigan-Flint Information Technology Services (Flint ITS) faces the difficult challenge of responding to the growing information technology needs of the Flint campus, while working to maintain an effective control environment given stretched resources and limited staff. The Banner System is functioning as intended; however, opportunities exist to improve overall security, privacy, and continuity of operations of the system. Flint ITS responded positively to the audit recommendations and all necessary corrective actions are targeted to be completed by the end of February 2014.

2. Summary of High-Risk Audit Issues

For this audit, University Audits identified the following high-risk issues.

Ref.	Issue	Risk	Action Plan Owner	Expected Completion
B.1.	ITS does not actively patch the Java client software on end user machines, causing Banner users' computers to be vulnerable to various exploits known to attackers.	High	Data Security Analyst Intermediate	December 2013
B.4.	Flint ITS does not conduct regular vulnerability scanning and remediation.	High	Data Security Analyst Intermediate	December 2013

3. Key Activities Audited and Conclusions by Sub-Activity

The scope of the audit was determined based on an assessment of the risks associated with the key activities of the Institute. This process included input from Institute management and interested parties from other University functions. The table below lists the key activities audited, along with the overall risks of the audit issues identified for each sub-activity

Key Activities Audited / Conclusions by Sub-Activity

IT Security	Sensitive Data	Audit Logs	Education	Documentation	Planning & Risk Assessment
🟥 Java Client Patch Management	🟨 Encryption	🟩 Audit Log Data	🟩 FERPA Awareness Training	🟨 System Documentation	⬜ Users Acceptance/Approval to Changes
🟨 Access Revocation	🟨 Non-Production use of PPI	🟨 Audit Logging Guidance		⬜ Project Management	
🟨 Web Application Security				⬜ Change Management	
🟥 Vulnerability Scanning					
🟩 Specialized Access					

Legend

🟥	🟨	🟩	⬜
High Priority Audit Findings	Medium Priority Audit Findings	No or Low Priority Audit Findings	Out of Scope (not audited)

Note: Section B of this report (Audit Issues and Management Action Plans) provides details of the high and medium risk issues identified during the audit. Low risk issues were communicated to unit management and they are not included in the report.

4. Audit Objectives

The primary objectives of the audit were to evaluate IT systems and security controls that affect the Banner data and system components. A vulnerability assessment of ancillary systems and managed Banner end-user computers was also completed. University Audits reviewed the following risk areas to assess the effectiveness of the control environment for Banner:

- IT security:
  - Web application vulnerability assessment of Banner SIS[2]
  - Java client patch management (Required to access Banner)
  - CVSS[3] vulnerabilities of Banner end-user computers
- Sensitive Data
  - Encryption of sensitive protected personal information (PPI)
  - Non-production use of PPI
- Audit Logging
  - Banner audit log contents
  - Documented Banner audit log guidance
- Documentation of system configuration and network diagrams
- Education and training
  - FERPA awareness training

5. Context and Key Considerations

Banner is an administrative database used to house all UM-Flint student-related data. The system tracks student activity from recruitment to graduation. Sensitive data such as social security numbers, which is subject to FERPA (Family Educational Rights and Privacy Act) are stored in Banner. The system is linked to an online interface called the Student Information System (SIS). SIS allows students to register for classes and faculty to submit grades.

The UM-Flint Banner environment consists of three main modules:

- The Student module provides functions that aid admissions, recruiting, and registration.

[2] A student information system (SIS) is a software application for education establishments to manage student data.

[3] Common Vulnerability Scoring System (CVSS) is a free and open industry standard for assessing the severity of computer system security vulnerabilities, and is under the custodianship of the Forum of Incident Response and Security Teams (FIRST). It attempts to establish a measure of how much concern a vulnerability warrants, compared to other vulnerabilities, so efforts can be prioritized.

- The Financial Aid module automates day-to-day financial aid tasks, disperses funds, provides self-service capabilities to students, and facilitates compliance with regulatory requirements.
- The General module provides services for general operations.

UM Flint Information Technology Services (ITS) provides the technical operational support, maintenance, and IT security processes for Banner. Ownership of the data is shared by several data stewards:

- Registrar
- ITS
- Financial Aid
- Undergraduate Admissions
- Graduate Programs
- Student Accounts

Banner governance is provided by the Information Systems Steering Committee (ISSC) and the Implementation Committee (IC). The Provost charged the ISSC to focus on administrative information systems that affect the entire campus, overseeing the Banner IC, and addressing the strategic direction of Banner.

The IC is responsible for the ongoing guidance of the Banner administrative data software and its interfaces. In addition, Banner administrative data software and its interfaces are supported by approved campus policies and procedures. The committee acts as a liaison between the technical staff, policy makers, and end-users of the UM Flint campus community.

B. Audit Findings and Action Plans

1. Java Update Process

High

Issue: ITS does not actively patch the Java client software on end-user machines, causing Banner users' computers to be vulnerable to various exploits known to attackers.

Risk: A successful exploit could allow an attacker to have complete control over an end-user machine.

Support:

- 90% of systems analyzed are vulnerable.
- Users are responsible for updating Java

Recommendation: Flint ITS should patch vulnerable machines with the latest compatible version of Java. ITS should identify an alternative to Java on end-user systems.

Management Action Plan: To reduce the risk associated with vulnerable Java on client machines, ITS will attempt to use application virtualization using Microsoft's App-V for any application that requires specific vulnerable versions of Java.

client.

- Systems administrators are unable to get stakeholder agreement on a single version of Java.
- 88% of machines are running on Java versions that are out of date by more than six months.

ITS will also fully implement third party patching to patch and keep clients on the latest patched version of Java. In the event that App-V will not work with a vendor's software, Java will be patched to the latest version of Java supported by said software and additional risk mitigation options explored.

Action Plan Owner: Data Security Analyst Intermediate

Expected Completion Date: December 2013

2. Access Revocation Process

Medium

Issue: ITS does not periodically review Banner user accounts to identify employees who have terminated employment and should no longer have access to Banner.

Risk: Data could be subject to malicious or accidental modification from former employees.

Support: ITS does not review Banner user accounts on a regular schedule to determine that they are only provisioned to current University employees with a need for access. University Audits identified several terminated employees who still had access to Banner. Some of the identified accounts belonged to employees with termination dates over six months old. Flint ITS relies on a manual process that requires departments to notify them regarding terminations and transfers.

Recommendation:
ITS should review all Banner user accounts and remove the accounts of users who no longer have a business need for access. On an on-going basis, ITS should periodically perform a similar review. ITS should work with Human Resources to improve the notification process for terminated and transferred employees.

Management Action Plan:
We should be able to crosscheck our active Banner IDs against M-Pathways employment records, with a simple query. When the query is complete, we will validate access once a month. In addition, we have just completed a process that went live in September 2013 to pull all employees from Peoplesoft in Ann Arbor. This will further facilitate validating user access in Banner.

Action Plan Owner: Banner User Coordinator

Expected Completion Date: February 2014

3. Web Application Vulnerabilities

Medium

Issue: ITS does not review the security of the Internet accessible portion of the Banner (SIS) web application.

Risk: A successful compromise could result in the exposure of PPI that is also regulated by FERPA.

Support: SIS is protected by an authentication system and is not directly accessible without assigned privileges. This application is only vulnerable to those with access (UM Flint Students, Faculty and Staff). However, if an attacker obtains the credentials of an authorized user, the attacker can use this access to exploit the system.

- Over 600 users have access to Banner.
- All current and former students have access to SIS.
- Over 100 potential high-risk (WASC) vulnerabilities identified.
- Several of the identified vulnerabilities could allow an attacker to execute unexpected commands and escalate privilege.

Recommendation: Flint ITS should review the vulnerability analysis report. Vulnerabilities found in locally built program code should be fixed and those in the vendor-supplied program code should be immediately referred to the vendor. ITS should give priority to remediation of high-risk vulnerabilities. ITS should perform web application security reviews at least annually and when major changes are made to the software by the vendor.

