

UNIVERSITY OF MICHIGAN

REGENTS COMMUNICATION

Received by the Regents
January 22, 2009

Item for Information

Subject: Report of University Internal Audits
October 2008 – November 2008

Background:

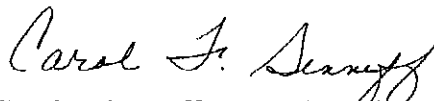
This is the report of the Office of University Audits activities for the period **October 1, 2008 through November 30, 2008**. The summaries of audits contained in this report were previously reported to members of the Regents' Finance, Audit and Investment Committee and included in discussions at Committee meetings.

Included in this report:

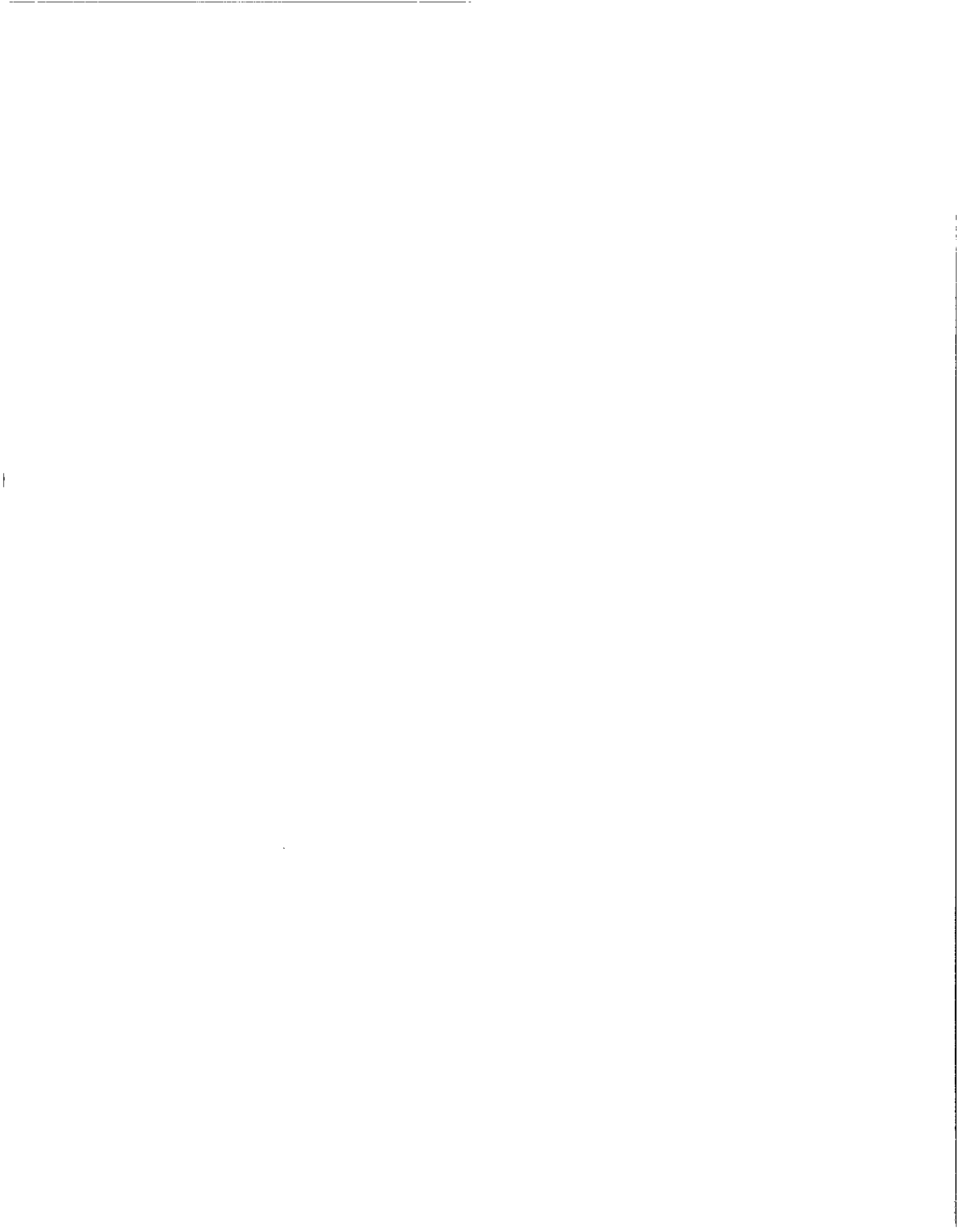
- Summaries of each audit report issued during the period, including Management's Plan to enhance specific control processes discussed with the audit client and presented in the report.
- Summaries of follow-up review reports issued during the period, including the actions taken by Management. Follow-up reviews are designed to give assurance that Management's Plan for corrective action has been implemented and controls are working appropriately.
- A report on the status of follow-up reviews as of **November 30, 2008**.

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

Respectfully submitted,



Carol F. Senneff, Executive Director
University Audits



ORIGINAL REPORTS

Campus

Plant Operations Construction Services

#2008-602

Issued November 4, 2008

Construction Services (CS) provides structural repairs, renovations, and small to medium construction projects directly to University customers. Occasionally, they subcontract with the University's Architecture, Engineering and Construction (AEC) department. In fiscal year 2008, approximately two-thirds of the revenue came from Campus units and one-third from the Hospital and Health Centers. During the same period, at least two-thirds of the CS projects were performed on a time and materials (T&M) basis in the last fiscal year. Recently, the Hospital and Health Centers have moved entirely to fixed-pricing and Hospital facilities management establishes the prices.

Project Management Reporting

Background: Approximately one-third of CS projects are cost estimated. All fixed price projects are formally estimated and approved by customers. A few customers develop informal T&M baseline estimates with CS managers. In addition to baseline project cost estimates, change order estimates are required for cost-estimated projects when CS identifies unanticipated work or when customers request additional work on the project. There is no department standard requiring estimated costs to be input to the Facilities Management System (FMS) system where actual costs are recorded. Change order actual costs are recorded in FMS as file header information, making it difficult to use the data automatically from the system to be reconciled with actual costs. Change order costs are also recorded and maintained in a spreadsheet by the Director. When estimates are developed and presented to customers, they are organized and subtotaled by work group components, such as carpentry or electricians, within the project. Project management reporting is primarily by project as a whole, or labor and materials by project. Fixed-price project reporting involves manually inputting statement of activity and other source information into an Excel spreadsheet. Standards vary between managers and foremen for tracking and maintaining project support information.

Opportunities: To strengthen project management controls and increase efficiency:

1. Initiate both baseline and change order component-detailed estimates for projects, including T&M projects.
2. Ensure that costs recorded in WinEstimator (a project cost estimating application based on national standard costs) and FMS correspond to each other by project, change orders, and components so that they can be integrated and reconciled automatically and reduce or eliminate manual re-keying of project data
3. Develop reports of estimated to actual labor and materials costs by work group and/or work type components across projects to identify best practices and support continuous improvement opportunities for estimating, productivity, and materials management.
4. Provide increased accountability for labor and materials costs with automated exception reporting of differences between estimated and actual labor or materials costs by specific work group and/or work type components.
5. Develop CS standard procedures for capturing, reporting, and reconciling project estimates and costs for labor and materials by component, and for maintaining project support information.
6. Obtain the assistance of a systems analyst or information technology (IT) specialist to ensure WinEstimator and FMS data are compatible and can be integrated automatically for reconciling and reporting, and reports are easily accessible to management.
7. Designate an IT champion to promote information systems skills among CS managers and foremen.
8. Request customer feedback regarding the estimating process as part of the CS continuous customer survey process.

