

THE UNIVERSITY OF MICHIGAN

REGENTS COMMUNICATION

Received by the Regents
January 18, 2007

Item for Information

Subject: Report of University Internal Audits
October 2006 – November 2006

Background:

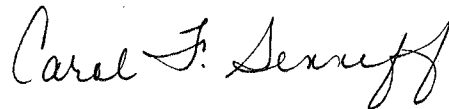
This is the report of the Office of University Audits activities for the period **October 1, 2006 through November 30, 2006**. The summaries of audits contained in this report were previously reported to members of the Regents' Finance, Audit and Investment Committee and included in discussions at Committee 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, 2006**.

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

Respectively submitted,



Carol F. Senneff, Executive Director
University Audits

January 2007

ORIGINAL REPORTS

Campus

Student Organization Accounts Services Operational Controls

#2006-104

Issued November 14, 2006

Student Organization Accounts Services (SOAS) is a unit within the Division of Student Affairs. SOAS works closely with Student Activities and Leadership, providing consulting services and assistance to Michigan Student Assembly (MSA) registered student organizations. There are approximately 1,200 student organizations at the University of Michigan.

This audit focused on specific departmental processes, evaluating controls over:

- Cash disbursements
- Cash receipts
- Training for members of student organizations
- Process of providing project grant numbers to MSA registered organizations only

There are some opportunities to strengthen procedures and related internal controls.

Control Issues:

Segregation of Duties – The SOAS Manager and the Office Supervisor have full access to the SOAS system which allows either of them to enter information necessary to generate checks. They are also authorized signers for the checking account and are able to reconcile the SOAS system accounts. Because there is limited staff in the area, segregation of duties is not possible.

Management Plan – SOAS management will work with the Accounts Receivable/Payable area in University Unions to develop a process for a post disbursement review of checks drafted by the SOAS office.

Sign-off on Disbursement Authorization Form – There are two SOAS representatives that are responsible for reviewing the Disbursement Authorization Form for completeness, appropriate supporting documentation, authorized signatures and disallowed expenditures. If a question arises, it is not readily apparent which representative reviewed the Disbursement Authorization Form and initiated the reimbursement process in the SOAS system.

Management Plan – The SOAS Manager has instructed the SOAS staff to initial the Disbursement Authorization Form once it has been reviewed. They have also added a field in the vouching system for the initials of the person entering data. University Audits verified that the new procedures are in place and working as intended. **This item is closed.**

Location of the Check Printer – The printer used to print checks is located in an open area between the desks of two SOAS representatives. This printer is accessible by the general public when the representatives are not seated at their desks.

Management Plan – SOAS management will begin printing checks on a printer in the SOAS Cash Office. The Cash Office has very limited accessibility.

Departmental procedures manual – SOAS has a limited procedure manual. Procedures should be documented for all significant activities within the unit including cash disbursements, account reconciliation and payroll procedures.

Management Plan – SOAS management is currently in the process of documenting procedures for all significant activities.

Adequate documentation –During the course of the audit, a sample of disbursements was reviewed for proper authorization and supporting documentation. An example of inadequate documentation was found.

Management Plan – SOAS management discussed with staff the importance of obtaining adequate documentation prior to approval of disbursements or the clearing of advances. This item is closed.

Based on the audit work conducted, it appears that internal controls are in place to provide an adequate level of assurance that University assets are properly safeguarded. SOAS does provide training opportunities and guidance to assist organizations in conducting their business operations. A follow-up to review the open items will be conducted during the third quarter of fiscal year 2007.

NCAA Compliance - Recruiting

#2007-405

Issued November 16, 2006

As a member of the National Collegiate Athletic Association (NCAA), the University of Michigan is obligated to comply with NCAA regulations. NCAA Bylaw 22.2.1.2 (e) requires member institutions to demonstrate that its rules-compliance program is evaluated by an authority outside of the athletics department at least once every four years. This audit focused on Bylaws 13.1 (Contacts and Evaluations) and 13.7 (Official Paid Visits) and fulfills a portion of that requirement. Bylaw 13.1 regulates the number of contacts and evaluations that occur per prospect as well as the time periods for making a contact or evaluation. A contact is defined as any face-to-face encounter between a prospect (prospect's parents, relatives, or legal guardian) and an ICA representative during which any dialogue occurs in excess of a greeting exchange. An evaluation is defined as any off-campus activity that assesses the academic qualifications or athletic ability of a prospect. This Bylaw also regulates telephone calls to prospects. A prospect's official visit to the University of Michigan, financed in whole or in part by the University, is governed by Bylaw 13.7.

The objective of this audit was to determine that the Intercollegiate Athletics (ICA) Department has procedures and controls to monitor contact with, evaluations of, and official paid visits from prospects in accordance with NCAA Bylaws 13.1 and 13.7.

Audit procedures included reviewing relevant Bylaws in Article 13 of the 2005-2006 NCAA Division I Manual and ICA policies and procedures to monitor recruiting and official visits, and performing detailed testing of football, men's basketball, ice hockey, men's swimming, women's swimming, women's tennis, field hockey, and water polo for the 2006 academic year.

Detailed testing included review and evaluation of the following:

- Recruiting travel records for a sample of coaches
- Recruiting telephone logs
- Official visit files
- Contact and evaluation logs
- Cell phone and office phone bills for the recruiting coaches of the specified sports

The following discussion explains areas where the record keeping and monitoring of recruiting activities can be strengthened.

Control Issues:

Recruiting Telephone Calls – The coaches' recruiting telephone logs are not always accurate which makes it difficult to determine compliance with NCAA Bylaw 13.1.3. We identified several occasions where a coach did not log a telephone call that exceeded the two minute threshold. The written telephone logs that the coaches are required to submit do not always match the telephone bills. There were a few instances that initially appeared to be violations of NCAA regulation that were explained as administrative errors in logging the telephone calls. Also, the method for recording telephone calls is not consistent within a sport or across sports.

Management Plan - NCAA telephone call regulations have been reemphasized with all coaches in conjunction with monthly NCAA rules education meetings. Coaches have been directed to show increased attention in documenting telephone calls to recruits that exceed two minutes (e.g., noting the correct date on compliance forms and specifying why the call exceeded two minutes). The expectation that coaches must document this information involving calls that exceed two minutes will continue to be included on telephone compliance resources provided to coaches periodically. Note: The Compliance Services Office (CSO) investigated the telephone calls made by the Michigan coach to the same prospect twice in one week on three separate occasions. It was determined that no violation of NCAA rules occurred based on a subsequent interview with the involved prospect and discussion with Verizon Wireless regarding their billing process (any outgoing call that rings in excess of 30 seconds is billed as a telephone call regardless of whether it was answered). The CSO will conduct a review of telephone bills for a sample of prospects on an annual basis.

Evaluation Records - The recruiting evaluation logs in the CSO's records do not provide enough detail to determine compliance with NCAA Bylaw 13.1. When coaches are attending events, such as a tournament, they are not consistently including a roster of the athletes participating in the event, or individually listing the specific prospects they are evaluating. Without complete records, it is not possible to determine the number of times a prospect was evaluated.