Management Action Plan: A review of the vulnerability analysis report will be completed within three months. We will address any issues found with locally built program code and identify to the vendor any remaining vulnerabilities. We will also begin a quarterly web application security scan with help from our security team

Action Plan Owners: Data Security Analyst Intermediate and Banner Systems Administrator

Expected Completion Date: November 2013

4. Vulnerability Scanning

High

Issue: Flint ITS does not conduct regular vulnerability scanning and remediation.

Risk: End-user computers are vulnerable to high- and critical- risk (CVSS) vulnerabilities allowing an attacker to impersonate the compromised user and access sensitive data.

Support: End-user computers that interface with Banner are vulnerable to high- and critical-

Recommendation: Flint ITS should regularly scan end-user machines and address findings based on priority and risk within 30 days of discovery.

Management Action Plan: Regular vulnerability scanning of client machines began during August 2013. The results of the vulnerability scan will feed into the security database that allows tracking of vulnerabilities risk vulnerabilities. Sensitive data hosted in a secure environment protected by firewalls can be at risk when systems that connect to secure systems are vulnerable.

- Over 670 hosts scanned. More than 3,400 vulnerabilities identified
    - 100 critical risks
    - Over 1,900 high risk
    - More than 1,070 medium risks

and how long they have gone unremediated.

ITS will use the results of the vulnerability scan to prioritize patching using SCCM and 3rd-party patching tools to patch discovered vulnerabilities before the next scheduled scan so remediation can be verified.

Action Plan Owner: Data Security Analyst Intermediate

Expected Completion Date: December 2013

5. Encryption of Protected Personal Information (PPI) — **Medium**

Issue: Data defined as PPI is not encrypted at rest or masked when displayed to an end user.

Risk: Compromise of PPI could result in significant financial loss, fines and penalties, and reputational damage.

Support: The Data Administration Guidelines for Institutional Data Resources state: “All data, regardless of where it is stored, will be afforded the same level of protection. Where practicable, sensitive data at rest and in transmission should be encrypted.”

Recommendation: PPI should be encrypted in the Banner database and the first five numbers of the SSN should be masked when presented to the end user. (SPG 601.14)

Management Action Plan: ITS will look into encryption of PPI at rest with Oracle Advanced Security option Transparent Database Encryption.

ITS will use partial character masking on all forms that contain SSN with first five characters masked with an ‘X’ and last four characters unmasked for a majority of users. A limited number of authorized power users will still have no masking.

Action Plan Owners: Banner Systems Administrator, Database Administrator Lead

Expected Completion Date: PPI at Rest – February 2014, SSN masking – December 2013

6. PCI compliance

Medium

Issue: Flint ITS developers can obtain a copy of the Banner database, which includes PPI, and use it in local development environments.

Risk: An incident where a local development is compromised resulting in the loss of PPI could result in significant financial loss, fines and penalties, and reputational damage.

Support: Flint ITS manages test servers that are loaded with production data that contain PPI. Flint ITS does not provide de-sensitized and de-identified data for use in non-production environments. PPI in a non-production environment, controlled by end-users, increases the potential for data loss or data leakage of sensitive data. ODBC (open database connectivity) services allow PPI to be accessed by anyone with Banner access. Controls to restrict the export of data via this method are not available.

Recommendation: Banner developers should not have access to datasets that contain PPI. A process to de-sensitize and de-identify data should be developed and implemented.

Management Action Plan: Our developers work to troubleshoot end-user data issues and therefore, they will always need access to non-de-identified data to facilitate that. In addition, data owners have signed off on developers having access to their data for the purposes of development and troubleshooting. Each developer is required to sign a confidentiality policy annually. In lieu of desensitizing data, we will enable fine grain auditing of the PPI data contained in the Banner database servers in order to provide a comprehensive audit trail.

Action Plan Owner: Database Administrator Lead

Expected Completion Date: April 2013

7. Audit Logging Guidance

Medium

Issue: Flint ITS has not provided guidance to developers regarding audit logs.

Risk: Inadequate logging of data may occur resulting in the inability to perform effective post-incident review.

Support: Flint ITS has not developed documentation that defines how audit logs should be configured and that describes the type of data to be collected. Federal standards state that an organization should develop, disseminate, and review/update an audit and

Recommendation: An audit and accountability guideline and procedure document should be developed and distributed.

Management Action Plan: Management concurs with the recommendation. A policy will be created for log collection. Procedures for implementing centralized log storage for each operating system and application in the Banner environment will also be created.

Action Plan Owners: Unix Systems

accountability policy. Flint ITS informally configures servers to transmit log data to a centralized server. The process is a standard practice but is not documented.

Administrator, Data Security Analyst Intermediate

Expected Completion Date: February 2014

8. System Documentation

Medium

Issue: Flint ITS staff does not adequately document information systems that support Banner and ancillary systems.

Risk: Effectiveness and responsiveness of day-to-day support is decreased and recovery times in the case of a disaster would be increased.

Support: Information about system configurations and knowledge required for supporting enterprise systems like Banner is lost when IT staff leaves UM-Flint. Obtaining information about system configurations, local system accounts, authentication methods, operating systems, and infrastructure items is dependent on the staff that originally installed and/or supports the system. Resource constraints are a limiting factor preventing the development and maintenance of effective documentation.

Recommendation: Flint ITS should document Banner and ancillary systems and develop an annual review process to keep documentation updated.

Management Action Plan: All operating systems and applications are configured based on vendor-provided instructions. This, in some way, mitigates the notion that "information and knowledge is lost when IT staff leave." That is, applications are configured against well-known published documents that are easily retrievable. Management has committed to the following:

- Create a system configuration policy
- Document in-house application architectures
- Document patch application, verification and scheduling processes
- Define an audit policy for each system
- Define a backup (including retention) policy for each system

Action Plan Owners: Unix Systems Administrator, Data Security Analyst Intermediate

Expected Completion Date: February 2014

Student Life - University Health Service 2013-206

Original report issued November 2013

A. Executive Summary

1. Overall Conclusion

University Health Service (UHS) has been in a state of transition since June 2012, when billing and practice management processes migrated to a new integrated patient management system called MiChart. The implementation of MiChart created a significant change and cultural shift for UHS from primarily manual and paper-driven processes to an integrated electronic process. MiChart is a multi-year clinical transformation project underway in the University of Michigan Health System (UMHS).

Changes to billing and operational workflows resulting from the MiChart implementation have left UHS with underdeveloped tools to manage and monitor their operations, especially patient billing operations. Additional MiChart troubleshooting expertise and staff training should address many current system problems. UHS also plans to develop a more structured relationship with UMHS and MiChart personnel to further set and define expectations for services provided and define organizational responsibilities. Finally, and not related to the MiChart transition, UHS has several Health Insurance Portability and Accountability Act (HIPAA) security and privacy issues to address. UHS management has responded promptly to the audit recommendations and has made a commitment to implement corrective actions, including several that have already been completed.

2. Summary of High Risk Audit Issues

For this audit, University Audits identified the following high-risk issues:

Ref.	Issue	Risk	Action Plan Owner	Expected Completion
1.	Some charges to patient accounts have not been billed, followed up on, or collected.	**High**	UHS Administrative Director	March 2014
2	UHS management is not yet able to effectively monitor clinical and business operations due to the lack of adequate understanding and development of MiChart reporting tools.	**High**	UHS Administrative Director	March 2014
5.	UHS is screening clinical staff against the federal excluded parties list, but is not screening all required employees.	**High**	UHS Administrative Director	Completed
6.	Required HIPAA Business Associate Agreements (BAA) are not in place with some vendors that have access to UHS protected health information (PHI).	**High**	U-M Procurement Services and UHS Administrative Director	December 2013

3. Key Activities Audited and Conclusions by Sub-Activity

The scope of the audit was determined based on an assessment of the risks associated with the activities conducted by University Health Service. This process included input from unit management and interested parties from other University functions. The table below lists the key activities audited, along with the overall risks of the audit findings identified for each sub-activity.