Construction Services (CS) Management Initiatives: CS management is implementing system changes to:

1. Develop work code (job-type) specific estimates in the newly acquired WinEstimator application for all fixed price projects and T&M projects with a cost estimate greater than \$15,000.
2. Input baseline costs into WinEstimator to be combined and reconciled with FMS actual costs as part of uniform job cost analysis and project tracking standards. Identify a means to include change order request estimates and costs in system-generated project metrics reporting.
3. Develop additional FMS reports to improve management of fixed price and T&M materials projects.
4. Identify variances between WinEstimator estimated and FMS actual labor and material costs when job cost analysis is performed in lieu of detailed tracking.
5. Establish standard procedures for job cost analysis.
6. Employ the expertise of the new IT Manager to maximize WinEstimator and FMS systems reporting support.
7. Utilize the IT Manager to promote technology skills among the department managers.
8. Initiate a survey to collect customer feedback regarding the estimating process. Feedback will be analyzed and applied to improve project estimate services to CS customers.

University Audits will follow-up on the status of the CS initiatives during the fourth quarter of fiscal year 2009.

Sponsored Programs Subrecipient Monitoring

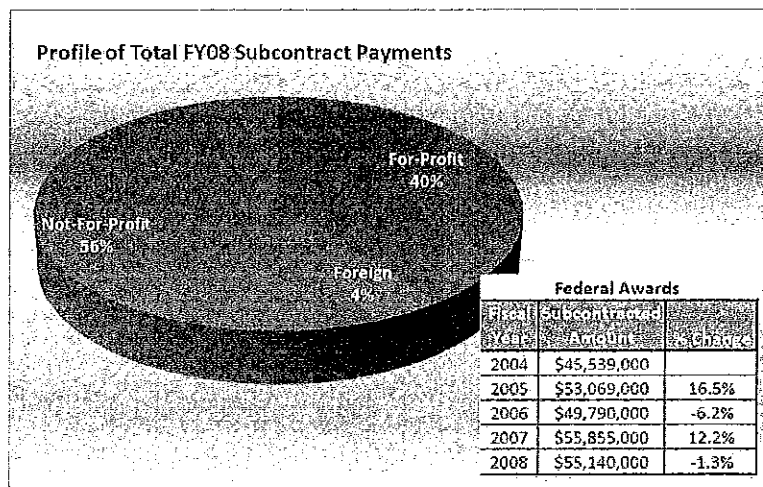
#2008-501

Issued November 21, 2008

University Audits reviewed subrecipient monitoring processes at the University of Michigan (U-M). A subrecipient is an entity that receives sponsored program dollars via a pass-through organization to conduct a portion of the research of a specific project. U-M received approximately \$875,800,000 in research funds for fiscal year 2008. Of this amount, approximately \$58,813,000 was passed through to subrecipient organizations, including \$55,140,000 in federal funds. As a pass-through entity, federal regulations generally require U-M to:

- Advise subrecipients of applicable federal laws and flow-down provisions from the prime agreement
- Monitor subcontract progress through milestones, deliverables, and other performance metrics
- Compare actual expenses to budget
- Review A-133 audit reports filed by subrecipients and monitor any relevant audit findings
- Inform the subrecipient of U-M's right to perform audits as necessary
- Monitor subrecipients work through on-site visits or other regular communication

The following table represents recent trends in the amount of federal research funds U-M passed through to subrecipients; the pie chart displays the profile of total (federal and nonfederal) payments to subrecipients during fiscal year 2008.



(Data obtained from U-M A-133 Audit Reports and MPathways)

The primary objective of this audit was to determine the adequacy of procedures to monitor and control the following processes:

- Monitoring of subrecipient activities for compliance with grant provisions and sponsor regulations
- Managing and reporting of disclosed conflicts of interest relative to subcontracts
- Ensuring the safety and proper treatment of human and animal subjects when such research is subcontracted
- Monitoring subrecipients' work for satisfactory completion prior to payment
- Appropriately classifying subcontracting versus purchasing activity

Control Issues:

1. Subrecipient Monitoring Guidelines - Principal investigators (PIs) bear the primary responsibility for monitoring subrecipients' work; limited guidance and training is provided to help ensure that PIs understand the extent of their responsibilities.

Interviews with PIs and review of available documentation revealed:

- The level of monitoring and documentation maintained by the PI and staff varies considerably across the University.
- Not all PIs clearly understand their responsibilities with respect to their subcontracts.
- Departmental administrators are regularly approving payments to subrecipients, attesting that work has been satisfactorily performed. In general, PIs are in a much better position to attest to the work performed.
- PIs are required to approve payments to subrecipients by certifying on a concurrence receipt that work is progressing and acceptable. Several payments were processed with the standard voucher cover page, which requires the signature of the "higher administrative authority," instead of the concurrence receipt.

Management Plan

- The Associate Director of Financial Operations will circulate an email communication to research administrators via the DRDA-Net email group with a reminder that prior to approving payments, the PI is responsible for certifying that subrecipients are performing work consistent with the subcontract and sponsor requirements. Best practice is for the PI to actually sign off on the concurrence receipt or voucher. If this is not possible, the research or department administrators should sign only if they have direct knowledge of the work performed or have received written assurance from the PI.
 - The cover letter sent to the PIs to sign at subcontract initiation will be expanded to include additional detail regarding the PI's responsibilities for monitoring the work of subrecipients, such as establishing milestones, requiring and reviewing progress reports on a regular basis, and approving payments.
 - Contract Administration and Sponsored Programs will develop and administer training that covers the sub-award process. The class will be open to all research staff, including PIs, and will cover items such as the subcontracting process, monitoring requirements, contact persons, and special topics such as export controls, human research subjects, animal research, and contracting with foreign entities. The training will be offered two to four times per year. Any materials developed as a result of this training will be made easily available to interested parties.
2. Monitoring for Federal Requirements - Federal Office of Management and Budget Circular A-133 requires the University ensure its subrecipients comply with applicable federal regulations. A-133 establishes standards for annual audits and requirements and applies to states, local governments, and non-profit organizations expending federal awards. Subrecipients are required to submit their A-133 audit report or a written certification to pass-through entities. Contract Administration obtains and reviews A-133 reports to help ensure compliance for non-profit entities; however, when subrecipients do not submit their reports, missing reports are not resolved until subcontract closeout.

Management Plan - A process will be developed to monitor subrecipients that are not required to have an A-133 audit. This process will include a questionnaire that can be sent to these entities periodically. Higher risk subrecipients may be required to submit additional supporting documentation.

3. Compliance Areas - Key compliance areas such as export control, animal use, and human subject research are routinely identified during the subcontracting process; however, requirements are not prominently stated.

Management Plan - The "Assurance" article in the subcontract template will be expanded to include compliance with animal welfare, human subjects, and export controls for all subcontracts, where applicable. The additional training and guidance for PIs will include responsibilities for informing the appropriate compliance organization within U-M and monitoring guidelines.

Based on the audit work conducted, the University is in compliance with applicable Federal guidelines. University Audits will conduct a follow-up review during the fourth quarter of fiscal year 2009.

Institute of Continuing Legal Education

#2008-202

Issued November 24, 2008

University Audits completed an audit of key business, operational, and information technology (IT) risks and controls at the Institute of Continuing Legal Education (ICLE). The primary objective of this review was to determine whether adequate and effective internal controls are in place to protect ICLE from key business, operational, and information technology risks. University Audits performed a comprehensive assessment of the risks related to ICLE business processes and resources, taking into account prior audits.

ICLE management relies on two internal financial applications: iMIS and Great Plains. The iMIS business software suite is used to track sales, payments, and customer accounts. Great Plains general ledger is used to separate and analyze expenses by functional area such as Publications, Administration, and Partnership. Perpetual inventory records for print media are reconciled directly with the warehouse provider's inventory system.

The Information Services (IS) team manages ICLE's web sites, digital media server, and operational and financial systems. The IS team also programs the web site, including the online store. They are currently performing a major upgrade of the web site which includes migrating from the ColdFusion platform to Microsoft .NET.

Business, operational, and information technology risks selected for audit included:

- Protection of copyrights
- Ongoing service and availability of product served via e-commerce
- Integrity of financial data as it moves from system to system
- Compliance with University security policies, including Information Security Incident Reporting Policy (SPG 601.25) and Information Security Policy (SPG 601.27)
- Processes for providing assurance of information and systems security
- Assurance that access to IT systems is authorized and appropriate
- Financial oversight mitigating the possibility of unauthorized financial transactions
- Assurance that cash collections are deposited intact

Control Issues:

- Removal of Access for Terminated Employees - University Audits compared iMIS user IDs to a list of current employees per M-Pathways, and noted two IDs belonging to employees who terminated in March and August 2008.