Management Plan - The Compliance Services Office (CSO) permits coaches to identify an entire high school or club team on their evaluation forms. Names of prospects are included only when the coach has a particular recruit in mind. Per NCAA rules, any observation of a prospect counts as an evaluation of all participants at that school or on that team. Thus, a review of evaluations based on identification of the high school or club team being observed is more inclusive and entails less risk of a violation. Also, coaches do not always have a specific prospect in mind when evaluating a team. Requiring a coach to provide a roster or insist they always provide the name of a prospect on a team would not improve this process. With two exceptions, all coaches' evaluation forms identified the high school or club team being evaluated. The two exceptions identified a tournament and provided a photocopy of the cover of the tournament book rather than a listing of teams evaluated. The coaches have been advised that either a listing of teams evaluated or the tournament book must be provided. The CSO consulted with the Big Ten compliance staff who noted that 1) the CSO is following national standard practice for monitoring evaluations, and 2) it is unnecessary to include rosters for the hundreds of teams evaluated as the administrative burden on the coaches and compliance staff outweighs the convenience of having rosters readily available for investigative purposes. Any investigation of evaluations of a specific prospect will typically require additional research as the CSO would not rely solely on coaches' compliance records, and documentation can be obtained on the back end with far less administrative effort. The CSO has asked coaches to provide rosters as available. However, we do not categorize the absence of rosters as an exception. The CSO will continue to consult with Big Ten and peer institutions to ensure our monitoring system for recruiting evaluations is in line with industry standards. In addition, the CSO will begin doing reviews for a sample of prospects on an annual basis. In the past, University Audits provided this review for a sample of prospects by mutual agreement.

Based on the audit work conducted, it appears that ICA has appropriate policies, procedures, and controls to monitor on-campus and off-campus recruiting activities in accordance with NCAA regulations. Improving the quality of recruiting support documentation and additional monitoring will increase assurance that the University continues to comply with NCAA regulations. University Audits will follow-up on the status of action plans during the fourth quarter of fiscal year 2007.

University Health Service – Charge Capture and Inventory Management

#2006-111

Issued November 14, 2006

University Health Service (UHS) reports to Student Affairs and is not affiliated with the University of Michigan Hospitals and Health Centers. UHS is made up of fifteen departments committed to promoting and protecting the health of students and other members of the University community. Serving approximately 70,000 patient visits per year, UHS is an independent resource of health care clinics located on central campus. UHS provides primary care to students, faculty, alumni and other University of Michigan affiliated groups.

The UHS Business Office is comprised of billing, administrative and coding staff. The Business Office is primarily responsible for processing all enrolled student charges covered under the health service fee, third party billings and payments received.

The objective of the audit was to evaluate the adequacy and effectiveness of existing controls over:

- Charging and billing student health services not covered under the health service fee (e.g. medications, immunizations)
- Inventory management of pharmaceuticals (including expired medication)
- Inventory management of UHS equipment

Opportunities to strengthen processes and the underlying internal controls:

Documented Billing Policies and Procedures - The Business Office processes all electronic billings for UHS clinic departments within the Medical Manager billing system. There has been an effort to improve billing processes during the past year. During a review of a sample of patient accounts, we observed several instances of:

- Incorrect account classification of write-off and adjustments
- Patient account write-offs without complete documentation
- Collection agency recoveries that had not been posted to corresponding patient accounts

During the course of this audit, the department corrected all of the incorrect classifications.

Management Plan - The UHS Business Office has been actively documenting policies and procedures. We will prioritize writing those that pertain to the gaps identified by this audit.

We will ask the Business Office Manager to report on key billing indicators, such as write-offs, adjustments and missing documentation to the Compliance Committee. The Committee is comprised of the UHS Director, Medical Director, Administrative Director and Ancillary Services Director. The Business Office Manager is Advisor to the Committee and a regular attendee. She has been asked to bring any future billing concerns to the Committee, whether or not they are related to Center for Medicare and Medicaid Services compliance requirements.

We have created a timeslot on Thursday mornings when the Health Service does not see patients. We will utilize some of this time for interdepartmental communication and training on the issues identified in this audit, and other billing issues as they arise. The Clinician Staff meetings will continue to be available as an ongoing mechanism for educating clinical staff on billing issues.

Coordination and Communication - The billing practice and functions are performed by employees in decentralized clinical areas and poses an opportunity for better communication and coordination among staff. The Billing Office has limited authority and/or responsibility over decentralized billing practices initiated by various staff. The Business Office consistently communicates concerns to management for immediate resolve. However, some issues may not always be addressed in a timely manner.

During our review, we observed inconsistent applications of stated billing processes. Control mechanisms established by Business Office staff are inconsistently exercised; impacting billing implications and resulting in excessive reliance on billing office staff resources. Most discrepancies that were identified were from 2005. Current activity appears to be working well and managed appropriately through improved mechanisms in place.

Management Plan - The corrective actions outlined under Documented Billing Policies and Procedures above will address these coordination and communication issues, especially between the Business Office and the clinical and clerical staff. It should also be pointed out that the relationship between the Business Office and the clinical leadership is strong and has proven very effective at implementing change. Not only does the Business Office Manager have regular access to the UHS Directors through the Compliance Committee, she also works closely with the Medical Director to address billing issues on an ongoing basis.

Some examples of major operational changes they implemented over the past year include:

- Creating a new lab requisition form that effectively links diagnosis codes with the tests ordered
- Developing new templates for properly documenting supervision by attending physicians
- Piloting programs to capture revenue for in-house consultations
- Creating a process for the Medical Director to immediately review any requests by clinicians to waive fees

Payment Processing-Unapplied Payments - UHS Business Office posts unapplied patient payments to an over/short account when there is a question regarding where it should be ultimately posted. Unapplied payments usually occur when the clinic has lost the patient's charge form or when documentation supporting the payment is unreadable (e.g. patient's name, account number etc.).

Based on discussion with management, unapplied payments sometime cannot be resolved unless a patient calls to investigate. The same individual who applies a mis-applied payment also corrects the account. Duties involving cash management that are not properly segregated may result in misappropriated funds. Unresolved payments remain in the over/short account.

Management Plan - UHS will create more appropriate classifications in our billing system to more accurately reflect unapplied payment activity. We will segregate functions so that the person who posts the unapplied cash transaction is not the same person who posts it to the patient account. Procedures will be written and communicated to appropriate staff.

Medical Record Documented Services - The Allergy Clinic maintains the original allergy clinic treatment record within the clinical department, not in the patient's actual medical record. It can take up to a year before the allergy treatment records are processed and placed in the patient's medical record.

Management Plan - We checked with UMHS and their situation is similar to that at UHS. Because of the frequency of patient visits for immunotherapy, it is not practical to keep the patient's central chart updated. At UHS this is less of a problem because all of our activity is onsite and the information in our Allergy Clinic is readily available to other clinicians throughout the building. In order to notify clinicians of the existence of Allergy records, the nurse in the Allergy Clinic stamps "Immunotherapy" on the face sheet in the patient chart, with a starting date for treatment. When treatment is completed,

the Allergy records are inserted into the patient chart. This should not be an issue when UHS brings up an electronic health record, probably in the summer of 2008.

Management of Patient Charge Forms - Patient services are documented on a patient charge form. The charge form documents the service and diagnosis code for billing purposes. During our review, we observed reports in which patient charge forms have been missing since 2005, without resolution. Current procedures do not allow for timely turnaround of missing charge forms.