Key Activities Audited and Conclusions by Sub-Activity

General Controls	Patient Registration and Eligibility	MiChart	Revenue Cycle, Collections, and Billing	Fiscal Responsibility, Procurement, and Payroll	Cash Handling	Pharmacy
🟩 Annual gap analysis	🟩 Eligibility	🟩 Role-based access controls	🟩 Third-party contract management	🟩 Annual budget processes and analysis	🟨 Separation of duties	🟩 Separation of duties
🟩 Policies and procedures	🟩 Registration process	🟨 Patient clinic flows and procedures (2 issues)	🟩 Timeliness of billing and collection	🟩 Statement of Activity reconciliation	🟩 Training	🟩 Inventory management
🟨 Awareness of Compliance Hotline	🟩 Classification rules	🟥 MiChart operation reporting	🟩 Accuracy of billing and collection	🟩 Review and approval	🟩 Exception reporting	🟩 Controlled substances
🟩 Occupational Safety and Environmental Health	🟩 Scheduling capacity	🟩 MiChart exception reporting	🟥 Accounts receivable	🟩 Travel and hosting and P-Cards	🟩 Cash handling	🟩 Disposal methods
🟨 IT risk assessment			🟩 Contractual allowances	🟩 Non-PO Activity	🟨 Credit card transactions	
🟩 Continuity of operations planning				🟨 Vendor purchases		
				🟩 Time reporting, review, and approval		
				🟩 Temporary employees, other, and overtime pay		
				🟩 Credentialing and privacy training		
				🟥 HIPAA compliance (2 issues)		

Legend		
🟥 High Risk Audit Findings	🟨 Medium Risk Audit Findings	🟩 No or Low Risk Audit Findings

Note: Section B of this report (Audit Issues and Management Action Plans) provides details of the high and medium risk issues identified during the audit. We communicated low risk issues to unit management and they are not included in the report.

4. Audit Objectives

- Cash handling and credit card transaction controls are adequate and in accordance with University policy
- Revenue cycle billing and collections are well controlled and documented
- UHS accounts receivable is monitored and adequately managed
- Contractual allowance process is reasonable
- In-house third-party payer contractual relationships are adequately managed
- Patients are eligible for services and accurately classified as students or non-students
- Controls have been implemented for role-based access in UHS MiChart
- Management has adequately addressed IT security risks
- Controls are adequate over fiscal responsibility, procurement, and payroll
- Practices over credentialing and privacy training are complete and adequate
- Pharmacy cash handling and inventory controls are adequate
- Knowledge of Compliance Hotline availability is adequate

5. Context and Key Risk Considerations

UHS is a health care clinic located on the central Ann Arbor campus of the University of Michigan. With approximately 70,000 visits per year, UHS is a highly utilized campus resource. UHS is part of Student Life and does not report to UMHS, but has a solid medical practice and referral relationship with UMHS providers.

U-M students from all campuses, U-M alumni, U-M faculty, staff, retirees, spouses, domestic partners, dependents 10 years and older, and guests of U-M affiliates are eligible to visit UHS. For students who are enrolled on the Ann Arbor campus, most UHS services are covered by a health service fee, which is collected as part of tuition and fees. Students or their health insurance are billed for non-covered services even if ordered by a UHS clinician. Non-students and non-enrolled Ann Arbor campus students are charged on a fee-for-service basis. Most services are covered in part by health insurance.

UHS provides ambulatory care, with no overnight stays, to meet most routine health care needs. Care is provided for illness or injury, chronic conditions, or preventive needs such as physical exams. The clinical staff are fully licensed and experienced and include more than 25 physicians, physician assistants, nurse practitioners, and nurses. In addition, UHS provides many specialized services, including:

- Allergy, Immunization, and Travel Health Clinic
- Eye Care Clinic and Optical Shop

- Women's Health Clinic
- Laboratory
- Nutrition Clinic
- Pharmacy
- Physical Therapy
- Radiology
- Mental Health
- Alcohol and Substance Abuse Counseling

As part of the UMHS MiChart implementation, in June 2012, UHS transitioned from a hardcopy patient medical record system to MiChart, an integrated health record and health management system. As part of that implementation, billing, scheduling, and clinic operations were migrated from an aging practice management system that could no longer support regulatory and business needs. UMHS Medical Center Information Technology (MCIT) provides Information Technology (IT) and logistical support for MiChart. UHS manages its own patient billing and collections in MiChart.

B. Audit Issues and Management Action Plans

1. MiChart Implementation: Accounts Receivable	**High**
Issue: Some charges to patient accounts have not been billed, followed up on, or collected. **Risk:** Unbilled or uncollected services that have aged significantly increase the potential for uncollected accounts receivable (A/R) and write-offs. **Support:** Due to problems during patient billing implementation, gross patient A/R for UHS increased to $1.6 million as of June 30, 2013, as compared to $670,000 at June 30, 2012. Related details include: • The allowance for doubtful accounts increased to $230,000 as compared to $108,000 at June 30, 2012. Given the age of the uncollected accounts, the allowance may not be adequate. • UHS was unable to access the MiChart collections module until June 2013, a full year after UHS MiChart went into production. • As of July 31, 2013, the MiChart Aging by	**Recommendation:** UHS should continue working with the MiChart Billing Team to troubleshoot ongoing billing and A/R problems, including correction of billing work queues and lack of reporting. The objective of this work should be to bill, follow-up, and collect patient charges promptly. **Management Action Plan:** UHS Administrative Director and Business Office Manager have arranged a meeting with the MiChart Professional Billing Senior Applications Programmer to develop a strategy for tracking and resolving ongoing billing and reporting issues on a timely basis. Several outstanding issues have been reassigned in the MiChart group in recent weeks. It is expected that a single point person will be assigned to work with UHS. As of September 30, accounts receivable were reduced to $1.1 million. **Action Plan Owner:** UHS Administrative Director

1. MiChart Implementation: Accounts Receivable — High

Payer report showed a $700,000 balance for uncollected accounts over 120 days old.

- One MiChart work queue was mislabeled (*2714 Do not touch UHS system copay undistributed catch all for deferral*). This caused approximately $300,000 worth of patient charges to not be billed.
- An unknown line item in A/R turned out to be valid patient pay accounts totaling $600,000 that needed follow-up collection efforts.
- There is a lack of meaningful reports from MiChart that provide detailed information to manage the A/R.

UHS was already addressing many of these issues prior to commencement of the audit.

Expected Completion Date: UHS goal for getting A/R in the $600,000 range - March 2014.

2. MiChart Implementation: Reporting Capabilities — High

Issue: UHS management is not yet able to effectively monitor their clinical and business operations due to the lack of adequate understanding and development of MiChart reporting tools.

Risk: Potential problems may go undetected and opportunities for improvement may not be identified.

Support: The previous UHS clinic management system was over 17 years old and was primarily a patient billing system with limited reporting capability. UHS management and staff have little experience or knowledge with the report writing capabilities of a robust clinic information system. The standard MiChart billing model, which was developed for a major academic medical center, was not designed for a student health service. MiChart has the capability to provide customized reporting to meet UHS operational needs.

Recommendation: Identify key performance indicators that management would like to track and monitor for UHS operations. Seek assistance from MiChart personnel to train UHS staff on development and production of MiChart reports that will provide meaningful operational reporting.

Management Action Plan: With the implementation of NextGen and MiWorkspace, UHS has reconfigured its IT department to be much more application focused. One systems analyst has been hired from MCIT and has been assigned responsibility for helping UHS navigate the UMHS environment to gain access to the people and resources needed to address these reporting issues. Another recently hired systems analyst has greatly enhanced our technical abilities to work on the various MiChart-related databases. A current UHS staff assigned to do MiChart training has been given additional training responsibilities. This person has also been assigned responsibility to work

2. MiChart Implementation: Reporting Capabilities

High

with our managers so they can learn how to pull reports from their own areas in MiChart. These three individuals will work closely with our certified MiChart report writer who is also a medical coder and can enhance the link between our technical staff and health care operations.