ICLE has two processes designed to remove access for departing employees. First, the employee's supervisor submits an account removal request form to the IS team. Second, the IS team reviews accounts once a year to verify that account holders are still employed at ICLE. Since employment of

these two individuals at ICLE terminated within the past year, the next of these annual reviews may have caught these accounts.

Management Plan - ICLE has removed the terminated employees' iMIS IDs. The ICLE Employee Life Cycle process has been amended to specify the removal of iMIS IDs for terminating employees. The End Cycle checklist completed by the Executive Secretary now requires notification of IS to remove the employee from all ICLE systems.

- **Role-based Access** - While reviewing ICLE employees' job titles and levels of access to the iMIS sales and customer management system, we noted that seventeen ICLE employees, not including the IS team and the Administrative Director whose access is unlimited, have broad read/write access to iMIS, including the right to post batches of sales transactions. Job roles with this type of access are varied and include managers, editors, sales representatives, customer service assistants, accountants, and temporary clerks and messengers.

Most ICLE employees have no access to iMIS. However, based on discussion of process flows with Accounting, the ability to post batches should not extend beyond the Business Office.

Management Plan - ICLE will further restrict the right to post iMIS batches by changing the authorization level in iMIS from level 4 to level 3. This will leave only three Business Office staff with the right to post batches. The IS staff and Administrative Director will also retain this right for emergency use only.

ICLE will also add descriptions of the iMIS authorization levels to the account request form, so that managers can select the level most appropriate for the job roles of new employees going forward.

Web Site Usage Monitoring - The ICLE Business Office reviews site usage in an informal and subjective manner. The raw data on site usage is available, but there has been no systematic method employed to detect trends or excessive use and to analyze data.

ICLE's terms and conditions of use prohibit customers from "excessive use" of subscribed materials. Without an objective history of use, ICLE could be in a position of policing this behavior without substantiated information to support their decisions. This would make enforcement of this provision difficult.

Management Plan - Individual usernames and passwords will be assigned to all the participating law schools for tracking usage. ICLE will also implement a notification system that identifies abnormal usage.

- **Backup Power Testing** - UPS (uninterruptible power supplies) are not tested annually, as the ICLE business continuity plan suggests. Power fluctuations and interruptions, even momentary ones, can trigger system outages and corrupt data. Although modern UPS are generally self-calibrated and self-monitored, an annual test in which utility power is disconnected is still prudent to ensure operating effectiveness of these critical devices.

ICLE servers do not automatically shut down gracefully when UPS power is exhausted and so could cause data corruption. Management indicated that additional software is required to automate graceful shutdown.

Management Plan - UPS units will be tested annually and power management software will be implemented for graceful shutdown of servers when UPS power is exhausted.

- Security Assessment Corrective Action - A comprehensive information technology security assessment using RECON (an in-house developed security framework) was completed by ICLE in November 2006 and noted significant shortcomings in a number of areas. The most severe risks in business continuity planning and incident management have been adequately addressed or are in process. High risks were also noted in limiting storage of sensitive data, password controls, firewall change control, and other areas. The IS team indicates these risks were addressed, but no documentation of the corrective action is available.

Reports from regularly scheduled TrustKeeper (a certified, remote assessment and compliance solution designed to help credit card merchants meet the security requirements of their credit card providers) security scans speak to ICLE's general responsiveness in addressing security issues. U-M contracts with TrustKeeper to scan University web sites that accept credit cards, including the ICLE web site, on a quarterly basis. The most recent report indicates the security posture for the ICLE web server, which is the most exposed ICLE system, is very good, and documents ICLE's efforts to investigate and remediate previously identified vulnerabilities.

Management Plan - ICLE will perform annual RECONs beginning December 2008. A change and action log will be stored with the security assessment progress report to provide ready documentation of risk remediation. These changes will also be reflected as appropriate in the IS team's best practices and business continuity plan.

Based on our examination of IT systems and business processes highlighted by our risk analysis, ICLE practices strong fiscal oversight and has implemented appropriate IT controls. This includes timely and thorough reconciliations, proper cash management, batch controls, e-commerce controls, and copyright oversight.

University Audits will follow-up on outstanding issues in the third quarter of fiscal year 2009.

School of Music, Theatre & Dance Fiscal Responsibilities
Issued November 26, 2008

#2008-815

University Audits completed a review of the central processes at the University of Michigan's School of Music, Theatre & Dance (SMTD) after consultation with and at the request of the Provost and the Dean. SMTD offers programs within the following departments: Composition, Conducting, Dance, Jazz and Improvisation, Music Education, Music Theory, Musical Theatre, Musicology, Organ, Performing Arts Technology, Piano, Strings, Theatre and Drama, Voice, and Winds and Percussion. University Productions and the Michigan Marching/Athletic Bands are also major components of SMTD. Additionally, SMTD manages MPulse Ann Arbor (MPulse), a residential summer performing arts program on the U-M campus servicing approximately 200 high school students from around the world annually.

SMTD Business Office experienced significant personnel changes in recent years. The newly created position of Chief Administrative Officer was filled in January 2007, and the Business Administrator for Finance and Personnel position was vacant from January through March 2008. The duties of these two positions bear the primary responsibility for financial oversight across SMTD.

The primary objective of this audit was to determine whether SMTD has adequate procedures to monitor and control processes related to:

- Financial aid
- Financial oversight
- Procurement
- Development
- Payroll
- MPulse
- Imprest cash funds

- Discretionary funds
- Effort reporting
- Conflict of interest/commitment

Control Issues:

1. Financial Oversight and Monitoring - Not all units within SMTD have adequate financial oversight and monitoring procedures to ensure appropriate fiscal management.
 - 1.1 Monthly Reporting/Budget to Actual Comparison - A central process for monitoring actual expenses against budgets is still under development; therefore, not all department level managers are held accountable for their budgets on a regular basis. SOM accounts are not structured at a level detailed enough to easily utilize U-M systems for management reporting.

As a first step towards improving the financial oversight and providing better management reports, the Business Administrator recently created several reports by re-entering U-M Data Warehouse data into Excel, and using control totals to reconcile the two systems. These reports provide budget-to-actual comparisons for the individual units within the SOM. Shadow systems increase the risk for inaccuracies and inefficiencies and should only be used when the University's system cannot accomplish the unit's objectives.

Management Plan - One of the departments not included in the review, University Productions, has established procedures for monthly reporting and budget review. The Business Administrator will consider using these processes as an example to help implement a process for all units within SMTD. The Business Administrator is in the final stages of completing an initial set of management reports that perform both functions. These reports are currently reviewed by the Chief Administrative Officer with the Business Administrator and are used to identify any areas of financial concern.

- Once completed, these reports will be the basis for establishing a new structure within M-Pathways that will result in multi-level reporting capabilities. Over the next several months, the Business Administrator will develop the new reporting structure based on the reporting needs as defined by the Dean and Chief Administrative Officer. A map will be created that defines how each existing budget line will convert to each new budget line. Upon recommendation from MAIS, a full switchover from the old system to the newly defined structure is implemented best during the fiscal year-end close between June 30 and July 12, 2009.
 - Upon completion of the identification phase, reports will be distributed monthly to stakeholders, either annotated with questions about activity, or with a request for follow-up as necessary. Explanations for significant variances will be documented.
 - The Chief Administrative Officer and the Budget Administrator have re-established a regular monthly meeting of financial and Human Resources staff from each reporting unit in SMTD. The intent is to share updates from central units, discuss areas of concern from reporting units, and to establish reporting and administrative consistency.
- 1.2 Statement of Activity (SOA) Reconciliation - At the start of the audit, SOAs for the majority of units within the SOM had not been reconciled to source documentation in over a year, due in part to the resignation of the previous Business Administrator. Since then, a new Business Administrator and a temporary staff person were hired to help bring this process up-to-date. Available documentation was collected and reviewed at a high level through August 2008. The primary person currently responsible for reviewing and reconciling the SOAs for the SOM accounts has access to both initiate and approve procurement vouchers, and is also responsible for generating management reports. Inadequate segregation of duties increases the risk of fraud, errors, or misuse of assets. Monthly SOA reconciliations are required by Standard Practice Guide section 500.1 Fiscal Responsibilities and help ensure that funds are used appropriately and recorded correctly.