In the physical therapy (PT) department, a charge form is not used. The department sends handwritten descriptions of services to the Business Office where billing and coding is completed. PT's departure from using the standard form has resulted in various billing issues for the billing office including duplicate processing, incorrect patient information, illegible writing and delays in processing.

Management Plan - The missing charge forms are for the most part related to follow-up visits, in one department, for which there is no associated revenue. However, UHS acknowledges that this is still a valid concern for control reasons. We will therefore ask the Business Office Manager to provide regular reports to the Administrative Director and the Medical Director for action. Periodic reports will also go to the UHS Compliance Committee.

The Physical Therapy Department has historically not used the standard charge form because it could not be configured to meet their data collection and scheduling needs. We will revisit these processes to see if the concerns are still valid. If the charge form is still a problem, we will look to implement a different type of electronically-generated encounter form to address the control issues. In the unlikely event that we are not able to identify a short-term solution, these issues will be addressed with the implementation of an electronic health record, probably in the summer of 2008.

Cash Handling in the Clinics - During our review, we observed that the Allergy clinic did not reconcile cash and patient charge forms prior to turning them over to the Business Office.

Management Plan - Currently this is only an issue for the Allergy Clinic. In the short-term, we have trained the Allergy Clerk on proper cash reconciliation procedures and the clerk stays at the end of the day until the cash is reconciled. The Business Office also provides back-up support to the Allergy Clinic. Longer-term, we are looking to renovate the lobby to accommodate a second cashier which will handle the high-volume Allergy Clinic activity as well as overflow from the existing lobby cashier.

Adequate Management of Inventory - The Information Technology (IT) department is responsible for the purchase and inventory of computer equipment. During our review, we observed the following:

- An IT Support Specialist is responsible for the purchasing and the disposition of equipment. While management reviews and maintains responsibility for purchasing decisions, management oversight of disposition activities does not exist. Procedures have not been developed outlining documentation and authorization for equipment sent to Property Disposition.
- The current inventory database contained some inaccuracies. The following issues were identified during a physical inventory review:
 - Several items of computer equipment were not found in stated locations. UHS personnel explained that sometimes items will be shifted to other areas for maintenance and that the log may not reflect the changes
 - Several Pharmacy desktops could not be located
 - A few pieces of computer equipment had not been tagged
- An in-house database spreadsheet used to track and monitor items sent to property disposition does not consistently log the date when the items were sent. The spreadsheet also does not identify the rationale for disposition of equipment (e.g. broken, retired etc.).

- Equipment items are kept in the fourth floor attic room by IT personnel prior to disposition or for long-term storage. Management does not have an accurate inventory of all items stored in the attic. There are approximately 125 equipment items currently stored in the attic. Accessibility is restricted to building maintenance, the IT Specialist and the IT Manager.

Management Plan - The ITS Manager will draft formal policies and procedures related to sound inventory management. This will include a description of what items need to be tagged and when they need to be inventoried. A complete audit of IT equipment will be undertaken. It will include leased items, such as the Pharmacy desktops, that are in the possession of UHS. An annual inventory report will be provided to the Administrative Director.

University Health Services has implemented an internal control environment that provides assurance that major risks are minimized in the areas of patient accounts billing and follow-up. University Audits will conduct a follow-up review during the third quarter of fiscal year 2007 to assess the progress of new procedures and new internal controls.

University of Michigan Autism & Communication Disorders Center

#2006-814

Issued November 21, 2006

The University of Michigan Autism & Communication Disorders Center (UMACC), a unit of the Horace H. Rackham School of Graduate Studies, focuses on improving the lives of individuals with *autistic spectrum disorders* and their families through research, training and education, and private and group clinical services.

The objective of this audit was to review operational controls associated with management of grant projects, charge capture and billing processes, appropriateness and approval of travel and other expenditures, handling of cash and other assets, and maintenance of patient confidentiality.

Control Issues:

Segregation of Duties - During the audit, we noticed several opportunities for UMACC to strengthen controls by segregating duties:

- The department timekeeper's signed time report is returned to her for processing
- The individual responsible for reconciling the Gross Pay Register is the backup timekeeper who also has access to update employee pay data
- A single individual is responsible for billing patients, collecting payments, and posting payments to patient accounts
- A single individual is responsible for creating non-patient invoices and entering the receivable into the non-patient receivable spreadsheet. This person is also responsible for depositing all cash receipts

Management Plan - To segregate duties associated with the payroll process, UMACC management outlined new procedures for timesheet data entry, authenticity of data entry, and reconciliation. The director will no longer return the center administrator's (CA) signed report to the CA, UMACC's primary timekeeper. The CA's signed time report will be given to the center accountant (CACCT). The CACCT will give a copy of the time report to the CA for data entry, but will maintain the original report for comparison to the Gross Pay Report (GPR) to ensure that the CA's time data is accurate. The CACCT, as the backup timekeeper, can also enter time data electronically. Therefore, one day after data entry, the CA will generate a report from the payroll system. To verify that there are no unauthorized changes, the CA will reconcile this report and the time reports to the GPR.

UMACC management also drafted new procedures to ensure that all charges for patient services are entered into Lytec, UMACC's patient billing system, and that all payments (patient and non-patient) are accounted for properly. To ensure that all visits are recorded, clinicians will be responsible for reporting

non-scheduled billable visits to the center coordinator and the CACCT. The CA will place security controls on Lytec to prevent the deletion of dates of service and prepayments. The CACCT will reconcile cash receipts, checks, and charges to the appropriate patient account. The CACCT will also run a monthly report to monitor patient activity. The CACCT will continue to be responsible for non-patient invoicing and reconciling the non-patient accounts receivable spreadsheet. However, the center coordinator (CC) will be responsible for entering non-patient invoices and payment information into the non-patient accounts receivable spreadsheet. This spreadsheet will be write-protected to prevent unauthorized changes. The CC will log all cash receipts daily. On a regular basis, the CA will reconcile this log to deposit receipts.

Cost Transfer Documentation - A review of cost transfer procedures revealed that detailed explanations for transferring costs between grants are not provided with transfer requests. To comply with University of Michigan and National Institutes of Health (NIH) regulations, UMACC's cost transfer procedures should require detailed explanations be documented for all transferred costs.

Management Plan – Effective October 2006, UMACC began providing detailed explanations for cost transfers on journal entries. UMACC will also provide detailed explanations for transfers initiated between December 2005 and October 2006. These explanations will be maintained at UMACC. UMACC management communicated these new procedures to the appropriate staff members. UMACC will document these procedures by calendar year end.

Authorized Refunds and Write-offs - Controls governing the refund and write-off processes do not provide assurance that all refunds and write-offs were authorized and verified. UMACC management can improve cash controls by reviewing and approving documentation supporting the validity of refunds and write-offs and verifying that only approved refunds and write-offs were processed.

Management Plan - Management revised refund and write-off procedures. The center administrator will review and sign documentation supporting refunds and write-offs before the center accountant processes the transaction. Both the center administrator and the center accountant will also maintain documentation supporting authorized refunds and write-offs for comparison to the statement of activity.