Action Plan Owner: UHS Administrative Director

Expected Completion Date: UHS goal is to make significant progress by March 2014, with continuing improvements thereafter.

3. MiChart Implementation: Check Out Procedures

Medium

Issue: The Nutrition and Physical Therapy clinics are not following MiChart check-out procedures.

Risk: Critical check-out activity such as receiving medical care instructions and scheduling follow-up appointments are not occurring consistently and could be detrimental to patient care.

Support: The Nutrition and Physical Therapy clinics do not require patients to go through a check-out procedure when no payment is due for the service provided. This situation occurs for student patients who are not required to pay for the service at the time of the appointment.

Recommendation: Develop clear guidance for MiChart procedures that require all patients to go through a check-out procedure. Provide guidance on implementation of this process in the clinics and monitor compliance.

Management Action Plan: The Director of Ancillary Services has directed the Nutrition and Physical Therapy clinics to implement procedures to check out all patients. On an ongoing basis, the Director will monitor the process.

Action Plan Owner: Director of Ancillary Services

Expected Completion Date: Completed.

4. IT Risk Assessment

Medium

Issue: The last risk assessment performed on UHS information technology (IT) systems and infrastructure is no longer valid due to recent changes in the UHS IT footprint.

Risk: UHS may fail to comply with the HIPAA Security Rule, which could result in civil and monetary penalties.

Recommendation: To comply with the HIPAA Security Rule, "Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by [UHS]." Schedule a new comprehensive IT risk assessment as soon as the

4. IT Risk Assessment

Medium

Support: UHS had a risk assessment performed by U-M Information and Technology Services (ITS) in 2010, which identified significant vulnerabilities. As part of mitigating the vulnerabilities, UHS transitioned to MiChart, MiWorkspace (an ITS managed desktop environment), Radiology Information System, and Laboratory Information System which reduced the amount of ePHI stored at UHS. UHS is also in the process of moving all local servers to ITS managed MiServer. Once this transition is complete, there will be no locally managed servers at UHS.

MiServer implementation is completed to validate efforts are providing the expected increased security.

Management Action Plan: UHS will arrange for ITS to perform a RECON security assessment in the third quarter of 2014.

Action Plan Owner: UHS IT Manager

Expected Completion Date: October 2014

5. Excluded Parties Screening

High

Issue: UHS is screening clinical staff against the federal excluded parties list but is not screening all employees.

Risk: UHS is at risk of noncompliance with federal regulations and could incur penalties and lose eligibility to accept Medicare patients.

Support: As a condition of accepting Medicare, UHS must screen all employees against the federal excluded parties list. The Office of Inspector General (OIG) has the authority to exclude individuals and entities from federally funded health care programs pursuant to the Social Security Act. UHS performs excluded parties screening on a monthly basis for their physicians, nurse practitioners, and physician assistants, but is not screening the entire UHS workforce.

Recommendation: UHS should include all employees in their monthly OIG exclusion list screening process. Coordinate with UM-Human Resources (HR) to include all UHS staff in periodic excluded party screening.

Management Action Plan: This function is now performed monthly on all UHS employees.

Action Plan Owner: UHS Administrative Director

Expected Completion Date: Effective immediately, management is manually screening all UHS employees against the federal excluded parties listing on a monthly basis. U-M Human Resources plans to institute systematic excluded party screening of all University employees within the next six months, which will allow UHS to suspend the manual process.

6. Procurement Practices: Business Associate Agreements

High

Issue: Required HIPAA Business Associate Agreements (BAA) are not in place with some vendors that have access to UHS protected health information (PHI).

Recommendation: U-M Procurement Services should immediately pursue agreements with all vendors that have access to patient information. When establishing new vendor relationships, UHS should make sure

6. Procurement Practices: Business Associate Agreements — High

Risk: UHS is at risk for incurring fines and penalties for patient privacy breaches.

Support: Seven vendors that have access to UHS patient information do not have an established HIPAA BAA. The BAA documents assurances from the vendor that:

- Systems and practices are HIPAA compliant
- Vendor will not use or disclose PHI except as permitted by law
- Vendor will cooperate with UHS to protect patient rights

The HIPAA rules require that covered entities enter into contracts to ensure that business associates will appropriately safeguard protected health information. The contract also serves to clarify and limit, as appropriate, the permissible uses and disclosures of protected health information by the business associate, based on the relationship between the parties and the activities or services performed by the business associate.

Procurement Services knows if the vendor will access patient information. UHS should perform annual monitoring of vendors to ensure current BAAs are on file for all vendors that access UHS patient information.

Management Action Plan: UHS has conducted an audit with Procurement Services of all existing contracts. Procurement Services is actively pursuing BAA agreements where needed. UHS Procurement will inform U-M Procurement Services when new vendors have access to patient information and monitor all applicable vendors on an annual basis.

Action Plan Owner: U-M Procurement Services and UHS Administrative Director

Expected Completion Date: December 2013

7. Procurement Practices: Use of Strategic Vendors — Medium

Issue: UHS does not always purchase medical supplies from vendors when there is an existing University vendor contract in place. One example is negotiated optical vendor contracts already in place at the Kellogg Eye Center.

Risk: UHS is paying more for medical supplies by using P-Cards, especially in the optical department.

Support: At University Audits' request, U-M Procurement Services performed an initial analysis of UHS spending and identified opportunities for cost savings using existing vendor contracts and relationships.

Recommendation: Work with U-M Procurement Services to analyze the UHS medical supply spending and establish more cost-effective procurement methods.

Management Action Plan: The Optical Shop is no longer using P-Cards to purchase supplies. UHS currently does take advantage of UMHS contracts in several areas such as Pharmaceuticals and IT consulting. UHS is currently working with UMHS Procurement to compare pricing with our common optical vendors. We will also work with Procurement to identify other common vendors that may be overlooked.

7. Procurement Practices: Use of Strategic Vendors — Medium

Action Plan Owner: U-M Procurement Services and UHS Administrative Director

Expected Completion Date: March 2014

8. Cash Handling Duties: Segregation of Duties — Medium

Issue: UHS does not always maintain segregated cash handling roles. Cashiers have both cash handling duties and daily deposit responsibilities.

Risk: Cash handling errors and misappropriation can go undetected.

Support: UHS collects and deposits over one million dollars a year in cash and checks. Testing of UHS daily deposits identified an incident where a cashier who prepares the daily bank deposit also collects cash in the clinics. Additional interviews with the Cashier Supervisor and analysis of cash handling roles determined this occasionally occurs when the cashiers need to cover for absent staff. According to Standard Practice Guide Section 519.03, *Cash Management Policies,* "University units must follow proper procedures and exercise internal controls when handling the collection and deposit of cash and checks. Necessary components of this system are: segregation of duties between personnel who process billing or receivables, receive funds, deposit funds, and those who reconcile transactions..."

Recommendation: Cashiers who perform bank deposit activities should not perform cash collection activities. On the occasion where this situation is unavoidable, the Business Office Manager or other management personnel needs to validate the deposit by reviewing and approving the daily batch cash reconciliation and the deposit packet.

Management Action Plan: UHS has implemented the recommendation to have the Business Office Manager review and approve daily reconciliations when there is insufficient separation of duties due to staffing issues.

Action Plan Owner: UHS Administrative Director

Expected Completion Date: Completed

9. PCI Compliance — Medium

Issue: UHS does not comply with Payment Card Industry (PCI) and Treasurer's Office standards. UHS management did not update the merchant contact and authorized staff information with the Treasurer's Office or make sure required staff credit card training is

Recommendation: The Administrative Director for UHS should identify the new Merchant Contact and complete the Merchant Change/Termination Form, located on the Treasurer's Office website. Once the Merchant Contact is assigned, an updated list of those

9. PCI Compliance — Medium

kept up-to-date. (TME 102 Merchant Certification)

Risk: If there was a data breach, UHS could face payment card issuer and industry fines along with losing the ability to perform credit card transactions.

