UNIVERSITY OF MICHIGAN

REGENTS COMMUNICATION

Item for Information

Subject: Report of University Internal Audits

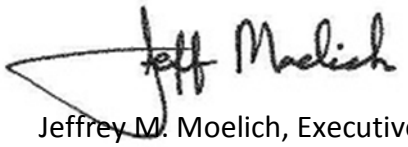
Attached is the report of activities completed by the Office of University Audits for the period **May 1 through June 30, 2015.**

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 **June 30, 2015**, 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,



Jeffrey M. Moelich, Executive Director
University Audits

OFFICE OF
UNIVERSITY AUDITS
UNIVERSITY OF MICHIGAN

Board of Regents
Internal Audit Reports –May 1 through June 30, 2015
September 17, 2015

Table of Contents

Reports Issued

College of Engineering: Electrical Engineering and Computer Science Department 2013-213

Report issued June 2015

A. Executive Summary

1. Overall Conclusion

The College of Engineering (CoE) provides substantial oversight and administrative support, allowing the Electrical Engineering and Computer Science (EECS) department, which is organized in two divisions, to focus on their mission of teaching and research. The two divisions coordinate business processes and have consolidated and streamlined some procedures. Examples include an internal purchasing approval system used by both divisions, shared human resources (HR) staff and processes, and a collaborative approach towards decisions affecting the department. EECS has strong financial and operational controls except for asset management.

Asset management in both divisions is not always proactive. An equipment and data intensive discipline such as engineering needs accountability and strong controls around equipment and data management. There are opportunities to improve controls to effectively secure and track high-value equipment and information assets. We are separately making recommendations to the Office of Property Control to provide better guidance and more timely equipment tagging.

2. Context and Key Risk Considerations

EECS is the largest department in CoE. EECS is a source of significant technology transfer, generating more inventions, agreements, and business start-ups than any other U-M unit. EECS is organized into two divisions, Computer Science and Engineering (CSE) and Electrical and Computer Engineering (ECE). A chair leads each division, with both acting as co-chairs for the department.

The undergraduate computer engineering degree unifies the department, with each division supporting other degrees and fields of study. The department offers bachelor degree programs in Electrical Engineering, Computer Science, and Computer Engineering. They offer masters of science and doctoral programs in Electrical Engineering, Electrical Engineering: Systems, and Computer Science and Engineering. The courses offered as well as enrollment numbers continue to grow rapidly. EECS currently has approximately 150 faculty members, 1,490 undergraduates, and 890 graduate students. EECS had more than $50 million in research expenditures and overall operating revenue of $98 million in fiscal year 2014.

EECS is located on North Campus with ECE housed in the newly renovated EECS Building and CSE in the newly constructed Bob and Betty Beyster Building. Both buildings contain a large amount of space dedicated to research, as well as teaching, student teams, and collaboration. Each division has multiple labs, each with a lab manager and staff. The Lurie Nanofabrication Facility is the largest lab in the EECS Building with over 20,000 square feet of cleanroom space. The fee-based facility is used by hundreds of internal and external researchers annually and is supported by its own team of engineers and technicians.

3. Audit Scope and Identified Risks

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

	Key Activities Audited					
	Grant Management	**Conflict of Interest/ Commitment**	**Asset Management and Lab Safety**	**Oversight of Finances**	**Visiting Scholars and International Travel**	**Recharge and External Services**
Sub-activities Audited	Federal and sponsored research procedures	COI/COC policy	Asset management process (Issue 1)	Gap analysis and internal control certification	Appointing and processing visitors	Recharge rate approval process
	Subcontract management and oversight	COI/COC reporting process	Asset tracking and tagging (Issue 1)	Financial oversight	Tracking visitors and requirements	Tracking services and usage
	Effort reporting	Conflict management	Off-site assets (Issue 1)	Discretionary funds	International travel	Billing
	Export controls	Compliance with university policies	Lab safety inspections	Account reconciliation		
	Security of research data (Issue 3)			Cash handling and credit cards		
				Centers and institutes oversight		

Sub-activities Audited	Gifts	Tech Transfer and Start-ups	Governance and HR	Purchasing	Financial Aid
	Monitoring gifts	Coordination with the Office of Technology Transfer	Committees and bylaws	Vendor utilization	Budgeting, awarding, and monitoring
	Endowed and designated funds	University policy and requirements	Interaction with minors (Issue 2)	Approval, oversight, and monitoring	Coordination with the Office of Financial Aid
	Non-cash gifts	Royalty revenue	Temporary employees	P-Cards	Management and monitoring of GSI's and GSRA's
			Special/ supplemental pay		
			Division coordination		

Legend: Overall risk conclusion for each sub-activity		
High Risk	Medium Risk	No Issues Reported

4. Audit Objectives

The objectives of this audit were to:

- Assess whether the process to manage research administration and effort reporting are consistent with university and departmental policies and key federal and sponsor requirements.
- Verify the conflict of interest/conflict of commitment (COI/COC) policy has been approved by the Office of the Provost, has been communicated to faculty and staff, and implemented with management plans where appropriate.
- Verify facilities are managed appropriately and that there is a process to tag, track, and report assets to Property Control. Validate that the corrective actions recommended during OSEH lab inspections were addressed.
- Verify appropriate financial oversight and monitoring to ensure appropriate use of university resources.
- Validate compliance with university policies and confirm there are appropriate policies and procedures in place to ensure safety of faculty, staff, and students.
- Validate compliance with university policies for visiting scholars and international travel.
- Determine whether recharge rates are accurate and billed in a timely manner.
- Determine the adequacy of procedures to ensure that restricted gifts are processed appropriately and used according to donor intent.

- Verify appropriate oversight of intellectual property.
- Evaluate compliance with the university human resources policies and the effectiveness of the governance structure within EECS.
- Determine whether purchasing controls are sufficient to demonstrate good stewardship and adherence to university purchasing guidelines.
- Determine whether unit-sponsored financial aid adheres to university policy.

B. Audit Issues and Management Action Plans

This section of the report provides details of the high and medium risk issues identified during the audit. See Appendix 1 for risk definitions.

1. Management of Assets	Medium

Issue: The department does not completely and accurately track and reconcile equipment.

Risk: Valuable assets critical for teaching and research may be lost, stolen, or damaged and go unnoticed, leading to potential forfeiture of federal funding and misstatement of financial records.

Support: The EECS department has a current net book value of $19.4 million in equipment assets, $1.0 million at CSE and $18.4 million at ECE. The Property Control Inventory Manual states that it is each department's responsibility to ensure the university's equipment that has a value greater than $5,000 is accurately recorded by performing an inventory reconciliation at least once every two years. Each department is required to conduct a physical inventory, compare the results to central equipment inventory records, and make all necessary adjustments. The last physical inventory was conducted in February 2014. Based on our testing, numerous discrepancies were noted in the most recent asset reconciliation.

Due to academic and research needs, and to avoid unnecessary spending, some high dollar equipment is portable and shared between labs. Assets can be moved within EECS multiple times each year. Additionally, there are fabricated assets that the researchers create in the labs by taking apart certain equipment, or combining multiple pieces of equipment into new equipment.

We tested thirty-five assets, ten for CSE and twenty-five for ECE. During the validation, we noted that:

- Some assets with a value higher than $5,000 (e.g., a robot, 3D printer, probe station and server) were not tagged.
- Some assets were retired prior to the inventory reconciliation in 2014 but this information was not communicated to Property Control.
- Some assets were difficult to find due to unfamiliarity of the assigned custodians with the current location of the assets.

In addition, there was one asset that did not belong to EECS but was located in their lab without a known reason. It took several weeks to locate all the equipment but all assets selected for testing were located in the end.

1. Management of Assets	Medium

Below are some additional observations that we noted:

- The current process does not require the facilities managers to be closely involved with the asset reconciliation; the lab managers mostly handle the process. Some equipment inventory responses provided to Property Control were incomplete and were not reviewed by the facilities managers.
- Communication between the staff involved with the asset reconciliation process is not effective; specifically, the ECE division did not contact the facilities manager at a non-College of Engineering location for validation of EECS equipment during the most recent asset reconciliation review.
- In some cases, procurement staff are assigned as custodians by the system defaults. These individuals are not familiar with the asset and its whereabouts. The custodian listed in inventory records should be generally knowledgeable about the asset and its location.

Recommendation:

1. Due to the complexity, value, and size of the EECS equipment inventory, consider conducting periodic cycle counts to detect untagged assets or record updates. Additionally, update the records for the assets that have been disposed of but not communicated to Property Control. Going forward, coordinate all assets that are ready for disposition with Property Control.
2. Educate staff, including facilities and lab managers, on Property Control procedures and their responsibilities for maintaining accurate and complete equipment inventory records to ensure the on-site and off-site inventory is counted and reviewed in detail when responding to Property Control's requests. Management should monitor the process and confirm that equipment existence is physically accounted for.
3. Consider changing current assignment of responsibilities:
    a. Facilities managers should be more involved during the account reconciliation process and be a key contact for Property Control. All responses from labs should be coordinated by facilities managers for better tracking and accountability.
    b. Assignment of custodians should align with the individual's role and familiarity with the asset, its changing location, and the lab.
4. Seek guidance from Property Control for tagging situations that are outside of the norm (e.g., fabricated equipment).
5. Assets that cannot be tagged (e.g., special handling due to sensitivity of the equipment, size of the asset) should follow the special tagging process directed by Property Control.

Management Action Plan:

1. Improve Departmental Business Process Document for Asset Inventory to include:
    - Assignment of duties
    - Assignment of custodians
    - When to seek guidance from Property Control for situations outside of the norm
    - Periodic cycle counts
    - Updating of assets to include disposed and repurposed equipment

1. Management of Assets	Medium

2. Educate staff on Property Control procedures
3. Change primary responsibility for assets from lab managers to facilities managers
4. Obtain custodian list from Property Control and review custodians and correct if necessary
5. Confirm that the verified equipment inventory lists from February 2014 are still accurate and update the system as necessary

Action Plan Owners: CSE and ECE department managers

Expected Completion Date: No later than November 2015 – it will be the time when Property Control initiates next bi-annual survey

2. Compliance with Policy on Minors	Medium

Issue: Background checks were not performed on any faculty, staff, or volunteers prior to the 2014 summer camp run by CSE.

Risk: Safety and security standards for programs with minors may not meet university requirements.

Support: Standard Practice Guide (SPG) Section 601.34, *Policy on Minors Involved in University-Sponsored Programs or Programs Held in University Facilities*, requires all programs and activities involving minors to follow a set of guidelines. This includes program registration and use of participant forms. Additionally, all authorized adults and program staff must adhere to an established code of conduct, submit to a criminal background screening, and complete training. The SPG was issued in January 2014 with the university requirements for background checks implemented on June 1, 2014.

In 2014, CSE offered their first computer summer camps for high school students. These day camps introduce college-level topics at an introductory level to high school students. The camps were held through June and July, which was within weeks of when the background checks became a requirement. Background checks were completed for the two faculty members running the course in November 2014, which was after the camp ended. Background checks were not completed for the staff or students that assisted with the camp. All other aspects of the policy requirements, such as program registration and staff training, were completed.

In 2015, ECE and CSE are both offering day camps for high school students. This will be CSE's second year and ECE's first year managing programs involving interaction with minors.

Recommendation: Conduct criminal background checks on all faculty, staff, and students involved in the upcoming summer camps as required by university policy. Confirm that the background checks are completed and evaluated prior to individuals working with minors.

2. Compliance with Policy on Minors	Medium

Management Action Plan: Background checks will be conducted on staff, faculty, and students scheduled to work with minors on departmental activities. In particular, this step is included in our overall camp checklist. Camp staff and the department HR manager will work together to run background checks on temporary hourly students at time of hire. The EECS department will run background checks on permanent staff and faculty when they are involved with events involving minors. All background check approvals will be tracked to ensure compliance.

Action Plan Owners: CSE and ECE Department Managers

Expected Completion Date: Immediately

3. Information Security	Medium

Issue: A comprehensive security risk assessment has not been performed on all sensitive and critical information assets.

Risk:

- Loss of intellectual property
- Loss of research data and funding
- Unauthorized data transfers

Support:

- SPG 601.27, *Information Security Policy* states, "each university unit will periodically identify and track sensitive and critical information assets under its control….risk assessments will prioritize risks and recommend appropriate mitigation strategies."
- A risk assessment has not been conducted on systems that are likely to contain sensitive, regulated, or high value intellectual property data, including the EECS-managed research information systems. The department has scheduled a Risk Evaluation of Computers and Open Networks (RECON) with Information and Infrastructure Assurance for early calendar year 2016.
- University Audits did not perform an in-depth review of IT security but identified no specific concerns related to the security environment in EECS.

Recommendation: In preparation for the upcoming RECON:

1. Identify and classify sensitive and critical information assets under EECS control. Information assets should be classified relative to the level of risk that their compromise may pose to the institution.
2. Ensure all sensitive and mission critical information assets managed by EECS are included in the RECON process.
3. Information and Infrastructure Assurance can provide guidance and support for this process.

3. Information Security	Medium

Management Action Plan: We have recently conducted a review of all information assets and will categorize them according to the level of risk that their compromise would pose to the institution. We will then work with Information and Infrastructure Assurance to ensure that all information assets are assessed through the RECON process.

Action Plan Owner: Information Systems Operations Manager

Expected Completion Date: The date is dependent upon migration to MiWorkspace decision and Information and Infrastructure Assurance's schedule.

Auditor's note: An expected completion date will be discussed and established with EECS management during the first follow-up discussion, three months after the report has been issued.

Computer Showcase 2015-203

Report issued June 2015

A. Executive Summary

1. Overall Conclusion

Information and Technology Services (ITS) manages the Computer Showcase (Showcase), which operates as a retail and repair service for U-M students, faculty, and staff. Showcase has two full-service locations: one on central campus inside the Michigan Union and one on north campus inside Pierpont Commons. Showcase is dealing with a changing retail environment and current management has inherited legacy operational inefficiencies. This, coupled with an incomplete view of current business processes, presents a complex challenge to the new Showcase leadership, which began developing plans to address these challenges strategically in 2014.

Computer Showcase is currently operating at a loss. The difficulty of competing with online vendors and local retail stores makes achieving financial sustainability a challenging goal. To enhance operational effectiveness, Showcase needs to assess current retail operating practices in an evolving higher education market and improve certain business practices to influence positive outcomes. There are opportunities for improvement in areas such as inventory management, service unit billing, credit memo reconciliations, payment processing, and the information technology used to drive informed business decisions.

2. Context and Key Risk Considerations

Showcase's mission is "*to be a destination on campus to learn and experience new technology" using "knowledgeable staff who can help the campus community find the best technology to help further the mission of the university and provide support when needed."* The ITS executive director for support services, ITS assistant director of consumer technology experience, and the program manager for Computer Showcase

and Tech Repair are all new to the university, resulting in this transition audit. ITS administration monitors Showcase's financial activities and understands auxiliary services must remain financially solvent in order to remain viable service offerings to the university community.

Showcase sales and repair functions report as separate operations. Due to vendor agreements (e.g., educational discounts), most of Showcase's products and services can only be offered to active U-M faculty, students, and staff. Showcase's retail division employs 7.5 full-time equivalents, including a program manager, business manager, sales manager, inventory coordinator, and a full-time IT support professional, as well as numerous temporary student employees. Showcase's retail goal is to break even. However, sales are declining; falling almost $2 million (from $11 million to $9.1 million) between fiscal years 2011 and 2014. Cumulatively, Showcase and Tech Repair have been operating at a deficit, posting losses ranging from $104,000 to $902,000 dollars in fiscal years 2011 through 2014. As of June 30, 2014, the operating fund balance was negative $1.4 million.

Between fiscal years 2011 and 2014, Showcase's profit/loss margin fluctuated widely and revenues declined. Potential causes include:

- Showcase is in direct competition with educational discounts and repair services offered at other area retail stores
- Sale margins on products are intentionally small to both stay competitive and provide a service to the university community
- Evolution of consumer spending habits including online retail options and existing pre-college electronic purchases
- General awareness of Showcase services and sales opportunities are not optimal due to low-visibility and sparse foot traffic
- Lack of ample parking at either location
- Vendor limitations on who may purchase goods and services from Showcase
- Computer Showcase is not presently a university preferred vendor

Showcase management is working to increase sales by focusing on three strategic areas:

- Investigating and pursuing revenue opportunities
- Reducing waste and increasing efficiencies
- Reevaluating and expanding customer base

3. Audit Scope and Identified Risks

The table below lists the key activities audited, along with the overall risks of the audit issues identified for each sub-activity. The scope of the audit was determined based on an assessment of the risks associated with activities related to Showcase retail sales and repair services. This process included input from ITS administrators and staff.

	B. Key Activities Audited					
	Inventory Management	**Repair Services**	**Physical and Technical Controls**	**Financial Monitoring and Reporting**	**Cash and Credit Card Handling**	**Unit Fiscal Responsibility**
Sub-activities Audited	**Segregation of duties (Issue #3)**	Certification assessment	System configuration and security	Budget process	**Segregation of duties (Issue #3)**	Hotline awareness
	Purchasing activity	**Purchasing activity (Issue #3)**	User accounts (Issue #5)	Daily sales reports	Change funds and employee certification	Timekeeping and scheduling
	Pricing and obsolescence strategy	Warranty activity	Firewall (Issue #6)	**SOA reconciliation and exception reporting (Issue #1)**	**Cash handling and deposit management (Issue #1)**	Payroll analysis
	Inventory counts and reconciliation (Issue #1)	**Customer data handling (Issue #2)**	Point of sale systems (Issue #7)	**Tax reporting (Issue #1)**	**SUB reconciliation (Issue #1)**	P-Card holder limits
	Vendor credits and rebates (Issue #1)	**Unclaimed property (Issue #2)**	Physical security and surveillance (Issue #8)	Payroll deductions (Issue #4)	Cash refunds and employee discounts	P-Card purchasing activity
	Gift card reconciliation		Credit card terminal security		Credit card handling and refunds	
	Key:	**High Risk**	**Medium Risk**	**No issues reported**		

4. Audit Objectives

The objectives of this audit are to:

- Assess the efficacy of processes for managing and tracking inventory
- Assess the adequacy of cash controls, including the use of change funds
- Evaluate sufficiency of controls to monitor financial transactions and reporting activity
- Assess workforce scheduling and payroll controls
- Evaluate purchasing controls
- Assess overall security of assets
- Determine effectiveness of controls over repair services
- Assess adequacy of credit card terminal controls
- Assess effectiveness of physical and technical controls
- Evaluate credit card and refund handling processes

B. Audit Issues and Management Action Plans

This section of the report provides details of the high- and medium-risk issues identified during the audit. See Appendix 1 for risk definitions.

