

THE UNIVERSITY OF MICHIGAN

REGENTS COMMUNICATION

Item for Information

Received by the Regents
November 17, 2006

Subject: Report of University Internal Audits
July 2006 – September 2006

Background:

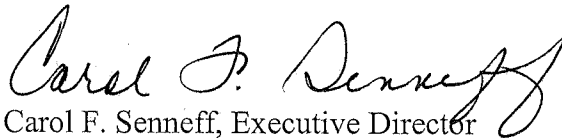
This is the report of the Office of University Audits activities for the period **July 1, 2006 through September 30, 2006**. The summaries of audits contained in this report were previously reported to members of the Regents' Finance, Audit and Investment Committee and included in discussions at Committee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

November 2006

ORIGINAL REPORTS

Campus

NCAA Miscellaneous Compliance Areas

#2006-412

Issued July 7, 2006

This audit addressed policies and procedure compliance with National Collegiate Athletic Association (NCAA) rules and regulations governing playing and practice seasons, coaching staff limits and contracts and rules education. Included in the review were the following sports: football, men's basketball, ice hockey, men's swimming, women's swimming, women's tennis, water polo and field hockey.

Audit procedures included:

- Reviewing relevant Bylaws of the 2005-2006 NCAA Division I Manual
- Examining playing and practice worksheets to determine compliance with preseason practice dates, initial competition dates, length of season limits and limits on the number of competitions
- Reviewing 2005-2006 Countable Athletically Related Activity forms
- Reviewing coaching staff lists and contracts
- Examining rules education meeting agendas, schedules, handouts and attendance sheets

Based on the audit work conducted, Intercollegiate Athletics has appropriate policies, procedures and controls in place to comply with the applicable NCAA regulations. **This audit is closed.**

Intercollegiate Athletics Sports Camps

#2006-410

Issued July 28, 2006

More than twenty sports hold camp sessions for approximately 8,500 youth during the summer session. Camp participants use Intercollegiate Athletics (ICA) facilities and residential campers stay in campus dorms. All camp directors are ICA employees. There is a signed agreement between ICA and each camp director and all camps must submit certain compliance documents. Some camps directors prefer to run their camps internally with the ICA Business Office; others prefer to run their camps as independent businesses.

The objective of this audit was to determine whether ICA policies, procedures, and practices during the 2005 camp season were in compliance with the National Collegiate Athletics Association (NCAA) rules governing sports camps and clinics.

There are some opportunities to improve the control environment.

Control Issues:

- Background checks – ICA has always communicated their expectation that camp directors arrange for background checks of camp staff; however, there is no written ICA policy on the subject. We noted confusion about whether or not student-athletes required a background check and observed inconsistent documentation regarding the need to perform background checks for ICA staff.

Management Plan – ICA will ensure that there are written agreements for all camps and that the agreements are properly signed and dated within the proper timeframe. With the Office of

the General Counsel, the appropriate steps to ensure that the contracts are properly authorized by the Board of Regents will be determined. ICA Business Office policies will be updated to address summer camp issues including merchandise sales.

- Contracts – areas where contracting can be improved:
 - o There were no written contracts for smaller camp sessions
 - o Contracts with external camp directors were not approved by the Regents, as required
 - o There was only a verbal agreement between an internal camp director and an employee independently selling merchandise during camp sessions
 - o In a few instances, contract documentation was not clear: ICA did not sign, camp director did not date or handwritten changes were not initialed or dated

Management Plan – ICA will ensure that there are written agreements for all camps and that the agreements are properly signed and dated within the proper timeframe. With the Office of General Counsel, the appropriate steps to ensure that the contracts are properly authorized by the Board of Regents will be determined. ICA Business Office policies will be updated to address summer camp issues including merchandise sales.

- Financial Records - Financial records for internal camps were well documented and showed a complete picture of camp operations. Camps run externally were not as clear either due to lack of complete documentation or multiple accounts used to manage camp funds. The financial disclosure form is a new control procedure that the Business Office implemented in 2005 to improve the transparency with external camps.

Management Plan – The external camp financial disclosure form will be expanded in order to obtain more meaningful and complete financial data. In addition, comprehensive instructions will be created to assist camp directors in completing the form. Reasonableness testing with other available documentation will be performed on a sample basis.

- Reconciliation of deposits and payments - The Business Office, acting as the bookkeeper for internal camps, does not receive camper rosters for reconciliation of all deposits. There is no reconciliation of staff rosters to actual compensation payments.

Management Plan – Reconciliation of deposits and staff payments to camp and staff rosters for internal camps will be performed on a sample basis.

- Time away policy – There is no written policy regarding recording exception time while working at camps. Although coaches do not have to report time, for other staff that work camps, time away may or may not be recorded on time reports for primary job responsibilities during camp weeks. The current practice is inconsistent. Because staff are being paid to assume secondary job responsibilities, it is important to make sure that there are no conflicts/commitment issues.

Management Plan – ICA will work with Human Resources to develop an appropriate camp “time away” policy which is consistent with University policy and applicable laws.

- Cash management – We noted that not all camps keep checks in a locked location. Although checks for internal camps are restrictively endorsed, there is a risk of theft and checks contain personal information that should be secured. Checks received are not deposited daily.

Management Plan – ICA will meet with Treasurer’s Office personnel to discuss the possibility of obtaining an exception to SPG 502.1 regarding daily deposits which would set reasonable thresholds for deposits.

NCAA compliance and camp documentation were found to be adequate and effective. A follow-up review of the outstanding issues will be conducted in the second quarter of fiscal year 2007.

Intercollegiate Athletics Booster Clubs

#2006-812

Issued August 3, 2006

As stated in National Collegiate Athletic Association (NCAA) Bylaw Section 6.4., “Responsibility for Actions of Outside Entities”, an institution has responsibility for its athletic program. This responsibility includes acts of individuals, corporate entities, or other organizations that are external to the university but considered representatives of the university’s athletic interests. Booster clubs are considered such representatives.

Intercollegiate Athletics (ICA) at the University of Michigan monitors booster club activities in a variety of ways. For instance, statements of disclosure are received from booster clubs to assure compliance with NCAA Bylaw 6.2.3 which requires an agreed-upon procedures report for “all expenses and revenues for or on behalf of a Division I member institution’s intercollegiate athletics program, including those by any affiliated or outside organization ...”. These statements are provided to the external auditors of the University of Michigan who provide a financial audit to the President of the University. University Audits and ICA agreed, in 2005, that University Audits would perform reviews of all booster clubs over a five year period. The University of Michigan Club of Greater Detroit and the M Club of the University of Michigan were selected for our current audit.

The University of Michigan Club of Greater Detroit sponsors a number of events throughout the year. Major events include the Football Bust, which honors seniors on the team with presentation of their M rings, trips to selected away football games and an annual golf outing. There are no dues for club members but to be eligible for membership you must be a member of the University of Michigan Alumni Association.

The M Club of the University of Michigan maintains the M Room above the pro shop at the University of Michigan golf course. It also sponsors football tailgates and brunches and the M Day golf outing. There are different types of memberships available to join the M Club and applicable dues.

The objective of this audit was to determine whether ICA maintains adequate control over the two selected booster clubs and that each club maintains adequate controls over their internal business processes and complies with applicable NCAA Bylaws and regulations.

Audit procedures included reviewing the bylaws and/or articles of association, meeting minutes, financial records and statements of disclosure of the selected clubs. Statements of disclosure were reconciled with the club’s financial records and supporting documentation, including year end bank statements and reconciliations. Material transactions of the selected clubs were reviewed to determine compliance with NCAA guidelines. ICA procedures were reviewed to determine proper monitoring and coordination of booster club activities.

Control Issue:

- The University of Michigan Club of Greater Detroit Articles of Association - The Articles of Association, Article Six-Dues, of The University of Michigan Club of Greater Detroit states that the sum of one dollar for each club member shall be paid from club funds as dues to the general Alumni Association of the University of Michigan. However, the online application for membership states that there are no dues but you must be a member of the University of Michigan Alumni Association to qualify.

Management Plan – The Assistant Athletic Director will contact the Executive Board of The University of Michigan Club of Greater Detroit regarding revision of the Articles of

Association to reflect that dues are not required of members who are also members of the University of Michigan Alumni Association.

Based on our review, ICA maintains adequate control over the two selected booster clubs and clubs maintain adequate controls over their internal business processes and comply with applicable NCAA Bylaws and regulations. We will follow-up during the second quarter of FY 2007 to make sure that the Articles of Association of The University of Michigan Club of Greater Detroit have been updated.

NCAA Compliance – Financial Aid

#2006-408

Issued August 8, 2006

As a member of the National Collegiate Athletic Association (NCAA), the University of Michigan is obligated to comply with NCAA rules and 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 concentrated on Article 15 of the NCAA Division I Manual and fulfills a portion of the requirement mentioned above. Article 15 specifies the types of financial aid that may be awarded to student-athletes, regulates the administration of such aid, and defines maximum institutional grant-in-aid limitations by sport.