Support: The individual who was identified as the merchant contact and responsible for tracking the annual training requirements is no longer working at UHS. This position has not been filled due to the ongoing work with Administrative Services Transformation (AST). Job responsibilities were divided among existing staff members at UHS but this responsibility was overlooked. PCI compliance standards and Treasurer's Office policy requires that the merchant contact and authorized staff are properly identified and trained:

- Merchant Registration Forms obtained through the Treasurer's Office showed merchant contact information and authorized staff that no longer work at UHS.
- 9 out of 21 individual's certifications for TME 102 have expired and one individual has yet to complete the initial certification.

personnel allowed to process credit card transactions should be submitted to the Treasurer's Office. The UHS Business Office Manager should be monitoring mandatory training for merchant accounts and identify personnel who need to complete the Merchant Certification training. Management needs to determine if other key job responsibilities remain unassigned.

Management Action Plan: The Administrative Director has submitted the Merchant Change/Termination forms with updated contact information as well as the updated authorized personnel list. While most of the staff have re-certified, the few remaining will be completed by October 31, 2013. Training requirements will be monitored regularly to ensure staff remain certified. UHS management will continue to review job responsibilities and re-assign as necessary.

Action Plan Owner: UHS Administrative Director

Expected Completion Date: Completed.

10. Patient Verification — Medium

Issue: UHS does not consistently verify patient's identification by requiring photo identification at registration or appointment check-in.

Risk: Medical identity misrepresentation can cause the provider to misinterpret medical history, previous medical tests, and medication allergies in the patient record. In addition, UHS will incur increased costs if unauthorized individuals use UHS.

Recommendation: Review current photo identification practices to ensure patient safety and consistent practices. Provide additional training on patient identifiers as needed.

Management Action Plan: UHS recognizes the concern for patient safety and the integrity of the medical record. UHS will review current identification practices and provide additional training on patient identifiers as needed. UHS will collaborate with UMHS Ambulatory Care to

10. **Patient Verification** — **Medium**

Support: The student environment increases the risk of nonstudents misrepresenting themselves as students to receive free medical care. Comparatively, Medicaid requires photo identification to deter fraudulent use of free medical services.

University policy requires all University faculty, staff, students, and retirees to obtain and maintain a single, current Universal Identification Card (MCard). The standard practice at the University is to show MCard identification to access University services and resources across campus. Photo identification is required to check out a library book or gain access to the recreation sports facility. UHS currently requires photo identification for the services at Laboratory, Pharmacy, and Medical Records but does not require photo identification for clinic appointments.

align identification practices. UHS will investigate whether use of a photo ID on a consistent basis is practical and whether we can use MiChart patient ID functionality. UHS will continue to check photo IDs if there is reason to doubt a patient’s identity.

Action Plan Owner: UHS Medical Director

Expected Completion Date: March 2014

11. **University Compliance Hotline** — **Medium**

Issue: UHS is not actively promoting the University Compliance Hotline to staff, students, patients, and others as a safe and confidential way to raise concerns regarding financial, regulatory, and patient safety issues.

Risk: Issues of non-compliance and concern may go unreported.

Support: Only one University Compliance Hotline poster was visible in a business area in the basement of the UHS building. No posters were visible on the other three floors, in the high-traffic public areas. In addition, in staff training materials, UHS was using an outdated phone number for privacy complaints.

Recommendation: Display University Compliance Hotline posters on all floors of UHS, visible in high-traffic areas for staff, student, and patients to see. Update information about the University Compliance Hotline in employee training material. Increase staff awareness and education of the Compliance Hotline.

Management Action Plan: Additional signs have been added to patient and staff areas. Staff were once again reminded by e-mail and will continue to be reminded of their responsibilities and how to access the hotline. Upon investigation, it was learned that the older phone number UHS had in its training materials had been forwarded to the hotline. However, UHS has updated all materials with the current number.

	Action Plan Owner: UHS Administrative Director **Expected Completion Date:** Completed

Follow–up Reviews

Payment Card Industry - Data Security Standard (PCI-DSS) 2013-310

Original report issued May 2013 Follow-up report issued October 2013

An audit of PCI-DSS compliance management processes was conducted and the report was issued in May 2013. A follow-up review has been conducted to assess the status and progress of management action plans that address identified issues. Significant progress has been made to complete the management action plans; however, one item remains open. A second follow-up will be conducted to assess progress on the remaining item during the third quarter of fiscal year 2014. **This audit remains open.**

Security Unit Liaison (SUL) PCI-DSS Training: The Treasurer's Office and Information and Infrastructure Assurance have developed a training packet designed to better inform Security Unit Liaisons about PCI-DSS. The packet requires Security Unit Liaison signatures attesting to having sufficient knowledge to mitigate PCI-DSS risks and understanding procedures to remain compliant. **Closed**

Self-Assessment Process: University Audits recommended that the Treasurer's Office develop a process to perform rolling on-site audits of select merchant accounts. These on-site audits should provide a greater level of confidence that the merchant is compliant with PCI-DSS and violations can be resolved before a breach of credit card data occurs. The Treasurer's Office has decided to obtain the services of a Qualified Security Assessor (certified by the PCI Council) to provide guidance and expertise in order to address PCI-DSS compliance concerns with the self-assessment process. **Open**

Required Vulnerability Scans: PCI-DSS requirements state that internal vulnerability scans must be performed. The audit identified that sufficient scanning was not conducted to meet PCI-DSS compliance. Information and Infrastructure Assurance began scanning units that accept credit cards using a Payment Card Industry Data Security Standard Page 2 payment application with an adequate scanning configuration to meet compliance requirements. **Closed**

Volunteer PCI Training: The audit identified that volunteers and other personnel were unable to complete the online PCI-DSS merchant training. The Treasurer's Office was advised to work with the Friends Gift Shop, and any other merchants that use volunteers for handling credit card transactions, to develop a process to ensure that all volunteers complete the required training. The Treasurer's Office has created a paper-based training packet to provide to units so staff such as volunteers can meet the training requirements. **Closed**

Matthaei Botanical Gardens Parking Meter Firewall: A compliance requirement was identified that requires systems accepting credit cards to be separated by a firewall from untrusted networks. A firewall was put in place which meets the compliance requirements stated in PCI-DSS. **Closed**

Payment Application Anti-Virus
A computer-based cash register with out-of-date anti-virus software was identified during the audit. PCI-DSS requires that anti-virus software should always be up-to-date. The unit updated the software and implemented a process to manually review the cash register computers for up-to-date antivirus software. **Closed**

University of Michigan Health System Friends Gift Shops 2013-310

Original report issued November 2012 Follow-up report issued October 2013

University Audits issued a report for the University of Michigan Health System (UMHS) Friends Gift Shops in November 2012. We recently conducted a follow-up review to assess progress toward addressing audit recommendations in several areas including cash handling, inventory management, and financial monitoring. Significant progress has been made in all areas, as noted below. **This audit is closed**.

Cash Handling Processes: At the onset of the audit, the Gift Shops were under new management. Practices established by previous management did not follow standard University cash handling practices and internal controls. Management substantially modified Gift Shops practices to align with University policies and processes and improved internal control. **Closed**

Changes included:

- Establishing an official Imprest Cash Fund through Financial Operations to use as a change fund
- Assessing and reassigning employee responsibilities so the person who prepares cash deposits does not reconcile deposits to financial records
- Requiring employees with cashiering responsibility to complete University online cash and credit card handling training courses
- Documenting new Gift Shops cash handling practices and building awareness among employees and volunteers
- Modifying credit card phone order forms so credit card number information is not retained after the sale is completed
- Investigating the feasibility of integrating the cash register and the credit card swipe machine

> **NOTE:** Due to vendor software limitations, it is not possible to process credit card transactions on the cash register in accordance with University and Payment Card Industry Data Security Standards. Management will continue to monitor software updates until the Gift Shops can integrate the two processes within university credit

card security standards. In the meantime, the Gift Shops will use separate approved credit card machines for credit card transactions.