1. Operating Procedures	High

Issue: Management has not reassessed and updated retail operations in accordance to university fiscal guidelines. An overall lack of understanding of availability and use of financial reports hamper efforts to significantly improve operational practices.

Risk: Inefficient practices could lead to revenue losses and inventory shrinkage, compromise vendor relationships, and result in extra effort to investigate avoidable discrepancies.

Support: University-recommended business practices are not always used for key business functions.

- Exception reporting: Management receives various M-Pathways system reports, but has not developed exception reports that may be critical in identifying adverse trends and anomalies.

- SOA reconciliation:
  - Invoices for partial orders are not investigated when internal reports show all items were received indicating readiness to be billed.
  - Although some invoices are reviewed and approved for payment, SOAs are not comprehensively reconciled, creating a risk that inventory purchases could be overpaid without notice.
- Sales process: Customers do not always show university identification, making it possible to circumvent Showcase sales guidelines, which can lead to issues with collectability of receivables.
- Inventory process: Inconsistencies may be concealed when physical inventory counts are not performed at each location on the same day and all counts are planned (i.e., no surprise spot checks). Physical counts taken by hand versus with a hand held collector and barcode scanner take more time and use more resources. Investigations of overages and shortages do not include reviewing credit memos to verify inventory adjustments associated with returns to vendors were handled correctly. The inventory team is not involved in pulling together and reconciling inventory used at off-site pop-up sales.
- Vendor credits and rebates: Credit memos and rebates, including vendor refunds for returned inventory and sales rebates for inventory purchases, are not always tracked and reconciled promptly.
- Cash management process:
  - Multiple cashiers work each cash register and individual cashiers may work more than one register during the workday making it difficult to assess responsibility for cash discrepancies and acceptance of counterfeit bills.

1. Operating Procedures	High

- Checks received by mail were not always kept in a secure location.
- Managers do not always prepare deposits in a closed area inaccessible to customers or conceal deposit bags while in route to depositories.
- Errors preparing deposits have resulted in misrouted funds and delayed deposits, resulting in the appearance of missing daily cash deposits.

- Security process: Daily sales information is not maintained in a secure location. Access to daily sales information provides information about the amount of cash in the store to employees, cleaning personnel, and other individuals who do not need to know the amount of collections in order to perform their job duties.
- Sales tax reporting process: The sales tax reporting process is overly complex and precludes the preparer from reviewing first-hand sales reports or other source information to support tax reports. Spreadsheets used in the process may contain extraneous information already reported on other internal reports. Properly formatted and protected spreadsheet templates could significantly reduce the amount of time required to prepare tax reports.
- Service Unit Billing: Payments from student account billings are not always reconciled to verify all receivables are credited. Sales data in journal entries do not always match data in files sent to Student Financial Services or the Payroll Office.

Recommendation:

- Explore training opportunities to gain a better understanding of current operating procedures for an academic retail environment. Enhance controls over critical business practices to decrease risks of losing valuable assets.
- Fully analyze business operations and develop exception-based reports for critical processes to identify opportunities for improvement. More consideration should be put into generating reports that are useful and meaningful at each management level. Business processes need to be better understood so the right reports can be designed and assigned to appropriate individuals for review.
- Refine Statement of Activity (SOA) review processes to verify the accuracy of payments and charges.
- Refer to and implement other suggestions in the *support section*.

Management Action Plan: The Computer Showcase has many business practices extensively documented and followed. Showcase has an opportunity to build upon this and better align training.

- Showcase will perform a comprehensive review of all processes and procedures. New documentation will be created and existing documentation will be updated, where needed. The end goal would be to have a cohesive repository of processes and procedures that will be consistently maintained and which all staff are trained to leverage. ITS has assigned resources to help with this effort.

1. Operating Procedures	High

- Based on the results of the above review, we will reassess existing exception based reporting to ensure proper identification of risks for critical processes at all levels of management. New reports will be created and existing reports will be updated, where needed.
- We will improve existing SOA reconciliation processes to ensure accuracy of charges.

Action Plan Owner: Computer Showcase program manager

Expected Completion Date: November 2015

2. Customer Data (Repair Services)	High

Issue: Showcase does not always follow their own policy on the handling and disposal of customer data.

Risk: Storing data obtained from a customer's hard drive on U-M systems and not erasing the data in a timely way increases the risk of unintentional data leakage. Leaked or misused customer data may contain sensitive research data, financial information, health records, or other personally identifiable information that could result in reputational damage and fines to the university.

Support: Repair services stored customer data when conducting a repair or attempting to recover data from a failed hard drive. Contrary to repair service's assertions that no customer data was being stored on U-M systems, the following was observed:

- Customer data was identified on a repair services computer used for data recovery.
- Customer data was found on a network-attached-storage (NAS) device. The data often contained full user account directories (e.g., all documents, desktop files, images, etc.) and was stored for several months after repairs were completed.
- Unclaimed customer computers and accessories were being stored beyond the point when they become U-M property.
    - Practice surrounding the handling of unclaimed repairs was inconsistent.
    - Devices containing customer data were in Showcase's possession for over a year.

Recommendation:

- Customer data should not be stored on U-M owned systems and devices; customer data should only be backed-up to customer-owned devices. Any exceptions to this practice should have controls that track and enforce the timely, secure erasure of customer data.
- Create a policy on the handling of unclaimed repairs, including the process to track all attempts to contact the customer.

2. Customer Data (Repair Services)	High

- Customer computers and accessories that become U-M property should be tracked and sent to Property Disposition within 30 days of becoming U-M property. Reutilization of parts should be documented as an exception and promote the timely, secure erasure of customer data.

Management Action Plan: The customer data that was found was from previous data backup practices that were retired last year. Upon discovery, the data was immediately wiped.

- Showcase developed a new policy, which was reviewed and approved by the Office of General Counsel (OGC), that details the process of requiring customers to provide a medium to store their personal files. Showcase no longer stores customer data on university-owned devices.
- Showcase revised the policy detailing their process for handling customer-abandoned computers, which includes information about tracking attempts to contact the customer.
- Included in the above policy are details around custody of abandoned customer equipment. Items retained by ITS Tech Repair are sent to Property Disposition quarterly or salvaged for departmental use.

Action Plan Owner: Tech Repair supervisor

Expected Completion Date: Completed during the audit

Auditor's Comment: University Audits will assess actions taken on this issue during the follow-up review.

3. Segregation of Duties	High

Issue: Key processes are not segregated in a manner that will prevent a single employee from executing a complete transaction without the involvement of others.

Risk: An employee may be able to both perpetrate and conceal errors or fraud in the normal course of business without detection. An employee could also be inaccurately determined culpable in the absence of clear checks and balances.

Support: U-M policy Standard Practice Guide (SPG) Section 519.03, *Cash Management Policies*, specifies that there be adequate segregation of duties between personnel who receive and deposit funds, and those who reconcile transactions. SPG Section 500.01, *Fiscal Responsibilities*, states that an adequate separation of duties requirement is essential to maintain an appropriate system of checks and balances. The following departures from the SPG were noted:

- Individual responsible for reconciling cash also prepares and deposits daily cash receipts.

3. Segregation of Duties	High

- Individual who programs and maintains the point of sale system also administers the surveillance and alarm system and has physical access to inventory, both during regular store hours and after-hours.
- Some employees who ring up sales have security access that may enable them to manipulate retail inventory levels.
- Individual responsible for reconciling and approving invoices associated with point of sale activations (i.e., iTunes and AppleCare card activations) also has the code to the activation system.
- Individuals responsible for maintaining the inventory system should not also be responsible for reconciling inventory to physical counts.
- Lack of documentation to the purchaser for the need to order out-of-warranty repair parts could result in parts purchased with university resources for personal use.

Recommendation: Assess roles assigned to staff to verify roles are compatible with job responsibility. For example:

- An employee responsible for the receipt of cash should not be able to record or authorize transactions in the accounts receivable ledger and customer accounts. Additionally, the person accepting payments from customers or preparing deposits should not be responsible for recording cash transactions (i.e., journal entries) or performing bank reconciliations.
- Employees involved in the purchasing function should not be able to write-off inventory or obtain custody of inventory directly or by influencing the shipment of inventory.
- Employees who have access to physical inventory should not be responsible for performing inventory counts or modifying perpetual inventory records. Someone who cannot modify the perpetual inventory system should complete the reconciliation of the perpetual inventory system to physical inventory counts.

Assess feasibility and revise process to track out-of-warranty repair parts in the retail operation's inventory system.

Management Action Plan: The Computer Showcase sales and inventory operations are staffed with 7.5 full-time employees. This makes it difficult to have 100% segregation of duties. Showcase will work on strengthening control in this area.

- Showcase will assess the business needs of specific roles in the point of sale and other electronic systems to ensure that only critical and required functions are available to staff. This includes adjusting tasks to create a segregation of duties between the business manager role and inventory control roles.
- Inventory counts will be transitioned from ordering and receiving staff to ensure blind counts are completed by staff who are not responsible for shipping or receiving.

3. Segregation of Duties	High

Action Plan Owner: Computer Showcase program manager

Expected Completion Date: November 2015

4. Payroll Deduction	Medium

Issue: Showcase employees do not always process payroll deductions used to pay for employee purchases in accordance with Showcase guidelines.

Risk: Failure to comply with standard guidelines for processing payroll deductions could result in lost or delayed revenues and an inefficient use of resources to investigate irregularities.

Support:

- Nine payroll deduction (PD) agreements processed between June and December 2014 exceed Showcase's maximum deduction limit of $2000. Agreements range between $2,027 and $2,359.
- Management does not have a clear process to make sure intentionally delayed PDs are eventually processed. Showcase sometimes accepts new agreements from employees who have existing agreements. The university's payroll system cannot accept new Showcase PDs before the first day of the month following payoff of a previous agreement. Therefore, to prevent overlapping, Showcase manually delays processing some PD agreements in a non-centralized manner.
- Against Showcase policy and good business practices, management occasionally allows customers to enter into multiple agreements by extending the payment period and adjusting existing monthly payment amounts to include additional purchases in the outstanding total amount due.
- Some incorrectly entered unique names and university identification numbers have resulted in extra work to investigate discrepant customer names.

Recommendation:

- Develop exception reports to identify PD inconsistencies. Use information from exception reports to educate cashiers who incorrectly process PD agreements.
- Develop a robust process to confirm PD agreements are sent to the Payroll Office for execution in a timely manner.
- Develop and circulate guidelines to managers and cashiers for adjusting previously established payment amounts to promote awareness and consistency of this process.
- Decrease data entry risks by implementing additional verification for manually entered customer identification information (e.g., initial entry and second verification entry requirement, or M-Card requirement with management override option for people presenting without ID cards).

4. Payroll Deduction	Medium

Management Action Plan: Payroll deduction provides a value-added service to university employees while allowing Showcase to reduce credit card fees. We have significant cost saving with relatively minimal risk.

- Showcase will revise internal payroll deduction policies to include both customer-facing policies as well as exception policies that allow Showcase management options to make reasonable exceptions for customers in the name of customer service.
- We will better document the process for multiple payroll deductions and develop reporting to ensure that all payroll deduction contracts are entered and followed up consistently.
- We have strong mitigating controls that make our process of taking legal ID in lieu of MCards sufficient when processing payroll deduction contracts and do not intend to pursue additional controls within Microsoft's Retail Management Solution.

Action Plan Owner: Computer Showcase business manager

Expected Completion Date: November 2015

Auditor's Comment: University Audits acknowledges Showcase's statement for not pursuing additional controls to mitigate risk associated with accepting a legal ID instead of requiring an M-Card. However, University Audits may review this action item during follow-up.

5. User Accounts	Medium

Issue: Certain IT credentials are shared or are not easily traceable to a specific user.

Risk: User accounts that are not uniquely identifiable make an audit trail difficult to establish and creates challenges in proper account management that may lead to unauthorized access.

Support: Through interviews and configuration assessment, the following was identified:

- A single, shared user account was used to remotely access the Showcase networks.
- A single, shared username was used to manage the camera system.
- 3 of 5 Active Directory administrator accounts were not identifiable to a specific end user.
- A single, shared username was used to activate gift cards.

Recommendation:

- Identify all users that have a business need to have access into Showcase networks and create unique usernames and passwords for each user.
- Create uniquely identifiable usernames for individuals who need to access the camera system.

5. User Accounts	Medium

- Change the Active Directory administrator naming convention to include the standard username of the end user or use description field.
- Create unique usernames for those that have a business need to activate gift cards.
- Add additional user accounts for removal in off-boarding procedures.

Management Action Plan:

- Showcase will reassess all user accounts to ensure individual ID's are assigned to only users that require access, with appropriate roles defined and documented.
- A new camera system that allows for unique user names will be explored to decide if it makes monetary sense to replace.
- Active directory user names will be updated to identify individuals who have server administrative access.
- Card activations will be updated to ensure only individuals who have the need to activate gift cards have access.
- Showcase will update off-boarding documents to ensure the removal of added accounts.

Action Plan Owner: Computer Showcase technical support analyst

Expected Completion Date: November 2015

6. Firewall	Medium

Issue: An ITS firewall protecting key Showcase servers is not configured in a secure manner.

Risk: Inadequately configured firewalls allow unnecessary network traffic to reach the servers, increasing the likelihood of system compromise and data exfiltration.

Support: Through manual and automatic testing, the following was identified:

- A network communication protocol that allows for remote access to the server was accessible from the U-M network.
- A protocol that allows for database connectivity was accessible from the U-M network.

Recommendation:

- Restrict identified protocols to only necessary IP addresses.
- Periodically assess, or work with ITS to assess, whether all firewall rules and changes promote an environment of confidentiality, integrity, and availability.

Management Action Plan:

- Showcase will restrict protocols to ensure access from only necessary IP addresses.
- Showcase will work with ITS Information and Infrastructure Assurance to promote an environment of confidentiality, integrity, and availability.

6. Firewall	Medium

Action Plan Owner: Computer Showcase technical support analyst

Expected Completion Date: November 2015

7. Point of Sale System	Medium

Issue: Showcase does not optimally administer and configure Microsoft's Retail Management Solution (RMS) software, Showcase's point of sale system.

Risk: Inefficient administration of software increases overall costs to maintain, hinders the ability to promote business functions, and may lead to unintentional data access.

Support:

- Reports created from RMS, including Showcase tax reports, are not always accurate or consistent.
- RMS does not aggregate purchase history between stores, which may lead to software and hardware licensing violations.
- A technical control does not exist to mitigate the risk of cashiers initiating the payroll deduction process for employees flagged as ineligible in RMS.
- RMS security levels and corresponding access were not aligned with the practice of least-privilege (i.e., minimum permissions necessary to perform job duties).
- A previous Showcase employee was allowed to retain an unnecessarily high level of access to RMS.
- Standard end-of-life for Microsoft RMS is July 10, 2016. End-of-life software no longer receives updates causing vulnerabilities and bugs to go unaddressed.

Recommendation:

- Assess necessary security level access for previous Showcase employee whose current job function necessitates RMS access.
- Assess RMS security levels and corresponding users to promote the concept of least-privilege and role-based-access-control.
- Thoroughly begin to assess alternative retail software solutions. Potential solutions should support existing and future business processes, while increasing the efficiency of informed decisions. If an alternate solution is not viable, identify, monitor, and mitigate associated risks with outdated software.

Management Action Plan:

- Leadership will reassess security levels of employees and document process for continual assessment of current employee list to ensure it is up to date.
- At this point, we will accept the risk that allows senior repair techs the ability to adjust counts that are required for them to perform their daily functions.
- An exploration of new POS software that has updated security and functionality will be performed. If costs are acceptable, a new system may be rolled out.

7. Point of Sale System	Medium

Action Plan Owner: Computer Showcase program manager

Expected Completion Date: January 2016

Auditor's Comment: University Audits will reassess risk acceptance of not adjusting senior repair techs access levels during follow-up.

8. Physical Security	Medium

Issue: Physical security at both stores could be improved.

Risk: Inadequate physical controls may increase the risk of theft.

Support:

- There is not a door separating the sales floor from the stock room enabling inventory levels to be visually identified by customers from the sales floor.
- Display and retail products are not always physically secured on the sales floor.

Recommendation: Assess feasibility of installing a door or other comparable solution between the sales floor and the stock room. Reassess current practices of not securing display and retail products.

Management Action Plan:

- Consideration of a door or other solution will be explored with ITS Facilities to understand the costs of separating the sales floor from the stockroom.
- At this time, the Computer Showcase accepts the risk of not physically securing demo items to the displays to foster customer engagement and drive sales. An assessment of total inventory loss is completed twice annually, which confirms our minimal instances of shrink.

Action Plan Owner: Computer Showcase program manager

Expected Completion Date: August 2015

Auditor's Comment: University Audits will assess trends and potential changes in the risk environment during follow-up.

Employee Supplemental Payments 2014-106

Report issued June 2015

A. Executive Summary

1. Overall Conclusion

Supplemental payments are intended to temporarily increase an employee's regular compensation. The payments may be used for one-time events, such as moving expenses for newly hired faculty or staff, or to accommodate longer-term situations, such as an employee who temporarily takes on additional duties.