Management Plan - Statements of Activity are now reconciled through August 30, 2008 and are now reconciled regularly within two weeks of data availability. The Business Administrator will review all reconciled accounts prior to the beginning of the next monthly cycle.

- The temporary staff member, hired to bring reconciliations up to the current month, will continue to be responsible for maintaining currency in account reconciliations. Though it is agreed that this arrangement is non-optimal, the financial constraints facing SMTD preclude hiring of additional permanent staff for the near future. A study will be performed over the next several months to determine a priority list of accounts to ensure that those accounts that reflect the highest financial risk will be reconciled within the first week of data availability, and the results incorporated into management reports.
- Access to initiate procurement transactions will be deleted from the Business Administrator's profile.
- Reconciliation best-practices will be investigated and shared with SMTD Finance/HR group and written procedures will be generated.

2. Procurement Observations - Procurement processes are not entirely consistent with University guidelines. Limited testing revealed:

- P-Cards used to purchase supplies and services greater than the \$5000 limit per transaction. Specifically, five purchases, by two P-Card holders, during fiscal year 2008 appeared to be split to avoid going through Procurement Services for a purchase order. Note: A few of these transactions were already identified through Procurement Services P-Card auditing. In these instances, a corrective plan was established.
- Business purpose not clearly stated for some expenses.
- Lack of documentation to support why University strategic vendors are not utilized.
- Inappropriate procurement methods used:
 - P-Cards used for purchases from University strategic vendors. This method will not guarantee the bargained-for price.
 - ATM withdrawals used to pay for an international summer program.
- Inadequate support documentation for a few expenses.
- Unallowable expenses charged to a P-Card, such as software.

In addition, SMTD does not have established thresholds and/or criteria for when a purchase must be reviewed and approved by a higher authority. Opportunities for efficiencies and better rates may be missed by not establishing guidelines for specific types of purchases that must be routed through one individual.

Management Plan - There are a number of transactions unique to SMTD that do not easily conform to the standard U-M procurement methods. We will continue to proactively work with central units to determine the most appropriate methods for addressing our specific procurement needs.

- Where infractions are identified after the fact, additional investigation of the business need will be performed and solutions identified. The Financial/Human Resources group will share expertise at their monthly meetings.
- For unique purchases, the Financial/Human Resources group will invite representatives from Procurement, the P-Card group, and any other central unit to help determine an acceptable method of processing these transactions.
- The Financial/Human Resources group will examine Procurement's list of strategic suppliers and develop a method to inform/remind cardholders of their options. The Financial/Human Resources group will also remind cardholders, approvers, and persons with procurement responsibility of the following:
 - Appropriate procurement method for goods and services above \$5000
 - Procurement documentation standards, including a clear business purpose

- Unallowable P-Card expenses
- For functions or accounts under direct responsibility of the Chief Administrative Officer, all significant purchases are being reviewed before approval is granted. Approval thresholds will be established based on discussions with each manager and will be finalized by the target date.

Related Information – Financial Aid

As previously mentioned above, this audit was requested by the Provost and Dean. Both expressed concerns about the operating deficit in the General Fund in 2007 and both the operating and projected deficit in the General Fund at the end of fiscal year 2008. In response to the competitive environment for recruiting the top students, SMTD had changed its method for awarding financial aid to an increased number of tuition-based awards which impacted fiscal year 2006 and fiscal year 2007. A significant increase in out-of-state awards also contributed to the deficit. Implementing the recommendations and corrective actions outlined above will help ensure SMTD is planning appropriately and making informed financial decisions to stay within the budgeted guidelines. This will also allow for monitoring regularly to quickly identify variances or trends. The Dean and top management are responsible for ensuring they are good stewards of the University's resources and that the budget is executed accordingly.

The following table highlights the change in scholarships/fellowships since fiscal year 2005 by fund type.

(Data from the U-M Sources/Uses Projection Reports)

Fund	FY 06 % Change	FY07 % Change	FY08 % Change	FY09 Projected % Change*
General	17.9%	50.5%	13.1%	-23.0%
Expendable Restricted	18.7%	1.6%	2.3%	6.9%
Designated	58.1%	-39.9%	-33.7%	24.3%
Total	18.6%	23.0%	8.0%	-10.2%

*SMTD updated the automated projections based on best available information as of September 30, 2008.

The Office of the Provost made two significant commitments that together will reduce the ongoing expenditures of the School by \$1M annually. Additional one-time funding has also been committed centrally to assist with the financial aid deficit associated with the entering cohorts for Fall 2005 and Fall 2006.

3. Documented Procedures - Key operational procedures for SMTD are not formally documented. Documented procedures provide a standard source of information for reference and training; job aids and checklists can assist staff in performing daily duties consistently.

Management Plan - As documentation is a time-intensive process, we will investigate the possibility of enlisting outside assistance to help with this process.

4. Written Delegation of Authority - Signing authority that has been delegated by the Dean to various individuals is not appropriately documented. SPG section 601.24 requires that all sub-delegations of authority to bind the University of Michigan to an obligation or promise be in writing and meet specific standards.

Delegations of authority should be in writing and include:

- Names and titles of individuals with delegated authority
- List of delegated responsibilities
- Guidelines for applying delegated authority
- Expiration date(s)

Management Plan - Management agrees with the above recommendation. We received a template document for delegation of authority and have begun noting areas where signature authority has been delegated. Formal documents will be generated, and a file created to track them. A note will be added to the Business Administrator's tickler file for regular review.

5. Imprest Cash Fund Management - University Audits identified eight imprest cash funds at SMTD from Accounts Payable data. The higher administrative authority on file with Accounts Payable for three of the funds is no longer a SMTD employee. Detailed review of one imprest cash fund from University Productions and one from SOM revealed the following opportunities for improvement:
- Neither fund is periodically reconciled by a person without access to the fund.
 - One of the funds is not reconciled on a regular basis.
 - Reconciliations are not documented.
 - A \$50 overage in one of the fund balances was noted.
 - One fund is not maintained at the appropriate balance, pending a reimbursement due since 2007.

Management Plan - A list of imprest cash funds, custodians, and higher authorities has been generated. A change form to update the higher administrative authority will be processed. A procedures document, which includes the requirement for monthly reconciliations, and a reconciliation template are being designed. Documents and procedures will be shared with fund custodians and higher authorities. Surprise reconciliations by someone other than the fund custodian will be performed once annually, at a minimum.

6. Payroll Observations - Payroll testing revealed:
- Time reports are not consistently signed by a higher authority with direct knowledge of hours worked.
 - Documentation to support prior approval of overtime hours was not consistently available.
 - Reconciler does not initial and date the Gross Pay Register (GPR) reconciliations.

Standard Practice Guide section 518.1 Payroll Controls requires that each time report be approved by the staff member's immediate supervisor or an authorized designee with direct knowledge that hours reported are true and accurate. Without proper authorization on time reports prior to entering data into the University's time administration system, employees may misrepresent actual hours worked, including adding overtime pay or not recording sick time and vacation usage. Clearly documenting when the reconciliation was completed and by whom increases accountability and makes it easier to confirm timeliness and appropriate separation of duties.

Management Plan - Management will develop a list of approvers and those staff for which they are responsible. Each time administrator will be trained on proper procedure for obtaining appropriate signatures and overtime authorization. Supervisors will be instructed to authorize overtime via email, with a copy to the time administrator. When someone else is in a better position to attest to the accuracy of an individual's time report, approval will be delegated to that person.

A procedures document will be generated detailing responsibilities for GPR reconciliation. Staff responsible for this function will be trained.