The University of Michigan Intercollegiate Athletics (ICA) Department is responsible for the administration of athletic awards. ICA and the Office of Financial Aid (OFA) coordinate efforts to monitor financial aid awarded to student-athletes.

PURPOSE AND SCOPE

The objective of this audit was to determine that ICA has appropriate policies, procedures, and controls to administer and monitor the awarding of financial aid to student-athletes in accordance with NCAA regulations.

Measures to determine the adequacy of policies and procedures over student-athlete financial aid included:

- Reviewing Article 15 of the 2005-06 NCAA Division I Manual
- Evaluating the effectiveness of coordination between the ICA and OFA
- Interviewing ICA and OFA personnel
- Reviewing the process to ensure accuracy of squad lists
- Recalculating financial aid awarded to a sample of student-athletes and counter and equivalency totals for the following sports: Football, Men's Basketball, Ice Hockey, Men's Swimming, Women's Swimming, Women's Tennis, Field Hockey, and Water Polo.
- Verifying training-table meal calculations and deductions
- Reviewing financial aid cancellations/reductions that occurred during the term

SUMMARY

Based on the audit work conducted, it appears that ICA has appropriate policies, procedures, and controls to award and monitor student-athletes financial aid in accordance with NCAA regulations. ICA and OFA personnel were cooperative and responsive during the audit. No areas of non-compliance were observed.

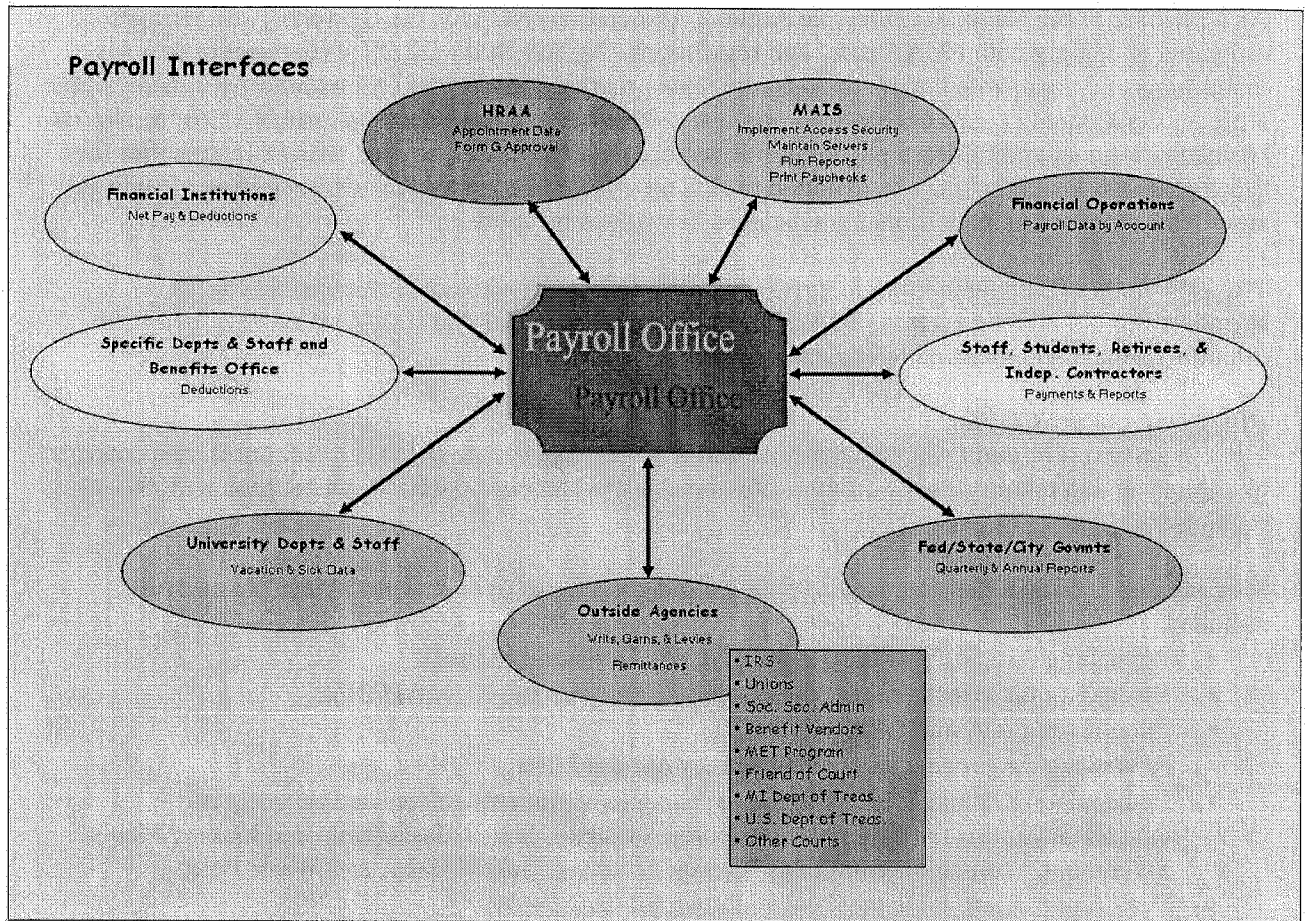
Financial Operations - Central Payroll Office Processes

#2006-101

Issued August 11, 2006

In conjunction with the Office of the Associate Vice President for Finance's review of departmental payroll processes, University Audits has completed an audit of Payroll Office processes. In fiscal year 2005, compensation and benefit expenses for the University of Michigan totaled \$2.6 billion; approximately 65% of the University's total operating expenses.

The Payroll Office is divided into nine sections: HR/Payroll Customer Service Center, Gross Pay, Attendance/Timekeeping, Deduction, Tax, Financial Services, General Services, Audit/Salary Transfers, and Payroll Processing. These sections work together to ensure that the University's 47,000 permanent and temporary employees are paid accurately and timely. This can only be achieved with the cooperation of others. Human Resources and Affirmative Action (HRAA) staff perform specific tasks that are critical to payroll operations, such as providing appointment information, initiating benefit deduction refunds, forwarding approved Form G- Special Stipend requests, and providing clarification to resolve issues on payroll discrepancy reports. HRAA occasionally collaborates with the Payroll Office to provide responses to units requesting resolution of issues affecting salary distribution, pay,



and benefits. Payroll relies heavily upon individual departments, staff, and external customers such as state and federal taxing authorities, unions, and Friend of the Court to provide the information necessary to process payments. Standard Practice Guide section 518.01 (*Payroll Controls*) outlines the procedures for processing payroll expenses. Additional policies address overtime pay, special payments, and the use of temporary workers. The Payroll Office has the ultimate responsibility for ensuring that the payroll function is operating in accordance with University, state, and federal rules and regulations.

The purpose of this audit was to determine if the Payroll Office has established effective processes and instituted controls to ensure that payments are processed in a timely and accurate manner. Detailed objectives included determining if:

- The overall control environment governing payroll processes is effective.

- Controls are in place within payroll processes to mitigate risk and provide management assurance that:
 - o Earnings and other payments are made in accordance with relevant terms and conditions of employment.
 - o Employee attendance information is accurately captured and employee benefit payments are properly authorized, calculated, and distributed.
 - o Deductions and withholdings are appropriate, properly calculated, and remitted to the appropriate agencies.
 - o Statements of earnings, fringe benefits, and required tax documents are appropriately prepared and distributed to employees.
 - o Payroll values are recorded accurately, completely, and timely.
 - o Other issues unique to the Payroll Office are processed in a timely and accurate manner:
 - Escheating Process
 - Payroll Fund Reconciliation Process
 - Other processes performed outside of M-Pathways
 - o Information Technology controls are effective:
 - PeopleSoft role-based security
 - Wolverine Access
 - Access to high-risk transactions

Control Issues:

- Reconciliation of Payroll Fund - Procedures need to be implemented to:
 - o Document reconciliation procedures and the procedures for monitoring the reconciliation of the payroll fund.
 - o Establish guidelines to ensure that adequate cross training is maintained to ensure these procedures are completed during extended leaves of absence.
 - o Review the status of reconciliations for all Payroll Office account codes and investigate any outstanding balances. Future reconciliations should be completed as soon after the end of the preceding month as is feasible. Design reconciliations so that all reconciling items have been identified, corrected, or written off.

Management Plan - Management will document reconciliation and review procedures. When staffing allows, Payroll will ensure these procedures are completed timely. Department administrators review balances at year-end; however, they may not effectively communicate transactions that need to be written off. Write-off procedures will be addressed. Reconciliations will be completed as soon as possible.

- Access Privileges to Logs - Payroll Customer Service Center employees use the Mail Log to track online check distribution to payees. The Online Check Log is used to control check stock usage and record online checks printed throughout the day. Employees in the Payroll Processing section perform a daily reconciliation of these logs to assure Payroll administrators that the employees who printed checks relinquished control of the checks to Customer Service Center employees. Restricting access to the Mail Log is a key control to account for online checks.

Review of access privileges to the subdirectory on the Payroll Office server containing the Mail Log disclosed that several staff members had unnecessary update access to the Mail Log. This subdirectory had previously been restricted in response to a prior audit; however, access reverted to allow too broad a range of access.