The lack of a central university resource to operate as the process or system owner has resulted in a great variance in how units process these payments. This inconsistency makes it difficult to generate accurate reporting and to monitor the amount and reasons for supplemental payments. Without adequate authority at the executive level, the process lacks active oversight. In addition, training information available online is outdated and inconsistent, and only covers the basics of how the transactions are processed. It does not provide guidance for approvers to consider in determining whether a supplemental payment is an appropriate use of university funds. Three-digit payment codes, also called earn codes, are used to designate the reason for supplemental payments. However, errors in the code documentation, inconsistent rules, and unclear definitions cause confusion and reduce the accuracy of the information input and ability to conduct high-level data analysis. Reporting is further hindered because the supplemental payment data resides in data tables that are unclear and undocumented. The centrally-developed system used to process these payments could be improved by activating existing features and by implementing additional controls or enhancements.

Addressing the recommendations in the audit report require changes to processes that could impact the entire university. As such, the president's office has committed to investigating these issues and developing a plan to address them. A high-level management response from the president's office is included in Section C.

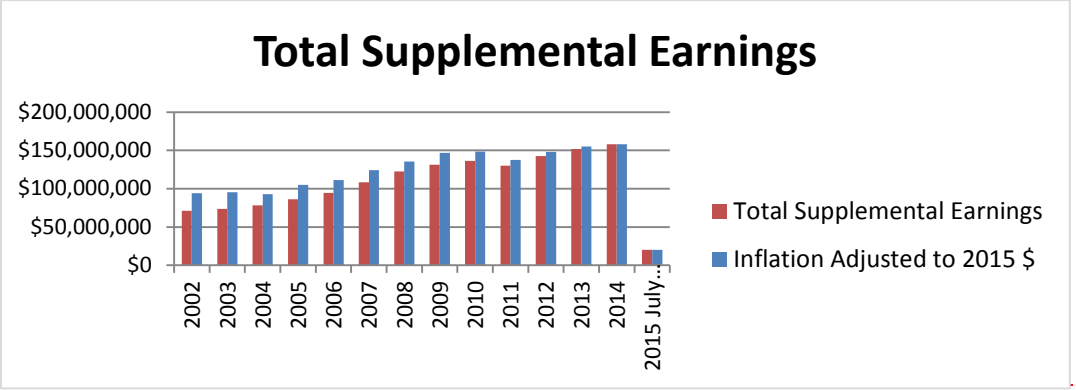
2. Context and Key Risk Considerations

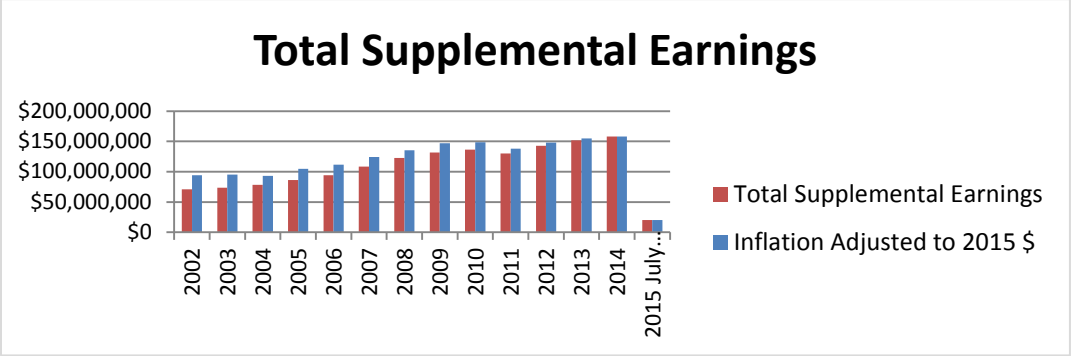
At the University of Michigan, compensation practices are largely managed by individual units. While the university provides software to process payments centrally, the individual decisions on when and how much to pay are made in the units.

The terms "supplemental payments" and "additional payments" are both frequently used on campus and refer to the same types of payments.

Historically, units processed supplemental payments using a paper form that was approved in the unit and sent to HRRIS (Human Resources Records and Information Systems) for manual processing. In 2011, a new automated process was rolled out to

the entire university. The new system, an Additional Pay Workflow in Wolverine Access, includes automatic approval rules that can be based on either employee type or tied to a specific earn code. For example, payments that will be tied to sponsored funds route to Finance-Sponsored Programs for a secondary approval. Payments to employees of UM-Dearborn or UM-Flint route to administrative officers there for secondary approval. Access to become an approver is managed through OARS, the Online Access Request System.





Note: Fiscal year 2015 data is through July 31, 2014.

The chart above demonstrates how supplemental payments have increased. In fiscal year 2014, supplemental payments totaled over $158M.

There are currently 343 earn codes that can be used to pay employees for various reasons. The majority of supplemental payments are processed through the new functionality; however, some must still be entered manually by HRRIS, such as payments for fellowships.

3. Audit Scope and Identified Risks

This review was not designed to identify fraud, which would have required selecting samples of transactions and working with administrative personnel in the units to provide justification for the payments. It was designed to be a review of the new supplemental payment transaction process, the university guidance for appropriate use, as well as monitoring, and oversight of these payments. Data analyzed during this review included all U-M campuses.

The table below lists the key activities audited, along with the overall risks of the audit issues identified for each sub-activity. The scope of the audit was determined based on an assessment of the risks associated with supplemental payments. This process included input from the many stakeholders and vested parties in the following offices: Payroll, Internal Controls, Tax Compliance and Planning, University Human Resources, Office of the Vice President for Communications, Finance, and the Office of the Provost.

	Key Activities Audited		
Sub-activities Audited	**University Guidance**	**Submission and Approval Process**	**Monitoring and Oversight**
	Process and/or system ownership (issue 1)	Use of earn codes (issue 2)	Existing monitoring reports (issue 3)
	Policies and procedures (issue 4)	Approver role	Tax exempt payments
	User training (issue 4)	System requirements (issue 5)	Earn code management (issue 2)
	Workflow implementation (issue 5)		

Legend: Overall risk conclusion for each sub-activity		
High Risk	Medium Risk	No Issues Reported

4. Audit Objectives

The objectives of this audit include:

- Evaluate existing guidance provided by central resources to assist and guide units in issuing and monitoring supplemental payments.
- Evaluate controls to enter and approve supplemental payments.
- Review existing monitoring processes.
- Perform data analysis of supplemental payment information to investigate patterns or trends.

B. Audit Issues and Management Action Plans

This section of the report provides details of the high and medium risk issues identified during the audit. See Appendix 1 for risk definitions.

1. Process or System Ownership	High

Issue: U-M has no central point of authority to provide unit guidance, issue policy, directives or best practices, monitor the overall supplemental payment process, or help Information and Technology Services (ITS) prioritize related system improvements.

Risk: The lack of central guidance or policy may reduce the control and consistency of the

1. Process or System Ownership	High

supplemental payment process. The lack of oversight and monitoring may result in payments processed inappropriately without detection. University administrators may be unclear on who to contact for assistance and support should they feel pressured to enter inappropriate supplemental payments or for other general questions. Necessary system upgrades or enhancements may not occur without adequate support for the resources these would require.

Support: Several groups across campus have different support roles in processing and managing supplemental payments. These include University Human Resources, HRRIS, Payroll, Tax Compliance and Planning, and ITS. Some of these units can advise on appropriate actions, but have no or limited authority to require that those actions be followed. U-M's decentralized model has historically supported unit autonomy and central units have had little executive support and minimal resources to provide more proactive involvement. System upgrades or enhancements require an authorized individual to direct ITS in the allocation of resources and, without a clear owner, nobody has been willing to make this a priority over other initiatives.

Recommendation: Establish central ownership for supplemental payments. Ownership at the executive level is vital to ensure active oversight. Work with the executive officers to determine the appropriate balance between oversight and unit autonomy. Develop guidance, policies, and best practices to assist university units processing supplemental payments. Include the input of stakeholders and process experts. Develop a communication strategy to ensure the university community is aware of the changes.

Management Action Plan: See Section C.

2. Earn Code Management	Medium

Issue: Earn code documentation has not been properly maintained resulting in inaccuracies. Further, much disagreement exists between the central units involved in the process as to whether the university should use more earn codes with specific detail or fewer earn codes with broader definitions.

Risk: Inaccurate earn code documentation could mislead and confuse units processing supplemental payments. Units using earn codes for reporting and analysis may misinterpret the data.

Support: Earn code documentation provided on the Payroll website was compared to the earn code tables in MPathways. Several inconsistencies were noted:

- Codes RES and FEL are not available in the workflow as indicated by the document.
- Two earn codes are set in the system to be tax exempt. However, the programming of tax-exempt codes is unclear and the tax department could not confirm they were correctly identified as tax exempt.
- Some code descriptions have slight variations between the documentation online and the system description that could change their meaning.
- Some rules in the workflow do not match stakeholder expectations. For example, auditors

2. Earn Code Management	Medium

were informed that all tax-exempt codes require Payroll approval, but some tax-exempt codes are not programmed to require that approval.

- An analyst in Payroll maintains the online earn code documentation by manually keying information after it has been entered into the system. This practice is inefficient and increases the likelihood of errors.
- Payroll has two versions of earn code documentation on its website- Earnings Code Definitions and Earnings/Time Reporting Codes. Much information is duplicated between them, but some information is inconsistent between the two documents.

Based on analysis of earn code use:

- Several codes have had minimal use over the past five years and may be unnecessary. As examples, TDT (10 Day Pay Engineers 1 1/2) and TDD (10 Day Pay Engineers double) have less than $20 in total over 5 years.
- Codes may not be used as originally intended. For example, Medical School uses INC, which is an incentive earn code, to pay the at-risk portion of earnings based on a faculty member's clinical or research components. It is guaranteed for the first year. Payments, particularly those made in the first year, may be inappropriately termed "incentives."
- There are situations that could fit under multiple earn codes and it is unclear which is most appropriate. For example, bonuses or incentives could fit under multiple earn codes.
- Some stakeholders interviewed stated there were too many active earn codes (creating confusion), while others said that there needed to be more codes (to make more detailed and transparent reporting possible).

Recommendation: Assess the level of earn code detail required to support the university's needs, considering the many possible users of this information. Add or remove codes as necessary and obtain approvals from appropriate individuals for all changes (e.g., the new process owner for all codes and including other departments as appropriate, such as Tax Compliance and Planning for codes designated tax-exempt). Review programmed workflow rules to ensure consistency with intent. Ensure that information is updated online promptly and shared with units. Develop a procedure to review the earn codes on an ongoing basis. Consider an annual earn code clean up, based on earn codes required for active labor contracts or the volume and frequency of code use. Involve Tax Compliance and Planning to ensure codes are appropriately identified as tax-exempt or not. Establish a Tax Compliance and Planning review or approval process when tax-exempt codes are added or modified. Populate the Payroll documentation by downloading earn-code data directly from M-Pathways and formatting as needed, instead of manually keying data. Consider combining the two earn code documents into one for simplicity.

Auditor's Note: In April, ITS indicated that a planned upgrade of the Additional Pay Workflow will add codes RES and FEL to the workflow.

Management Action Plan: See Section C.

3. Reporting and Monitoring	Medium

Issue: Supplemental payment data does not facilitate effective or efficient reporting.

Risk: Management may make decisions based on analysis of inaccurate data, negatively affecting university employees or the university itself. Inappropriate supplemental payments may go undetected. The university may not be able to meet reporting requests of top management.

Support:

- Many of the most useful data points from the Additional Pay Workflow do not exist in the Data Warehouse, such as Comments, Approver, or Creator. This limits the ability of units to create meaningful queries to monitor their own activity and validate appropriate use of supplemental payments.
- Most of the Additional Pay Workflow tables are not documented, which is typical for datasets that are only in PeopleSoft. Data that is part of the Data Warehouse is documented in data dictionaries, but the project team decided not to add Additional Pay data to the Data Warehouse so a data dictionary was not developed.
- Additional Pay Workflow tables are not logically grouped, frequently duplicated, and unique identifiers, such as a transaction ID, do not appear consistently. It was difficult for auditors, HRRIS experts, or even for the original programmers and developers from ITS to join the tables in meaningful ways to produce detailed analysis.
- Tax Compliance and Planning does not obtain or receive information regarding the activity of tax-exempt supplemental payments. Such reporting would allow them to better benchmark the university's activities against peer institutions, identify unusual trends, or determine the impact of proposed changes in tax law.
- By policy or workflow, there are few rules governing supplemental payments. However, there is no monitoring performed on the few process rules that do exist. For example, e-mailed guidance from the provost and University Human Resources advises that merit raises issued as lump sum payments of $10,000 or more must be reviewed and approved by a dean/director and a vice president. However, there is no timely or efficient way to verify that the appropriate reviews and approvals were obtained.
- While units have some reporting available to them, such as eNotification reports that are sent to department managers monthly, quarterly, and annually, the needs for higher level monitoring reports were never considered.

Recommendation: Determine what workflow information should flow to the Data Warehouse based on reporting needs and document the supplemental payment tables. Ensure data tables are logically grouped, that data can be uniquely identified and matched between related tables, and that data is not duplicated within tables other than by the unique identifiers (e.g., primary keys). Once there is clarity on ownership of the supplemental payment process, monitoring responsibilities can be assigned. Individuals or groups tasked with monitoring should work with ITS to develop reporting that would enable effective and meaningful monitoring and oversight of supplemental payments. Tax Compliance and Planning should work with Payroll or ITS to design a report and implement analysis procedures on tax exempt payments.

3. Reporting and Monitoring	Medium

Management Action Plan: See Section C.

4. User Training	Medium

Issue: The university has issued little guidance to units on how to appropriately administer supplemental payments. Supplemental payment training documentation is incomplete and, in some cases, inaccurate.

Risk: Payments may be administered inconsistently. Users may be unclear on how to process transactions and make unintended errors. Units may spend unnecessary time researching directions on their own or working with 4-HELP.

Support:

- Standard Practice Guide Section 201.85, *Non-Appointment Related University Compensation,* offers minimal guidance on managing supplemental payments.
- Guidance from the provost and University Human Resources emailed to units during the merit increase time period offers the option of using one-time payments in addition to or in lieu of merit increases but does not explain when this would be considered appropriate.
- In MyLinc, there are 16 training documents referencing supplemental payments. Much of the training is outdated.
- Guidance was issued jointly by the provost and the interim chief financial officer for the most recent Annual Salary Program. This included whether to use merit increase or lump sum payments. The guidance is linked from the Office of Internal Control's employment written procedures template, but the links are broken.
- The training only provides users and approvers the step-by-step process to perform their tasks in the workflow. There are no comments, suggestions, or guidelines for approvers regarding the accuracy or appropriateness of the transaction.
- Directions for processing additional payments have minor errors (e.g., use of double tab).
- There is no directive to keep job descriptions current, which could identify when a former additional duty is now part of an employee's regular responsibilities.
- There is no directive for units to regularly review and monitor supplemental payments at an appropriate level.
- There is no guidance or mandate as to when another unit, such as the Office of General Counsel or Tax Compliance and Planning, should be consulted.

Recommendation: Enhance unit guidance on processing and monitoring supplemental payments. Review all additional payment training documentation. Modify, update, delete, or create documentation as needed to provide units with clear, simple, and effective information. Training information should include not only step-by-step directions to process transactions, but also advise users (particularly approvers) to be cognizant of the appropriate use of the payments. Establish clear requirements for a unit's responsibility to monitor and assess ongoing payments.

Management Action Plan: See Section C.

5. Additional Pay Workflow	Medium

Issue: The Additional Pay Workflow does not include all features promoted during the initial rollout. System upgrades could provide gains in efficiency and compliance.

Risk: The current system could allow payments to continue without detection after additional duties have ceased or even after the employee transfers to a different unit. Units may be maintaining paper records to support transactions that are processed entirely online. A central office that needs to validate the appropriateness of a payment has no ability to review the back-up documentation without making a request to the issuing unit, which could cause an administrative burden.

Support: The workflow system could be enhanced by including additional features or activating existing features that are not in use. Consider the following opportunities while planning for future upgrades of the system:

- In training provided to all units, a promoted feature was the ability to upload supporting documentation as an attachment in the system. However, the upload feature was never activated. Units are currently maintaining documentation locally.
- Data analysis identified that many units are using spaces to circumvent the requirement to include a comment describing the purpose of the supplemental payment. There is neither monitoring to identify such activity nor a unit tasked with the responsibility to do so.
- There is no end date requirement for supplemental payments entered directly into the system. Some payments observed have an end date of 9085. There is no central periodic review or monitoring that would identify these perpetual payments to verify appropriateness.

Recommendation: Enable attachments for the additional payment workflow and require units to attach all supporting documentation. Modify the system edit rules to increase compliance with the requirement to use the Comments field, such as increasing the minimum required characters. Modify system edit rules to enforce a shorter time period (e.g., one year) for all ongoing supplemental payments so that units can reassess the appropriateness of the payments. Ensure the system edit rules apply for payments entered manually where appropriate. Develop monitoring for compliance and determine a process to work with units who submit payments inappropriately including training and escalation steps.

Auditor's Note: In April, ITS indicated that the functionality for adding attachments to the Additional Pay workflow will be activated during a July 2015 upgrade.

Management Action Plan: See Section C.

C. Management Action Plan

The President's Office has recently charged a working group, headed by the provost and chief financial officer, to review and benchmark against peer institutions:

- Salary levels of executive leadership
- Compensation disclosure practices
- Overall use of non-base pay

The working group is staffed by University Human Resources and will use the recommendations in this report to advise their work.

English Language Institute 2015-206

Report issued May 2015

A. Executive Summary

1. Overall Conclusion

University Audits recently completed an audit of business operations and fiscal responsibilities at the English Language Institute (ELI). The institute reports to the College of Literature, Sciences, and the Arts (LSA), and provides language instruction and academic support. The institute has undergone significant reorganization and leadership change over the past few years.