7. Staff Conflict of Interest/Commitment Policy (COI/COC) - SMTD COI/COC policy for staff is drafted, but still pending approval within SMTD and has not been implemented. All University departments are

required to have an approved COI/COC policy and appropriate management action plans where potential conflicts exist.

Management Plan - Though the staff policy was approved by the Policy Review Group by the deadline, the policy was never fully implemented within SMTD. We found that as we began to implement the staff policy, the wording of the document, i.e., a few of the examples, seemed to be causing more confusion than clarity. We therefore decided to stop full implementation on the staff COC/COI until it could be clarified. Some discussion has occurred and additional draft language is being generated for review. Once the updated policy has been approved by the central Review Group, policy will be disseminated to staff, and appropriate documentation generated as necessary per policy requirements.

8. **Miscellaneous MPulse Observations** - MPulse is SMTD's residential summer youth performing arts program. Based on discussions with MPulse personnel and reviewing select documentation, processes appear to adequately ensure the safety of campers; however, during this review University Audits observed the following:

- The person responsible for processing credit card payments for the MPulse camp fees is also the person responsible for processing refunds.
- The merchant copy of the credit card receipts includes the entire credit card number with the expiration date. The Program Coordinator currently blackens out the complete number and expiration date before securing the files in a locked filing cabinet; however, programming the terminal to truncate these numbers would more adequately protect this sensitive data and improve efficiencies.
- A travel advance is used for petty cash fund needs during the operation of the program.

Management Plan - A new on-line processing system is currently being developed with the Treasurer's Office. The Business Administrator has now been assigned the responsibility of processing refunds. The Business Administrator will review Fifth-Third Bank statements to monitor refund activity.

The Program Coordinator is currently updating internal documentation, and generating an updated Service Level Agreement.

An imprest cash fund will be requested.

We are investigating the ability of the Treasurer's Office to program the terminal to truncate the credit card number when printing.

University Audits will conduct a follow-up review early in the first quarter of fiscal year 2010 to assess progress on action plans.

Information Technology

College of Engineering Research Computing

#2008-302

Issued October 29, 2008

The College of Engineering (CoE) is home to thirteen departments. Research is a major focus within the College. CoE's patents accounted for nearly half of all patents filed by University of Michigan entities in fiscal year 2007. The CoE is home to eight research professors (including associate and assistant levels), sixty-one research scientists (including associate and assistant levels), and five research investigators.

Each department at the CoE has its own information technology (IT) support team. Each IT group is responsible for the day-to-day administration of most of their department's computers. This includes deploying new computers, installing operating systems and other software, installing updates, performing maintenance, and troubleshooting. The IT professionals do not administer all of the machines used for research. Instead, many of

the researchers and/or their student assistants manage their own research computers. For the purpose of this review, our definition of 'unmanaged' refers to any system not administered by the department's formal information technology professionals.

For networking needs, the CoE utilizes CAEN (Computer Aided Engineering Network). CAEN supports the College's entire network infrastructure. They work in partnership with each department's IT group to provide service to the end users. CAEN also provides basic network monitoring, and system scanning on request.

The purpose of this audit was to assess the security posture of unmanaged computers used primarily for creating and storing research data. This report discusses security across the CoE as determined by detailed reviews of three selected departments. University Audits reviewed controls in Atmospheric, Oceanic, and Space Sciences (AOSS); Chemical Engineering (CHE); and Electrical Engineering and Computer Sciences (EECS).

While unmanaged machines were the focus of this audit, University Audits examined some managed machines as well. This was done largely at the request of the clients, but also to provide a benchmark for comparison with the unmanaged machines. At AOSS, all six unmanaged machines were scanned, along with seventeen managed machines. At CHE, all eight unmanaged machines, and five managed machines, were scanned. At EECS, 136 unmanaged machines, twelve managed machines, and an unmanaged cluster were scanned. The comparatively large number of systems scanned in EECS is due to the high volume of computer research performed there.

This audit examined:

- Potential vulnerabilities identified on managed and unmanaged machines found by using third party scanning software
- Processes and procedures developed for users and systems administrators in the selected departments
- Firewall placement and configuration by the IT professionals at the selected departments
- Initial system configuration procedures and standards used by IT professionals at the selected departments
- Privileges granted to users acting as systems administrators

Control Issues:

- Vulnerable Systems - Mature operating systems provide a solid platform for computing. However, they also contain more known vulnerabilities. Hackers and legitimate security researchers have had time to find the weak spots. University Audits used a system scanner to evaluate vulnerabilities on a sample of machines at selected departments within the CoE. The scans highlighted multiple systems with high-risk vulnerabilities. Left unaddressed, these systems become easy targets for hackers, malware, and viruses.

Management Plan - CAEN will develop processes for regular scheduling and completion of scans, as well as analysis and sharing of results with department business administrators and department IT.

- Unnecessary Services - Services are applications that allow a computer to interface with its components and the rest of the world. In order to carry out their functions, servers and workstations run a number of services. While some services like e-mail, web browsing, and hardware interfaces are necessary and appropriate; there are instances when computers run services that are neither. Examples of services that may not be necessary or appropriate under certain circumstances include web servers, telnet, remote desktop, and database servers. The results of system vulnerability scans across the CoE revealed many computers (servers and workstations) running unnecessary services. These unnecessary services are common targets of attack from hackers and malicious software.

Management Plan - Using scan data from CAEN, department IT will work with system administrators to identify and classify services that may be unnecessary. Department IT will work with the department business and system administrators to determine the necessity of these services, and assist them in disabling services that are agreed to be unnecessary. Services determined to be necessary will be documented, and department IT will assist the system administrator in securing the service.

- Unknown Ports and Services - Computers use services to perform their everyday functions. Services use ports as their means of communication. When a computer receives data, the data destination port on a machine helps the computer identify what service needs the data. A vulnerability scan of a system informs the system's administrator which ports are open, and which services are "listening" on the open ports. Results from vulnerability scans performed by University Audits at selected departments in the CoE found a number of computers with ports associated with unknown services running. Leaving unnecessary ports open on a computer is like leaving doors open on a home; it provides easy access and invites unauthorized entry.

Management Plan - Using scan data from CAEN, department IT will work with system administrators to identify and classify any unknown ports and services. These ports and services will be documented and addressed in the same manner as unnecessary services.

- Unknown Systems - The networks within the CoE are kept open and easy to connect to for the convenience of their users. This gives students and faculty a great deal of flexibility in addressing their computing needs. It allows researchers to easily add unmanaged machines to the computing environment. However, this also allows other unknown, potentially non-standard, unsupported, systems access to the network. These systems may not conform to the security standards of the department's IT group, and could cause harm to the network and systems on it. There is currently no procedure for discovering, and handling unknown systems.

Management Plan - CAEN will work with department IT to develop appropriate procedures for the identification and handling of unknown systems.

- Unsupported Devices - An unsupported device is defined as anything that uses the network and is not directly supported by IT staff. In the CoE, this includes sensors, measuring devices, various laptops, and smart phones (i.e. the Blackberry and iPhone). While these devices are not actively supported by CoE IT, they still make active use of the network, and in some cases carry U-M data. IT staff currently have no guidelines for handling these non-standard items. While these devices are technically unsupported, IT staff indicates that they assist users with them when possible.

Management Plan - CAEN will work with department IT groups to determine what devices are used, what devices users want to use, and what devices they think may be used in the near future. This group will develop a best practices guide for users utilizing non-standard devices. A document providing guidance to IT staff members will be created.

- Users with System Administrator Privileges - Security best practice dictates that users be given restricted accounts on their computers. This prevents the user from accidentally making critical changes, inadvertently installing malicious software, or making changes that could harm other systems on the network. Sometimes a user's needs create the necessity to give that user administrator-level privileges. CoE IT departments do not currently have documented processes in place to determine who gets this privileged access.

Management Plan - CAEN and department IT will develop the recommended documentation and strategy for monitoring systems where users are utilizing the administrator account as their primary account. Department IT and administrators of unmanaged machines will work together to reduce the number of administrator accounts used as primary accounts. CAEN and department IT will develop a strategy for monitoring systems where users are using the administrator account as their primary account.