Inventory Management Practices: Gift Shops lacked robust processes for managing inventory. Management took the following actions to strengthen inventory controls:

- Initiated a bar-coding process for store merchandise
- Purchased scanners and a dedicated laptop to process deliveries more quickly and accurately
- Contracted with a third-party vendor to complete a Gift Shops-wide physical inventory count and ensure all items are bar-coded
- Implemented a cycle count process to monitor and account for inventory
- Reviewed and revised the employee discount program to ensure compliance with University policy
- Installed software on select desktops to allow management to view security camera feeds
- Documented Gift Shops inventory processes

Management currently does not track inventory transfers between the four shops and the gift cart. Management will revisit this topic after the next full inventory count. **Closed**

Financial Monitoring and Reporting Practices: Management significantly improved financial monitoring and accountability by initiating processes to:

- Reconcile credit card sales and other financial activity on Statements of Activity
- Compare Gross Payroll Registers (GPR) to work schedules and hardcopy timekeeping reports
- Verify pay rates on GPRs
- Perform price audits to check for discrepancies between price stickers and prices entered in the point-of-sale system

Closed

Timekeeping and Scheduling Processes: Gift Shops management is considering the practicality of moving to the University's self-service timekeeping system. **Closed**

In the meantime, to improve timekeeping processes:

- Management follows University payroll policies regarding paid and unpaid work breaks
- Management created a delegation model to process payroll in the absence of the primary approver

Procurement Practices: Management discussed opportunities to reduce inventory costs with UMH Contracts and Procurement staff. Expense report approval workflows have been modified to include the Store Manager, who has greater knowledge about the validity and reasonableness of expenditures. **Closed**

Samuel Zell & Robert H. Lurie Institute for Entrepreneurial Studies 2012-222

Original report issued May 2013 Follow-up report issued November 2013

The Samuel Zell & Robert H. Lurie Institute for Entrepreneurial Studies (ZLI) revised several processes in response to audit recommendations from the audit report issued in January 2013. The unresolved items from our June 2013 follow up review have been remediated. **This audit is closed**:

Management Oversight

- Written documentation of key financial processes has been completed.
- ZLI leadership has formally documented procedures for escalation of missing documentation and late payments.
- Formal approval of financial transactions has been implemented.

Closed

C.S. Mott Children's Hospital and Von Voigtlander Women's Hospital Telecommunication Closets 2012-313

Original report issued January 2013 Follow-up report issued November 2013

An audit of the telecommunication closets at the C.S. Mott Children's Hospital and Von Voigtlander Women's Hospital (C&W Hospital) was completed and report issued in January 2013. A follow-up review has been conducted to assess the status and progress of management action plans that address issues identified in the report. The follow-up identified that significant progress has been made to complete the management action plans. **This audit is closed.**

Communication Cabling Layout: Ethernet cables entering the telecommunication closets in office and clinical portions of C&W Hospital were observed to be resting on drywall edges that showed signs of pinching and stress on the cables. A follow-up inspection of the rooms identified during the audit revealed that Medical Center Information Technology (MCIT) has installed devices to prevent the cables from resting on drywall edges allowing the cables to enter the closets reducing the risk of damage. **Closed**

Room Signage: Appropriate signage is necessary to facilitate adherence to proper procedures when working in the telecommunication closets, and providing quick access to critical information, for examplein the event of an outage due to human error. A visual inspection of the closets identified that proper room signage has been installed that describes the service level category for the room. **Closed**

Locking Cabinets and Doors: To mitigate the risk of damage resulting from improper physical access or accidental damage, University Audits recommended that locks be added to cabinets located in telecommunication closets. Follow-up confirmed all cabinets have been updated with locks. **Closed**

Environmental Temperature: Telecommunication rooms should be equipped with effective environmental monitoring systems. Adjustments in temperature should be made to the rooms that are colder than recommended so that their ambient temperature is raised to an appropriate level. Stakeholders should revise the certification and training manual to agree on a standard temperature that meets the cooling needs of the equipment while considering cost and a safe work environment. **Closed**

The rooms identified as being colder than recommended have been corrected to maintain an appropriate temperature. A room that did not report the temperature during the audit now correctly reports the temperature. A common temperature has been agreed upon by the appropriate stakeholders and documented in the manual.

Inventory Process: The audit identified several devices in the NurseCall system that were not entered into the BioMedical inventory management system. The recommendation was made to enter the devices into the system. BioMedical Device Management completed a full inventory and updated their inventory database to include all devices not previously entered into the system. **Closed**

Ownership: The telecommunication closet certification and training manual has been updated to include procedures for bringing issues to the attention of the governance group that oversees the closets. Issues that cross organizational boundaries have historically been difficult to resolve due to the division of responsibilities. Now that the certification and training manual has been updated and provides instruction, these issues can be addressed. **Closed**

Access Controls: Several user accounts for terminated employees were discovered on the access list that manages access to the closets. MCIT and Hospitals and Health Centers Security (HHC Security) committed to improving the process of de-provisioning access to the closets. MCIT and HHC Security have agreed upon an improved process to review access on a semi-annual basis. **Closed**

Security Camera Monitoring: The certification and training manual indicated that security cameras were to be installed in all telecommunication closets. MCIT opted to remove that requirement from the manual as costs outweighed benefits. The manual has been updated to remove the security camera requirement. Because cameras were not installed in accordance with this policy and security was judged adequate, elimination of this policy does not negatively affect security. **Closed**

Access Monitoring Controls: Procedures to gain access to the closets were inconsistent. Procedural gaps were identified by the discovery of missing documentation required for granting users access. HHC Security have modified their access control procedure to address the gaps and inconsistencies and collaborated with stakeholders to gain acceptance of the procedure. **Closed**

Servers in Communication Rooms: The telecommunication closets are designed to meet the availability needs of the life safety telecommunications equipment at C&W Hospital. The closets are not designed for hosting servers. Servers have a specific set of needs better suited for a data hosting facility. The audit found several servers located in the communication rooms that were installed without prior approval from MCIT. MCIT committed to work with Hospital Facilities to develop an authorization process for approval or denial of equipment in communication closets. The telecommunication closet certification and training manual has been updated to include a provision that defines the procedure for requesting equipment to be installed in a communication room. The manual also includes a statement that unapproved equipment will be removed at the equipment owner's expense. **Closed**

University Hospitals and Health Centers Community Health Services – Programs and Services 2012-214

Original report issued June 2013 First follow-up report issued April 2013
Second follow-up report issued December 2013

The University Hospitals and Health Centers Community Health Services-Community Programs and Services (CPS) audit report was issued on June 28, 2012. A follow-up review was performed and memo issued on April 17, 2013. At that time, management's action plans were in progress but not finalized. A second follow-up was recently conducted to determine the status of corrective actions taken. CPS management has put controls in place to address all of the audit issues, except one related to independent contractors. All audit issues are summarized below.

Interpreter Services Program - The Interpreter Services Program employs both contract and employee interpreters. The audit identified that time-worked reporting practices were inconsistent among independent contractors, staff interpreters did not consistently log office hours worked, and disclosure and conflict of interest statements were not consistently used.

Management Action Plan	April 2013 Status	November 2013 Status
Interpreter Services has implemented annual conflict of interest disclosure for newly hired interpreters. During the annual review process in August, all conflict of interest disclosures will be updated for existing staff.	In process	All interpreters have been directed to use M-Inform, the University's online conflict of interest disclosure system. **Closed**
Formal work standards, including consistent time keeping practices are under	Lead interpreters are periodically reminded to watch for and correct	Work standards for employee interpreters are in place. CPS is working with UMHS

development and will be communicated with staff.	inaccurate time reporting.	Procurement to identify contract terms and scope of work standards for independent contractors. **Open** - Expected completion March 31, 2014.

Monitoring Loan Activity - At the time of the audit, loan records for the Foreclosure Prevention Program were incomplete and inaccurate.