ELI management has good oversight and control over fiscal responsibilities and management of day-to-day business operations, especially on-campus activities. Business operations are well coordinated with the LSA Shared Services operations, and there is strong stewardship of limited resources. There are opportunities to improve controls over off-campus learning experience programs and interaction with minors. Management has already started working with the LSA Center for Engaged Academic Learning (CEAL), the Office of the General Counsel, and Risk Management to provide additional guidance to students, faculty, and staff engaged in off-campus activities.

2. Context and Key Risk Considerations

ELI was founded in 1941 as the first university-based English for Second Language (ESL) program in the U.S. ELI's mission is to "provide language instruction, academic support, and intercultural training that would enable all members of the U-M community to excel in their professional endeavors throughout their academic careers." ELI reports to the Associate Dean for Undergraduate Education.

In the past five years, ELI has undergone significant reorganization to better align with the core mission of providing academic language instruction. The research and testing divisions were spun off to a separate joint venture, the university's in-house language-testing requirement for entering foreign graduate students was eliminated, and most of the undergraduate courses were moved to the Sweetland Center for Writing. Because of these changes, ELI's annual operating budget has declined from $2.3 million in fiscal year 2011 to $1.3 million in fiscal year 2014. A new director was appointed at ELI in May 2014 after an interim director was in place for approximately a year.

ELI lecturers develop curriculum, teach English as a second language, provide graduate student instructors (GSI) language and cultural training, and operate student clinics to help with writing and speaking assignments. Lecturers also work collaboratively with other U-M units such as the Ross School of Business, Center for Research on Learning and Teaching, Law School, and Taubman College of Architecture and Urban Planning to provide orientation, training, service-learning courses, and field opportunities to students, GSIs, and teachers. Many ELI programs work with other U-M units, constituents such as migrant farm workers, and service organizations such as Ann Arbor Public Schools, Family Learning Center, and the First United Methodist Church to provide English language training.

The new ELI director is addressing several challenges:

- Identifying and eliminating barriers to student enrollment
- Developing additional revenue generating models for delivering ELI services
- Streamlining ELI's activities with LSA shared services, and
- Improving internal marketing efforts to ensure that students are aware of ELI courses and other services

3. Audit Scope and Identified Risks

The table below lists the key activities audited, along with the overall risks of the audit issues identified for each sub-activity. The scope of the audit was determined based on an assessment of the risks associated with ELI and included input from ELI and LSA management.

	Key Activities Audited					
	Program Management	**Grade Changes**	**Financial Oversight**	**Human Resources**	**Purchasing**	**COI/COC and Compliance**
Sub-activities Audited	Summer programs (3)	Policies and procedures	Funds flow	Contract obligations	Vendor utilization	Conflict disclosures and management (2)
	Interactions with minors (1.A)	Authorized changes	Annual budget process	Hiring and time reporting	P-card usage	Awareness of the hotline
	Domestic travel and affiliation agreements (1.B, 1.C)		Statement of account reconciliation	Supplemental pay		
	Revenue recognition		Cash handling and credit cards	Temporary employees		
			Internal controls			

Legend: Overall risk conclusion for each sub-activity

High Risk	Medium Risk	No Issues Reported

This audit focused on unit level operations and administrative processes for ELI, and ELI interaction with LSA shared services. The following areas were not part of the scope of this audit:

- Cambridge Michigan Language Assessments (CaMLA), the language testing joint venture with Cambridge University (Cambridge Michigan Language Assessments)
- LSA shared services processes
- Sweetland Center for Writing
- ELI curriculum and teaching activities

4. Audit Objectives

This audit was part of the fiscal year 2015 audit plan. The objectives of this audit were to:

- Evaluate unit management and oversight of summer programs, off-campus programs, and university related domestic travel
- Assess controls over the grade change process
- Assess controls over funds flow into the unit, budgeting, reconciliations, internal control gap analysis, cash handling, and credit card transactions
- Assess controls over employment, payroll, and time keeping functions
- Assess controls over vendor utilization and P-Cards
- Determine if management has an effective process to manage the conflict of interest/conflict of commitment (COI/COC) process
- Evaluate awareness of the Compliance Hotline

B. Audit Issues and Management Action Plans

This section of the report provides details of the high and medium risk issues identified during the audit. See Appendix 1 for risk definitions.

1. Off-campus Programs	High

A. Interactions with Minors

Issue: Faculty and staff were not aware of and had not implemented the policy outlined in Standard Practice Guide (SPG) 601.34, *Policy on Minors Involved in University-Sponsored Programs or Programs Held in University Facilities.*

Risk: Safety and security standards for programs with minors may not meet university requirements.

Support: SPG 601.34 sets forth policy that promotes the health, wellness, safety, and security of minors participating in programs conducted under the direction and authority of the university at locations on and off campus.

The ELI programs and courses involve faculty and student interactions with minors at locations off-campus. Minimum university requirements, such as program registration, training, and background checks have not been implemented.

1. Off-campus Programs	High

Recommendation: Work with university resources such as CEAL and Risk Management Services to comply with SPG 601.34 requirements. Consider developing an ELI specific handbook that includes guidance to faculty, staff, and students working with minors that includes:

- Program registration requirements
- Code of conduct
- Criminal background screening
- Participant requirements
- Training requirements (e.g., Clery Act, safety and security, sexual and other unlawful harassment)
- Reporting obligations

ELI can leverage the guidance provided in the existing policy handbooks of the School of Education and other experienced U-M units for developing guidance specific to their off-campus program requirements. The children on campus website, http://childrenoncampus.umich.edu, contains information on background check procedures, program registration, toolkits, templates, and training materials.

B. Domestic Travel Guidance

Issue: Unit responsibilities regarding domestic travel for university related purposes have not been clearly defined and documented.

Risk: The university may take on unnecessary liability and incur reputational damage.

Support: ELI programs and courses involve day trips to southeastern Michigan locations. ELI does not provide faculty and students guidance on use of personal, chartered or university vehicles. Insurance requirements, safety awareness, and conduct expectations are not communicated to program participants.

Recommendation: Work with university resources such as the Center for Engaged Academic Learning (CEAL), the Office of the General Counsel, and Risk Management to develop a unit policy for identifying and communicating travel guidance and best practices to staff and students such as:

- Pre-departure orientation and training in topics such as safety, use of vehicles, insurance, alcohol, and drugs
- Training and guidelines for the unit administrator to effectively manage domestic travel
- Code of conduct and responsibilities for students involved in travel
- Expectations of faculty and staff accompanying the students
- Baseline procedures to follow and key university resources to contact in case of an emergency

1. Off-campus Programs	High

C. Affiliation Agreements

Issue: Management has not established and authorized student placement affiliation agreements with external organizations.

Risk: The university may take on unnecessary potential liabilities in case of disputes or adverse events. ELI students may not be covered for expenses or damages incurred while acting within the scope of their assignment.

Support: As part of their practicum requirements, students enrolled in the ELI 390 fall/winter course volunteer to either teach or assist instructors in teaching English reading and writing skills in multiple community-based settings.

ELI does not have written agreements for student placements with school districts, learning institutes, and community social service agencies. Associations are based on historical relationships or student interest.

Recommendation: Work with the Office of General Counsel to determine when agreements are necessary and what information and stipulations should be included. Identify and document expectations regarding signature of these agreements so that agreements are signed with appropriate signature authority. Consider coordinating activities with the School of Education, which has existing affiliation agreements with Ann Arbor Public Schools.

Management Action Plan: ELI has begun partnering with CEAL to revise planning and logistics for ELI courses and programs that involve community engagement and off-site travel. CEAL will work with ELI to address the concerns raised here:

A. **Working with Minors:** Beginning in Summer 2015, a CEAL staff member will visit the ELI 390 class to deliver a training/orientation session on working with minors before students begin their fieldwork teaching assignments at local migrant farm worker camps (summer) or local service organizations (fall/winter). By the beginning of the fall term, ELI will work with CEAL to produce an ELI Handbook for off-site programs that includes sections on working with minors and when background checks are required.

B. **Domestic Transportation:** Beginning in summer 2015, a CEAL staff member will visit the ELI 390 classes to deliver a training/orientation session on university guidelines for off-campus travel. By the beginning of the fall term, ELI will work with CEAL to produce an ELI Handbook for off-site programs that includes ELI-specific guidelines on domestic transportation to ensure that faculty, staff, and students are aware of their obligations and of best practices for domestic travel.

1. Off-campus Programs	High

C. **Affiliation Agreements:** ELI and CEAL will work with the Office of General Counsel to review current community placements in the fall and winter sections of ELI 390 to ensure that appropriate affiliation agreements are signed with appropriate signature authority by the start of the fall term.

Action Plan Owner: ELI director

Expected Completion Date: September 2015

2. Conflict of Commitment	Medium

Issue: Lecturers are not always following union contract and university policy requirements to disclose work commitments outside of their primary ELI responsibilities.

Risk: Lecturers may engage in work activities that may have a potential to interfere with their primary work obligations either in actuality or in appearance.

Support: Lecturers have attested that they have declared all conflicts or have no conflicts to declare in their May 1, 2013 – April 30, 2014, Annual Activity Report. However, the lecturers are not disclosing other work commitments within the university as required by contract and LSA policy:

- In fiscal year 2014 and fiscal year 2015 to date, 5 lecturers received additional payments from other U-M units.
- While some lecturers have occasionally provided verbal disclosures, management is either unaware of these commitments or learns of them after the fact. Some work commitments are longstanding and may have been approved by previous directors; however, these commitments are not reevaluated periodically.
- For the academic year 2014 and 2015, two ELI lecturers have 80% appointments while the remaining nine lecturers have 100% appointments, so all had an obligation to disclose commitments prior to entering into them.

ELI follows the LSA Faculty COI/COC policy that requires faculty to disclose any potential conflicts of interest or commitment as soon as they arise. The Lecturers Employee Organization (LEO) contract specifies that:

- Lecturers promptly disclose potential conflicts in compliance with the disclosure mechanism set forth in the applicable unit implementation policy.
- Lecturers with an appointment of 0.8 FTE or greater obtain the approval of the academic unit in which they are employed prior to engaging in activities outside of the unit.

Recommendation: Reinforce with faculty and staff the need to follow university policy and the LEO contract to disclose and discuss external commitments and interests to management in writing prior to accepting work outside of ELI even though they may not, individually or collectively, conflict with the individual's primary obligations. Consider developing a unit specific COI policy that addresses ELI's circumstances and needs.

2. Conflict of Commitment	Medium

Management Action Plan: At an ELI faculty and staff meeting on April 3, 2015, faculty and staff were reminded that U-M and LSA COI/COC guidelines require them to disclose all professional activity they perform outside the unit in a timely manner and that ongoing, long-term outside commitments need to be reviewed at least once a year. They were asked to report all activity outside of ELI on their Annual Report, due in May. This information was also included in the cover email they received with the call for annual reports. By the beginning of the 2015-2016 academic year, ELI will formulate COI/COC guidelines for ELI faculty and staff, which clarifies university and LSA COI/COC requirements as they specifically pertain to ELI.

Action Plan Owner: ELI director

Expected Completion Date: September 2015

3. ELI Summer Programs Admissions	Medium

Issue: Management does not verify language proficiency scores for non-U-M students admitted to ELI's summer programs. Exceptions to the admissions process are not documented and approved.

Risk: Unqualified students may be admitted to the program.

Support: ELI offers three summer programs for international students: English for Legal Studies (ELS), English for Business Studies (EBS), and the English for Academic Purposes (EAP). Applicants input their language proficiency score information and attach a copy of their admission letter to a U.S. university while submitting the online application.

Summer program requirements specify that:

- Applicants be admitted to a U.S. university for the upcoming fall semester
- Applicants not accepted into a U-M degree program meet minimum language proficiency score requirements.
- Applicants admitted to a degree program at U-M and who apply before the application deadline have priority over non-U-M students, who may be admitted on a space-available basis.

University Audits sampled 25 out of the 68 students who had been accepted into the summer 2014 programs and determined that:

- The program coordinator made a decision to accept one student not admitted to any U.S. university for the ELS summer 2014 program and did not document this exception or seek director approval.
- ELI did not verify the language proficiency scores for two students admitted to non U-M universities and for one student who had not been admitted to any U.S. university. ELI relied on the language proficiency score information entered by the students while submitting their online application.

3. ELI Summer Programs Admissions	Medium

Recommendation: Obtain official language proficiency scores to verify eligibility. Document all exceptions to the summer programs admission process. Obtain and document approval of the program coordinator and the ELI director prior to accepting students who do not fulfill all admission requirements for the summer programs.

Management Action Plan: We have revised our summer programs application form to require applicants who have not been accepted to a U-M degree program to submit proof of their language proficiency test scores. We have also added language to our summer programs web page noting that the ELI director and the appropriate U-M admissions office must approve any exception to the requirement that students are admitted to a U.S. university for the fall term.
Action Plan Owner: ELI director

Expected Completion Date: Completed

University of Michigan Health System Data Sharing 2015-404

Report issued June 2015

A. Executive Summary

1. Overall Conclusion

Developments in healthcare information technology and government initiatives for electronic health records and meaningful use have led to the establishment of distributed data systems such as health information exchanges (HIEs) and quality initiatives (QIs) to enable the sharing of patient records and health information. Vast quantities of clinical data are created by or shared with U-M hospitals and clinics and the Medical School. This includes clinical data sharing for research, quality monitoring, and health information exchanges with third parties. The current data sharing model relies heavily on individual responsibility and understanding of privacy, rather than systemic institutional controls. The inability to fully and consistently meet privacy protection obligations may result in violations of federal law and significant monetary fines.

In a highly regulated environment such as healthcare, the importance of establishing responsibility for oversight and transfer of protected health information is significant. It is important for the health system to control the flow of sensitive data into and out of the entire organization. University Audits identified several opportunities to improve controls over management of identifiable health information. Specifically, improve the process of allowing patients to opt-out of having their protected health information shared with health information exchanges, remediate previously identified data security deficiencies, and provide monitoring and oversight of data agreements that involve protected health information.

2. Context and Key Risk Considerations

The development of electronic health records (EHR) allows data sharing between health care providers to improve clinical decision-making at the point of care. Data sharing of sensitive health information between third parties has become a critical component of ensuring quality and continuity of patient care. The Health Information Technology for Economic and Clinical Health Act (HITECH) enacted as part of the American Recovery and Reinvestment Act of 2009 promotes the "Meaningful Use" of EHR by providing incentive payments to healthcare providers. To qualify for incentive payments, providers must adopt EHR technology and use it to achieve certain objectives, such as exchanging patient information with providers, reporting, and meeting quality measures.

There are multiple data sharing arrangements in the health system. Below is a list of the more common sources:

- Health Information Exchange (HIE): electronic movement of health–related information to allow sharing of a patient's medical record between health care providers
- Quality initiatives (QIs): Evaluation of current medical processes across hospitals using large scale data analysis to recommend best practices
- Honest Broker Office: provides minimally necessary protected health information (PHI) for research purposes, rather than allowing large numbers of individuals access to confidential systems
- Health System data warehouse (HSDW): the comprehensive University of Michigan Health System (UMHS) data repository that includes clinical, financial, operational, and benchmarking data

See Appendix 3 for key terms used in this report.

3. Audit Scope and Identified Risks

The table below lists the key activities audited, along with the overall risks of the audit issues identified for each sub-activity. The audit scope was determined based on risk assessment discussions with the following groups: UMHS leadership, Office of Research and Sponsored Programs, Medical School Regulatory Affairs, and U-M Office of Research. The general topics of data use and data sharing are very broad, so the audit scope was narrowed to include clinical and patient data for functions used in selected quality initiatives, health information exchanges, and some aspects of research.

In a separate communication to UMHS management, we have recommended assessing the UMHS oversight and data governance of faculty-led quality initiatives within the Medical School.

	Key Activities Audited			
	Health Information Exchanges	**Internal Data Sharing (HSDW)**	**Honest Broker Office**	**Data Use Agreements**
Sub-activities Audited	Business associate agreements in place	Data sharing controls	Policies and procedures	Central process and record-keeping (Issue 3)
	Policies and procedures	**Monitoring plans (Issue 1)**	Data sharing controls	Policies and procedures (Issue 3)
	Adherence to industry guidelines	Access controls	Review process	Retention guidance (Issue 3)
	Access controls	**Data security (Issue 1)**	Access controls	Contract termination and disposition (Issue 3)
	Patient opt-out (Issue 2)		Data security	

Legend: Overall risk conclusion for each sub-activity		
High Risk	**Medium Risk**	**No Issues Reported**

4. Audit Objectives

The objectives of this audit include:

- UMHS participation and role in the Great Lakes Health Connect Health Information Exchange
- Review of data use and sharing by a sample of the collaborative quality initiatives, specifically those where UMHS has collaborated as a lead site with Blue Cross and/or the State of Michigan
- How the Health System data warehouse is accessed and security is managed
- An assessment of the data use and sharing process facilitated by the Honest Broker Office that fields research requests.
- The general control environment surrounding Data Use Agreements (DUA) with external partners that involves protected health information

B. Audit Issues and Management Action Plans

This section of the report provides details of the risk issues identified during the audit. See Appendix 1 for risk definitions.

1. Health System Data Warehouse (HSDW)	High

Issue: UMHS management has not maintained a control environment in the data warehouse that sufficiently allows detection of and monitoring for unauthorized use and disclosure of protected health information.

Risk: There is a greater risk of unauthorized use, inappropriate disclosure including identity theft, and HIPAA (Health Insurance Portability and Accountability Act) privacy violations. A lack of HIPAA compliant data protections can result in reputational damage and monetary penalties.