Accounting Errors - A review of P-Card statements, invoices to third-party sponsors (re-bills), and other expenditures revealed several transactional errors including:

- Incomplete re-bills to sponsors
- Personal expenses not reimbursed by the traveler
- Business expenses not reimbursed to the traveler
- Hosting event incorrectly charged to a federal sponsor

Management Plan - The P-Card reconciler (the center accountant) will review P-Card rules on a regular basis to ensure that she is up-to-date on current changes. A pre-travel form delineating what the sponsor will reimburse will be completed and approved by the Rackham Budget Office. A travel checklist will be used to ensure that all re-bill activity is complete and accurate. The checklist will also be used to ensure that the traveler is reimbursed for personal funds used during travel and that the traveler reimbursed the University for personal items charged on the P-Card. The center accountant will reconcile re-bill invoices separately to the appropriate statement of activity. The grant administrator provided the center accountant with current copies of all UMACC grant budgets to ensure the appropriateness of charges placed on the grant.

Personal Expenses Charged to P-Card - A traveler charged personal expenses for hotel accommodations extended beyond business purposes to a P-Card and later reimbursed the University via the P-Card ATM Reconciliation form. Per the Accounts Payable P-Card training guide, "it is a policy violation to use a P-Card for personal expenses." The traveler may charge nominal expenses for personal items such as in-

room movies and the use of the hotel's gym facility to the P-Card while the P-Card holder is on travel status. The traveler must reimburse the University for these expenditures.

Management Plan - UMACC administrators held an in-service for P-Card holders on September 19 and October 8, 2006 to review P-Card policies, including personal expenses charged on cards.

Auditor's Comments: UMACC administrators confirmed that all P-Card holders attended in-service training. They also provided us with a copy of the in-service handout, which confirmed their intent to discuss charges for personal expenses. **This item is closed.**

Documented Processes - UMACC does not have written documentation describing many of its business processes. Written policies and procedures codify management's criteria for executing an organization's operations. They document business processes, personnel responsibilities, departmental operations, and serve as training tools for employees.

Management Plan - UMACC has already documented several of the procedures listed above. UMACC will continue to document its policies and procedures. In-service training will be ongoing and held during regularly scheduled staff meetings in order to inform staff of new/revised policies and procedures. Completed policies and procedures will be added to UMACC's policies and procedures manual.

University Audits will review the implementation of management's action plans during the fourth quarter of fiscal year 2007.

Graduate Medical Education – Veterans Administration Billing

#2006-128

Issued November 30, 2006

University Audits conducted a review of current procedures to bill the Veterans Administration Medical Center (VAMC) for resident services. This review was requested by the University of Michigan Health System (UMHS) General Counsel's Office and Graduate Medical Education (GME).

The Ann Arbor Veterans Administration Medical Center has contracted with UMHS to provide University residents for clinical rotation. There are approximately 108 full-time equivalents (FTE) actively assigned to twenty-five clinical departments in the VAMC. Residents are employees of the University of Michigan Hospitals and Health Centers (UMHHC) and provide both inpatient and outpatient services. Oversight for the VAMC rotation is provided by the Graduate Medical Education Office (GME) of the Medical School in conjunction with various clinical departments. VAMC rotations allow residents the opportunity to attain knowledge and skills that might not otherwise be experienced.

The GME Office is responsible for all aspects of oversight and regulation of the ACGME-accredited programs at the University of Michigan. Some of the functions of the office include: 1) providing residency program assistance, 2) maintaining credentialing and other documentation of residents and fellows, and 3) conducting internal reviews for accreditation purposes. GME is also responsible for billing the VAMC for resident services. The GME office uses MedHub, the residency management tool system, as the source for monitoring and managing resident information.

The objective of the audit was to determine the adequacy and effectiveness of procedures governing resident billing practices.

Audit focus included the following:

- Program Coordinator attestation of resident services
- Accuracy of reporting hours by residents
- Accuracy of billing resident services to VAMC

- Risks associated with UMHS residents assigned to VAMC and participating in University business

Control Issues:

Inefficient billing processes - Because of inefficiencies within the VA system, GME had to adopt multiple, time-consuming procedures to bill the VAMC for services.

VAMC billing is often delayed as a result of delays in receiving timesheets from the VA (for example, the GME Office received June, 2006 timesheets during the week of November 20, 2006), as well as the difficulty in reconciling the VA timesheet documentation with MedHub. There were instances where the VAMC may be under billed for services due to this inability to resolve discrepancies.

Residents are assigned to the VAMC in advance of their scheduled service times. Changes to the schedule may occur as a result of UMHHC department needs and priorities. Resident activity, including changes to schedules, is managed in a very decentralized manner by both the VAMC and UMHHC. Current billing procedures do not always capture correct or complete charge information. The implementation of a new billing procedure would eliminate many of the internal control weaknesses identified in this audit.

Management Plan - The house officer/coordinator will sign-off on the activity identified on the timesheets. This information will be submitted to the GME Office for billing. The GME Office will collect rotation schedule information for each training program. Errors to this schedule will be discussed with program coordinators to ensure accuracy of attested information.

The GME Office will identify issues, define action needed to address them and develop/implement corrective processes that reflect a goal of accurate reporting of all details of program trainee rotation schedules. In February 2006, a meeting was held with VA personnel to review the billing processes at each institution with a goal of improved information flow and timely submission of required documentation. An agreement has been reached ensuring that respective needs be met. VA timekeepers will now have direct contact with the UM program coordinator of the trainee to resolve rotation issues before the VA timesheets are submitted and the final invoice is prepared.

Education of trainees as to accurate reporting of clinical activities will be enhanced. Departments currently provide an overview of schedules and location for training. GME will develop institutional documents to provide details of the obligation and expectations. These will be made part of the new trainee orientation materials and for department use when rotation goals and objectives are discussed.

Use of Social Security Numbers - GME uses social security numbers as an identifier in billing the VAMC for services. Standard Practice Guide section 601.14, Social Security Number Privacy Policy prohibits the use of social security numbers as the primary account number or identifier for an individual. The existing VAMC-UMHS disbursement agreement established in 1992 is outdated and indicates that social security numbers be furnished when invoicing.

Management Plan - Use of social security numbers on invoices is discontinued.

Defined Roles and Responsibilities for VAMC Billing - There is an inconsistent understanding and application of GME and program expectations to support the accuracy of VAMC billing and tracking of resident time. Areas of inconsistency include the method to manage and process:

- Adjustments to rotation schedules (including journal entries)
- Discrepancies between VAMC timesheets and UMHS rotation schedules
- Resident FTE adjustments
- Verification of residents' physical presence

Coordination between GME and program coordinators is essential to ensure accuracy and timeliness in the current billing process.

Management Plan - Regular and frequent communication between the program coordinators and GME office staff will continue. Coordinator training sessions and informational meetings will be held regularly throughout the year. This schedule includes meetings every other month for the coordinator group at large, as well as ad hoc, topic-specific smaller group sessions. As in the past, new hire orientation sessions will continue to train new program coordinators in one-on-one sessions with the GME administrator and in larger groups of new coordinators.

Information on the GME website will be updated regularly to share new information. New information will continue to be provided at bi-monthly coordinator meetings. Updated budget information will be provided to staff and explained to ensure knowledge and understanding. Procedural changes on accreditation, credentialing and budget processes will continue to be distributed throughout the year or upon request.

With completion of the billing process review, the new revised billing procedure and flowchart will be finalized and shared with the program coordinators. Timekeepers at the VAMC are to correspond directly with the UM program coordinators to resolve rotation discrepancies before they enter data on the timesheets. VAMC timekeepers will be invited to attend future coordinator meetings to ensure a more collaborative approach for process review and information sharing.