Management Action Plan	April 2013 Status	November 2013 Status
Housing Bureau for Seniors (HBS) management is in the process of reviewing loan records and updating the list of active loans and accounts receivable balances. Inactive older loans will be researched and written off if deemed uncollectable. A confirmation requiring a response will be sent to loan holders on an annual basis to verify loan status. Follow-up will be done with non-responding loan holders. Management will also explore other collection options.	HBS staff reviewed 118 files by performing an online search with the Washtenaw County Register of Deeds. The review resulted in identifying 39 cases ready to close due to foreclosure, death, loan discharge, or no lien in place. U-M Office of General Counsel reviewed and revised the mortgage and promissory note documents. Contact was made with all loan recipients and additional methods of follow-up are being explored.	The Foreclosure Prevention Loan Program manager met with UMHS Financial Services for assistance in discharging the uncollectible loans and writing off the accounts receivable balances. UMHS Financial Services will process the journal entries as part of November business and will set up a process with HBS staff to reconcile the loans and process necessary transactions on a regular basis. **Closed**

Cash Handling Practices - CPS has multiple sources of cash collections: donations, fundraising events, fees, billable services, and sales. The audit identified an inconsistent approach to cash handling across programs in the Department.

Management Action Plan	April 2013 Status	November 2013 Status
CPS program directors are in the process of developing standard cash handling processes and procedures across all collection points.	In process	CPS has developed cash handling procedures that are now included in the department procedures manual. **Closed**
Cash collections for guesthouse room fees are now collected centrally at Med Inn.	In process	In order to centralize cash collection of the guest house fees, the credit card terminal has been installed at Med Inn and staff have received credit card, cash handling, and

		depository training as appropriate to their duties. Collection of fees for the Wilmot House will begin at Med Inn in January 2014. **Closed**
CPS staff who handle cash will complete annual cash handling training.	In process	The requirement for staff to complete required training is documented in the cash handling procedures. Staff have completed required training. **Closed**
All cash collections will be reconciled monthly by an individual who is separate from the collection and deposit process.	In process	The requirement for proper segregation of cash handling duties is documented in the cash handling procedures. Reconciliations are completed on a monthly basis. Managers are reviewing the reconciliation to ensure separation of duties. **Closed**

Credit Card Controls - The Interpreter Services program accepts credit cards as a form of payment for classes and book sales. The program did not have proper controls in place over the use of credit cards. With the Guest House fees moved to central collection at Med Inn, CPS has improved customer service to house guests by offering payment by credit card.

Management Action Plan	April 2013 Status	November 2013 Status
Internal policies and procedures are under development.	In process	CPS has developed and implemented credit card control procedures that are now included in the department procedures manual. **Closed**
Staff are in the process of completing annual credit card handling training.	In process	The requirement for the Med Inn staff to take the credit card training has been written into the Med Inn contract. All Med Inn staff have completed the credit card training. CPS Director will monitor the completion of the required annual training. **Closed** All Interpreter Services staff

		have completed the credit card training. The Interpreter Services manager runs the appropriate report to maintain a roster of employees authorized to process credit card transactions and maintain documentation of the annual training requirement. **Closed**

Monitoring Accommodations Activity - U-M has contracted with Medical Hotel Management Corporation and Select Hotel Management Inc. as third party vendors to operate the Med Inn Hotel, which is used by inpatient family members and patients receiving outpatient services. At the time of the audit, CPS management provided limited financial oversight of the vendor activities that include control of hotel revenue and expenditures.

Management Action Plan	April 2013 Status	November 2013 Status
CPS has requested that Select Hotel Management provide monthly detailed financial reporting, including key indicators and budget variance reporting. On a monthly basis, CPS management will monitor trends and review reports and underlying documentation with the vendor.	In process	The CPS Director receives monthly financial operation reports from the vendor and meets with them on a bimonthly basis. The Med Inn manager tracks and the CPS Director monitor the guest house financial activity on a monthly basis. **Closed**

Training and Performance Evaluations for Hospital Volunteers - Volunteer Services manages a large staff of volunteers, many who work in the hospital. At the time of the audit, management was experiencing a low return rate for the Volunteer Orientation and Training Checklist from volunteers' supervisors, and had not implemented the departmental policy of completing annual performance evaluations of volunteer staff.

Management Action Plan	April 2013 Status	November 2013 Status
Management has reminded supervisors of the importance of completing, signing, and returning the checklist. Management will periodically review volunteer files to ensure checklists and performance evaluations are	The process has been changed on how Volunteer Orientation and Training Checklists are returned to the Volunteer Services Office. The volunteer is given a return-addressed stamped envelope and is instructed to send their TB test result along	In October 2013, Volunteer Services implemented a new database to enable coordination and management of the Volunteer Services business and operational processes. The new database provides the ability to track the Volunteer

completed.	with the Training Checklist to the Volunteer Services Office after their first day of training. Program manager stated that there is a better response with this new process.	Orientation and Training Checklist and the annual performance evaluations for volunteer staff. **Closed**
Annual performance evaluation criteria and process are under development.	No action has been taken on volunteer performance evaluations.	The Volunteer Services manager has developed the annual performance evaluation document and is in the process of implementing periodic evaluations. **Closed**

Annual Certification of Internal Controls and Gap Analysis - At the time of the audit, CPS management had completed the Annual Internal Control Certification but did not use the required gap analysis self-assessment tool to assess internal controls.

Management Action Plan	April 2013 Status	November 2013 Status
Management is in the process of completing the gap analysis assessment for fiscal year 2012 and is identifying gaps and updating processes. The process will be completed in time for the annual August 15th internal controls sub-certifications.	CPS Director completed the fiscal year 2012 gap analysis. University Audits recommended that for future internal control certifications, the gap analysis be completed by the individual program manager who will be most knowledgeable of program operations.	CPS Director delegated completion of fiscal year 2013 gap analysis to the individual program managers. In July 2013, UMHS Financial Services provided training to CPS staff on the process. A follow-up training session was provided in October 2013 to finalize the fiscal year 2013 gap analysis. **Closed**

CPS Director has emphasized to program managers the need to maintain controls and process improvements on an ongoing basis. University Audits will return in March 2014 to perform a final follow-up of the one remaining open issue.

Open Audits Follow-up Table
As of December 2, 2013

Audit Title	Report Date	Issues	Expected Completion
University of Michigan–Flint Educational Opportunity Initiatives 2010–211	2/18/2011	Strategic oversight and guidance; campus support and collaboration; budget and financial management; staff management; event management; business continuity; documentation of policy and procedure	First Follow-up April 2012 ______ Second Follow-up April 2013 _____________ Third follow-up December 2013
Division of Student Affairs Recreational Sports – Club Sports 2010–816	3/2/2011	Sponsored student organizations; guidance; financial management; practice, game, and fitness space; medical support; property	First Follow-up October 2011 ______ Second Follow-up April 2013 __________ December 2013
Financial Considerations for International Activity 2011–101	6/30/2011	Coordination of effort; documented policies and procedures	February 2014

Audit Title	Report Date	Issues	Expected Completion
UM–Flint Business Continuity 2011–303	8/12/2011	BCP standards template	First Follow-up March 2012 ___________ Second Follow-up December 2012 ___________ Third Follow-up September 2013 __________ Fourth Follow-up June 2014
e-Verify 2011-302	2/20/2012	Contract information; identification of employees; document retention; e-Verify notice requirements; subcontract language; e-Verify System user access	December 2013
University of Michigan Flint Office of the Provost 2012-204	4/17/2012	Strategic plan funding model and procedure; organizational structure and resources; policy and procedure manual; delegation of authority; management oversight; gift fund management;	First Follow-up April 26, 2013 ___________ December2013
Information and Technology Services DNS - Domain Name Service 2012-301	5/2/2012	Recursion on authoritative name servers; host operating system; performance metrics; server access	First Follow-up January 7, 2013 ___________ Second Follow-up April 2013 ___________ December 2013