Support: HIPAA security rules require institutions with electronic protected health information (ePHI) to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

- The Health System data warehouse contains over 20 years of hospital and identifiable clinical patient data. There are individuals accessing data for payment, treatment, and operational purposes, and users that are accessing data for research.
- Accessing patient data for payment, treatment, and operational purposes does not require patient consent, but accessing PHI for research purposes requires either human subjects Institutional Review Board approvals or special handling, such as removal of specific patient identifiers.
- The Health System data warehouse lacks system activity tracking tools to investigate privacy complaints. This includes monitoring tools such as audit logs and security incident reporting.
- The UMHS Compliance Office performed a security risk assessment of the Health System data warehouse in 2011. The risk assessment found that in the event of a data breach, audit records do not contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. As of the time of our audit, this high-risk finding remains uncorrected and MCIT management has indicated that there are no current plans to correct the deficiency.

Recommendation: Ensure the Health System data warehouse is HIPAA compliant. Address the unresolved high-risk deficiencies in access control policies and procedures, including account management, access enforcement, auditable events, and content of audit records identified in the 2011 UMHS Compliance Office risk assessment. Develop, document, and deploy monitoring controls.

Management Action Plan: UMHS and Health System data warehouse leadership along with the UMHS Compliance Office are actively working together to determine the best solution for mitigating all the high and moderate risk areas. A detailed action plan and timeline has been developed and deployment in all areas will continue during the next six months.

Action Plan Owners: Chief Medical Information Officer, Health System data warehouse management, and Compliance Director Information Security, UMHS Compliance Office

Expected Completion Date: As of the report date, detailed action items have been developed and implementation plans initiated. Most will be completed by December 2015, with final implementation of all by June 2016.

2. Patient Non-disclosure of Health information	**Medium**

Issue: UMHS opt-out procedures are not transparent regarding the policy and technologies that directly affect a patient's identifiable health information, including a patient's right to opt-out of health information exchanges. UMHS cannot confirm that a patient's right to opt-out has been accommodated.

2. Patient Non-disclosure of Health information	Medium

Risk: There could be poor patient relations because of a data breach caused by a health information exchange that contains UMHS patient health information outside the health system's direct control.

Support: The openness and transparency principle in the HIPAA Privacy and Security Framework indicates there should be openness and transparency about policies, procedures, and technologies that directly affect individuals and/or their individually identifiable health information. UMHS does not provide clear notice of how a patient's health information is shared with other providers and institutions.

- UMHS has partnered with HIEs and other providers to improve the continuity of care and overall quality of health care services. UMHS should take this opportunity to proactively communicate to patients regarding the positive benefits of involvement in a statewide HIE.
- Under Michigan privacy laws, patients have the right to opt-out of having their information shared with HIEs. UMHS relies on a third party exchange to block any sharing with providers or other exchanges for patients who wish to opt-out.
- UMHS has no effective process for determining which patients have opted out of sharing their information with the exchange. The exchange cannot provide a list of UMHS patients who have opted out, and limited testing of the opt-out process by the UMHS Compliance Office failed.

Recommendation: Provide transparent patient communication regarding their involvement in HIEs, the benefits of participation, and their right to opt-out of the exchange. Track the patients that opt-out, validate that the process has effectively occurred, and build a notification flag in the electronic health record that will indicate the patient has elected to opt-out of sharing their data.

Management Action Plan: The Office of Health Information Management (HIM) will partner with the UMHS Compliance Office and Ambulatory Care Services as well as UMHS committees such as the Health Information Exchange Operations Subcommittee and the Health Records Standards Committee to create patient education materials describing UMHS' HIE involvement.

Because patients may request opt-out directly from HIEs or through another provider connected to that HIE, internal efforts to track and flag requests for opt-out would not provide a complete picture. The UMHS Compliance Office and HIM will evaluate HIE contract performance in terms of honoring UMHS patient opt-out requests.

Action Plan Owners: Director, Health Data Quality and Compliance and Compliance Director for Privacy, Policy and Education

Expected Completion Date: Initial steps by July 2015 with full implementation by January 2016

3. Central Oversight of Data Use Agreements	Medium

Issue: UMHS is entering into data agreements without general oversight and controls when acting as a hosting site for some clinical quality initiatives.

Risk: There is a risk of not meeting our contractual obligations to secure identifiable clinical data from other health providers hosted at UMHS. Inappropriately secured PHI is at a greater risk of privacy breach and identity theft, which can lead to reputational damage, civil penalties, and monetary fines.

Support: UMHS is institutionally agreeing to act as data hosting sites for clinical quality initiatives that analyze and store PHI without procedures or processes in place to verify we are complying with HIPAA privacy standards.

- UMHS does not have a master list of executed agreements and there is no centralized process for executing data use agreements. In the event of a data breach, details of storage and handling would be difficult to assess. Allegations of patient privacy violations and identity theft would be difficult to disprove.
- Audit interviews with the UMHS Compliance Office, Honest Broker Office, Office of Technology Transfer, and Office of Research and Sponsored Projects determined that all of these offices are assisting faculty with executing data use agreements without a centralized process or the ability to cross-reference.
- Faculty and staff self-report their need for the data and agree to comply with federal regulations and security provisions, but there is no UMHS-wide guidance on how to comply with the standards. IT staff are often unaware that protected data is stored on their servers.
- Terms of each data use agreement vary and there is no guidance on standard language requirements to protect the university.
- Some agreements are open-ended and do not address data ownership or disposition at the end of the project.

Recommendation: Develop UMHS-wide requirements including an oversight process for data use and sharing agreements. Consider adopting data use agreement standards from the federal Department of Health and Human Services. Include minimum data use standard details such as data custodian, responsibilities of each entity, point of contact, ownership, data transfer, media and method for exchange, recordkeeping, retention, and disposition. The data use agreement could then serve as a control mechanism for tracking the location of the data and the reason for the release. Verify through periodic assessments that UMHS is complying with the terms of the agreements.

Management Action Plan: UMHS Compliance will convene a working group to develop a corrective action plan. The plan will include:

- Identification of operational units that UMHS Compliance will partner with to improve HIPAA privacy and security compliance for clinical quality initiatives, where UMHS is the data hosting site and where protected health information is involved

3. Central Oversight of Data Use Agreements	Medium

- Strategy to streamline data agreement storage location for future quality initiatives receiving protected health information, with a goal toward a central location
- Strategy to locate and inventory current clinical quality initiatives, where UMHS is the data hosting site
- Strategy to improve guidance for clinical quality data users on HIPAA-compliant data sharing, see UMHS Compliance website at http://www.med.umich.edu/u/compliance/area/research/datause.htm.

Granting that UMHS template data use agreements are HIPAA-compliant, UMHS Compliance will review its template agreements currently located in UMHS policy 01-04-342 *Limited Data Sets,* with input from the Health System Legal Office, and revise as practicable. Note that the template agreements are in current use by UMHS Compliance, the Health System Legal Office, Honest Broker Office, and Office of Research and Sponsored Projects.

Action Plan Owners: UMHS Chief Compliance Officer and Associate General Counsel, Health System Legal Office

Expected Completion Date: Plan and implementation timeline will be developed by December 2015.

University of Michigan Health System MyUofMHealth Patient Portal 2015-302

Report issued June 2015

A. Executive Summary

1. Overall Conclusion

MCIT has taken significant steps to mitigate high-risk findings identified during the audit of the MyUofMHealth patient portal, however, some residual risk remains. Due to an oversight, there was one instance where a security update was not installed that exposed the portal to a critical vulnerability. MCIT acted quickly to resolve the issue during the course of the audit once they were notified. Additionally, the secure communication protocol has a vulnerability that could allow a malicious actor to compromise the connection between a patient and the portal. Since resolving this issue would result in limiting access to the portal for certain patients who use older operating systems, management has committed to evaluating the risk to make a decision to accept this risk or fix the vulnerability and restrict some patients from accessing the portal.

Overall, the patient portal is well managed and the teams responsible for it have responded quickly to address risks, and have been receptive to recommendations. Once the findings listed below are resolved, the security of the portal will be greatly improved.

2. Context and Key Risk Considerations

The UMHS MyUofMHealth patient portal is a component of the Epic Electronic Medical Record (EMR) system. This system is called MiChart at U-M. MiChart is a modular and integrated clinical information system. The patient portal component of the overall MiChart system is called MyChart.

In 2012, the self-service portal was established providing patients access to portions of their own health records. The portal went live during August 2012 as part of the Ambulatory Care Services migration to MiChart. At the time of this report, the portal serves over 186,000 patients with over 185 new patients every day. The portal provides patients with the ability to access portions of their EMR, request prescription renewals, schedule appointments, view, and manage EMR of children and other adults (patient proxy), view test results, health history and immunization records, and communicate with physicians. Patients can also submit payments and access insurance coverage information. Access to the portal is possible via web browser at MyUofMHealth.org or with a mobile application. The patient portal assists clinical staff by shifting non-urgent communications from telephone and postal mail to the web.

The Medical Center Information Technology (MCIT) MiChart team is responsible for managing and maintaining the patient portal. The Health Information Management Department (HIM) assists end users with access to the portal, adjusting errors in medical records, and is responsible for the patient proxy process.

3. Audit Scope and Identified Risks

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

Key Activities Audited						
Sub-activities Audited	**Access Controls**	**PCI-DSS**	**Patient Proxy**	**IT Security**	**IT Security**	**IT Security**
	Logical system access	Merchant policy agreement	Diminished capacity proxy process	Internet exposed services	Patient account password safety (issue 3)	Security event log monitoring (issue 1)
	Application event log monitoring (issue 4)	Self-assessment process	Support documentation	**Vulnerability detection and remediation (issue 1)**	File integrity monitoring (issue 1)	Secure configurations (issue 1)
	Patient portal password reset process (issue 3)	PCI-DSS compliance (issue 1)	Child proxy limitation and deactivation	Network isolation	Security certificate maintenance	Brute force mitigation
	Audit logging			Mobile application secure communications	Application whitelisting (issue 1)	Privileged system access (issue 2)
				Penetration test	Anti-malware	

Legend: Overall risk conclusion for each sub-activity		
High Risk	Medium Risk	No Issues Reported

4. Audit Objectives

This audit:

- Evaluated overall privileged and patient access processes
- Verified that the PCI-DSS compliance and related credit card merchant requirements are met
- Assessed the effectiveness and adequacy of patient proxy privacy controls
- Assessed IT security risks
- Ascertained system stability and availability controls
- Reviewed patient portal monitoring and alerting processes
- Assessed backup and restore processes
- Assessed the effectiveness of change management controls

B. Audit Issues and Management Action Plans

This section of the report provides details of the high and medium risk issues identified during the audit. See Appendix 1 for risk definitions.

1. IT Security	High

Issue: MCIT has not fully secured the publicly accessible patient portal web servers.

Risk: Sensitive and regulated data could be exposed by exploiting software vulnerabilities or from server misconfigurations. An incident that results in data loss or compromise could damage the reputation of the university. Data loss could result in financial losses and possibly penalties and fines.

Support: University Audits testing indicated that the web-based secure communications protocol is vulnerable because it uses depreciated encryption ciphers. Any data transmitted by the patient portal to a user is at risk for exposure; including patient data and patient and privileged (e.g., super user) account passwords.

Testing also identified that a critical vulnerability, which could allow an attacker to remotely execute code, was not patched. Once we informed MCIT of the missing security patch, it was deployed to the portal web servers and the vulnerability was mitigated.

Scan results from vendor-provided security tools determined that the server configurations do not meet vendor-recommended best practices and could contribute to data leakage risks.

The audit also identified some areas where recommended security controls are lacking.

- File integrity monitoring (NIST[1] 800-115)
- Application whitelisting (NIST 800-167)
- Monitoring of security event logs (NIST 800-92)

Recommendation: MCIT should make the appropriate modifications to the patient portal web servers so that vulnerabilities in the secure communication protocol are mitigated in a timely way. Management should adjust server configurations to meet vendor-recommended best practices and an assessment should be conducted on a regular schedule to determine if configurations have been altered. Internet-exposed servers should be patched as soon as practical after the vendor releases a patch. Due to the ease of server compromises and increase in the number of health record data losses, patches should be applied within a week of when the vendor releases a patch for critical vulnerabilities. MCIT should consider implementing a file integrity monitoring solution and allowing only approved processes to run. Security event logs should be sent to a centrally controlled and secured log analysis system.

[1] The National Institute of Standards and Technology (NIST) is a federal technology agency that works with industry to develop and apply technology, measurements, and standards. The NIST 800 Series is a set of documents that describe United States federal government's computer security policies, procedures, and guidelines.

1. IT Security	High

Management Action Plan: To address the risks identified in this item we are taking the following actions:

- In general, security patches for the Patient Portal servers are installed within three days of release. The MCIT Enterprise Hosting and Integration Services (EHIS) team is responsible for the installation of the updates. The EHIS team has implemented a weekly process to verify all applicable updates have been installed.
- The EHIS team will implement file integrity monitoring. File integrity will be monitored with a specialized tool along with using access control lists for file access. File integrity monitoring will be deployed on patient portal production servers and a baseline of the system will be performed. These changes will be complete by June 12, 2015.
- The patient portal servers will be configured to send all event log information to the MCIT log repository servers. Data will be retained for one year. Dashboards and alerts will be created for monitoring of events. All production log data will be sent to the log repository by June 12, 2015. Baseline dashboards and alerts will be complete by June 26 2015.
- File integrity log data will be maintained in the tools database for 1 year.
- We recognize that the system still allows the use of old SSL protocols. In 2012, we modified the webserver SSL settings so that it negotiated the secure SSL protocols first and then unsecure SSL protocols last. This was implemented this way so that we did not risk breaking legacy browsers and at the time, it was the Microsoft recommended best practice to resolve the SSL man in the middle attacks. As of January 2015, 4.4% of the patient portal access was from legacy operating systems that may not be able to access the portal if we completely remove the SSL 3.0 protocol. The status on the potential use of depreciated encryption ciphers will be presented to the MiChart Patient Portal Workgroup for comment. An overview of the problem and the comments from the Patient Portal Workgroup will be presented to the MCIT Executive Leadership team who will determine if we should disable the use of SSL 3.0.

Action Plan Owner: MiChart Tech Team Manager, MCIT

Expected Completion Date: September 2015

Auditors Comment: In April 2015, Microsoft released new guidance to address use of old SSL protocols. They currently recommend that SSL 3.0 be disabled and to only use TLS protocols. New PCI-DSS guidance requires that SSL 3.0 and TLS 1.0 be disabled immediately or a mitigation plan be in place to have it done by June 30, 2016. Due to the complexity required for a successful attack, the residual risk of not fixing this item would not be considered a high risk.

2. Privileged System Access	Medium

Issue: MCIT does not always remove unnecessary privileged access to the patient portal public web servers[2].

Risk: Data could be lost, modified, or compromised. System stability and availability could be compromised due to accidental or malicious actions.

Support: The patient portal web servers host the Epic MyChart software. A patient connects to one of the web servers to access a portion of their electronic medical record. Any data passed through the web server could be visible to an administrator level account using advanced techniques to scrape data from memory. This technique is commonly used by malicious software and recently resulted in millions of financial records being leaked by a large retail chain. To prevent unauthorized access to patient data, privileged access to these servers should be limited to only authorized personnel. For example, University Audits discovered the following accounts with privileged access:

- Unused test account
- Unused support account
- Vendor contractors no longer assigned to UMHS

Upon discovery and notification, MCIT immediately removed all unauthorized privileged accounts.

Recommendation: At least quarterly, MCIT should review the patient portal web server access control lists and remove the privileged accounts when the account holder no longer has a legitimate need for elevated privileges. Time limits on accounts for non-employee contractor access should be enforced.

Management Action Plan: MCIT agrees to do a quarterly review of all accounts that have access to the patient portal servers.

By current policy, accounts for non-UMHS staff are valid for a maximum of 1 year.

Action Plan Owner: MiChart Tech Team Manager, MCIT

Expected Completion Date: June 2015

3. Patient Password Security	Medium

Issue: MCIT does not fully secure patient access to the patient portal due to weak password complexity requirements and an inadequate password recovery process.

Risk: Weak passwords may allow an attacker to impersonate a patient and gain access to protected health information (PHI). Because of these actions, the reputation of the University would be damaged and U-M would be subject to fines and fees.

[2] A webserver that is globally accessible by anonymous users via the Internet.

3. Patient Password Security	Medium

Support: The audit identified that password complexity settings for patient users use a 6-character minimum. A common good practice is to set the password complexity minimum to at least 8 characters. The longer the password, the stronger the security of the patient account. Additionally, the portal is configured with the vendor default of four challenge questions. The existing challenge questions include one question specifically not recommended by NIST 800-118. The default challenge questions request information that could be easily discovered by performing a search using a search engine or from social media profiles.

When a user calls the portal support phone number, they are connected to the HIM call center. Call center staff have not received social engineering awareness training and may be tricked into letting a malicious actor gain access to patient accounts.

Recommendation: MCIT should increase password complexity requirements so that the minimum numbers of characters are set to at least eight and add language to the portal to inform patients that more complex passwords are possible.

The patient portal should be modified to include more robust challenge questions that will give a variety of choices to patient users and that do not ask easily discoverable information. Password length and complexity should meet or exceed industry good practices such as those found in NIST 800-118 standards or the Open Web Application Security Project [3](OWASP) where appropriate.

To further increase patient account security, MCIT should research and consider offering patients an option of two-factor authentication with the patient portal software.

Management Action Plan: The Michart team will increase the minimum password length to 8 characters and add verbiage to the portal web site suggesting users choose complex passwords.

The MiChart team will implement an improved set of challenge questions.

At this time, the Epic system does not support the use of two-factor authentication for the patient portal. The MiChart team will review new development from Epic and evaluate future offerings related to security and authentication.

Action Plan Owner: EpicCare Ambulatory Manager

Expected Completion Date: July 2015

[3] The Open Web Application Security Project (OWASP) is a 501(c)(3) worldwide not-for-profit charitable organization focused on improving the security of software.

4. Monitoring Event Logs	Medium

Issue: MCIT does not effectively monitor the patient portal event logs consistent with the appropriate service level tier.

Risk: Unresolved application errors could cause system instability that would result in unplanned downtime. As a result, patients would not be able to use the portal.