Management Plan - At management's request, Business & Finance Information Technology (BFIT) has restricted access to the Mail Log subdirectory. In addition, the entire subdirectory structure was reviewed. The first annual review has been completed.

This issue has been appropriately addressed and is closed.

- Payroll Office Access - Because of their job responsibilities, Payroll Office staff have special roles within the HRMS system that allow them to perform functions such as correction of historical payroll data, printing of online checks, updating paysheets and paylines, and updating deductions and tax data. A global review of security roles in comparison to job duties and further restriction of privileges is important to strengthen security within the payroll application.

Management Plan – Management will:

- Perform a review of critical security roles and permission lists based on job responsibilities. Payroll management will determine where the 'superuser' privilege can be removed and will work with HRAA management to coordinate access privileges with assigned job duties.
 - Document the procedures related to the quarterly review of access they perform.
- Segregation of Duties - During this audit, we noticed several opportunities to strengthen controls by properly segregating duties. Duties associated with authorization, custody, record keeping, and reconciliation should not overlap.

Management Plan - Someone other than the individual who posts the payments to the accounts receivable records now collects and reconciles cash and checks. Management will establish procedures to monitor data created/modified by Payroll employees who have the ability to set-up new employees and modify job data. The directors of Payroll and HRAA agree that access roles and permissions should be reviewed periodically. BFIT has restricted access to the subdirectory.

- System Access and Compliance Training - Administrative data users in the Payroll Office have access to sensitive information, which if used irresponsibly, may violate the rights and privacy of employees, students, patients, and other individuals whose data resides on University administrative systems. The Access and Compliance Form documents employees' understanding of their responsibilities as users of sensitive data. It is also used to confirm the employee's agreement to abide by University policies and applicable state and federal laws pertaining to the proper use of sensitive data. The Payroll Office did not adequately document and retain Access and Compliance Forms for all employees. Additionally, training materials related to system access and compliance requirements are outdated.

Management Plan - Management is now using the online course to train new employees. Payroll periodically reminds employees of their responsibilities to safeguard information. All employees will be required to sign a new Access and Compliance Form annually. Payroll will retain these forms for at least one year.

University Audits verified that payroll managers are utilizing online training, providing periodic information security reminders, and have collected signed compliance forms for fiscal year 2007. **This issue is closed.**

- Workstation Controls - Written policy should address acceptable password management for both Kerberos and workstation passwords because of the sensitivity and confidentiality of payroll data and the risk of unauthorized modification.

Payroll management encourages users to logoff or lock workstations when they are not using the system, but does not require it. To perform payroll functions, users enter through Wolverine Access, which times out after 15 minutes of inactivity.

Management Plan - Management will include the password management policy in the Associate Vice President for Finance orientation materials. Management will meet with staff to discuss password changes and the acceptable use of computing resources annually.

- Payroll Queries – The Payroll Office runs several queries prior to the on- and off-cycle pay runs to assist in detecting data errors and other exceptions. These queries appear effective, but the reasons for the established parameters are not documented and are not apparent. Payroll Office management does not periodically review the parameters established for these queries.

Management Plan - Management will review query parameters to determine if reports are capturing the information intended. They will also document the rationale used to determine query parameters.

- Quarterly Online Check Review Process - Payroll's off-cycle online payment process is used to create paper checks outside of the normal pay period. During a review of this process, University Audits noted that:
 - o Less than 2% of the checks were reviewed. The sample size did not appear sufficient to conclude that appropriate documentation was created and retained.
 - o Although the process for creating off-cycle checks includes controls over proper authorization for checks, the documentation collected as part of this review did not always include evidence of payment authorization.
 - o Payroll did not review online check documentation of two employees who created checks during the period.

Management Plan - New procedures are in place. Management combined tables to include net pay information for each transaction and increased the sample size. The three highest net pay line items and two additional line items will be reviewed. Management will also ensure that payment authorizations are reviewed and that a sample of documents will be reviewed for each individual who created an online check during the period.

EARNINGS AND OTHER PAYMENTS

- Outsourced Time Entry - Time and labor data entry for approximately 13,084 of the University's 58,000 bi-weekly and monthly time reports has been outsourced to an independent vendor who subcontracts to overseas vendors. An interruption in the services provided by this independent vendor may result in inaccurate and untimely payments and create an enormous burden to Payroll Office management and staff.

Management has a responsibility to recover from such disruptions in a minimum amount of time at minimal cost. This requires careful preparation and planning.

Management Plan – Management will perform a business impact analysis to gain an understanding of the underlying risks and consider the potential impact to the Payroll Office and the HRMS CPU in MAIS if services provided by this vendor or its subcontractors are interrupted or discontinued. Procedures will be documented.

- Department Time Entry - An independent vendor inputs 22.5% of the University's time reports. The inherent risks associated with outsourcing this task include, but is not limited to, failure of transmission and duplication. The potential for errors from the use of OCR (optical character

recognition) equipment and human interpretations of data is also present. Management is concerned about the lack of competitors who can perform this service for the University.

Management Plan - Management will review the time entry self-service function for department timekeepers after the next upgrade to the HRMS Time and Labor module. If it provides a more user-friendly interface, Payroll management will solicit assistance from University executives to persuade departments to use electronic time data entry.

The responsibilities of the Payroll Office are critical to the University and touch all faculty and staff. The Payroll Office relies on controls within individual departments to provide reliable information and verify the accuracy of reported time, payments, deductions, withholdings, and paid time off balances.

In our opinion, the Payroll Office has established effective processes and instituted appropriate controls to ensure that payments are processed in a timely manner and in accordance with the information provided by HRAA and other internal and external departments and agencies. Payroll employees review several reports to identify inaccurate data.

The Payroll Office relies on individual departments to provide reliable source data and verify the accuracy of the Gross Pay Registers. The majority of the University's time reports are input into the HRMS system at the departmental level or through an electronic interface. The Payroll Office has effective controls in place to assist in the prevention of payroll data errors. Management has implemented controls such as:

- Prevention of update access to the operator's own payroll records is programmed into the HRMS system.
- A series of pre-calculation queries are run to analyze source data so corrections to potential rejects and errors can be made to payroll data before a final payroll is processed.
- Process monitoring of production payrolls is done and documentation is maintained by MAIS and Payroll.
- Audit trails for critical payroll transactions such as online checks, updates to payroll data, additional pay (other than base pay), and job (appointment) data (including setting up people for one-time checks) is systematically maintained.
- System level access controls exist to prevent unauthorized access directly to payroll tables.
- Wolverine Access contains effective controls over employee business transactions in the HRMS system and self-service transactions such as viewing paychecks and leave balances.

Although precautions are taken to verify the accuracy of data before the payroll is run, management acknowledges that mistakes happen. The Payroll Office has effective processes in place to verify and document payroll corrections. Payroll Office staff appear proficient in their work and capable of handling inquiries about inaccurate and missing payments.

A formal follow-up of outstanding issues will be conducted in the third quarter of fiscal year 2007. Because of the close relationship between Payroll and HRAA, an HRAA audit should be considered in the future.

Intercollegiate Athletics NCAA Compliance – Eligibility

#2006-407

Issued September 29, 2006

The objective of this audit was to determine that ICA has appropriate procedures and controls to certify and monitor student-athlete eligibility in accordance with Big Ten Conference and NCAA regulations. A high-level review of academic performance program reporting procedures was also performed. Procedures to evaluate the adequacy of the eligibility certification and monitoring processes for initial, continuing, and transfer student-athletes included:

- Reviewing Article 14 of the 2005-06 NCAA Division I Manual and Rule 14 of the Big Ten Conference Handbook
- Interviewing ICA and the Office of the Registrar [RO] personnel
- Reviewing ICA and RO procedures for initial, continuing, and transfer eligibility
- Reviewing certification, academic, and admissions documentation for a sample of initial and continuing student-athletes from the following sports: Football, Men's Basketball, Ice Hockey, Men's Swimming, Women's Swimming, Women's Tennis, Field Hockey, and Water Polo for Fall 2005 and Winter 2006 terms

Based on the audit work conducted, it appears that ICA has appropriate procedures and controls to certify and monitor student-athlete eligibility in accordance with NCAA and Big Ten regulations. Procedures to report student-athlete enrollment, academic success and graduation rates appear to be consistent with NCAA requirements. ICA and RO personnel demonstrated expertise in eligibility regulations. No areas of non-compliance were observed.

Minority Engineering Program Office (MEPO)

#2006-813

Issued September 29, 2006

University Audits has conducted a review of the Minority Engineering Program Office (MEPO) in the College of Engineering (CoE). This audit was requested by the Associate Dean of Academic Affairs, CoE and the Executive Director of Resource Planning and Management (RPM), CoE.

MEPO supports the recruitment and retention of underrepresented student populations in the CoE at the University of Michigan. MEPO offers numerous programs and services and is divided into five primary areas of operation.

- Academic Support Services
- Administrative Services
- Outreach and Recruitment
- College Support (Retention)
- Student Support and Development

RPM provides administrative support services for MEPO and other CoE departments including: financial planning and management, human resources, and facilities planning and management. As the main administrative unit of the College, RPM reports directly to the Dean and works closely with leadership to sustain and advance the academic mission of the College.