VAMC Billing Monitoring and Tracking - The GME office does not sufficiently analyze or manage accounts receivable balances from VAMC. Most processes are manual and reporting does not indicate aging of balances and status of monthly payments or follow-up.

During the audit period, there was no evidence that disbursements made by VAMC were consistent with the 1992 agreement which specifically states that VAMC will issue prepayments each month based on an estimate of services from GME. When the final estimate is issued, the estimated payment is to be deducted and the balance forwarded to the GME Office.

Management Plan - Analysis and management of accounts receivable balances from the VAMC will be efficiently monitored and tracked. Specific individuals have been assigned responsibility for oversight and management. Issues or concerns regarding accounts receivable balances will be communicated to the GME administrator for timely resolution. Regular meetings will continue to occur between the GME Office and Hospital Financial Services to discuss billing status and the GME staff to review billing. When ongoing issues are identified in these sessions, refinements are suggested and implemented.

Communication with the VAMC occurs regularly to discuss status of timesheets and/or payment; these usually occur via telephone conversations or email. These “informal” communiqués will be replaced with more formal reminder/dunning correspondence.

Reports regarding aging, status of payments or follow-up with the organization are maintained. Follow-up regarding the status of late timesheets or payment occurs via telephone conversations, and email.

Prior to July, 2005 VAMC payments were made to the University on an “as billed basis”. With this process, there was significant lag time from receipt of timesheets for creation of the invoice to receipt of payment. The VA has reverted to the pre-payment methodology that was described in the original signed agreement. Since that time, payments made to the University each quarter are based on estimated activity. An invoice is later submitted that reflects actual resident activity. The result is payments that are current. Submission of timesheets to the GME office continues to be several months behind. A letter will be sent to the VA in the event of significant delays with receipt of timesheet data or payments.

Follow-up to management plans to improve the procedures for billing the Veterans Administration Medical Center for resident services will be conducted during the fourth quarter of fiscal year 2007.

Credit Card Processing

#2006-121

Issued November 30, 2006

The University of Michigan receives payments and gifts from students, faculty, staff, alumni, donors, and others in various forms including credit card payments. Depending on the business needs of the organization, such credit card payments are made in person, over the phone, through the mail, via fax, or over the Internet. All cardholder account information that passes through the University payment systems is sensitive. Without proper safeguards in place this information is vulnerable to internal and external compromises which can lead to fraud and identity theft.

The Treasurer's Office is responsible for coordination of all e-commerce¹ and credit card acceptance throughout the University. If a unit is accepting credit cards at the University, it must be registered with Treasurer's Office – Card Services and have signed a Service Level Agreement (SLA) which defines the roles and responsibilities of the Treasurer's Office, Financial Operations and the University department (merchant) as they relate to credit card processing.

Another requirement of all credit card merchants at the University is compliance with the Payment Card Industry Data Security Standard (PCI DSS). An industry standard regulated by a board made up of MasterCard, Visa, American Express and Discover Card, the PCI DSS applies to any merchant that transmits or processes credit or debit card information. This standard was created to provide common payment card industry security standards for safeguarding sensitive cardholder data. It establishes network security and business practice guidelines including deadlines, auditing requirements, and stiff penalties for noncompliance in order to protect cardholders' account and transaction information. These requirements came into effect June 30, 2005 and apply to all merchants and service providers that store, process, or transmit cardholder data, including all University merchants.

There are over 200 units throughout the University that accept credit cards. Many of these units have multiple merchant numbers bringing the total number of merchants contracted with the Treasurer's Office/Card Services to approximately 400. For the purposes of PCI DSS, the University treats each of these merchants independently. All University units storing, processing, or transmitting cardholder data, are required to:

- Build and Maintain a Secure Network
- Protect Cardholder Data
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor and Test Networks
- Maintain an Information Security Policy

The audit focused on a sample of eight University merchant areas chosen from the merchant list provided by the Treasurer's Office:

- Institute of Continuing Legal Education
- Business School Executive Education
- Pierpont Commons
- Office of Gift Administration
- Physicians Billing Office
- New Student Programs
- Dental Patient Services

¹ Electronic Commerce (e-commerce) is the act of conducting retail operations through the Internet.

- Dental Continuing Education

These merchants represent a total of 32 merchant numbers and a cross-section of various credit card processing methodologies. Five merchants in the sample accept credit card payments over the Internet.

Control Issues:

Updates to the Service Level Agreement - University merchants began signing the Treasurer's Office Service Level Agreement (SLA) in 2002. Since then, the SLA has been updated, but many of the merchants were unaware of the added requirements:

- The SLA should be updated to address compliance with payment card industry standards.
 - The agreement should state that "Credit / debt card transactions must comply with the requirements of the Payment Card Industry Data Security Standards (PCI DSS) rules."
- The SLA should specifically address validation for electronic and phone credit card transactions.
 - The SLA requires merchants to "validate all cards by ensuring the signature on the back of the Card matches the signature on the transaction receipt." This is standard practice in all cases where the credit card is presented at the merchant's site. However, validating signatures in this manner for electronic/on-line (Internet) or telephone transactions is not feasible because the physical credit card is not provided for these types of transactions.
- The SLA should be updated to make all merchants aware that the last four digits of the credit card number may be stored.

Management Plan - The Treasurer's Office, in conjunction with Information Technology Security Services (ITSS) is in the process of developing a document to address Payment Card Industry (PCI) compliance to both business and information technology (IT) personnel. These changes along with those mentioned above will also be referenced in a revised SLA that will be distributed to all units.

Communication of Payment Card Industry Standards - Communications between the Treasurer's Office and the University credit card merchant community needs to be improved. The requirements imposed by the PCI on processing credit cards, protecting payment card data and securing IT systems that process such sensitive data should be discussed with University merchants as part of the periodic meetings between Treasury personnel and credit card merchants on campus.

Management Plan - The Treasurer's Office, in conjunction with ITSS, is in the process of developing a document to address PCI compliance to both business and IT personnel.

Incident Response Plans - The PCI DSS requires all credit card merchants have an incident response plan in place to deal with improper disclosures of sensitive cardholder data. Standard Practice Guide (SPG) section 601.25 outlines the incident reporting policy for all University units. The SLA further instructs that if a merchant experiences a "hacking" incident concerning their credit card operations, or suspects such an incident has occurred, the Treasurer's Office Card Services must be notified immediately. The revised SLA will incorporate reference to this SPG.

Management Plan - SPG section 601.25 outlines the incident reporting policy for all University units. The revised SLA will also incorporate reference to this SPG.

Documenting Information Security Policies - Information security policies, including policies for access control, application and system development, operational, network and physical security are not formally documented by all credit card merchants. In order to be in compliance with the PCI DSS, all credit card vendors must:

- Establish, document, and distribute security policies and procedures
- Perform a periodic risk assessment that identifies threats, and vulnerabilities

- Review and update policy annually and when the changes occur to their credit card processing environment
- Monitor and analyze security alerts and information, and distribute them to appropriate personnel
- Administer user account and authentication management, including additions, deletions, and modifications
- Monitor and control all access to data

Management Plan - The current compliance documents being authored by Treasury and ITSS will provide clearer guidance and reference for the merchants.