Support: MCIT does not have a process for monitoring application errors logged in the event log. Using the Windows Application Event logs, the audit identified over 70,000 instances of the same error logged in 8 months from one production patient portal server.

The MCIT on-call policy requires that MCIT services have an operating level agreement (OLA) or service level agreement (SLA) documented in the MCIT support management platform. Currently there are no SLA or OLA documents available for the patient portal that does not comply with the on-call policy.

MCIT services are categorized into one for four service levels. Each level provides a set of expectations of service and support availability. Below are the service level definitions in which MCIT has stated customers can expect:

- **Tier 1 Platinum:** Services with operations that have the highest requirement of availability, the lowest recovery time, with the quickest response time to incidents as defined per the service tier model.
- **Tier 2 Gold:** Services with operations that have a high requirement of availability, a fast recovery time, with a fast response time to incidents as defined per the service tier model.
- **Tier 3 Silver:** Services with operations that have a moderate requirement of availability, can take some time to recover, with a need for a moderate response time to incidents as defined per the service tier model.
- **Tier 4 Bronze:** Services with operations that have the least requirement of availability accept data loss on some scale or entirely, with a need for a response to an incident that can involve some time associated with it as defined per the service tier model.

MCIT has not made a decision as to what service level the patient portal should meet. No service level expectation document has been created and MiChart staff are unclear what service level the patient portal should be considered. As a result, service levels cannot be guaranteed.

Recommendation: MCIT should proactively monitor the patient portal for application errors in the event log. Service level expectations should be defined, documented, and the appropriate documents developed to meet the MCIT on-call policy requirements. Once the expected service levels are documented, steps should be created and periodically reviewed to verify that service levels are met.

4. Monitoring Event Logs	Medium

Management Action Plan: As documented above, all application event log data will be sent to the MCIT log repository. Log data will be retained for one year. Alerts and dashboards will be created to proactively detect application errors.

All components of MiChart, including the patient portal, are considered to be an Enterprise Operation Class (EOC) level application. Any outage for the patient portal would be analyzed as part of the MCIT Enterprise Service Incident Review (ESIR) process. Part of the ESIR analysis is the duration of the outage. System availability is calculated by subtracting the outage times for all unplanned outage from the total available hours. There have been no unplanned outages for the patient portal since it went live in August 2012. An overview of the problem and the comments from the Patient Portal Workgroup will be presented to the MCIT Executive Leadership team who will determine the appropriate service level for the patient portal and develop documents necessary to meet MCIT On-Call policy requirements.

Action Plan Owner:

- Event Log Monitoring - MiChart Tech Team Manager, MCIT
- Patient Portal Service Level - Information Systems Executive, MCIT

Expected Completion Date: September 2015

Follow–up Memos Issued

Closed

AST Shared Services-Vendor Selection and Payment 2014-812

Report issued April 2014 Follow-up report issued May 2015

In July 2014, University Audits completed a review of the Administrative Services Transformation (AST) Shared Services vendor selection and payment processes. University Audits identified several opportunities for improvement:

- Transparency and disclosure of additional project work outside the original competitively bid scope of work
- Documentation of outside interest disclosures and management plans for potential conflict of interest and conflict of commitment situations
- Clarification of the executive vice president and chief financial officer's (EVPCFO) delegation of authority related to procurement contracts and amendments
- Timely disclosure, via the Board of Regents reporting mechanism, of non-competitive purchase awards

University Audit recently conducted a follow-up review and management has either completed corrective action plans or completion is well underway. This audit is **closed**.

Contract Change Orders – Approval: Additional work outside the original project scope was awarded to Accenture using change orders to the original contract. In response to the finding, Procurement buyers were instructed when processing contract change orders to assess whether the RFP fully supports any added services. Where applicable, buyers are now adding language to the RFP project scope and requirements section to provide notice to bidders that there may be related additional work beyond the original RFP requirements. **Closed.**

Conflict of Interest/Conflict of Commitment – Management Plans: At the time of the audit, key decision makers in Business and Finance (B&F) verbally discussed potential conflicts of interest or commitment (COI/COC) with the EVPCFO (at that time), however such discussions and resulting management plans were not documented, as required by B&F policy. The Office of the Executive Vice President and CFO is currently using the university M-Inform Disclosure System to document outside interests and potential COI/COC. All senior B&F staff are current in making disclosures using M-Inform. As M-Inform is used primarily in research and the health system, the B&F senior staff is also providing process improvement feedback to the M-Inform development team. **Closed.**

Contract Change Orders – Delegated Authority: Leadership has taken the opportunity to review and update the Delegation of Authority table that is part of Standard Practice Guide Section 601.24, *Delegation of Authority to Bind the University to External Agreements on*

Business and Financial Matters. The interim director of Procurement Services is leading the updating initiative with involvement of other stakeholders, including Office of General Counsel, Treasury, Facilities and Operations, Sponsored Programs, Human Resources, and representatives from the Dearborn and Flint campuses. Due to the breadth of this project and the need to include multiple parties, the project is expected to be finalized and approved in the late summer or early fall. As the initiative is well underway, this issue is **closed.**

Non-Competitive Purchasing: In July 2014, Procurement Services implemented a robust querying process to improve reporting on non-competitive awards. Standard Practice Guide Section 507.01, *Procurement General Policies and Procedures* was substantially updated and now includes additional language regarding the competitive bidding and sole-source justification process. The revised guidance was issued in January 2015. The updated SPG was widely publicized in the University Record and in communications directed to deans, directors and department heads. **Closed**.

Michigan Dining – Residential 2013-213

Report issued September 2013

First follow-up report issued September 2103
Second follow-up report issued March 2014
Third Follow-up report issued October 2014
Fourth follow-up report issued June 2015

University Audits issued a report for the Residential Dining Services audit in November 2012. An initial follow-up review was conducted in September 2013, a second in March 2014, and a third in October 2014. A fourth follow-up was conducted to assess progress toward addressing audit recommendations related to financial reporting and inventory control. Substantial progress has been made with regard to both issues. **This audit is closed.**

Financial Management and Oversight

- Comprehensive financial and operational metrics are being provided to Michigan Dining leadership as well as dining hall managers. The following reports and metrics have been completed:
    - Food cost and inventory metrics
    - Detailed revenue and expense reports with ratios
    - Productivity metrics indicating meals per labor hour and labor cost per meal
    - Meal plan participation including meals served and meals plan data
    - Headcount and staffing reports

  These reports are sent to the appropriate individuals on a weekly, monthly, quarterly, or annual basis, depending on the needs of the user. Student Life finance management continues to work with IT specialists in hope of automating the reports. The consolidation of chartfields and account codes for Student Life units in fiscal year 2016 will further improve the meaningfulness and detail in the reports. Many of the positive changes in Michigan Dining are due to a transition in leadership and reorganization. In

2014, the director for Michigan Dining was hired and a new financial manager for Student Life was assigned. The finance team's efforts toward providing consistent and meaningful reports for housing, unions, and dining management have been substantial.

- Weekly inventory counts are now conducted and cost of goods sold is calculated for all residential dining operations. Based on review, inventory counts, sales, and food cost by vendor are consistently tracked for all residential dining halls. This data is tracked in spreadsheets that are shared among dining hall managers and Michigan Dining leadership. **Closed.**

MIServer 2013-213

Report issued April 2014 Follow-up report issued May 2015

University Audits issued the MiServer audit report in April 2014. The audit report contained three action-items. A follow-up review was conducted in October 2014. The follow-up review determined Information and Technology Services (ITS) completed two out of the three recommendations. The remaining open action-item recommended was to improve Service Level Expectations (SLE) between ITS and the customer.

ITS has resolved the final open audit recommendation. **This audit is closed.**

Service Level Expectations (SLE): University Audits suggested that the SLE identify how availability metrics will be monitored and reported, as well as define a course of action for missed metrics. Additionally, University Audits recommended defining recovery time objectives (i.e., how long it should take to restore a server) in the SLE and to implement a method for requiring positive acknowledgement of the SLE by the customer. ITS has defined recovery time-objectives, added a link to the SLE in the MiServer portal page, and implemented a checkbox to acknowledge customer agreement to the SLE. ITS has also defined course of action for missed metrics and will implement availability reports in fiscal year 2016. Closed.

Office of Technology Transfer 2014-213

Report issued August 2014 Follow-up report issued May 2015

University Audits issued a report for the Office of Technology Transfer (OTT) audit in August 2014. A follow-up review was recently conducted to assess progress toward completion of management action plans. Key procedures have been documented and some work procedures have been improved. All issues in the report are being addressed. **This audit is closed.**

Documentation of Key Procedures: Continuity of Operations, Emergency Mode Operations, and Disaster Recovery Plans are documented. This documentation includes steps for what would need to be done with TechTracS, the third party software they use to manage intellectual property (IP), for both short-term outages as well as long-term outages as a result of a disaster. Steps have also been documented for backup storage and recovery.

Work was done to update the existing Continuity of Operations Plan (COOP) and identify critical operations. While work was done to augment the plan, the document is based on an outdated template. The most updated template was provided to OTT and will be used to update the COOP. Division of Public Safety and Security Emergency Management will be consulted for guidance to ensure completion of the plan. **Closed.**

Work Procedure Efficiencies: Work procedures were improved, specifically the process to review and resolve discrepancies in patent maintenance fees with the vendor that manages patent portfolios. Several procedures related to these maintenance fees were streamlined and automated. The process that used to take a month takes only a day now. Rather than paying the total amount indicated on the vendor's quarterly invoice, OTT only pays what is owed based on their records, which are more current. For the last quarter, this resulted in a payment that was $79,000 less than the amount indicated on the invoice.

The process to communicate IP created under sponsored activity to the Office of Research and Sponsored Programs (ORSP) remains manual. There were attempts to automate the process but the decision was made to maintain the current manual process as the communication helps the Patent Administrator to identify errors in the system.

There have also been efforts to pursue potential automation of inventor appointments from the university human resource system into TechTracS. OTT consulted with University Human Resources and the software vendor to identify the best way of going about this change. Until the data feed is established and tested, the administrative manager will continue to pull all human resources data on a monthly basis and provide it to the patent administrator to use as a lookup table when updating records. Initially, they believed that all duplicate records would need to be removed or consolidated prior to implementation of the data feed, but that has since been determined not to be true. To address duplicate records, the patent administrator now consolidates records for an inventor whenever a new invention report is received. This will help to clean up the records going forward. **Closed.**

UM-Flint Educational Opportunity Initiatives 2010-211

Report issued February 2011

First follow-up report issued April 2012
Second follow-up report issued April 2013
Third follow-up report issued September 2014
Fourth follow-up report issued June 2015

University Audits reviewed the EOI Office and issued an audit report in February of 2011. Follow-up reviews were conducted in April 2012, April 2013, and September 2014. Since that time, oversight of EOI has been temporarily assigned to the senior vice provost and dean of graduate programs. He has actively engaged with both EOI staff and UM-Flint leadership to maintain EOI's programs.

Under the senior vice provost's leadership, EOI has made significant improvements in managing program activity, finances, and staff. UM-Flint leadership intends to begin a search for a permanent director for EOI and attests that continuing to strengthen the internal control environment will be an important responsibility of the new director. As a result of the significant improvements completed or in process, **this audit is closed.**

Strategic Oversight and Campus Collaboration: EOI programmatic activity was assessed by a consultant retained by the UM-Flint Chancellor. The final report, issued in November 2014, contains several recommendations already completed or being considered to strengthen EOI's existing programs and collaboration in the UM-Flint community. EOI programs have been reorganized into two distinct categories: college programs and pre-college programs. Much work has been done to review the programs for opportunities to streamline without altering the mission of EOI. For example, the senior vice provost coordinated with the Student Success Center to take advantage of similar goals with EOI's Promise Scholars program. There are weekly meetings to discuss the status of the program with leaders from both the Student Success Center and EOI, including the senior vice provost. EOI staff are now representatives on various campus committees, which has also helped connect EOI with other campus programs. **Closed.**

Budget and Financial Management: The senior vice provost is evaluating the financial reporting needs of the department to ensure those needs are met efficiently. Significant support has been received from the UM-Flint Financial Services and Budget department related to reporting and accounting. The vice chancellor for business and finance has committed to covering the deficit accumulated under prior leadership, which will be completed as part of the closing of fiscal year 2015. Cost containment has helped EOI to be on track to end fiscal year 2015 with a positive balance. **Closed.**

Staff Management: The senior vice provost is working with EOI staff to ensure all employees receive the upcoming annual performance evaluation. EOI permanent staff now have monthly meetings to discuss upcoming initiatives or activities, unless significant events affect scheduling abilities. This has enabled all staff to be better aware of other EOI programs and how they relate to each other. Review of meeting minutes from January, March, and April 2015 demonstrate that meetings are well attended, including the senior vice provost. Topics include long-term planning, program reports, and financial matters. New policies, such as a department timekeeping policy and pre-authorization spending forms, are also introduced and discussed. Efforts should continue to document EOI internal policies and address non-compliance. Templates for many internal policies and procedures are available from the Office of Internal Controls (OIC). The budget manager has begun working with the senior vice provost to complete the gap analysis worksheets in preparation for UM-Flint's future plans for unit sub-certification (currently UM-Flint certifies at the executive officer level only). Completion of these worksheets will also help develop documentation for EOI procedures. **Closed.**

Event Management: UM-Flint Event and Building Services (EBS) staff confirmed that coordination with EOI has greatly improved. EBS policies for advance bookings, notice of cancelled events, and food policies are generally followed. Efforts should continue to reinforce compliance with EBS policies. **Closed.**

Continuity of Operations and Disaster Recovery: EOI staff generally save program information on the UM-Flint managed network drives to ensure they are accessible only by authorized individuals. Notes from staff meeting minutes and review of the shared drives confirm that key information is properly stored. Staff receive regular reminders to monitor sensitive data for appropriate security. **Closed.**

Open

Biomedical Engineering 2014-301

Report issued September 2014 Follow-up report issued June 2015

University Audits issued a report for the audit of the Biomedical Engineering department in September 2014. A first follow-up was recently conducted to assess progress toward addressing audit recommendations. One item has been fully addressed and management continues to work on completing action plans for other items. Biomedical Engineering is currently undergoing a restructuring of its operations and has been moved to Clinical Engineering Services along in the Radiology and Engineering Department. The change in organizational structure has delayed the progress of completing action plans. University Audits will conduct a second follow-up in November of 2015. The status of the issues from the audit report is noted below. **This audit remains open.**

Medical Device Security: Biomedical Engineering management started the process of evaluating the security of medical devices. Due to the volume of devices and the skills set required, Biomedical Engineering has enlisted the assistance of MCIT and the MSIS service provider committee. A security risk mitigation plan for each device type has not yet been developed. The status of the plan and security assessment of medical devices will be reviewed during the next follow-up. **Open.**

User Access Controls: Biomedical Engineering is currently in the process of moving to a new system to manage the lifecycle and support of medical devices. The new system uses a product called Asset Information Management System (AIMS) by Phoenix Data Systems, Inc. It is designed to better address the needs and requirements needed to effectively manage medical devices. The goal for completing the move is fall of 2015. University Audits will assess the user access controls in AIMS during the next follow-up and review management actions that are still in progress. **Open.**

Audit Logs: Security event logging for the current asset management tracking system (Maximo) has been enabled and configured to collect information necessary to determined who logged onto the system, when they logged on and logged off, where they logged on from, and other identifying information. Maximo is in the process of being replaced by AIMS and will require the system to be configured to perform effective logging of security events. Biomedical Engineering has requested that University Audits provide suggestions for effective security configurations for the AIMS system. During the implantation of AIMS, Biomedical Engineering and University Audits will collaborate to identify effective security controls. **Open**

IT Documentation: Biomedical Engineering started the process of developing service level agreements (SLA) with key customers. Documentation of key processes and the asset lifecycle of medical devices is currently in progress. A review of these process documents and SLA's will be conducted during the next follow-up. **Open**

Protected Health Information (PHI) Removal: Biomedical Engineering management gathered the best practices used at U-M Hospitals and Health Centers (UMHHC) and Medical Center Information Technology (MCIT) department. Currently, they are putting together a matrix that will clarify the responsibilities for removing PHI. Additionally, they are planning to integrate the requirements into AIMS, which will also include some other Health Insurance Portability and Accountability Act (HIPAA) requirements. **Open**

Preventative Maintenance Scheduling: Since the transition to AIMS started, the Biomedical Engineering department has been exploring the functionalities of the system and discovered certain reports that will help address previous process deficiencies. The department reviewed all the parts that exceeded $5,000 and identified 2,000 items that needed to be on Preventative Maintenance (PM) schedule, of which 1,500 have already been scheduled. The plan is to do a full inventory of all the medical equipment by the end of 2015. **Open**

Statement of Activity Reconciliation: The reconciliations that were incomplete at the time of the audit have been completed. The reconciliation process has been taking place monthly. The Facilities Department financial director is now reviewing and approving reconciliation results on a monthly basis and any cases of non-compliance are reported to the units. The reconciler completed some additional training. Since the organizational structure is still changing there will be more discussions regarding segregation of responsibilities, definition and documentation of roles, and expectations along with the required training and support. However, financial reporting, including reconciliation process will continue to be managed by the Facilities department. **Closed**

Part Inventory Management: Stock parts were separated from non-stock parts. The goal is to do a full inventory of non-stock parts by the end of 2015. A business and procurement specialist position has been created. One of the responsibilities assigned to this position will be to create an inventory of all parts and track it regularly. Biomedical Engineering will also do site visits to other institutions and learn how they handle parts. The department has also purchased an electronic card reader, which is in the final installation phase. **Open**

Personnel Procedures: Biomedical Engineering management revised the on-boarding checklist and is now providing it as part of the new employee package, but has not included it in the written policy. No off-boarding policy has been drafted yet. The department has made progress in documenting the job descriptions but still has some to complete. Once the job descriptions are finalized, Biomedical Engineering will be able to create a training plan for each job. **Open**

Donor & Alumni Relationship Tool 2013-106

Report issued June 2014 Follow-up report issued May 2015

University Audits issued a report on the Donor & Alumni Relationship Tool (DART) in October 2013. An initial follow up review was conducted in June 2014. A second follow up was recently conducted to assess progress toward addressing audit recommendations related to Dev/Net application security, organization of key information, completion of a data dictionary, and better utilization of information obtained through the help desk hotline. While there has been progress made, all issues remain open and a third follow up review will be completed in January 2016. **This audit remains open.**

- **Office of University Development (OUD) Dev/Net Web Application Security:** The OUD intranet website uses versions of technology that are no longer supported by the respective vendors. The website was developed 10 years ago using programming practices that are vulnerable to malicious attackers. An attacker could access sensitive donor data by exploiting a part of the website that was accessible to anyone who created a friend account (self-created guest account). The website contains some sensitive constituent data that is restricted to development staff.