MEPO, along with other CoE departments, has experienced several transitions in executive leadership during recent years. MEPO currently reports administratively to the Associate Dean of Academic Affairs in the CoE. Prior to June 2005, the department reported to the CoE Associate Dean of Undergraduate Education. MEPO revenue was \$1.7 million during FY 2006 (through April). The program received more than \$730,000 in expendable gifts during this period. The program employs more than 100 temporary and contract workers during the year.

The objective of the audit was to determine the adequacy and effectiveness of the internal control environment. The Summer Engineering Academy, Summer Engineering Institute (SEI) and Life Academy programs were the primary areas reviewed during the audit. Audit procedures evaluated:

- Program Eligibility Criteria
- Participant Application and Evaluation Process
- Donations and Funding Relationships with External Companies
- Review and Authorization of Expenses (including travel)
- HR/Payroll Practices and Payments to Contractors
- Equipment and Inventory Management

- Conflicts of Interest

Control Issues:

- Greater collaboration and communication must occur between MEPO and RPM regarding the internal control environment, financial transactions and strategies needed to support program goals and objectives. The Account Manager/Specialist should be sufficiently empowered to take steps needed to ensure propriety of financial transactions and enforce internal control standards.
- Existing relationships and transactions that create a potential conflict of interest with the Director of MEPO must be adequately disclosed or re-disclosed, evaluated and managed consistent with Standard Practice Guide section 201.65.
- The Director should review and approve all expense documentation submitted by MEPO personnel for reimbursement and/or payment.
- Partnership and affiliation agreements with external parties must be signed only by those individuals appropriately delegated responsibility by the Board of Regents to commit University resources. The terms, conditions and funding associated with such agreements should undergo a legal and financial review to ensure propriety and consistency with University protocols.
- Payroll activity including overtime pay, time reporting and temporary employment must be processed in a manner consistent with University guidelines.
- Consistent employment procedures should be implemented by MEPO including screening against the state's registered sexual offenders list, use of standard pay methodology, regular evaluation of workers, and verification of student enrollment status. A central employment file should be maintained for each employee. This file should be periodically checked for completeness and support the hiring process.
- An equipment list of all donated and purchased equipment should be created and maintained. This listing should include a description of the item, the date acquired, the value/cost, the person to whom the item was assigned and location. MEPO should coordinate with CoE personnel to ensure responsibility for tagging and entry of purchases is adequately performed. Items should be appropriately secured and monitored periodically.
- Measures must be implemented to better monitor and restrict transactions that could result in employees receiving a personal benefit from University transactions they initiate. Examples included excessive staff meals and possibly inappropriate cell phone plans/utilization.
- University requirements for engaging independent consultants must be followed consistent with Standard Practice Guide section 201.86, including documentation to support nature of work to be performed, qualifications of worker, arms-length selection, rate of pay, number of days to be worked, contracting and invoicing.
- MEPO and RPM should collaborate with Development to establish a formal and central process by which they will be informed of gifts received on behalf of the program. MEPO should work with Accounting and unit leaders to ensure each gift is appropriately classified and utilized. A detailed reconciliation should be performed.
- P-Card and other expense transactions must include sufficient documentation to support business purpose as well as recipients/beneficiaries.

Management Plan - The Associate Dean and the Executive Director of RPM, in conjunction with all parties involved in the audit, prepared a comprehensive CoE management plan in response to poor programmatic and administrative practices noted during the audit. It is a comprehensive operational plan to make MEPO and RPM partners while creating an expectation of compliance and control within

the MEPO organization. The following are key action items from the plan, which in totality addresses programmatic practices, administrative practices and budgets.

- A programmatic mentor will assist in reviewing MEPO's mission and goals and to refocus, where necessary, the projects that support these goals. Outcomes anticipated from this review include a clear mission statement; a set of current objectives to accomplish that mission; and criteria for assessing the success of programs and activities.
- A management coach will be assigned to assist MEPO for a 3-month interim period. The management coach and MEPO Director will meet weekly to address management issues such as budgeting and meeting program goals, appropriate hiring and payroll practices, inventory control, proper processing of contracts and selection of program participants.
- MEPO will outline specific objectives for the year as part of the general budgeting planning process. A system modeled on sponsored projects will be implemented to improve planning and budgeting.
- Each responsible program director will prepare detailed budgets that explicitly link expenditures to the activity's programmatic goals and desired outcomes. These detailed budgets will be approved by the MEPO Director. All exceptions to the approved budget must be authorized by the Associate Dean.
- Each major activity will be assigned a unique project/grant so that funds and expenditures can be captured appropriately.
- RPM will conduct post-activity audits to ensure compliance with the original budget.
- The MEPO Director will sign P-Card statements and requisitions, certifying that he has reviewed transactions for appropriateness.
- MEPO staff will receive training about budget and management fundamentals along with a written notice from the Associate Dean regarding the stewardship responsibilities of their positions.
- MEPO staff, like all other CoE staff, will be required to certify that they have read and understand the CoE staff conflict of interest policy and that they are abiding by its tenets. CoE conflict of interest managers will follow CoE's conflict of interest policy by recording and taking steps to manage any potential conflicts that MEPO staff might disclose.
- The MEPO Director will work with MEPO staff to develop a procedures manual to document appropriate administrative practices.
- The Associate Dean, RPM Director and MEPO Director will conduct a resource needs/utilization review, which will include consideration of whether there is a need to appoint either a Unit Administrator or an Associate Director for MEPO.

The CoE plan includes a schedule for regular meetings between the MEPO Director, management coach, programmatic mentor, RPM and Associate Dean. These meetings will help to ensure continued progress toward fulfillment of the management plan and toward improved internal controls for the program, college, and University.

University Audits will perform a follow-up review during the third quarter of fiscal year 2007 to evaluate the implementation of corrective action measures outlined in the CoE management plan.

Issued September 29, 2006

University Audits has completed a review of selected administrative processes that support animal research in five units across campus. The audit was conducted in collaboration with the Office of the Vice President for Research (OVPR) and the Unit for Laboratory Animal Medicine (ULAM). The review included ULAM and four research laboratory units distributed in three departments across campus:

- Department of Pharmacology, Medical School—two units within the department (Pharma 1 and Pharma 2)
- Department of Psychology, College of Literature, Science, and the Arts (Psychology)
- Department of Molecular, Cellular and Developmental Biology, College of Literature, Science, and the Arts (MCDB)

Units were selected to include ULAM and non-ULAM animal care, a variety of species, research drugs, and Medical School and College of Literature, Science, and the Arts departments.

The objective of the audit was to determine the level of assurance provided by internal controls over animal research administrative processes including:

- Animal safety
- Staff safety
- Equipment and supplies inventory
- Controlled drug inventory
- Animal care documentation
- Disaster planning
- Facility security
- Purchasing activity
- Employee timekeeping

Control Issues:

- Controlled Drug Inventory - Drug Enforcement Agency (DEA) controlled drugs used in the research units included cocaine, diazepam (valium), morphine, ketamine and pentobarbital. Two key controls consistently provided a low level of assurance across all five units: maintenance of drug inventory records and transfer of accountability for drug possession.

Inventory Records - Inventory records did not reconcile to drugs on hand in the three units where reconciliation was attempted. Reconciliations are not performed, documented and validated by a second person at periodic intervals in any of the five units reviewed. All five units had drug inventory records that were inaccurate, incomplete or missing. Accountability for controlled drugs cannot be maintained without accurate, validated inventory records.

Transfer of Accountability - There is insufficient transfer of accountability in the chain of drug possession.

- Single individuals receive, open, record, and secure drugs. Without second party validation, there is no assurance that the total amount received is actually secured for research use.
- More than one individual in each unit has independent access to controlled drugs.

These access rights override dual-control, or the requirement for two people to participate in and validate accurate recording of drug removal from secured storage. Drugs could be removed from secure storage without record or timely detection.

- In two of the units reviewed, expired drugs pending pick-up by the Office of Safety and Environmental Health are not adequately secured. They are placed in containers in a hallway or a frequently used closet where multiple department personnel have access. Transfer of accountability for the drugs is not validated by signature of the party assuming custody.

The University has not established guidance or standards for animal research controlled drug inventories similar to standards for other liquid assets like cash and equipment. There is no specific unit charged with providing support and oversight to departments maintaining animal research controlled drug inventories.

Management Plan - The Office of the Vice President for Research, in collaboration with the Medical School, is charging a task force, consisting of representatives from OVPR, the Medical School, University Hospital, ULAM, University Committee on Use and Care of Animals (UCUCA), General Counsel's Office, University Audits and representative faculty investigators to re-design the administrative process for distributing and overseeing controlled substances used in the context of laboratory animals care and research. The Task Force will, in addition, develop guidance for faculty investigators with regard to their responsibilities for security, inventory management, and accountability. The Task Force will be expected to report by the end of the 2006 calendar year.