Each of the merchants in the sample is addressing the control weaknesses in the unit specific procedures. A follow-up review with Treasury and unit management will be conducted in the third quarter of fiscal year 2007.

Information Technology

Computing Environment CoSign Web Authentication

#2006-303

Issued November 28, 2006

The CoSign web authentication system was implemented four years ago by the University of Michigan Computing Environment (UMCE), which is a division of Information Technology Central Services. UMCE supports web services, the U-M gateway website, directory services, email, domain name service, and login servers. In addition, UMCE provides hosting for websites and databases. They are also responsible for CoSign which was initially developed by the University and is currently open source. This means it is available and free to the public to use and modify. It is an industry standard and is part of the National Science Foundation Middleware Initiative.

CoSign is a secure single sign-on web-based authentication mechanism that provides secure and positive authentication to protected web services and applications at the University of Michigan. A CoSign failure would impact users and applications throughout the University. Typically there are about 150 CoSign-enabled applications running concurrently and approximately 190 running at peak periods. These application providers rely on CoSign to handle authentication and to ensure integrity of and security over electronic credentials. With the documentation and scripts provided by UMCE, internal service providers can implement CoSign independently.

Authentication attempts to ensure that the person requesting access is the person who owns the credentials and not an impostor or hacker. In the authentication process, CoSign uses cookies (small identification files), unickname and Kerberos passwords to establish identity. A single sign-on process allows users to authenticate once and access multiple protected web resources without signing on again during that session.

The audit focused on determining the following:

- The logon process provides positive authentication to protected services
- The logoff process disables access to all services
- Use of cookies does not expose data or violate user privacy
- The application is secured from unauthorized access and modification
- The "Friend" system (accounts created by non-affiliated users) grants access only as authorized
- System passwords are properly managed
- Systems are monitored for vulnerabilities
- Audit trails identify source of suspicious activity

Control Issues:

Password Transmission - As it is currently configured, an exposure exists in CoSign because Kerberos passwords are transmitted over the network. This exposure is minimized on University-administered machines by keeping operating systems up-to-date with security patches and other updates and using the anti-spyware module in the University-supported virus-scanning software. Additionally, "phishing" (the act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft) presents a problem for any service that transmits passwords.

Available technology can eliminate transmitting passwords by using digital certificates which are basically attachments to electronic messages used for security purposes. The most common use of a digital certificate is to verify that a user is who he or she claims to be.

University Audits recommends that transmission of Kerberos passwords be discontinued, if possible. Options to authenticate using CoSign without transmitting the Kerberos password include implementing Public Key Infrastructure (PKI), Simple Protected Negotiation Mechanism (SPNEGO), a combination, or some other certificate-based authentication process for CoSign related functions. University Audits also recommends that UMCE work with Information Technology Security Services (ITSS) to educate users on combating phishing attacks.

Management Plan - We agree that we should offer PKI and SPNEGO but it's not practical to eliminate password transmission entirely for the foreseeable future. We are researching options for use with CoSign and currently use PKI for the Radmind file management system. We expect implementation during 2007. Additionally, UMCE will work with ITSS to launch an education campaign that helps users tell the difference between weblogins and impostors.

Server Location - All four redundant CoSign servers are in the same physical location. This is considered a single point of failure because all four servers could be affected by an environmental or other problem specific to this one location and CoSign would be disabled. In the event of such a failure, a server at a different location would need to be configured, loaded with software, and tested.

UMCE is aware of this vulnerability and did have a CoSign server located in a separate facility, but this server was moved back to the original location due to firewall issues.

Management Plan - Although servers are currently located in two separate buildings, they are next to one another and are subject to the same environmental events. At least one of the servers (depending on the load) will be moved to the new MITC Computing Center when it becomes available. This is targeted for March 2007.

Policies and Procedures - Although comprehensive documentation exists for the CoSign application, enhancements could be made to unit level documentation.

- A policy addressing retention of CoSign log files has not been adopted and written. The policy should include retention, disposal, where logs are stored, who has access, and for what purposes information is made available.
- Documented instructions or procedures to resolve potential issues, as indicated by Tripwire messages, and to assign responsibility are incomplete. Tripwire is run to identify and track unauthorized changes made to files. An email is generated if a change is processed outside the approved method. Email messages are sent to the Web team each time Tripwire is run until the questions are resolved. There is an on-call rotation schedule, and on-call staff members are aware of procedures including escalation procedures.

Procedures for program changes have not been written. Procedures should include approvals, assignments, code standards, testing, documentation, implementation and backout. The CoSign team follows standard procedures and there is separation between programming and deployment.

Management Plan - This is an issue for the UMCE that we recognize and are committed to work on as part of both disaster recovery and Avian flu planning. We will complete written procedures in areas specified. Documentation of the logout process is being completed at this time. The on-call rotation schedule indicates responsibility. Staff members are aware of standard procedures for responding to messages and for program changes. We will seek retention guidelines from appropriate committees, document details, and follow the guidelines.

A formal follow-up of out-standing issues will be conducted during the fourth quarter of fiscal year 2007.

FOLLOW-UP REPORTS

Medical Center Information Technology (MCIT) Financial Internal Control Assessment #2005-367
Original Report issued June 16, 2006 Follow-up Report issued November 14, 2006

Safeguarding of Capital Assets: A new supplier has been selected to replace M-Stores to tag and brand newly purchased IT equipment. University Audits has discussed and reviewed the new procedures for tagging assets with MCIT personnel. **Closed**

Management has taken appropriate corrective action. **This audit is closed.**

Counseling and Psychological Services Purchasing Controls #2006-809
Original Report issued May 12, 2006 Follow-up Report issued November 14, 2006

The original audit was performed in conjunction with an investigation being performed by the Department of Public Safety into alleged improprieties associated with the use of a University issued P-Card.

The Division of Student Affairs (DSA) has implemented policies and procedures to strengthen the internal controls over P-Cards and other business functions of the division units. DSA has developed P-Card guidelines which have been distributed to all P-Card holders, reconcilers and administrators. In addition to these guidelines, DSA has compiled Basic Unit Financial Guidelines to provide all staff members involved in financial activities with a brief synopsis of fiscal responsibilities for financial review, purchasing, cash handling and payroll. Both documents contain several references to University sources of additional information.

During the course of the audit, University Audits decided to extend the audit review to include a sample of other DSA units. The Career Center and Services for Students with Disabilities have been selected for review, the results of which will be issued under a separate cover upon completion.

The status of the audit issues and actions taken to strengthen the internal control environment within CAPS and the Division of Student Affairs are outlined below.

Authorization to obtain and use a University of Michigan procurement card

Control Recommendation: P-Card's should not be issued to an employee without documented needs and responsibilities of the P-Card holder. The documentation should include what can be purchased and dollar limits. The need for every departmental P-Card should be reviewed at least annually. If the need for the P-Card no longer exists, the card should be cancelled. P-Card holders must not delegate or share use of their P-Cards as in accordance with the P-Card Holder Agreement signed by all P-Card holders.

Corrective actions taken by CAPS:

- CAPS has implemented procedures to track the flow of documents through the reconciliation process.

- CAPS has complied with University policies and no longer transfers to, assigns to or allows P-Cards to be used by anyone other than the P-Card holder.
- A memo containing the original signature of the CAPS director, two associate directors and the administrative assistant senior have been submitted to the Dean of Students office and the DSA Finance Office.