  OUD committed to removing friend account access as a short-term solution and replacing the site as a long-term solution. The friend account access has been removed. OUD has begun the process of replacing the intranet website by moving to another website hosting platform and developing new sites (using Google Sites and other tools).

  The current OUD intranet website serves the development community at large and hosts many sites for OUD departments. OUD has formed a task force to address the website move, including definition of business requirements, review of software options, and allocation of staff resources. As a proactive measure, OUD has developed and documented a process that will be used when a move to a new platform has been decided by the taskforce. The task force plan will be created by the end of fiscal year 2015 and some early implementation may be underway, provided resources are allocated (see Service Enhancement Initiative below).

- **Service Enhancement Initiative**: To manage the service provided to the university community, OUD has launched a service enhancement initiative. The goal is to address business needs strategically and prioritize projects so the highest priority items have sufficient resources and support to be implemented. The initiative has involved submitting all projects (approximately 80 this round) for prioritization. Projects were submitted in April 2015. OUD leadership will complete ranking the projects by the end of May 2015. A preliminary project roadmap for fiscal year 2016 will be developed. Then, by September 2015, the projects will be scoped to determine resource availability.

  While remediation of the outstanding issues will need to be addressed through the service enhancement initiative, OUD has taken some steps to mitigate risk or gather information for future action. These include:
  - **Organization of Key Information (Intranet Site)**: To ensure the final intranet site will meet the needs of users, OUD has established a task force to assess user awareness and use of sites like Dev Net and Google Sites and to determine how Google Analytics is used. The task force includes OUD and user employees from the units.
  - **Completion of Project Tasks (Data Dictionary)**: To mitigate the risk of not having a data dictionary available, OUD's reporting group has prepared documentation to help users be more effective when using the U-M provided Business Objects reports. They have drafted a Google site that provides suggestions on preparing queries for popular information requests. Additionally, the reports in Business Objects contain information designed to help the user more easily use the queries. This combination of information may help address user needs until the data dictionary can be provided.
  - **Help Desk Information**: Footprints has undergone significant enhancements to better track and categorize tickets that are logged through the hotline. The enhancements aid OUD in assessing the amount of time and resources used on specific issues. With the enhancements already made and the reduction in tickets due to the maturity of DART and user familiarity, further updates will be a low priority item.

Medical Center Information Technology Data Center and Arbor Lakes North Campus Data Center 2012-307

Report issued January 2016

First follow-up report issued March 2014
Second follow-up report issued September 2014
Third follow-up report issued January 2015
Fourth follow-up report issued June 2015

University Audits conducted a review of Medical Center Information Technology (MCIT) managed data centers and issued the audit report in April 2013. The report recommended that MCIT develop a continuity of operations plan (COOP) that identifies the critical functions of the data centers and key personnel. This plan should address data center recovery and continuity

strategies to maintain critical functions and disaster recovery procedures used to restore IT infrastructure systems that support critical functions of the data center.

MCIT is making progress by developing an effective IT disaster recovery strategic plan. The current objectives are to refine both the IT disaster recovery plan and the accompanying information system contingency plan (ISCP), put the minimum infrastructure in place to support disaster recovery (DR) planning and ISCP development, and ensure that recovery is in place for platinum and gold services (i.e., services identified by UMHS as having the highest availability requirements, quickest response to incidents, and lowest recovery times).

In response to the audit recommendations, MCIT Infrastructure and Systems Operations staff coordinated meetings with key personnel throughout the university with a goal to develop a cohesive COOP. The following has occurred since the last update in December 2014:

- Most roles and responsibilities have been defined and assigned.
- Development of several components of the DR plan has begun with the formation of DR
- Created workgroups. Each workgroup has specific objectives and assigned deliverables. Below are the currently defined workgroups:
    - Disaster Recovery Assessment
    - Disaster Recovery Initiation
    - Disaster Recovery Execution for each service level
    - IT Service Assessment
    - Disaster Recovery Testing
    - IT Service Recovery

The DR plan is moving forward and is currently focused on Infrastructure. The first components to be included are Exchange (e-mail and calendar), MiChart (electronic health records), and other infrastructure-supported platinum and gold application services.

Funding approval for hiring dedicated staff to support the disaster recovery plan has not yet been decided. MCIT indicated that a decision should be made after the DR plan is submitted to the MCIT Operations Management Committee in July 2015.

MCIT efforts to date are producing a well-designed disaster recovery plan. To be effective, the plan must undergo necessary and regular testing. Successful implementation is contingent on funding for dedicated and temporary staff. Without funding, the IT disaster recovery plan will not undergo effective testing and implementation of the plan will be delayed, which could result in loss of data and disruption of services the health system.

We will continue to monitor MCIT's efforts at defining a comprehensive COOP. This is an ongoing process. We plan to conduct further follow-up procedures during the second quarter of fiscal year 2016. **This audit remains open.**

Museum of Zoology 2014-208

Report issued January 2016 Follow-up report issued June 2015

University Audits issued a report for the Museum of Zoology (UMMZ) audit in September 2014. A follow-up review was recently conducted to assess progress towards completion of management action plans. Progress was made on all issues and two of the five issues were closed. A second follow-up will take place in January 2016. **This audit remains open.**

Import and Export Permits: The department is in the process of drafting a business case to be presented to the College of Literature, Science, and the Arts for a registrar position that would oversee collections within UMMZ and the Herbarium. The department has drafted a description of the registrar position and benchmarked against other institutions to gain a better understanding of what the position responsibilities will entail and the level of effort needed. Data has been collected from collection managers regarding the inflow and outflow of specimens to gain an understanding of how much effort will be expended towards import and export compliance. The department perspective is that the hire of a registrar would be most effective after the move from the Ruthven Museum to the Varsity Drive complex. **Open.**

Handling of Hazardous Materials

- Lab Safety Training: Collection managers now require all individuals handling chemicals to complete OSEH required lab safety training. Certificates of completion are maintained for each lab in the blue binder documenting Chemical Hygiene Plans. The training requirement has been implemented as part of the on-boarding process.
- Transport of Specimens: Specimens preserved in alcohol are now picked up and transported by LSA Movers on Thursday of each week. The specimens are picked up directly from the lab/office space. Collection managers package the specimens based on a mandatory OSEH training session given in November 2014 that focused on safely packaging specimens. **Closed.**

Documentation of Procedures: Collection managers continue to work on curation manuals and some progress has been made. Comprehensive curation manuals are completed for some collections but not all. These comprehensive manuals are shared on M+Box to be used as a template for other manuals in progress. The completion of curation manuals will likely be delayed until the implementation of the new database software, Specify, which manages species and specimen data. Some collection managers are waiting to update manuals because many procedures will change due to the transition to Specify. The implementation of Specify will be the first time all divisions have used the same software. **Open.**

Management of Keys: The move from Ruthven Museum to the Varsity Drive location will resolve the physical key issue. This move is currently scheduled for 2016, possibly beginning in spring. At the new facility on Varsity Drive, access to the building, collection space, and lab space will be managed by keycard access only. The collection and lab spaces will be locked at all times. Physical keys will only be used to access individual office space in the building.

Keycard access will continue to be managed by the administrative specialist after the move. Museum leadership has attended meetings and taken part in discussions with the Division of Public Safety and Security, Risk Management, and the Key Office to gain an understanding of access and security plans for the new facility.

For the newer Biological Sciences Building that is scheduled to be complete in 2018, a key exchange process will be implemented in which the department will maintain keys to the new building and only provide them in exchange for old keys. Security access for the building is expected to be set up similar to the Varsity Drive facility, with physical keys used only for individual office space. **Closed.**

Management of Artwork: The UMMZ scientific illustrator continues to inventory art as it is found. The focus is on illustrations and fine art although occasional papers, miscellaneous publications, and some other items are being inventoried as well. More art is expected to be uncovered during UMMZ's move to Varsity Drive this fall. University Audits provided the scientific illustrator with names of experts in the U-M Museum of Art for guidance on how to inventory efficiently and preserve art appropriately. When all art has been identified, Risk Management will be consulted to obtain appropriate insurance coverage. **Open.**

Payment Programs for Research Subject Incentives 2012-501

Report issued September 2014 Follow-up report issued May 2015

University Audits reviewed payment programs for research subject incentives and issued an audit report in September 2014. Several of the audit issues were closed at the time of the final report. Some remaining items have been fully addressed, but management continues to work on completing action plans for other items. University Audits will conduct a second follow-up in December of 2015. The status of the issues from the audit report is noted below. **This audit remains open.**

Form 1099 Tax Reporting Compliance: A performance agreement between ISR, Tax Compliance and Planning, and Procurement Services has still not Finalized. The ongoing efforts to resolve final details continue. While ISR provided the Human Subjects Incentive Payment Office (HSIP) with a full year of payment data for calendar year 2014 as agreed, the data was missing key data fields and the Tax Department was not able to combine it with other university data for 1099 reporting. A preliminary review by the HSIP Office identified inconsistencies that, when resolved, should help HSIP and ISR refine their processes and clarify unit responsibilities. **Open.**

Internal Control and Operational Efficiencies

- **Collection of Payment Data**: ISR now uses a standardized template to collect payment information from study teams who pay research participants in cash. ISR continues to investigate methods to more efficiently obtain this data directly from software used by the study teams that already has some of the required payment information. **Closed.**

- **Subject Incentive Cash Fund**: The ISR subject payment imprest cash account has been reduced to $150,000. The cash counts are completed by two individuals, one of whom has no access to cash. Due to staffing concerns and the length of time it takes to complete the count, ISR has elected to move to a bi-monthly count instead of a monthly count. However, at the time of our follow-up, both individuals did not initial or sign the count documentation. University Audits will verify at the next follow-up that both individuals are signing off on the counts as originally agreed. **Open.**
- **User Developed Application:** ISR updated documentation for their check writing system and also worked with ITS to complete a RECON risk assessment of the system. The RECON identified several high vulnerabilities. At the next follow-up, University Audits will verify that ISR has addressed the high-risk vulnerabilities identified in the RECON. **Open.**

Updating of University Policy: Standard Practice Guide (SPG) Section 501.07*, Research Subject Incentives*, was updated to reflect current policy and remove references to using P-Cards to pay research subjects. An outdated SPG was deleted. **Closed.**

System Compliance Monitoring Opportunities: The HSIP system now flags payment requests for a method of payment that does not match what the IRB originally approved. These flags alert the HSIP staff to review the request in more detail to research the discrepancy. Typically, this involves a study team that requests cash to purchase IRB-approved gift cards. The HSIP Program Manager is developing reporting to monitor these payments after issuance to validate they were processed appropriately and follow up with the study teams when necessary. In addition, HSIP meets monthly with ITS and keeps a list of desired enhancements or upgrades to the system. University Audits verified that the system generates a flag and that the HSIP manager's preliminary monitoring reports have been used to contact study teams for clarification. **Closed.**

Third Party Vendors: Use of third-party vendors, such as Amazon MTurk, to pay research subject incentives is in violation of SPG 501.07. However, use continues to grow across campus, including researchers who would traditionally use HSIP and those who are part of ISR. The HSIP Program Manager had taken the lead on researching this issue. His research has been shared with leadership in tax, treasury, and procurement, including new risks that were unknown at the time of the original audit. However, there has been no decision on how to manage this growing risk. Additional support is necessary to resolve this item. The interim associate vice president for finance has tasked the project management office to assemble a workgroup to further research and develop standards to resolve this item. **Open.**

Remote and Telecommuting Employees 2014-110

Report issued October 2014 Follow-up report issued May 2015

University Audits issued a report for the Remote and Telecommuting Employees audit in October 2014. University Human Resources (UHR) made the following commitments to help units enhance management of remote and telecommuting employees:

- Define telecommuting and remote employees
- Provide clear guidance on contacting the Office of General Counsel when employing individuals outside of Michigan or the United States
- Revise UHR website to help identify and boost awareness of key resources
- Consider the risks and feasibility of collecting information on remote and telecommuting locations

A follow-up review was recently conducted to assess progress toward completion of management action plans. Although significant progress has been made, all issues will remain open and a second follow-up review will be completed in December 2015. **This audit remains open.**

Remote/Telecommuting Policy: The university did not have a policy that established clearly defined requirements for remote and telecommuting employees. UHR worked with the Office of Internal Controls to modify the Employment Gap Analysis Tool. The revised tool includes controls to discuss new job offers for employment outside of Michigan or the United States with the Office of General Councel and to ensure units have a formal telecommuting agreement for all applicable employees.

UHR will revise university Standard Practice Guide Section 201.05, *Work Rules and Conditions*, to require units to execute telecommuting agreements. The revised policy will also include a link to UHR's webpage pertaining to flexible work arrangements and remote employees. The target date for the revised policy is September 2015. **Open.**

Remote/Telecommuting Resources and Guidelines: At the time of the audit, UHR provided guidance for remote and telecommuting employees, but the guidance was not easily retrievable or linked to university policy and procedures. To help units identify key resources and more easily navigate to the resources, UHR agreed to review the current information as part of an existing project to review and update websites.

UHR is working with the Work/Life Resource Center to revise websites and clarify information including defining remote and telecommuting employees. Updated information will help units understand when a formal agreement is required. The target date for the revision is fall 2015. **Open.**

Remote/Telecommuting Population: The University does not centrally track or maintain key data regarding remote and telecommuting employees, such as work addresses. In April and May 2015, UHR met with administrators from the Tax Department, the Payroll Office, the Office of Risk

Management, and the Office of the General Counsel to discuss the importance of having accurate employee work addresses. All parties agreed that units bear primary responsibility for monitoring employee location, but having accurate employee work addresses on file would also be useful for addressing situations such as insurance coverage.

UHR will revise the telecommuting agreement to require units to maintain current work addresses for employees working offsite. Additionally, UHR will develop a job aid (e.g., work flow) to educate units on the proper procedure. If units follow the process, Shared Service Center personnel will receive the information and enter it into the payroll system, allowing departments (e.g., Risk Management) to obtain the data internally. **Open.**

School of Education 2014-209

Report issued September 2014 Follow-up report issued June 2015

University Audits performed an audit of the School of Education (SOE) and issued an audit report in September 2014. The following is a summary of the eight audit issues included in the report and a description of the corrective actions taken by management. Corrective actions were completed for four of the issues. A second follow-up will be conducted during January 2016 to assess progress on the remaining four issues. **This audit remains open.**

Affiliation Agreements: Management did not consistently establish and properly authorize affiliation agreements with schools/school districts that train student teachers.

The affiliation agreement template has been revised and vetted with the Office of the General Counsel. The SOE Dean of and the Vice Provost for Global and Engaged Education will sign affiliation agreements on behalf of the university. SOE plans to have the new affiliation agreements signed by the university and all school districts by July 2015. All signed affiliation agreements will be housed in a designated shared folder.

SOE is also developing a database to house all affiliation agreement details and track five-year dates for updating/re-signing agreements. A protocol that will require clinical placement coordinators to confirm that an affiliation agreement is on file prior to placing student teachers each semester will be documented by October 2015. **Open.**

Fire Alarm System: The current fire alarm system was not audible in certain sections of the SOE building to warn occupants about fire emergencies.

A new fire alarm system and a public address system were installed for the south side of the SOE building in August 2014. The new system was successfully tested by Occupational Safety and Environmental Health and by the State of Michigan Fire Inspector in August 2014. The new fire alarm system for the north side of the SOE building is scheduled to be operational by fall 2015.

SOE has designated floor marshals who have been trained by the Division of Public Safety and Security to handle emergencies related to fire, medical, and weather related events. The floor marshal contact list is maintained by the SOE Facilities Office. An annual fire drill was conducted in April 2015. The facilities manager periodically meets with the floor marshals to discuss building safety issues as they arise. **Open.**

Risk Evaluation of computers on Open Networks (RECON) – Security Issues: SOE had not completed corrective actions for all recommendations made to address high or severe risk security issues identified by the last RECON conducted in 2011.

Information and Infrastructure Assurance conducted a new RECON for the SOE MiWorkspace environment in 2015 and identified 30 action items, of which 28 were the responsibility of Information and Technology Services (ITS). The new RECON noted that accounts must be de-provisioned when faculty and staff leave SOE to prevent unnecessary access to the environment after departure. To address the remaining two action items, the off-boarding checklist has been updated with a step to work with ITS to terminate access to all university systems upon departure of faculty and staff from the SOE. **Closed.**

Graduate and Undergraduate Grade Changes: SOE leadership had not documented and communicated graduate and undergraduate grade change policies to all academic departments. There was a lack of clarity of expectations regarding review of grade changes.

SOE leadership has conferred responsibility for changing grades to the instructor of the course. The SOE Registrar's Office is working with ITS to develop a report in M-Pathways Student Administration that lists all grade changes for every SOE course, including independent and cross listed courses offered in a given term. SOE plans to provide this report to the program chairs each semester for review. However, the report has not been tested, and expectations regarding responsibility and review of grade changes have not been defined or communicated to all academic departments in SOE. The target date for completion is October 2015. **Open.**

Equipment Tracking – Research Incentive and Discretionary Funds: SOE did not have a process to track non-capital equipment and other property, including tangible, non-consumable items purchased using research incentive (RESIN) funds and discretionary funds.