Action plans have been initiated in the ULAM, MCDB, and Pharmacology Departments. Plans vary by department and include controls to:

- Provide greater assurance that inventory records are maintained on a current basis and are complete and accurate. Inventory record procedures and forms have been implemented or enhanced.
- Reconcile inventory records to drugs on hand periodically and require second party validation. Protocol information is being added to laboratory drug sign-out logs to support random, periodic tracking to research records.
- Strengthen controls for assuring accountability in the chain of controlled drug possession. Units will require two people to open packages of newly acquired drugs and validate accurate recording of them in inventory records, obtain signatures from parties assuming custody of expired drugs for transport and disposal, and review identification for individuals assuming custody of drugs for transport to laboratories. Dual control, or the presence of two people to validate transfer of drugs to or from secure storage, is being implemented where staff resources permit.

Psychology Department management will collaborate with relevant department faculty and staff to research their options further and develop an action plan by the end of October 2006.

- Purchasing Activity

- o Non-ULAM Animal Purchases - Animal purchases made directly through the procurement system rather than through ULAM may not be accounted for against UCUCA approved research protocols and required animal census reporting. In August 2005, routing of non-ULAM animal purchases to UCUCA for pre-approvals was discontinued.

Management Plan - ULAM and UCUCA administrators are working with Michigan Administrative Information Services to obtain routine system reports of non-ULAM animal purchases. A report of non-ULAM purchases made through the procurement system has been completed. A report of P-Card animal purchases will be completed by October 2006. Reports will be e-mailed to UCUCA, prompting a UCUCA request to

the principal investigator for a completed 8225 D form that is used to report animal acquisitions.

- o Purchase and Receipt of Supplies - Roles and responsibilities assigned to department staffs do not ensure that all purchases are appropriate, made available for department use, and agree with purchase documentation.
 - Personnel who have access in the procurement system to make purchases are also responsible for reviewing the statement of activity and for generating a shadow spreadsheet of expenditures that principal investigators review. The risk of diverted assets increases when one person initiates and reviews expenses in the University's procurement system.
 - Supplies delivered to central business office locations may be left for laboratory staff pick up or delivery in unsecured locations. Packages are not signed for when picked up by laboratory staff and contents may not be signature-verified on packing slips and provided to statement of activity reconcilers. The possibility of diverting assets is increased when there is no audit trail of possession or validation of package contents.

Management Plan - Unit action plans are being implemented to improve accountability for purchased goods in the three department business offices with reported issues. Psychology, Pharmacology and MCDB department actions vary and include controls to:

- Ensure more than one person is aware of purchase transactions. Due to limited staff resources in the units, it is not possible to separate access to procurement system purchasing from responsibility for reviewing expenditures on the statement of activity. To reduce the risk of unauthorized purchases, department administrators will perform random sample reviews of purchasing transactions.
- Secure packages until they can be delivered to or picked up by laboratory staff. Specific central business office staff members will sign for purchase deliveries and assume responsibility for them until they are transferred to laboratory staff.
- Provide validated documentation of purchase receipts. Laboratory staff will sign for the purchased items when picked up from the department business office. They will validate package contents to purchase request records and provide documented validation for the statement of activity reconciler.

MCDB will develop procedures for receiving purchased goods as part of implementing a new department purchase order system and process flow. An implementation plan will be proposed in December 2006 and completed in July 2007. Interim procedures for receipt of goods will be determined and implemented by December 2006.

- Animal Facilities and Laboratory Security - Although controls related to animal security are generally effective, there are opportunities to improve physical access security to animal facilities and research laboratories in each of the five units. Strong access controls are especially valuable in environments with relatively high employee turnover engaged in high-risk activities.
 - o Security Access Reviews - Periodic review of security card and key access to animal care facilities and research laboratories is not performed in any of the units to ensure they are assigned to current employees and are appropriate to specific job duties. One department was tested for appropriate assignment of keys and results indicated that at least five terminated employees still had possession of master and sub-master keys. At least two current employees had questionable need for keys. A second department was

uncertain about disposition of master and sub-master keys provided to an administrator who had left the department.

- o Security Card Access - Access to each ULAM facility is not limited to those employees with a need to perform job duties. Due to dispersed animal facilities and technical card limitations, all ULAM staff is granted access to all ULAM facility card readers. Consolidation of facilities to the new, more optimally configured Biomedical Science Building will alleviate some of the dispersion. While flexibility and mobility of animal care staff is important, granting unlimited card access throughout all facilities may not be consistent with security objectives.

Management Plan - Academic departments will initiate different controls including periodic reviews of card and key access, employee exit interview process improvements for reinforcing key returns, and annual combination lock changes. A badge and challenge system is being considered in the Psychology Department to reduce risks associated with student turnover on a semester basis. Other departments will assume any residual risk associated with student turnover. ULAM management will evaluate assignment of employee groups within ULAM to determine which individuals could have more limited access.

- Disaster Planning - Non-ULAM animal care disaster recovery plans were not documented in one unit and required documentation improvements in two others. Failure to maintain a written, detailed plan could result in loss of animals.

Management Plan - During the audit, a disaster recovery plan was documented in one unit and expanded to include more comprehensive detail in the other two units.

Based on audit procedures, animal and staff safety, and equipment and supplies inventory controls are effective. There are opportunities to improve the effectiveness of controls related to purchasing and receipt of goods, facility security, animal care documentation and disaster planning. Animal research drug inventory controls do not provide sufficient assurance that diversion of DEA-controlled drugs would be prevented or promptly identified.

Management Advisory Memorandums with detailed issues and recommendations were issued to ULAM and to each department where the audited research units reside. Management has responded with action plans to address the issues. Follow-up reviews will be conducted to determine the implementation status of individual department action plans and will be reported collectively in January 2007.

Information Technology

UMHHC Biomedical Engineering IT Security

#2006-402

Issued July 12, 2006

This audit was conducted to assess the adequacy and effectiveness of policies, procedures, and control mechanisms in ensuring the security, integrity, and availability of Biomed-managed information systems. The focus of this audit was the Nurse Call system which notifies University of Michigan Hospital nurses when patients need assistance or are in distress.

A project to replace the Nurse Call system with the Responder NET Nurse Call Information System is underway. The new system will have the capability to obtain patient information through its server interface to the Hospital Admission/Discharge/Transfer system (ADT).

Client Discussions:

- Data Security – Based on initial discussion and observation, it was presumed the Nurse Call server retained electronic Protected Health Information (ePHI) obtained through its server interface with the Hospital ADT system. Testing, however, revealed that the Nurse Call system does not contain ePHI. The only patient data in the Nurse Call system are patient name and registration number. All other information directly relates to calls from patient rooms for services.
- Authentication and Password Security – Nursing Administration uses a shared ID to run reports. The new Responder NET software installation will eliminate the need for a shared ID.
- Physical Facility – While the Nurse Call server room in the Biomed area does not meet best practices for computer facility design and construction, the environmental and physical access controls are adequate for the specific needs of this computer.

A review of systems controls will be scheduled for audit after the new Responder NET system is deployed. **This audit is closed.**

UMHHC Security Services/Access Control – Card Access Security

#2006-306

Issued September 8, 2006

An audit of the University of Michigan Hospitals and Health Centers (UMHHC) card Access Control System (ACS) has been completed. Initially, the audit was designed to include campus card access. However, discussions indicated the campus system currently in use will be replaced with the version in use at UMHHC. It was decided to audit UMHHC card access only, at this time.

The ACS is supported by the Security and Entrances Services/Access Control unit. Security and Entrance Services is a division of the University of Michigan Department of Public Safety. The Access Control unit is charged with providing a safe environment for patients, visitors and staff through access control and monitoring of entrances.

The Access Control System controls approximately 494 doors and 50,000 ID cards covering the University Hospital, C.S. Mott and Women's Hospitals, and approximately 24 offsite locations.

The primary audit objective was to determine whether the Access Control System and related procedures protect buildings, contents, and people from damage, theft, disruptions, and unauthorized access and use. Detailed control objectives included determining whether:

- Cards are properly stored, assigned, distributed, and eliminated
- Termination and transfer procedures ensure timely processing
- Data is correctly classified according to sensitivity and secured according to University policy and regulations
- Card usage is tracked, restrictions are applied, and inappropriate activity is resolved
- Monitoring of alarms and backup power contingency enhance safety
- Physical security over the server room is restricted based on job responsibilities
- Logical security over the ACS and database provides protection from unauthorized access and modification
- Vendor access is appropriate and monitored
- Network security is implemented to prevent unauthorized access
- Audit trails provide identification and confirmation of activity
- Backup procedures and retention policies for ACS data are adequate

Control issues:

- Server Security - There are weaknesses in the controls over the Access Control System (ACS) hardware and software compared to generally accepted host security practices such as those

identified by the National Institute of Standards and Technology. Weaknesses can allow unauthorized access and misuse of resources:

- o Neither Security Services who owns the ACS server or MCIT who helped set up the server maintain the integrity of the operating system on this server. No one is assigned responsibility to install and test updates to the operating system. Virus protection exists on the server but is not kept up-to-date. Failure to maintain current software is critical; however, in this installation, the impact of this weakness is partially mitigated. Security Services along with MCIT has created a secure network only allowing hardware registered in the MCIT router table access to the system. In addition, access to the Internet from the server is prevented.
- o Security scans for open services, vulnerabilities, and software patch levels are not performed on the network. Because MCIT equipment is not registered in the router table, their monthly scans do not include the ACS server. UMHS is in the process of writing a policy which will require IT service providers to ensure network scans are performed.
- o The 'superuser' logon account for the operating system is shared by the vendor and most of the authorized Security Services staff. The password for this account has not been changed in two years. There is no ongoing monitoring of use of this account.