Corrective actions taken by DSA senior management:

- Applications for new P-Cards require written justification of business purpose. Applications are forwarded to the DSA Finance Office where the need and dollar limits are reviewed again before submission to the P-Card Office.
- A process for the periodic review of P-Card needs has been developed. The first review will occur in December 2006. In response to the audit, DSA senior management indicated they would perform this review as part of the fiscal year end procedures; however, due to the time constraints of fiscal year end activities it was decided that a review at calendar year end would provide time for a more thorough review.
- The directive that P-Card holders must not delegate or share use of their P-Card is included in both the DSA P-Card Guidelines and Basic Unit Financial Guidelines.

University Audits reviewed a CAPS P-Card statement for evidence of tracking through the reconciliation process. A copy of the memo containing the original signatures of the aforementioned CAPS personnel was obtained from the DSA Finance Office. University Audits reviewed a recent P-Card application for written justification of business purpose. We reviewed both the P-Card Guidelines and the Basic Unit Financial Guidelines as established by the division senior management.

Monthly supervisory review and approval of P-Card statements

Control Recommendation: The CAPS director should review for any P-Card activity on a monthly basis. He is in a position to know what constitutes acceptable purchase but has the responsibility to get a full and acceptable explanation of any questionable item on the statement. Upon completion of a thorough review, the director should sign or initial and date the statement. P-Card holders should also be reviewing their own P-Card statements to prevent unauthorized purchases from being made on their card.

Corrective actions taken by CAPS:

- The director of CAPS reviews P-Card statements in detail before submitting them to the associate dean of students for review.

Corrective actions taken by DSA senior management:

- Specific guidelines for the review and approval of P-Card statements are contained in the P-Card Guidelines as previously discussed. The guidelines contain listings of appropriate and prohibited P-Card purchases. Proper support and documentation requirements are also discussed in the document.
- DSA senior leadership was provided with a listing of P-Card holders and card attributes. The communication ensures unit directors have a direct knowledge of all P-Card holders within their unit.
- Monthly P-Card activity reports are provided to unit directors and senior leadership by the DSA central finance office.

University Audits reviewed one CAPS employee P-Card statement and all the supporting documentation. University Audits obtained and reviewed a copy of the listing of P-Card holders and card attributes that was provided to senior leadership. The director of the central finance office provided University Audits with a copy of the log documenting the dates P-Card activity reports were provided to unit directors and senior management.

Student Affairs finance office P-Card review

Control Recommendation: DSA central finance reviewers must have the authority to thoroughly question and investigate any unusual or incomplete documentation, purchase requests, or business purpose explanations. The issues should be escalated to the level of the holder's supervisor and the manager of the DSA central finance office. Issues should be logged along with their disposition. Periodic reviews of the log and trend analysis should be performed by the director of the finance office as well as the directors of each unit within DSA.

Corrective actions taken by DSA central finance office:

- The DSA finance office has instituted a formal review process that includes recording and tracking the receipt of reconciled P-Card statements, issues related to the statements and disposition of those issues. A standard memo has been developed to communicate issues and questions to P-Card holders. The unit director for the P-Card holder is copied on the communication.
- The director of the DSA finance office monitors P-Card issues and performs periodic trend analysis of P-Card issues and occurrence of issues per P-Card holder.

University Audits reviewed a copy of the electronic spreadsheet used to track monthly P-Card reconciliation process. We also obtained an example of a "P-Card statement is being returned & requires your attention" memo and verified the issues listed were relevant.

Budget review

Control Recommendation: Budgets must be a priority in managing the activity in any unit. This includes reconciliation of monthly statements of activity and comparison against planned activity-both revenue and expense. Any deviation or unusual expenses should be investigated and resolved immediately. There must be a separation of duties. The person who is initiating purchases should not be reconciling the budget.

CAPS should also prepare and manage a budget specific to any project. No one in CAPS knew how much money was being spent on the two unit projects. Budget management not only aids in the detection of potential fraud but is a necessity for prudent fiscal management.

Corrective actions taken by CAPS:

- The director of CAPS now pre-approves all non-recurring purchases for the unit. He also reviews the statement of activity detail for any transactions that he has not approved for which he requests supporting documentation and explanation for the purchases. The director and the administrative assistant senior meet regularly to discuss the financial activities of the unit.
- CAPS receives monthly statement and budget information from the DSA finance office. The CAPS administrative assistant senior breaks down this data into more detailed categories for variance analysis with the detailed unit budget. The director of CAPS reviews the budget to actual variances with the administrative assistant senior and request explanations for any variances.
- The DSA finance office reviews gross pay registers for accuracy. The director of CAPS performs a secondary review of the gross pay registers verifying reasonableness and existence of all payees.
- Project accounts are established for special projects prior to any significant activity related to the project.

Corrective actions taken by DSA senior management:

- As mentioned previously, DSA developed basic unit financial guidelines which were distributed to all staff with financial responsibilities.

- DSA has implemented a process that requires each unit director and senior leadership to review the financial statements for their unit/s. A signed certification is required indicating that monthly financial statements and related details have been reviewed. Another component of this process involves the review of deviations from budgeted revenues and expenses, unit directors and senior leadership are required to submit written explanations for the deviations to the central finance office.
- The vice president for Student Affairs has reiterated to unit directors and senior leadership the necessity for fiscal responsibility. The discussion included responsibility for effective use of resources and financial controls.

The executive director of University Audits and other University Audits management have attended various DSA meetings to discuss fiscal responsibilities and financial controls. University Audits also reviewed an example of a unit financial statement and certification statement.

Division of Student Affairs management continues to be engaged in the review and enhancement of existing business policies and procedures to ensure the control structure in place is adequate to support the mission of the Division and safeguard the assets of the University. Management has taken appropriate corrective action. We will review the Career Center and the Services for Students with Disabilities units for compliance with DSA policies and procedures to ensure these enhancements have been communicated and implemented throughout the Division. We will report accordingly under separate cover. **This audit is closed.**

Web Grade Entry Project

Original Report issued March 16, 2006

#2006-103

Follow-up Report issued November 14, 2006

Access Controls: Security access reports have been produced and sent to the Registrar's Office for review of systems analysts and developers update access to production data. This program of reporting current privileges, along with documentation of security roles and purpose of the access, was extended beyond the Registrar's Office to Human Resources Management System and Financial Information data owners. Frequency is every other month. **Closed**

Identifying Unauthorized Grade Changes: A query was written and is run periodically to identify grade changes of at least one grade. Review includes identifying an excessive number of changes by one person and random checks back to paper authorizations. **Closed**

Password Management: Password minimum length was increased and an inactivity timeout was implemented. The special character requirement and restricted re-use was implemented when the move from Novell to Windows was completed during October 2006. **Closed**

Grade Approval: The Registrar has met with the Senior Vice Provost for Academic Affairs twice to discuss creating and distributing a policy and guidelines for academic units defining the accepted use of 'grade' and 'approve' privileges including guidelines for assigning grading and approval privileges to Graduate Student Instructors. They agree that some change needs to occur. The Registrar and the Senior Vice Provost for Academic Affairs are scheduled to meet to provide further clarification and some guidance on how this might be presented to faculty. **Closed**

Management has implemented corrective action on all major audit recommendations. **This audit is closed.**

Intercollegiate Athletics Booster Clubs

Original Report issued August 3, 2006

2006-812

Follow-up Report issued November 14, 2006

The University of Michigan Club of Greater Detroit Articles of Association Articles of Association (bylaws) have been revised and approved to state that dues are not required but that you must be a member of the University of Michigan Alumni Association to qualify for membership.