- Updating Firewalls - Firewalls are essential to network security. They provide perimeter security, a barrier between machines on the network and the outside world, keeping the network more secure. Firewalls are just specialized computers. Like normal computers, they sometimes have vulnerabilities that need to be patched. Network scans performed by University Audits at selected departments within

the CoE discovered firewalls with unpatched high-risk vulnerabilities. Vulnerabilities that are left unpatched provide attackers with an easy point of attack on a system. A compromised firewall supplies an attacker with easy access to the network it is in place to protect.

Management Plan - CAEN and department IT will develop documentation detailing the firewall update process and schedules for periodic scans. A department IT staff member will be designated by the department to regularly check for updates.

- **Machine Setup** - IT support groups at each department within the CoE perform nearly all of the new system builds and configurations. This provides for well-configured and secured machines being deployed to users. Currently, none of the IT support groups at selected departments within the CoE have their build or setup processes documented. Documentation helps ensure systems are properly and consistently configured. Without a documented setup procedure, it is easy for technicians to miss security-related configuration steps.

Management Plan - Current practices will be reviewed and documented.

- **Procedural Documentation** - Throughout the CoE, IT groups have found creative and effective ways of handling a variety of problems. Good practices are in place for system configuration; incident handling; addressing vulnerabilities, and dealing with non-standard devices. Many of these solutions are not documented. Documentation will help ensure a consistent approach to system administration throughout the departments.

Management Plan - CAEN and department IT will perform a review of current documentation to ensure that it is up to date. Current practices that are not documented will be. A periodic review of CAEN and department documentation will be scheduled and performed.

The overall security posture of research machines in the CoE areas examined by University Audits is good. University Audits will perform a formal follow-up to the outstanding issues during the fourth quarter of fiscal year 2009.

Michigan Administrative Information Systems Degree Audit Process

#2008-123

Issued November 14, 2008

The Degree Audit System seeks to provide consistent views for degree audit reporting to all University units. Degree Audit data provides faculty and staff the ability to:

- Monitor students' progress toward a degree
- Assess data to predict course demand
- Observe trends in courses used to meet requirements

The Degree Audit Report is an internal University document used to assist the advisor and the student in determining if requirements for a degree have been met, or which requirements need to be completed prior to awarding a degree. The Report can also be used for graduation clearance. It is not an official transcript or an official U-M document. It is, however, confidential and may be released only to the student and others with a need to know.

Students may request and advisors may grant “**waivers**” or other “**exceptions**” to the Degree Audit requirements. There are four types: Course Directives, Requirement Waivers, Requirement Changes, and Requirement Overrides. Such exceptions are student-specific:

- A **Course Directive** allows a course that is not normally accepted to complete a requirement.
- A **Requirement Waiver** is used to bypass a specific academic requirement.
- A **Requirement Change** is used to modify the amount of units or courses needed to complete a requirement

- A **Requirement Override** is used to replace a specific academic requirement.

Like degree qualifications, exceptions and course waivers differ within each unit. Waivers are designed to comply with a unit's curriculum and academic policy. The Office of the Registrar does not verify or oversee waivers within schools. Although units are trained by the Office of the Registrar to enter exceptions, each unit is responsible for entering its own exceptions.

University Audits examined processes at MAIS, the Office of the Registrar, and in three different academic units¹ to evaluate the adequacy and effectiveness of the internal controls governing the Degree Audit System regarding:

- Access security
- Data integrity
- Process integrity
- Availability
- Control over exceptions/waivers

Control Issues:

- Academic Advising - The Degree Audit Report was designed to assist with academic advising and tracking of a student's progress toward graduation. However, in some situations, the Degree Audit Report may give misleading information for the completion of requirements by including in-progress course work.

Management Plan - The Office of the Registrar will consult with schools, colleges, and departments to identify areas for improvements in the business processes and report needs. This consultation will include an overview of the features of the interactive Degree Audit Report. The interactive Degree Audit Report was rolled out in the June 2008 upgrade of the M-Pathways Student Administration software. It is important for clients of the system to understand the role in-progress coursework plays in the interactive degree audit process because the interactive report is the foundation of functionality to be implemented in the future. Future functionality to be implemented will integrate Degree Audit, Course/Class Search, Backpack, and Registration.

- Calculating GPA's When Courses Are Repeated - In certain programs, a student is required to earn a minimum GPA in their major or area of concentration to earn a degree. Schools and colleges allow flexibility in adjusting credits and major/concentration GPAs for certain programs when classes are repeated. For example, in some schools, like Music, a class may be repeated several times to improve skills. In such cases, the grade should be substituted rather than accumulated. In other schools, proper calculation of concentration/major GPA requires inclusion of all occurrences of a repeated course. The Degree Audit System treats repeated courses the same as the academic record (transcript) which uses the credit on the first occurrence of a course in its calculations. Therefore, for some major/concentration GPA requirements, the Degree Audit System gives misleading information when a student repeats courses. In order to eliminate this confusion, some users of the application continue to use the same manual processes used before implementation of the Degree Audit System for determining a student's major/concentration GPA with repeated courses.

Management Plan - The Degree Audit System uses courses from a student's official academic record (i.e., transcript) in its evaluation, using earned credit and honor points from each course. In some schools, colleges, and departments, flexibility in the calculation of a concentration/major GPA is allowed. Two of the methods for calculating the concentration/major GPA include 1) using all occurrences of a repeated

¹ Detailed testing of Degree Audit System was performed in three user areas:

- College of Engineering
- Ross School of Business
- School of Music

course and including only the highest grade of a repeated course, or 2) using all occurrences of a repeated course and including an average of the grades for that repeated course. These practices differ from the school, college, and department rules regarding credit for repeated coursework and, as such, need values of the GPA data that are not on the student academic record. These practices present challenges to the set-up of the Degree Audit Report since both are exceptions to the fundamentals of the Degree Audit System by using courses from a student's official academic record. The calculations for these two exceptional processes cannot be done in the Degree Audit System.

The Office of the Registrar, in consultation with schools, colleges, and departments, will re-evaluate the approach taken in those schools, colleges, and departments where concentration/major GPA calculation exceptions are used. Consultations may result in some Degree Audit System setup changes and the evaluation of current business processes to manage these exceptional calculations.

- Entering Exceptions - Entering student-specific changes to degree requirements (exceptions) in the Degree Audit System can be extremely time-consuming and complex. There are many screens to navigate and the response time of the system is slow, so it often takes users several minutes to enter one exception. Because of this, academic areas often wait to enter exceptions until many have accumulated. This time-lag causes the Degree Audit Report to reflect an invalid student status until exceptions are entered.

Management Plan - The Office of the Registrar and MAIS will consult with schools, colleges, and departments to identify areas for improvements in the business processes and system needs. Modification of the Degree Audit System to send email notification to a student upon data entry of an exception will be evaluated when the M-Pathways Student Administration notification system is implemented.

Academic units across the University use degree audit reporting for academic advising and graduation clearance. The Office of the Registrar has a systematic and well-controlled process for integrating departmental requirements into the Degree Audit System. Although the Office of the Registrar has no approval authority over exceptions, they train the schools and colleges to enter exceptions correctly. The Office of the Registrar proactively monitors graduation requirements to ensure they are properly reflected in the system.

Actual data, including exceptions, is stored in M-Pathways. Use of the M-Pathways system to track degree audit data provides consistent degree audit reporting to all University units. Access to degree audit tables in the data warehouse and degree audit reports is controlled by M-Pathways and governed by the MAIS access policies and guidelines. A test of these logical controls determined the application is secure.

Because of the complexity of reporting on degree qualifications and exceptions coded at a department level, some units have created shadow systems that pull data from M-Pathways into other applications for reporting. MAIS is attempting to eliminate the need for these supplemental systems. It is important that the M-Pathways system represent the primary source of data for degree audits.

A formal follow-up to the outstanding issues will be conducted during the first quarter of fiscal 2010.