Management Plan - Security Services worked with MCIT to set up a secure network. We will investigate options, review risks, and make a decision regarding whether it is necessary to assign responsibility for server maintenance and monitoring.

We will review information on software scanning products including Retina. We will schedule a scan and follow-up on vulnerabilities. We will run scans monthly.

We will assign individual 'superuser' accounts where possible. When vendor projects are completed, necessity for access may be reduced. This would allow restricting vendor access.

- Vendor Remote Access - The vendor responsible for application software and firmware upgrades to ACS, as well as maintenance for controllers and card readers, offers remote diagnostics of problems and error conditions. In order to use the remote vendor diagnostic service, a modem needs to be connected to the server and set on auto-answer in advance of the request. The vendor can dial-in, logon, and provide a password to get to the server. The vendor then has full access to the server and database. Presence of this active modem potentially allows unauthorized dial-up access to the Access Control System server, bypassing network security.

Management Plan - The modem line to the Access Control Server was disconnected. If support is necessary through dial-in, approval to plug in the modem will be granted by the Security Operations Manager on duty. This is now the policy, and it will be written and communicated to appropriate staff.

- Operations Procedures and Cross-training - Written procedures required to administer the ACS application have not been completed. One staff member has much of the responsibility for activities supporting the ACS application, such as programming, setting up access codes and privileges, processing terminations and transfers, coordinating updates with the vendor, and handling backup and recovery. Procedures documenting tasks and responsibilities are necessary.

In the event the staff member was not available for an extended period, it would be helpful to have a user manual including emergency procedures and training guides. According to departmental management, such documentation is on the list of tasks to be accomplished.

Management Plan - Backup exists for some functions and cross-training for other jobs will be completed. We agree an additional person should be trained to process terminations and transfers. Documentation for critical procedures will be completed.

- Security Access Control Policy - Security Services is completing the UMHHC Policy for Security Access Control. This document is well presented and includes policy statements and responsibilities of Hospital employees. Procedures related to use of Mcards and keys are included.

Security Services is also in the process of developing written policies, procedures, and guidelines specifically addressing data security and the Access Control unit.

Management Plan - We agree the need for written policies, procedures and guidelines for Access Control System data exists, and we are currently working on them. Information from the Security Officer Training Tasks manual and orientation material will be used as applicable.

- Facilities Control Center (FCC) Server Room Access - Three administrative staff members of Security Services have access to the room where the Access Control System server is located. Their job responsibilities do not require this access.

Management Plan - Access has been removed. Administrative staff members no longer have access to the server room. University Audits agrees. **This issue is closed.**

- UMHHS relies on the Security Services Access Control unit to grant approved access to UMHHS facilities in a timely manner, prevent access by unauthorized parties, and monitor critical areas for security breaches. Management has implemented controls to address the detailed control objectives of this audit within the ACS application as well as departmental procedures.

In our opinion, management has implemented effective controls within the Access Control System to help ensure the safety of patients, staff, and visitors. The ACS provides a reasonable level of assurance that access to areas protected by this system is authorized and data is available for reporting and monitoring.

A formal follow-up of outstanding issues will be conducted during the third quarter of fiscal year 2007.

UMHHC Pathology IT Security

#2006-401

Issued September 29, 2006

An audit of information security controls related to key departmental information systems has been conducted in the Department of Pathology at the University of Michigan Hospital.

Pathology performs laboratory analysis of medical specimens for the University of Michigan Health System (UMHS) and non-University health care providers. Orders and results are collected, managed, and distributed through a series of processes centered on a Laboratory Information System (LIS). The LIS is critical to Pathology's mission.

The Pathology Data Systems group (PDS) manages all non-research information technology assets in the department, including the LIS and a number of subsidiary systems. Two of these subsidiary systems are the Citrix servers, providing remote LIS access; and script servers, a data processing engine for lab results. Other systems extract and analyze LIS data, and route reports to electronic patient files and to physicians. All of these systems retain or process Electronic Protected Health Information (ePHI), which requires strong security measures. The LIS interfaces directly with partner hospitals Toledo, Mount Clemens, and Botsford.

Our objective was to assess the effectiveness of policies, procedures, and control mechanisms in ensuring the security, integrity, and availability of several key Pathology information and support systems. These are the LIS, file servers, Citrix servers, and script server.

Based on the analysis of potential risk and the requirements of these policies, the internal controls evaluated were:

- User authorization and termination
- User classification
- User account management
- Physical access control
- Disposal of computers and storage media
- System access control
- Transmission access control
- Authentication
- Password control

Control issues:

- Control of server room access - The Pathology server room can be accessed without a key or keycard during business hours (7am - 5pm, Monday through Friday).

The server room's front door is accessed through the lobby of the Pathology Data Systems (PDS) suite, and is unlocked for convenience while PDS staff are present. The outer entrance to the suite has a proximity card reader that is deactivated during business hours to allow non-IT Pathology staff to enter the lobby for assistance.

Specific PDS staff members are assigned to monitor the lobby area and the server room for visitors and intruders. The server room's front door is locked with a key when there is no one to watch it. These actions provide a minimum level of access control, but could be improved with the addition of a locked-down proximity card reader to the server room's front door.

The server room's back door already has a proximity card reader configured identically to the lobby reader, but locked down 24 hours a day 7 days a week. Pathology requested a reader for the server room's front door six to eight months ago, but no work order was ever issued.

Management Plan - The Pathology server room is being remodeled. After remodeling, the server room will have a single entrance secured by a card reader. To more immediately mitigate the risk, Pathology will install an electronic combination lock on the server room's front door. The combination will be known only to PDS staff.

- Periodic review of card reader access - Pathology Data Systems (PDS) has conducted one review of their facility's card reader access list with the assistance of the Hospital Key Office. Management indicated that such a review could be conducted every six months, and formal procedures developed to support it.

This plan would comply with Section IV.A.8 of the supplement to UMHS 01-04-500 *Security of Information Systems*, which requires that locks and card readers on computer facility entrances be audited bi-annually to ensure current authorizations.

Management Plan - PDS will work with the Hospital security team to establish a periodic review of card reader access.

- LIS password controls - The VMS operating system version on which the Laboratory Information System (LIS) is based does not differentiate between upper and lower case in passwords. This dramatically reduces the number of character combinations possible for LIS account passwords, increasing the system's susceptibility to password cracking attempts.

The risk may be partially mitigated by network access controls preventing LIS connection attempts from outside the UMHS network. These controls have not been tested by University Audits.

Management Plan - Pathology concurs with the recommendation, but must accept the risk at this time. The department is currently evaluating replacement options for the LIS that will enforce strong, case sensitive passwords.

Implementing case sensitivity in the current LIS would require either upgrading the VMS operating system or switching to external authentication such as Kerberos, both of which are expensive undertakings. Upgrading VMS would require recertifying all of the LIS software components and interfaces. External authentication is technically complex and requires extensive study and planning, procedural changes, and staff retraining. Either option would compete heavily for resources with the LIS replacement project, which is the highest priority and will ultimately resolve the issue.

Auditor's Comments: Pathology is accepting a reasonable amount of risk. University Audits accepts this response, but will follow-up informally to verify that the replacement LIS resolves the issue. **This item is closed.**

The audit identified several areas where internal controls supporting information security can be improved. Many other controls, including the overall management of accounts and the secure disposal of computers, were found to be adequate and effective. A follow-up to the outstanding issues will be conducted in the third quarter of fiscal year 2007.

Medical School Anesthesiology IT Security

#2006-404

Issued September 29, 2006

The Department of Anesthesiology is a unit of the U-M Medical School responsible for delivering anesthesia to patients of the University of Michigan Hospitals and Health Centers. Anesthesiology works closely with the Emergency Department and Trauma Burn Center at U-M Hospital (UMH). These departments share a patient information system built on GE Centricity software.

Centricity—also referred to as MorCARE—is a generalized clinical information system. It provides a central data collection and tracking point for patients requiring Anesthesia, Emergency Department, or Trauma Burn services. The system stores data from monitoring and metering devices, physician notes, as well as consents, scanned documents, and casework. Information is used for research, data mining, and initiatives to improve patient care, as well as documentation for billing. A second system generates reports containing Centricity data for department users.

Anesthesiology's Clinical Application Services team (CAS) manages Centricity and related systems. CAS also develops and maintains clinical computer workstations in the inpatient units, operating

rooms, and other areas that are used to access Centricity and other UMHS clinical systems like CareWeb. All of these systems retain or process Electronic Protected Health Information (ePHI).