Management has taken appropriate corrective action. **This audit is closed.**

UMHHC Vendor Visitation

Original Report issued January 30, 2006

#2006-118

Follow-up Report issued November 30, 2006

UMHHC Vendor Visitation Practices

The Compliance Office split the vendor visitation policy into two unique policies (vendor and staff conduct). Copies of the draft policies were provided to University Audits.

- Hospital and Health Center (HHC) Contracts and Procurement Department has been working with Ambulatory Care to initiate awareness of Contract and Procurement policies and vendor visitation conduct.
- Monitoring of controls over unauthorized vendor activity is on-going. These controls include communication to Contracts and Procurement regarding prohibited vendor activity and non-compliance to established policies. Contracts and Procurement continues to forward the vendor orientation log to Entrance and Security Services on a weekly basis to validate vendor training. Vendors arriving without any record on the log are not permitted to enter any Hospital facility and are redirected to Contracts and Procurement for training of vendor policies.

Security and Entrance Services implemented a new badging system at the main Hospital. This system is scheduled to go live by November 30, 2006. Security and Entrance Services Department is reviewing plans for implementation of a new server that will assist in monitoring additional security stations that have been established at two Mott locations. Additional stations will be considered as needed.

- Quarterly meetings between the Contracts and Procurement, the UMHS Compliance Office, and Entrance and Security Services departments have been ongoing since January 2006 and will continue to address reported issues.

Coordination between the UMHS Compliance Office, HHC Contracts and Procurement, and Security and Entrance Services has been established and proven valuable to the overall management of this process.

Monitoring of Vendor Visits

- The Compliance office has built an improved workflow around vendor monitoring. Monitoring criteria has been established and incorporated in draft policies.
- Security and Entrance Services reviews and identifies vendors listed on the vendor orientation log provided by Contracts and Procurement on a weekly basis.
- The new badging system and additional stations will contribute in efforts to provide additional monitoring.
- Security and Entrance Services reports vendor violations to HHC Contracts and Procurement.

Identification of Sanctioned Vendors

- Contracts and Procurement reviewed the vendor master list during February 2006 to identify excluded vendors under HHS Office of Inspector General OIG guidelines. On February 28, 2006, Contracts and Procurement implemented the Excluded Party Search System (EPSS) software for monitoring sanctioned vendors.

- During March 1-3, 2006 two vendors were identified as an exact match. These vendors were deactivated immediately so no other transactions could take place.
- Central campus vendor maintenance began checking the OIG exclusion list for all new vendors on April 18, 2006. Contracts and Procurement is notified if any are identified on the OIG list.

Management has taken the appropriate measures to strengthen vendor visitation controls. **This audit is closed.**

University Audits – University of Michigan
Open Audits Follow-up Table
November 30, 2006

Audit Title	Report Date	Status	Expected Completion
Utilities Services Energy Billing System 2005-337	11/2/05	Significant progress has been made. Issues to be addressed are security policies, encryption of a password, and status of the virtual firewall	December 2006
UMHHC Radiology IT Security 2005-338	5/23/06	Management is addressing issues related to physical access to the server room, passwords and user IDs	January 2007
UMHHC Security/Access – Card Access Security 2006-306	9/8/06	Cross-training and server security issues related to the Access Control, and documentation of department policy are the issues that are being addressed	January 2007
UM Medical School Anesthesiology IT Security 2006-404	9/29/06	Removal of SSNs from the Centricity system, physical access to the server room and securing workstations in public areas are the issues still being addressed	January 2007
UMHHC Pathology IT Security 2006-401	9/29/06	Installation of another proximity card reader on Pathology's server room and implementation of a periodic review of access are the outstanding issues for follow-up	March 2007
University of Michigan Computing Environment CoSign Web Authentication 2006-303	11/28/06	Issues being addressed include relocation of a server and formalization of departmental procedures	June 2007
Credit Card Processing 2006-121	11/30/06	The Treasury Office is updating the Service Level Agreement with merchants across campus	March 2007
Professional Fee Billing Compliance 2005-126	12/22/05	New organizational structure is been established; additional controls are being implemented	January 2007
UMHS MLabs 2006-112	1/19/06	Management is implementing corrective action measures	January 2007
UMH Patient Transfers 2006-124	4/20/06	Multi-disciplinary team has been established to design, implement, and evaluate discharge procedures, roles and responsibilities	January 2007
UMHHC Vendor Discounts, Allowances, and Rebates 2006-119	7/19/06	Vendors are being asked to send remittances directly to UMHHC Purchasing Department to reduce the number of days required to process a deposit	December 2006

UMHS Materiel Services Center 2006-106	9/29/06	Identification of staff authorized to receive goods, reconfiguration of the dock to restrict access, pre-numbering receiving reports and conducting periodic cycle counts are the open issues	March 2007
University Health Services – Charge Capture and Inventory Management 2006-111	11/14/06	Strengthening controls over billing and cash handling; formalizing related procedures	March 2007
Parking Services 2006-202, 2022	1/06/06	Documentation is nearly complete: significant changes in leadership; management is re-evaluating processes	December 2006
Michigan Public Media Phase I 2006-806	3/24/06	Policies have been documented and communicated to all staff	Follow-up memo issued 7/31/06 2 nd follow-up planned for January 2007
Michigan Public Media Phase II 2006-806	4/24/06	Significant reorganization and implementation of control policies and procedures is in progress	December 2006
School of Music Internal Control Assessment 2005-216	6/6/06	Storage issues are being assessed; roles & responsibilities for the box office revenues are being revised	December 2006
Library Special Collections 2006-205	6/16/06	Library administration is working to strengthen the controls discussed during the audit	January 2007
Intercollegiate Athletics Sports Camps 2006-410	7/28/06	No compliance issues: operational improvements being implemented regarding background checks, contracts, financial records, reconciliations, time away policy and cash management	January 2007
Financial Operations – Central Payroll Office Processes 2006-101, 102	8/11/06	Management is addressing issues related to account reconciliations, segregation of duties, processing of online checks, time entry and state taxes. There are also IT-related concerns over payroll queries and password management policies	December 2006
College of Engineering – Minority Engineering Program Office 2006-813	9/29/06	CoE and MEPO created a thorough management plan to address the audit issues; will review progress ongoing	March 2007
Office of the VP for Research Animal Care Administrative Processes 2006-102-3	9/29/06	Management in units and centrally will address action plans	January 2007
Student Organizations Accounts Services Operational Controls 2006-104	11/14/06	Developing a process for post-disbursement review of checks, relocating the check printer, and completing the procedures manual	March 2007

NCAA Compliance – Recruiting 2007-405	11/16/06	Improving the quality of recruiting support documentation	June 2007
Autism & Communication Disorders Center 2006-814	11/22/06	Procedures will be documented	May 2007
Graduate Medical Education – Veterans Administration Billing 2006-128	11/30/06	Improving procedures that support billing from the VA for UM Graduate Medical Education	April 2007