Healthcare

University of Michigan Hospitals and Health Centers Cashier's Office
Issued October 17, 2008

#2008-206

University Audits performed an audit of the University of Michigan Hospital Cashier's Office (HCO). In fiscal year 2008, HCO deposited \$172 million in patient payments and other revenue and disbursed approximately \$7.1 million in checks.

Specific objectives of the audit included assessing:

- Employee and management roles and responsibilities to determine if appropriate segregation of duties exists
- Controls over and management of HCO's check writing process
- Controls governing the security of cash and cash equivalents to determine whether assets are safeguarded
- Reconciliation processes to verify that cash/cash equivalents activities are appropriately reconciled and managed
- Compliance with department, UMHHC, and University policies and procedures
- Controls implemented as a result of prior-year audits

Control Issues:

- **Segregation of Duties** - Proper segregation of duties decreases the risk of fraud, errors, or misuse of assets. During this audit, University Audits noticed several opportunities to strengthen controls by segregating duties or implementing compensating controls. Specifically:
 - *Cash Receipt Function*: One teller who accepts payments on patient accounts also posts payments to patient accounts receivable ledgers and reconciles the Online Posting Report to HCO's Posting Journal. (Note: HCO policies prohibit tellers from posting payments they collected.)
 - *Credit Card Function*: Three tellers who process credit card transactions (sales and refunds) can also post payments and charge backs to patient accounts. One teller is also responsible for reconciling credit card charges to the monthly charge statement from Fifth Third Bank.
 - *Check Writing Function*: Three tellers who can write checks and have access to blank check stock are also responsible for signing checks (using a signature plate) and delivering checks to the intended party. Two of the three tellers can also upload checks into the positive pay system and are responsible for creating and uploading journal entries into U-M's General Ledger System. The bank sends positive pay exception reports directly to HCO management.

Adequate segregation of duties ensures no one individual employee can complete a significant business transaction in its entirety. To minimize the risk of errors and misappropriation, different employees should perform each of the four major functions associated with processing a transaction: authorization; custody; record keeping; and reconciliation.

Management Plan

- The responsibility of reconciling daily cash receipts from the online report to the posting journal will be reassigned to an individual outside HCO. This will ensure that someone other than a HCO employee has control over the reconciling function.
 - Payments will continue to be posted to patient accounts by someone other than the teller who accepted the payment. Both individuals' initials will appear on HCO's copy of the receipt. This will ensure no single individual can complete the transaction in its entirety.
 - Management will look into the possibility of a special charge master description code whereby only management will be authorized to post credit card payments into patient accounts. As a result, tellers will be responsible for processing payments and management will be responsible for posting the payments.
 - The daily check upload transfer responsibilities will be transferred out of the cashier's office to the UMHHC Accounting Office on Green Road, segregating the duties of writing the checks and sending the list of checks to the bank.
 - The bank will send positive pay exception reports to the UMHHC Accounting Office. HCO will no longer receive these reports.
- **Bank Statement Reconciliation and Check Writing Practices** - During a review of bank statement reconciliations, University Audits noted that outstanding (unreconciled) items were not investigated and cleared and that the individual who reconciles the bank statement does not receive positive pay exception reports. Bank statement reconciliations and review of positive pay exception reports are important controls that help detect irregularities. University Audits also noted that:

- HCO staff is the bank's primary contact. UMHHC administrators may not be alerted about irregularities noted and reported by bank officials.
- HCO staff voids checks without approval from the UMHHC Accounting Office.
- Several checks were not recorded on the check register (maintained in Quicken). (Note: All checks were subsequently accounted for as voided checks.)
- Over 100 travel advance checks written between June and August 2007 took between 16 and 85 days to post to the General Ledger.
- The Accounts Payable office does not receive timely notification of travel advance disbursements. This practice creates timeliness issues and delays the reconciliation process. In some instances, advances are not accounted for in the correct accounting period.
- HCO accepted several refund requests submitted on the wrong form or on an outdated form.
- Amounts listed on several travel advance forms were crossed out and rewritten. There was insufficient information to determine whether changes were approved by a higher administrative authority.
- HCO disbursed funds to travelers/hosts after the departure/event date listed on the Travel/Host Advance form.

Management Plan

- UMHHC Accounting Office personnel will work with HCO staff to balance HCO's bank account and develop practices to improve management of the reconciliation process.
 - HCO management will work with UMHHC Accounting Office to ensure check sequences are in order and there are no unrecorded voids or missing checks.
 - HCO staff will work with Accounts Payable to shorten turnaround time on travel advances. Both parties will try to adhere to a target date of no more than 60 days, provided the request is submitted by the requestor within a reasonable amount of time prior to the departure/event date. (Note: Checks cannot be posted to the General Ledger until they are picked up or voided.)
 - HCO will refrain from accepting forms that have information crossed out.
 - HCO staff will be reminded that funds should not be disbursed after the departure/event date listed on the Travel Advance form.
- HCO Check Writing - HCO uses Quicken personal business software to generate checks and performs as a stand-alone accounts payable function that is not designed with appropriate controls to support a payable function of over \$7 million a year.
 - Quicken is not designed with standard accounts payable/check writing controls such as restricted vendor/payee set-up, tracking of voids, and audit trails.
 - The opportunity exists to bypass U-M Procurement controls.
 - A large dollar volume of vendor and accounts payable information, including 1099 tax reporting information, is not captured in University systems such as M-Pathways or reported for tax purposes.
 - Significant accounts payable transactional information is not assessable to management and other University business functions.

Management Plan - Administrators will facilitate ongoing discussions regarding the impact of reassigning certain check writing responsibilities to Accounts Payable, University Payroll Office, and Hospital Billing. Discussions should include, but not be limited to, timing issues, process changes, control ramifications, and the overall benefits versus drawbacks. To undertake this initiative, it may be necessary for administrators to assemble a focus group that includes key individuals from affected departments.

- Recharging Patient Accounts for Voided Credit Card Payments - Charge backs (refunds initiated by credit card providers) are not posted to patient accounts. HCO credits patient accounts after credit

card payments are processed. However, when credit card providers refund patients for amounts originally paid to U-M, HCO does not bill the refund to the patient's account.

Management Plan

- Hospital Cashier's Office: Management has developed and implemented a process for posting charge backs to patient accounts.
 - UMHHC and Treasurer's Office: UMHHC Administrators will review charge back activity at other UMHHC facilities to ensure credit card refunds are appropriately applied to patient accounts. UMHHC administrators, in cooperation with the Treasurer's Office, will develop documented procedures for handling charge backs and disseminate procedures to appropriate staff.
- Follow-up of Outstanding Vouchers - During a review of outstanding vouchers, University Audits noted that in January 2008, HCO had unpaid imprest replenishment vouchers dating back to October 2007. HCO management usually follows up on unpaid vouchers after 90 days. A timelier follow-up would have alerted HCO to a missing \$5,201 imprest replenishment check from Accounts Payable. The check, dated October 17, 2007, remained unpaid and missing as of January 2008 and was discovered as a result of University Audits' surprise cash count. The check was subsequently cancelled and reissued.

Management Plan - HCO management and Accounts Payable resolved the missing payment matter. HCO has received a replacement check from Accounts Payable. HCO management also revised follow-up guidelines. HCO will follow up with Accounts Payable when vouchers are outstanding 60 days or more.

- RAC and IDX forms - RAC and IDX forms are three-part receipts used to record payments received on outstanding patient accounts. HCO's process for reconciling RAC and IDX forms does not account for all forms. One copy of the form is used as a customer receipt.

Management Plan - HCO management revised the RAC form reconciliation process. RAC forms are now logged upon delivery and used in number-order sequence.

Based on the audit work performed, the HCO has established good cash handling controls. Due to the breadth of activities outside of normal cashiering operations, control improvements are needed in check writing, patient account posting, and General Ledger journal entries. University Audits will follow up on the status of action plans during the fourth quarter of fiscal year 2009.

FOLLOW-UP REPORTS

UMHHC Social Work Gift-Funded Programs Follow-up

Original Report issued May 29, 2008

#2008-804

Follow-up Report issued November 10, 2008

P-Card Multiple Users

Management has provided P-Cards to all staff authorized to initiate purchases for the Guest Assistance Program and is no longer sharing one P-Card among multiple users. Management also worked with U-M Procurement to analyze procurement needs and set appropriate P-Card limits.