The critical Centricity databases are housed in the Taubman Machine Room operated by Medical Center Information Technology (MCIT). Remaining servers, including less critical Centricity components, are housed in an Anesthesiology server room. CAS is constructing a companion server room to allow redundancy and improved assurance of system availability.

Our objective was to assess the effectiveness of policies, procedures, and control mechanisms in ensuring the security, integrity, and availability of Anesthesiology's Centricity information system and clinical image workstations. The internal controls evaluated were:

- User authorization and termination
- User classification
- User account management
- Emergency preparedness
- Physical access control
- Workstation maintenance and security
- Disposal of systems and storage media
- System access control
- Authentication
- Password control
- Audit trails

Control issues:

- Storage of social security numbers - Patients' Social Security numbers (SSNs) are stored in Centricity, but there is no known business, clinical, or research use for them in this system.

The client indicated that Centricity receives and stores patients' SSNs from the Hospital Admit / Discharge / Transfer system (ADT). Clinical Application Services (CAS) is not aware of any current research use of this SSN data. They indicated that the vendor would need to provide technical assistance to disable the SSN feed and remove the data.

Management Plan - A written request has been submitted to the vendor to facilitate the SSN removal from the Centricity database. The vendor has provided the proper method to remove SSNs and disable them in the HL7 feed. This method is being tested and verified through a test system before implementing in production.

- Physical access control - Both existing and newly adapted server rooms are secured by physical keys with strictly limited distribution. While these access controls are adequate, the installation of proximity card readers would reduce risk exposure due to theft or copying of keys. It would also allow management to periodically obtain and review a definitive list of individuals with access to the rooms.

Additionally there is currently no mechanism for recording entrance and exit of individuals to and from the server rooms. Proximity card readers would also provide reliable audit trails of staff entrances and exits.

Management Plan - A proposal for installing card readers has been submitted to Anesthesiology administration. CAS is obtaining cost and scheduling estimates from UMHS Facilities to support the action.

- Physical locks on workstations - Workstations managed by Clinical Application Services (CAS) in areas categorized by the institution as "UMHS Public" are not consistently secured

against theft. In some of these areas the workstations are secured in locked cabinets; in others there are no retention devices.

According to UMHS Workstation Physical Location Guidelines posted by the UMHS Compliance Office, UMHS Public locations include inpatient rooms, exam rooms, and Emergency Department bays—all of which have CAS clinical image workstations.

Workstations not continuously attended in UMHS Public areas should be physically secured against theft when unattended, as required by Section IV.C of the supplement to UMHS 01-04-500 *Security of Information Systems*.

Management Plan - CAS will evaluate the proper locking mechanisms for clinical image workstations in the designated UMHS Public areas. Once the proper locks have been identified, requests will be submitted to purchase and install them.

The audit identified several areas where internal controls supporting information security can be improved. Many other controls, including workstation restrictions, the overall management of accounts, and the secure disposal of computers, were found to be appropriate and effective.

A formal follow-up to the outstanding issues will be conducted in the third quarter of fiscal year 2007.

Healthcare

UMHHC Vendor Discounts, Allowances, and Rebates

#2006-119

Issued July 19, 2006

Medicare reimbursement principles require providers to report all discounts, allowances, and refunds of expenses as reductions in costs on the annual provider cost report. Medicare prohibits providers from reporting discounts, allowances, and refunds as income if this results in an overstatement of allowable costs. University Audits performed an audit to determine whether costs reported on the 2005 Medicare cost report were overstated as a result of misclassifying expense reimbursements. Included in the review were:

- Fiscal year 2005 cash receipt transactions classified as other revenue
- An evaluation of certain Medicare cost reporting practices to determine whether the annual provider cost report is completed in accordance with Medicare reimbursement principles
- Procedures for processing and recording expense reimbursements in the Pharmacy, Materiel Services, Radiology, and UMH Purchasing departments
- UMH draft policy on Vendor Rebates

Control Issue:

- Depositing – Standard Practice Guide section 502.1 requires departments to deposit checks and cash on the date of collection. In fiscal year 2005, the Pharmacy department received 106 expense reimbursement checks. The average number of days from the check date until deposit was 30; the total number of days to process deposits ranged from 2 to 147.

Management Plan – Staff members have started contacting vendors who process vendor rebates. Vendors are asked to send all remittances to the UMHHC purchasing department.

Medicare cost reporting practices used by the Reimbursement and Appeals Office adequately mitigate the risk of overstating expenditures on the Medicare Cost Report. Vendor rebates and other discounts were included in non-patient other revenue. Expenditures are reported net of other revenue on the Cost Report. University Audits will conduct a follow-up review of the one open issue during the second quarter of fiscal year 2007.

An audit of the adequacy and security of the Materiel Services Center (MSC) receiving and warehousing functions was conducted for fiscal year 2006. Materiel Services is part of the University of Michigan Health System (UMHS) Operations and Support Services Division and reports to the Associate Director of Operations and Support Services. The MSC is responsible for receipt, storage and transfer of goods to Hospital departments.

The audit focused on the following controls:

- Goods received are properly authorized and recorded accurately and promptly
- Quality control over goods received ensures that goods are properly and accurately inspected and goods not meeting specifications are properly rejected
- Goods stored in the warehouse are safeguarded against damage or theft
- Environmental controls in the warehouse, control access to inventory and provide a safe work environment for MSC staff
- Transfer of items to UMHS units provides timely and accurate delivery of both inventoried and non-stock items

Audit procedures included:

- Interviews conducted with staff in Dock 5 receiving, MSC Customer Service, Transactional Purchasing and Warehousing to understand MSC process and evaluate risk
- Review of segregation of duties to determine that MSC employees receiving goods are not authorized to purchase goods
- Observation of physical receipt of inventory at Dock 5 to determine:
 - Goods are properly inspected
 - Receiving reports are accounted for properly
- Assessment of working and safety conditions on the dock and in the warehouse
- Review of the annual physical inventory and related reconciliation to assess the inventory control process
- Examination of the formal contingency plan to assure that it adequately addresses disruption in service
- A test of items received to determine if they were:
 - Supported by a properly executed purchase order
 - Properly entered into M-Pathways receiving and inventory records
- A test count of inventory items was performed and reconciled with the M-Pathways inventory system
- A sample test of transfers of items to UMHS units was tested to assess the appropriateness of accounting and documentation

Control Issues:

- Formal Authorization for Receivers of Goods - Authorization of MSC employees authorized to receive goods is not formally documented. Goods are received by dock staff until 3:30 PM and by supervisors after 3:30 PM. If discrepancies arise between vendors and UMHS regarding receipt of goods and subsequent payment of invoices, the receivers of such goods should be accountable. With no formal authorization, accountability is not established.

Management Plan - Materiel Services will develop a list of all department staff authorized to receive goods. In addition, the Warehouse Operations Supervisor will develop a training/competency document on receiving processes. This will be reviewed with all department staff who may receive goods. Materiel Services will use the M-learning tool for tracking and verification of whom is authorized to receive goods.

- Physical Access to Dock 5 - Dock 5 receives all major items for University Hospital, the Taubman Health Care Center and the Cancer and Geriatric Center. It is located on the north side of University Hospital on the B-2 level. Access to Dock 5 is not being properly limited to MSC staff authorized to receive goods. Because of its location between the parking lots and the main entrance, the doors to Dock 5 are being used by Hospital employees as a staff entrance. This represents a potential safety hazard because at times of heavy activity, there are pallets, boxes and other items on the dock. Because the doors are being used for staff entry and exit, the increased foot traffic on the dock raises the risk of items disappearing from the dock or the warehouse.

Management Plan - A Planning and Investigation request to determine the feasibility to create an employee entrance/exit on the north side of the building has been submitted to the UMH Facilities Projects department. An idea being explored is to establish an employee entrance/exit on level B1. In the interim, additional signage will be installed and Materiel Services will follow up with Security to control and monitor dock traffic.

- Accounting for Receiving Reports - Since non-stock goods are not inventoried, a receiving report prepared indicating the delivery address provides the sole evidence that the goods have been received. These receiving reports are not pre-numbered. Pre-numbered receiving reports provide a trail to confirm deliveries and verify compliance with established procedures. Without pre-numbering of receiving reports, it is much more difficult to locate a specific report if a delivery is questioned and to account for all reports. Pre-numbered receiving reports should be reconciled on a regular basis and any missing reports should be investigated.

Management Plan - Materiel Services will order pre-numbered receiving forms and implement. Staff will also be instructed on how to void incorrect forms to ensure that all numbered forms are accounted for.

- Inventory Cycle Counts - During our test count of inventory items, four of ten items had a variance of greater than 5%. MSC policy states that any deviation over 5% is unacceptable. Our test count of ten items yielded four items where counts were more than 5% lower than recorded units in M-Pathways, six were within acceptable variance rate from what was in M-Pathways. These items are low dollar, high volume items. The discrepancies noted most likely represent "mispicks" caused by stockkeeper choosing either the wrong count or the wrong item.