Audit Title	Report Date	Issues	Expected Completion
UMHHC Community Health Services-Community Programs and Services 2012-214	6/28/2012	Interpreter services	First follow-up April 2012 ___________ Second Follow-up December 2013 ___________ April 2014
UM-Dearborn College of Engineering and Computer Science 2012-302	6/29/2012	Financial oversight; documented policies and procedures; conflict of interest and commitment; training and facility safety; contracts, grants, and agreements; asset management; gift handling and monitoring; Engineering professional development; incident response plan; key logs; vulnerability scans; configuration control policy; disaster recovery plans of IT; data security procedures	January 2014
Transportation Research Institute 2012-502	9/13/2012	Standardized project management; compliance with University guidelines; fiscal responsibilities; monitoring and budget reporting; information technology controls; documented procedures and expectations	October 2013
UMHHC Wireless Medical Devices 2012-315	10/29/2012	Wireless connection security; inclusion of MCIT in the procurement process	February 2014

Audit Title	Report Date	Issues	Expected Completion
Residential Dining Service 2012-216	11/21/2012	Financial management and oversight; CBORD training	First follow-up issued September 2013 March 2014
Travel and Expense Management System 2012-103	11/27/2012	Central Monitoring; unit reporting; training and customer service; data validation; expense report auditing	December 2013
MCommunity Enterprise Directory and Identity Management System 2012-310	1/11/2013	MCommunity server security; service agreements, identity management policy; server access; password hub; test environment; security information and event management; SIEM security	February 2013
Office of the Vice President for Global Communications and Strategic Initiatives 2012-211	1/30/2013	Procurement management; oversight; document retention; delegation of authority; A/R reconciliation; impress cash; conflict of interest/commitment; temporary staff appointments; timekeeping	January 2014
Law School 2012-208	02/04/2013	Disclosure of Conflicts; Fund Establishment; Event Reconciliation; Administrative and Staffing Efficiencies; Procurement Compliance; Clinic Administration; Gift and Cash Handling; International Travel Registry; VendaCard Dispenser Form	December 2013

Audit Title	Report Date	Issues	Expected Completion
School of Information 2012-215	3/22/2013	Development office procedures; faculty appointments; continuity of operations; RECON; travel registry; Concur approval	December 2013
Detroit Center 2012-814	4/8/2013	General control environment; financial monitoring and oversight; funding model; space management/reservation system; procurement, travel, and hosting; continuity of operations planning; asset management	December 2013
University Unions 2012-201	4/25/2013	Supplemental systems; imprest cash funds; payroll processes – AFSCME overtime record keeping; documented procedures; credit card merchant processes	December 2013
Medical School Department of Family Medicine 2013-211	04/25/2013	JEPP program; physician compensation model; procurement practices;	December 2013
Medical Center Information Technology and Arbor Lakes/North Campus Data Centers 2012-307	4/26/2013	MCIT Managed Data Centers lack a comprehensive continuity of operations plan	COOP Meetings June 2013 September 2013 ___________ Next update scheduled for March 2014

Audit Title	Report Date	Issues	Expected Completion
College of Literature, Science, and the Arts Kelsey Museum of Archaeology 2012-201	4/26/2013	Museum store purpose and objective; inventory management, pricing and security; cash handling; use of a cash register; change fund; security staff; security training; physical access control; international travel planning	March 2014
Molecular and Behavioral Neuroscience Institute 2012-211	5/15/2013	Long-term financial viability; business practices; billing and lab safety and security; information technology management;	December 2013
Knight-Wallace Fellows Program 2013-202	6/18/2013	Procurement; time and pay; administrative processes	December 2013
Frankel Center for Judaic Studies 2013-219	06/20/2013	Expense reporting; cash handling; international travel registry; conflicts of interest/conflicts of commitment; administrative procedures	January 2014
Office of Student Publications 2013-203	07/18/2013	Strategic Plan and Vision; External Bank Account/Student payments; Documented Policies and Procedures; training; accounting system; IT services; recharge rates; Internal Controls certification and Gap analysis; procurement contracts; imprest cash fund; facility access; travel approval and tracking; COI/COC	March 2014

Audit Title	Report Date	Issues	Expected Completion
School of Natural Resources and the Environment 2012-210	09/06/2013	Center/institute oversight; effort certification; admissions documentation; lab safety; documented processes	April 2014
UM-Dearborn College of Arts, Sciences, and Letters 2013-204	9/30/2013	Financial oversight; conflicts of interest/conflicts of commitment; safety of minors; agreements with third parties; faculty course releases and stipends; records and advising; roles and responsibilities;	June 2014
UM-Dearborn Office of Financial Aid 2013-201	9/30/2013	Peer review recommendations; fund reconciliation; Banner award testing; business continuity; documented policies and procedures; OFA wolkload assignment; employee training; concentration of duties; conflicts of interest or commitment;	June 2014
ITS Implementation of M+Box 2013-310	10/13/2013	Review of administrative accounts; de-provisioning of user accounts	April 2014

Audit Title	Report Date	Issues	Expected Completion
College of Engineering Research Software Licensing 2013-310	10/21/2013	Software licensing and usage; software for commercial research; acceptance of "click-through" licenses; tracking of software licenses in nanotechnology labs; creation of a research lab; definition of PhD student; recording software purchases to program codes; software purchases classified as professional licenses	April 2014
Donor & Alumni Relationship Tool (DART) 2012-103	10/24/2013	Changes to the Default Master Encryption Password; OUD Dev/Net Web Application Security; DART Web Application Security; Network Vulnerabilities; Terminations and Periodic Review of User Access; Organization of Key Information; Assignment and Completion of Project Tasks; Ongoing User Training; Use of Help Desk Questions; System Utilization Metrics	April 2014
A. Alfred Taubman Medical Research Institute 2013-310	10/30/2013	Gift funds; award recipients outside U-M; Scholar award accountability; establishment of project/grant in University systems; unspent funds; Scientific Advisory Board	April 2014

Audit Title	Report Date	Issues	Expected Completion
University of Michigan-Flint Banner System 2013-310	11/05/2013	Java update process; access revocation process; web application vulnerabilities; vulnerability scanning; encryption of PPI; Access of PPI; audit logging guide; system documentation	May 2014
Student Life University Health Service 2013-206	11/13/2013	MiChart implementation: accounts receivable, reporting capabilities, check out procedures; IR risk assessment; excluded parties screening; procurement practices: Business associate agreements, use of strategic vendors; cash handling duties: segregation of duties; PCI compliance; patient verification; University Compliance Hotline;	May 2014

Appendix 1: Audit Issue Risk Definitions

Risk	Definition
High	• This issue describes a control breakdown with a combination of potential impact and likelihood of occurrence to create **significant risk** to the audited entity. A high-risk issue generally requires **immediate** corrective action, or implementation of an interim control to minimize the risk until permanent corrective actions occur. • A high-risk issue could be a repeat medium-risk issue (i.e., during the last audit, the same issue was reported, but was not corrected on a sustainable basis). • University Audits generally follows up on high-risk issues within six months after the audit, and requires unit management to provide a status within three months after the audit.
Medium	• This issue describes a control breakdown with a combination of potential impact and likelihood of occurrence to create **enough risk** to require corrective action **within six months**. • A medium-risk issue could be a repeat low-risk issue (i.e., during the last audit, the same issue was reported, but was not corrected on a sustainable basis). • University Audits generally follows up on medium-risk issues within six months after the audit, and requires unit management to provide a status within three months after the audit.
Low	• This issue describes a control breakdown with potential impact or likelihood of occurrence to create **low-risk** and attention by unit management. Low-risk issues do not require senior management attention. • Low-risk issues are not included in the audit report; instead, they are reported directly to management of the audited unit. • University Audits does not formally follow-up on low-risk issues.

Appendix 2: Audit Issue Follow-Up Process

High and Medium Risk Issues: Every three months until completed, unit management should report the status of their action plans to University Audits. At six months, and every six months thereafter until the actions are completed, University Audits will conduct follow-up procedures to verify the actions are complete and are effectively managing the risk. University Audits will summarize the results of each six-month follow-up review in a written memo.

Low Risk Issues: Unit management is expected to address all low risk issues, which may be reviewed during our next audit. However, a status update is not required and University Audits will not conduct follow-up procedures.