Using Concur and Statement of Activity reports, the SOE Office of Financial Management and Planning (OFMP) currently tracks non-capital equipment purchases in a spreadsheet housed in the shared folder. The SOE Information Technology Office periodically reviews the OFMP spreadsheet and updates their database with any technology related purchases such as hard drives, cameras, computers, laptops, monitors, and printers. The database contains additional technical details such as serial numbers to easily identify and account for high-risk consumable items and equipment that belong to the university. **Closed.**

Building Keys and M-Cards: SOE did not obtain positive verification that departing staff members, faculty, and graduate student employees have returned assigned building and storage cabinet keys. SOE does not revoke key card access for all departing faculty, staff, and graduate student employees.

The entire SOE building will be rekeyed in summer 2015. A kick-off meeting is scheduled for June 2015 to discuss the logistics of the project. The SOE Facilities Office will work with ITS and the U-M Key Office on the rekeying project and the target date for completion is October 2015. Supervisors are now responsible for collecting keys from departing SOE employees and returning them to the SOE Facilities Office. The SOE Facilities Office will reimburse key deposits as necessary and maintain an internal spreadsheet of all key assignments. The SOE faculty and staff termination checklist has been updated to reflect this practice.

The SOE Facilities Office is in the process of reconciling current staff, faculty, and graduate employees against everyone with key card access in the system to identify individuals whose key card access needs to be revoked. The target date for completion is October 2015. The SOE Office of Human Resources has included SOE Facilities Office staff in their personnel change notification email group to inform them of upcoming employee terminations so that key card access can be revoked in the system. **Open.**

Conflict of Interest and Conflict of Commitment: Management did not have an effective process to consistently implement the conflict of interest (COI) and conflict of commitment (COC) policy.

In the future, all new staff members will complete the COI/COC and the Confidentiality Statement forms upon hire. All new faculty members will complete the COI/COC form upon hire. SOE has updated the on-boarding checklists to reflect this practice. All faculty members will renew the COI/COC form annually with their Faculty Annual Report submission instead of doing so at different times during the year. University Audits verified that a sample of staff members hired since August 2014 had completed the COI/COC and Confidentiality Statement forms as part of their on-boarding process. One faculty member hired since August 2014 had completed the COI/COC form as part of their on-boarding process. **Closed.**

Joint Appointments: All joint appointment agreements did not contain consistent guidelines that address key issues and define the roles and responsibilities of the schools/colleges and the faculty.

SOE consulted with the provost's office to confirm that existing joint appointment agreements need not be updated. For all future inter- and intra-school appointments, SOE will use the Memorandum of Understanding (MOU) templates developed by the provost's office that contain guidelines defining key aspects of a joint appointment. All new MOUs will be submitted to the provost's office for review no later than six months from the start of the joint

appointment. To date, there have been no new joint appointments at SOE since the implementation of this process. **Closed.**

Subsequent to the audit, SOE management reached out to the Bentley Historical Library (Bentley) for assistance with their records management process. During summer 2015, Bentley will work on a project to evaluate documents currently stored at SOE. The goal of the project is to:

- Develop an inventory of SOE archives and assess the records collection
- Match active records to retention dates based on retention rules for various record types that need to be stored onsite
- Identify inactive records that no longer need to be retained and recommend them for destruction
- Identify high-value archives and transfer them to the Bentley pending approval of the Dean's office

Wireless infrastructure in the SOE building is being upgraded in accordance with the ITS upgrade initiative. Over 90% of SOE staff and 75% of faculty have transitioned to MiWorkspace with the reminder scheduled for transition during the annual computer upgrade cycle.

Social Media 2014-201

Report issued August 2014 Follow-up report issued May 2015

University Audits issued the Social Media audit report in August 2014. The report had three action items. University Audits recommended working with those responsible for social media locally in the schools, colleges, and departments at the university to create and implement an overall strategic plan for social media addressing deployment and management of social media platforms; updating acceptable use guidance for faculty, students, and staff to include use of social media; and coordinating with other university primary social media providers, ITS, University Human Resources, and the Office of Admissions to create training and leverage training opportunities

Global Communications and Strategic Initiatives has made significant progress in addressing each of these recommendations. Below is a detailed update of the current status of each audit recommendation. Each bullet represents a step in the Management Action Plan created to address each recommendation. **This audit remains open.**

Social Media Strategy:

- Complete the inventory and individual assessment of all primary social media channels that currently represent the University of Michigan. **Closed.**
- Build a concrete network of social media representatives responsible for content management of each identified channel. **Closed.**
- Conduct regular meetings of social media representatives. **Closed.**
- Formalize policy for social media account creation and educate users on the availability of the Office of UMSocial for guidance and consultation. **Open.**

- Create and adopt a plan for unified message role out in instances of specialized campaigns, announcements, and emergency response among social media representatives, public affairs, and other key stakeholders. **Open.**

Acceptable Use Guidelines:

- Update the acceptable use policy for faculty, staff, and students to include social media. **Open.**
- Educate faculty, staff, and students on the potential risks of social media as related to HIPAA, FERPA, and NCAA legal and regulatory requirements. **Open.**
- Create an active channel of communication between the Office of UMSocial, ITS, and the Office of General Counsel. **Closed.**
- Author an acceptable use agreement template to be distributed and/or adopted for new employee orientation, student orientation, training, or other events. **Open.**
- Continue development of pertinent resources on socialmedia.umich.edu. **Closed.**

Training and Awareness:

- Incorporate social awareness slide into new employee orientation and other presentations across campus, such as the Department of Public Safety and Security safety video. **Closed.**
- Create a Brown Bag series on social media topics available to staff and faculty. **Closed.**
- Identify opportunities to partner with skilled faculty and staff using social media and conducting relevant research to host live chats and opportunities for education and engagement. **Closed.**
- Provide regular updates from the U-M Social Media website that highlight new developments, research, and topics in social media. **Closed.**
- Set standards for presentation of personal and unaffiliated individuals through social media, including username and biographical protocol. **Open.**

University Audits will follow-up with Global Communications and Strategic Initiatives in December 2015 to assess the status of the remaining open items.

Open Audits Follow-up Table
As of June 30, 2015

Audit	Report Date	Open Issues	Follow-Up Memo Issue Target Date
UM-Dearborn College of Engineering and Computer Science 2012-302	June 2012	Financial oversight; documented policies and procedures; gift handling and monitoring	First follow-up April 2014 _____ Second follow-up February 2015 _____ Third follow-up scheduled for September 2015
Medical Center Information Technology and Arbor Lakes/North Campus Data Centers 2012-307	April 2013	MCIT Managed Data Centers lack a comprehensive continuity of operations plan. Note: This issue requires long-term corrective actions and planning efforts are ongoing.	COOP Meetings June 2013 September 2013 _____ First follow-up March 2014 _____ Second follow-up September 2014 _____ Third follow-up January 2015 _____ Fourth follow-up June 2015 _____ Fifth follow-up scheduled for December 2015

University Audits
Summary of reports issued – May 1 through June 30, 2015

Audit	Report Date	Open Issues	Follow-Up Memo Issue Target Date
Molecular and Behavioral Neuroscience Institute 2013-214	May 2013	Long-term financial viability	First follow-up January 2014 _____ Second follow-up August 2014 _____ Third follow-up March 2015 _____ Fourth follow-up scheduled for November 2015
Office of Student Publications 2013-203	July 2013	Strategic plan and vision; documented policies and procedures; training; procurement contracts	First follow-up June 2014 _____ Second follow-up February 2015 _____ Third follow-up scheduled for September 2015
School of Natural Resources and the Environment 2012-210	September 2013	Effort certification; admissions documentation; lab safety; documented processes	First follow-up June 2014 _____ Second follow-up February 2015 _____ Third follow-up scheduled for September 2015

Audit	Report Date	Open Issues	Follow-Up Memo Issue Target Date
UM-Dearborn College of Arts, Sciences, and Letters 2013-204	September 2013	Conflicts of interest/ conflicts of commitment; agreements with third parties; faculty course releases and stipends; roles and responsibilities	First follow-up June 2014 _____ Second follow-up March 2015 _____ Third Follow-up scheduled for October 2015
UM-Dearborn Office of Financial Aid 2013-201	September 2013	Conflicts of interest or commitment	First follow-up June 2014 _____ Second Follow-up February 2015 _____ Third Follow-up scheduled for September 2015
College of Engineering Research Software Licensing 2013-310	October 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; classification of software purchases	First follow-up April 2014 _____ Second Follow-up October 2014 _____ Third Follow-up originally scheduled for May 2015; rescheduled for July 2015

University Audits
Summary of reports issued – May 1 through June 30, 2015

Audit	Report Date	Open Issues	Follow-Up Memo Issue Target Date
Donor and Alumni Relationship Tool (DART) 2013-106	October 2013	Changes to the default master encryption password; Office of University Development 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 metrics	First follow-up June 2014 _____ Second Follow-up May 2015 _____ Third Follow-up scheduled for January 2016
Financial Operations Cost Reimbursement Office Effort Certification Process 2013-501	January 2014	Maximum allowable effort on federal projects; data validation	First follow-up October 2014 _____ Second follow-up originally scheduled for May 2015; rescheduled for July 2015
Department of Chemistry 2013-212	March 2014	Recharge billing; facility access and security; support for lab fees; system configuration documentation; chemical inventory documentation; inaccurate asset inventory records	First follow-up February 2015 _____ Second follow-up scheduled for September 2015

University Audits
Summary of reports issued – May 1 through June 30, 2015

Audit	Report Date	Open Issues	Follow-Up Memo Issue Target Date
Export Controls 2014-404	April 2014	Governance; recordkeeping; education and training; Lack of return or destroy procedures; foreign nationals; IT security; overseas travel	First follow-up November 2014 _____ Second follow-up originally scheduled for June 2015; rescheduled for July 2105
UM-Dearborn Information Technology Services 2014-216	May 2014	Vulnerability detection and remediation; malware detection and remediation; account provisioning and de-provisioning; network segmentation; software asset management ; it disaster recovery and business continuity; it change management; fixed asset management ; P-Card review process; management reports; conflict of interest/ commitment	First follow-up February 2015 _____ Second follow-up scheduled for September 2015
School of Dentistry 2014-215	May 2014	Credentialing; adjunct onboarding and oversight; additional compensation payments; conflict of interest and conflict of commitment; student discount eligibility verification; graduate program admission	First follow-up March 2015 _____ Second follow-up scheduled for October 2015

University Audits
Summary of reports issued – May 1 through June 30, 2015

Audit	Report Date	Open Issues	Follow-Up Memo Issue Target Date
General Laboratory Safety 2014-401	July 2014	Safety culture; oversight and monitoring; defining the lab population and identifying hazards; training and education; monitoring reports and trend analysis; safety role definitions; communication and awareness	First follow-up March 2015 _____ Second follow-up scheduled for September 2015
Student Domestic Travel – Sponsored Teams and Groups 2013-110	July 2014	Process owner; policy and guidance	First follow-up March 2015 _____ Second follow-up scheduled for October 2015
Bentley Historical Library 2014-201	July 2014	Detroit Observatory; security of facilities; contract oversight; DRP; environmental controls in archives; insurance for fine art; collection backlog management; time reports and travel expenses	First follow-up March 2015 _____ Second follow-up scheduled for October 2015
University of Michigan Health System MiChart Revenue Cycle 2014-112	July 2014	Segregation of duties	First follow-up April 2015 _____ Second follow-up scheduled for November 2015

University Audits
Summary of reports issued – May 1 through June 30, 2015

Audit	Report Date	Open Issues	Follow-Up Memo Issue Target Date
University Library 2014-217	July 2014	Cash handling; PCI compliance; verification of equipment inventory; Statement of Activity reconciliations; disaster response and recovery plan; IT change management; IT support management	First follow-up March 2015 _____ Second follow-up scheduled for October 2015
Office of Technology Transfer 2014-213	August 2014	Documentation of key procedures; work procedure efficiencies	First follow-up May 2015 _____ Second follow-up scheduled for December 2015
Social Media 2013-307	August 2014	Social media strategy; acceptable use guidelines; training and awareness	First follow-up May 2015 _____ Second follow-up scheduled for December 2015
Sponsored Programs Office of Contract Administration 2014-502	September 2014	Subrecipient monitoring roles and responsibilities; subrecipient eligibility requirements	First follow-up April 2015 _____ Second follow-up scheduled for November 2015
School of Education 2014-209	September 2014	Affiliation agreements; fire alarm system; graduate and undergraduate grade changes; building keys and M-Cards	First follow-up June 2015 _____ Second follow-up scheduled for January 2016

University Audits
Summary of reports issued – May 1 through June 30, 2015

Audit	Report Date	Open Issues	Follow-Up Memo Issue Target Date
Payment Programs for Research Subject Incentives 2012-501	September 2014	Tax reporting compliance; internal control and operational efficiency; HSIP procedures; enhancing training; updating University policy; system compliance monitoring; third party vendors	First follow-up May 2015 _____ Second follow-up scheduled for December 2015
Museum of Zoology 2014-208	September 2014	Import and export permits; documentation of key procedures; management of artwork	First follow-up June 2015 _____ Second follow-up scheduled for January 2016
Remote and Telecommuting Employees 2014-110	October 2014	Remote/telecommuting policy; remote/ telecommuting resources and guidance; remote/telecommuting population	First follow-up May 2015 _____ Second follow-up scheduled for December 2015
UM-Dearborn Athletics 2014-214	October 2014	Varsity sports compliance; classification of club sports; children on campus; liability protective measures; facility rental contracts and accounts receivable; hiring of relatives; monitoring and approving employee time worked; cash handling and credit card management	Follow-up scheduled for May 2015

University Audits
Summary of reports issued – May 1 through June 30, 2015

Audit	Report Date	Open Issues	Follow-Up Memo Issue Target Date
Biomedical Engineering 2014-301	October 2014	Medical device security; user access controls; audit logs; IT documentation; protected health information removal; preventative maintenance scheduling; part inventory management; personnel procedures	First follow-up June 2015 _____ Second follow-up scheduled for January 2016
U-M Health System Office of Clinical Safety 2014-211	November 2014	Protected health information; payment processes; system access and documentation; inconsistencies in claims information; quality reviews; patient grievances	Follow-up originally scheduled for June 2015; rescheduled for July 2015
Pathology Laboratory Information System 2014-305	December 2014	Security vulnerabilities; IT documentation of key procedures; LIS user access controls	Follow-up scheduled for July 2015
School of Information - Information Technology Report 2015-211	February 2015	Vulnerability detection and remediation; system and change management; account provisioning and access management; password management; firewall; physical security; hardware and software asset management	Follow-up scheduled for September 2015

Audit	Report Date	Open Issues	Follow-Up Memo Issue Target Date
UMHS IT Governance 2014-303	February 2015	IT and overall governance structures; IT within UMHS; authority to govern IT; IT shared services; coordination of IT at UMHS; relationship with the University of Michigan IT community	Follow-up scheduled for September 2015
Online Access Request System 2014-111	February 2015	Unit liaisons requesting access for themselves; unit liaison training; unit transfers; roles and role descriptions; review of access requests; OARS continuity of operations plan	Follow-up scheduled for September 2015
Department of Pathology 2015-210	March 2015	MLab agreements; MLabs revenue cycle; equipment management; off-boarding process; annual code of conduct attestation; faculty compensation model	Follow-up scheduled for October 2015
Museum of Anthropological Archaeology 2015-209	April 2015	Management of collections; collaborative agreements; permits; OSEH compliance monitoring; travel oversight; access management	Follow-up scheduled for November 2015

University Audits
Summary of reports issued – May 1 through June 30, 2015

Audit	Report Date	Open Issues	Follow-Up Memo Issue Target Date
Department of Biological Chemistry 2015-208-2	April 2015	Sensitive institutional data; monitoring conflict of interest; research investigators; effort certification	Follow-up scheduled for November 2015
Medical School Department of Pharmacology 2015-208-3	April 2015	Sensitive institutional data; recharge activity	Follow-up scheduled for November 2015
Medical School Department of Surgery Division of Anatomical Sciences 2015-102	April 2015	Inventory management and recordkeeping; anatomical donations database; management of specimen loans; recharge and rebill services; security of sensitive data; escalating non-compliance or other concerns; documented policies and procedures; updating and approving legal agreements and forms; documented agreements	Follow-up scheduled for November 2015
English Language Institute 2015-206	May 2015	Off campus programs; conflicts of commitment; ELI summer program admission	Follow-up scheduled for December 2015

University Audits
Summary of reports issued – May 1 through June 30, 2015

Audit	Report Date	Open Issues	Follow-Up Memo Issue Target Date
Employee Supplemental Payments 2014-106	June 2015	Process of system ownership; earn code management; reporting and monitoring; user training; workflow system	Follow-up scheduled for January 2016
College of Engineering: Electrical Engineering and Computer Science Department 2015-201	June 2015	Management of assets; compliance with policy on minors; information security	Follow-up scheduled for January 2016
ITS Computer Showcase 2015-203	June 2015	Operating procedures; customer data (Repair Services); segregation of duties; user accounts; firewall; point of sale system; physical security	Follow-up scheduled for January 2016
University of Michigan Health System Data Sharing 2015-404	June 2015	Health system data warehouse; patient non-disclosure of health information; central oversight of data use agreements	Follow-up scheduled for January 2016
University of Michigan Health System MyUofMHealth Patient Portal 2015-302	June 2015	IT security; privileged system access; patient password security; monitoring event logs	Follow-up scheduled for January 2016

Appendix 1: Audit Issue Risk Definitions

Risk	Definition
High	• 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).
Medium	• 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).

Appendix 2: Audit Issue Follow-Up Process

High- and Medium-Risk Issues: Every three months until completed, unit management will informally update University Audits on the status of their action plans. At six months, and every six months thereafter until the actions are completed, University Audits will follow up to verify the actions are complete and are effectively managing the risk. University Audits will issue a follow-up memo on the results.