A complete physical inventory is conducted annually by MSC. This count was taken on June 17, 2006, resulting in a count which was .4% higher (in units) than the amount listed in M-Pathways. Due to the volume and type of goods, and in light of the results of the physical inventory, the chance that the undercounts were the result of theft was minimal.

Management Plan - Materiel Services is developing a plan and re-structuring its work assignments in order to initiate a cycle count process.

Based on the audit work conducted, University Audits found the MSC receiving and warehouse processes to be well controlled. MSC management is focused on creating a strong control environment. Goods received are properly authorized, supported by purchase orders, and accounted for on an accurate and timely basis. Upon receipt, goods are inspected and items not meeting specifications are rejected. The MSC warehouse is safeguarded against damage or theft and provides a safe work environment. Items transferred to UMHS units are delivered accurately and timely.

University Audits will conduct a formal follow-up review during the third quarter of fiscal year 2007 to review the implementation of process changes to further strengthen the control environment for MSC receiving and warehouse functions.

FOLLOW-UP REPORTS

Michigan Public Media – Phase I

Original Report issued March 24, 2006

#2006-806

Follow-up Report issued July 31, 2006

The Michigan Public Media Phase I audit report was issued on March 24, 2006. University Audits has completed a follow-up review of the status of corrective actions on the audit recommendations.

The audit was performed at the request of the Department of Public Safety and senior management in response to allegations of improprieties associated with in-kind trade underwriting agreements. The audit was the first of two audits conducted to evaluate the adequacy and effectiveness of key internal controls within the organization.

The status of the audit issues and actions taken to strengthen the internal control environment surrounding each area of significant control weaknesses identified in the original Phase I report is outlined below.

Oversight and Accountability of In-Kind Trade Agreements

Policies and procedures have been developed to support a much stronger internal control structure as it pertains to underwriting agreements which include in-kind trade.

- Michigan Public Media has established and implemented a new underwriting policy that has been in effect since June 1, 2006. The policy outlines specific procedures that include approval, authorization, rate setting, restrictions and provisions, utilization of standard forms, and contract retention. All policies will be reviewed on an annual basis and modified as changes are needed to ensure adequate internal controls.
- A new gift and gratuity policy has been established. Every employee is required to review and sign a copy of the policy attesting to their understanding. Signed copies are maintained in each employee's personnel file.
- A conflict of interest form has been established. The target date has been set for September 2006 for submission of all signed conflict of interest forms.

Tracking mechanisms have been established for recording actual utilization of the trade through the use of Delta Flex for Radio and other planned excel spreadsheets for Television. Management has gone a step further by looking into a trade log to be implemented and included as part of their reported financials on trade usage.

Each policy and procedure has been shared and discussed with all staff at Michigan Public Media. While sound controls are now in place and appear to be working, University Audits will conduct an additional follow-up review during November 2006 to ensure that there is consistent and appropriate application of these controls. This review will include limited testing of transactions.

Management of On-Air Announcements

- Michigan Public Media has completed and established an underwriting policy for on-air announcement time. A broadcast order form has been developed and is currently used by staff to record and track on-air credits.
- Continuity request forms used for the request of airtime are now completed and approved prior to submission.
- Management has established a new rate card system and restricts employees from formal bidding with clients. Rates will be communicated and negotiated by management only.

The policy will be reviewed annually to ensure adequate controls are added if needed. Periodic monitoring will occur to ensure compliance with new procedures established. All staff has been appropriately trained and has received communication regarding authorized practices. University Audits will conduct a limited review during November 2006 to ensure appropriate application of established procedures.

Bonus Payments

- Michigan Public Media has established a new bonus policy that will be implemented in FY07. The new bonus structure has been reviewed and approved by General Counsel and Human Resource personnel. Per policy, new offer letters will be presented and signed by employees for FY07.

Management will be reviewing the bonus structure annually to ensure that necessary adjustments are made as needed. Standard evaluations will be maintained on file to support bonus and other performance measures. Evaluation documentation will be maintained in each employee's file. University Audits will review a limited sample of offer letters and evaluations made during FY 07.

Purchasing and Inventory

- Michigan Public Media has revised and communicated their purchasing guidelines effective April 5, 2006. All staff will be trained effective July 31, 2006. Inventory recording mechanisms have been tightened; however, additional control procedures are planned for implementation. University Audits will review a limited sample of purchasing and inventory transactions to ensure compliance with revised policies.

Appropriate Documentation and Oversight of Expenses

- Michigan Public Media has revised and communicated P-Card guidelines to all P-Card holders, reconcilers, and supervisors. Management has obtained signed attestations from all staff regarding their understanding of P-Card Guidelines. These attestations are maintained in each employee's personnel file.

A copy of the revised P-Card guidelines has been provided for Audits review and outline guidance relating to P-Card holder responsibilities and procedures specific to Michigan Public Media. The policy now requires receipts for every expense regardless of the dollar amount. Meal expenses have been reduced (breakfast and lunch \$20 and dinner \$45). Management will review policies and procedures annually to ensure controls are added as necessary to ensure compliance. Training and education will be provided by July 31, 2006.

Michigan Public Media continues to engage in improving business operations. All policies are available on the Michigan Public Media's shared drive and accessibility has been communicated to all staff. A second follow-up review of Phase I issues will be conducted during November 2006 to substantiate that all policies and procedures are working well. That review will include limited testing of transactions to confirm that Michigan Public Media processes reflect the newly implemented policies and procedures.

Gerald R. Ford School of Public Policy

Original Report issued March 27, 2006

#2005-219

Follow-up Report issued September 29, 2006

- Purchases Over \$5,000 Threshold: University Audits' Review of Ford School's revised purchasing policy, indicated that it adequately strengthened purchasing practices. Management will communicate the revised policy to key staff and update its Faculty and Staff Handbook after the executive committee and senior staff members finalize the policy. The business & grants manager reviews vendor reports to ensure that faculty and staff members adhere to Ford School and University purchasing guidelines. **Closed.**
- Managing Research Projects: Ford School's administrative office has oversight responsibility for the centers co-sponsored by the school that focus on specific policy concerns. Ford School

administrators plan to increase their oversight over these research centers to provide better control of the centers' resources. Ford School management is in the process of defining the scope of their review of research center activity. Management requested that University Audits provide guidance to help define the scope. University Audits personnel met with Ford School administrators to provide risk assessment information. **Closed.**

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

School of Information

Original Report issued May 1, 2006

#2005-215, 315

Follow-up Report Issued July 31, 2006

- Imprest Cash Reconciliation - Surprise cash counts are being conducted on a quarterly basis by an independent person. **Closed**
- Monitoring Computer Resources - A reference to the University policy regarding personal use of University resources was added to the Administrative Rights Service Level Agreement (SLA). Everyone signing the SLA will be reminded of their responsibility regarding installing software on the School of Information owned machines. **Closed**
- Data Security - A Data Security Policy was developed based on management needs. Review of this policy indicated that it properly addresses the issue of protecting institutional data. This policy is awaiting approval by the dean. **Closed**
- Information Technology Threat Assessment - IT management is working closely with Information Technology Security Services (ITSS) on the IT security assessment. One system administrator was sent to the ITSS security training; the IT manager has assumed the role of the School of Information security liaison. The security liaison develops security assessment plans for School of Information departments under the direction of ITSS. At its completion, the plan will be forwarded to University Audits. **Closed**
- Backup and Recovery - Backup and recovery plans have been developed and are awaiting approval by the School of Information deans. These plans adequately address the issue of responding to an emergency, or other occurrences of damage to systems containing institutional data. **Closed**
- Departmental Policy Manual - School of Information management continues to work on the development a policy manual. Several policies have been drafted which will be made available to faculty and staff through the intranet in the near future. University Audits will continue to monitor this issue informally, but the School of Information is committed to completing this policy manual. **Closed**

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

University Audits – University of Michigan
Open Audits Follow-up Table
September 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
Web Grade Entry 2006-103	3/16/06	Completing a detailed review of access roles and privileges to Student Records	October 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
Professional Fee Billing Compliance 2005-126	12/22/05	New organizational structure is been established; additional controls are being implemented	November 2006
UMHS MLabs 2006-112	1/19/06	Management is implementing corrective action measures	October 2006
UMHHC Vendor Visitation 2006-118	1/30/06	Compliance Office drafting policies and procedures	October 2006
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
MCIT Financial Internal Control Assessment 2005-367	6/16/06	Only open issue relates to safeguarding assets	October 2006
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
Parking Services 2006-202, 2022	1/06/06	Documentation is nearly complete: significant changes in leadership; management is re-evaluating processes	November 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 November 2006
Michigan Public Media Phase II 2006-806	4/24/06	Significant reorganization and implementation of control policies and procedures is in progress	October 2006
Counseling and Psychological Services Purchasing Controls 2006-809	5/12/06	Will be conducting a broader review including other departments under Student Affairs	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	November 2006
Library Special Collections 2006-205	6/16/06	Library administration is working to strength 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	December 2006
Intercollegiate Athletics Booster Clubs 2006-812	8/3/06	The Articles of Association for the U-M Club of Greater Detroit should be revised to reflect that dues are not required but members must belong to the U-M Alumni Association	November 2006
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