Cash Receipt Processing

Management has developed cash receipt procedures that strengthen asset security, ensure completeness and accuracy of transactions, and appropriately segregate duties. They are currently in the process of rolling out these procedures to Social Work staff.

Emergency Funds

Social Work no longer disburses cash in excess of the \$200 limit established by the Hospital Cashier's Office. Emergency needs in excess of \$200 a day, which are used for patient basic needs such as utilities and housing, are paid by check or credit card directly to the vendor providing the service.

Policies and Procedures

Management has updated the Guest Assistance Program policies and procedures for providing assistance to patients and family members. A process is now in place to periodically review the policies and update accordingly.

All corrective action was completed or is well underway. **This audit is closed**

Office of the Vice President for Communications (OVPC) Fiscal Responsibilities Follow-up #2008-211
Original Report issued May 29, 2008 Follow-up Report issued November 10, 2008

Segregation of Duties

The OVPC management has improved segregation of duties in the following processes:

- *Gross Pay Register (GPR) reconciliation.* GPRs are reconciled against original time documents by an employee independent of the timekeeper. Where the timekeeper performs this function, a higher administrative authority reviews the GPR for reasonableness. Unit directors perform appropriate monitoring and regular review of the GPRs.
- *University Record revenue collection.* University Record has segregated the duties of invoicing customers, collecting payments, and making cash deposits.
- *University Record Service Unit Billing (SUB) process.* An employee independent of those who initiate charges verifies the SUB file for accuracy and completeness. Management and IT staff are working on implementing an electronic download of this file from the University Record advertising database.

P-Cards

The OVPC management has strengthened controls over P-Cards by taking the following actions:

- Implementing a second higher authority review on administrative assistants' P-Card statements.
- Documenting delegation of authority in writing by signing the "P-Card Maintenance Forms" and performing higher administrative authority review where appropriate.

Cash Deposits

The OVPC units have ensured compliance with University cash deposit policies by making daily deposits or otherwise obtaining and following Treasurer's Office approved exceptions.

Web Yellow

Web Yellow is a database used by MM&D to track expenses, bill clients, and process revenues. MM&D management has taken action to improve controls over Web Yellow by:

- Performing daily backups via the Information Technology Central Services Tivoli Storage Manager (TSM) offsite network backup system.
- Implementing a change log for Web Yellow and effectively using it to document functionality changes.

The Office of the Vice President for Communications (OVPC) management has strengthened controls as discussed during the audit. **This audit is closed.**

- Open and Unbilled Patient Encounter Forms (PEF): UMOPC significantly reduced the number of open PEFs (see comparative chart below) and implemented monitoring procedures.

Open/Unresolved Patient Encounter Forms for UMOPC Visits

Age of PEFs	May 1, 2007 Census Report	March 7, 2008 Census Report	March 26, 2008 Census Report	October 24, 2008 Census Report
More than 1 year old	941	96	22	2
6 months to 1 year old	522	178	75	20
Less than 6 months old	986	743	730	642 (see Note 1)
TOTAL Open PEFs	2,449	1,017	827	664 (see Note 2)

Note 1: UMOPC business requires long cycle times. The interval between the patient's first visit and the final fitting may be as long as six months due to delays in obtaining pre-authorization from third-party payors, multiple fittings, and patient cancellations and postponements.

Note 2: UMOPC practitioners also see patients at the U-M Medical Center and Domino's Farms. These visits are not reflected on the Census Reports referenced above. In March 2008, there was a combined total of 72 open PEFs six months and older for these locations. On October 24, 2008, there was a combined total of ten open PEFs greater than six months old for these locations.

UMOPC will continue to monitor PEFs, with emphasis on PEFs six months and older, to ensure encounter forms are resolved on a timely basis.

- Charge Entry Accuracy: UMOPC developed, implemented, and documented an effective management review processes to improve charge capture efficiency.
- Reconciling Inventory to Billing Data: UMOPC made considerable progress in implementing an inventory management system. The inventory system is in place and computers are installed in patient examination rooms. UMOPC will continue to work with personnel from Contracts and Procurement to finish vendor setup and full implementation.
- Cash Handling Procedures: UMOPC management developed and documented procedures for reconciling patient payments to the monthly Statement of Activity. UMOPC management has assumed the responsibilities of ensuring reconciliations are performed accurately and on a timely basis.
- Quality Assurance Program: UMOPC has made satisfactory progress in establishing a quality assurance program. UMOPC developed an RFP (Request for Proposals) to find an outside party with orthotics and prosthetics experience to review and evaluate UMOPC's medical record documentation. U-M Procurement Services mailed RFPs to prospective vendors and has started receiving bids. U-M Procurement Services will continue to work with UMOPC until a vendor is selected.

Management completed appropriate steps and corrective action on audit recommendations. **This audit is closed.**

**Open Audits Follow-up Table
November 30, 2008**

Audit Title	Report Date	Issues	Expected Completion
Information Technology Central Services Software Licensing and Distribution Billing Systems and Practices 2007-106	2/7/08	Documentation of procedures for licensing negotiations and billing	December 2008
Physical Security at Harlan Hatcher Graduate Library 2008-303	9/2/08	Emergency exits; alarms and monitoring systems; fire safety; safety or patrons and staff; storage; deferred maintenance; procedures	January 2009
University Health Service HIPAA IT Security 2008-309	9/2/08	Practice management system; verification of internet access; intranet tools server; data access procedures; security policy	March 2009
College of Engineering Research Computing 2008-302	10/29/08	Vulnerable systems; unnecessary services; unknown ports and services; unknown systems; unsupported devices; users with system administrator privileges; updating firewalls; procedural documentation	May 2009
Institute of Continuing Legal Education 2008-202	11/24/08	Removal of access for terminated employees; role-based access; website usage monitoring; backup power testing; security assessment	March 2009
University of Michigan Hospitals and Health Centers Emergency Department 2008-112	05/09/08	Training Action Plan	January 2009
Patient Privacy 2008-401	5/28/08	Policies and Procedures; training	January 2009
Medical School Pulmonary and Critical Care Medicine Operational Review 2008-207	9/26/08	Grant key personnel; travel and hosting	March 2009
University of Michigan Hospitals and Health Centers Cashier's Office 2008-206	10/17/08	Segregation of duties; bank statement reconciliation and check writing practices; follow-up of outstanding vouchers; duplicate facility refunds	June 2009
Matthaei Botanical Gardens & Nichols Arboretum, Business Office Internal Control Review 2007-817	6/19/07	Strengthen cash handling procedures; instructor payments; credit card refund controls; remove unnecessary sensitive data in files. We will observe and review the annual plant sale in May 2008	December 2008
Intercollegiate Athletics Academic Support Services 2007-408	7/18/07	Student counseling practices; employment and payroll controls; staff training and development	December 2008
University Human Resources Family and Medical Leave Act 2007-403	12/17/07	Training; update relevant SPG sections; written notifications	March 2009

Audit Title	Report Date	Issues	Expected Completion
Transportation Services 2007-101	1/28/08	Controls over physical access; system user access levels; commercial driver's license testing; vehicle inventory monitoring; fuel inspection upon delivery; gross pay register review; imprest cash fund; formal policies and procedures	December 2008
I-9 Employment Verification Process 2007-823	1/29/08	Filing timeliness; automation; training	December 2008
University of Michigan – Flint Chancellor's Office 2008-205	9/30/08	Roles and responsibilities; conflict of interest; disaster recovery; reconciliations; segregation of duties; procedures	February 2009
Plant Operations Construction Services 2008-602	11/4/08	Project management reporting	June 2009
Sponsored Programs Subrecipient Monitoring 2008-501	11/21/08	Written guidance for PI's; subcontract template	June 2009
School of Music, Theatre & Dance Fiscal Responsibilities 2008-815	11/26/08	Financial oversight and Monitoring; several procurement and payroll observations; documented procedures; written delegation of authority; imprest cash management;	July 2009

