UNIVERSITY OF MICHIGAN

**REGENTS COMMUNICATION**

Received by the Regents
February 17, 2011

**Item for Information**

Subject: Report of University Internal Audits
**September through November 2010**

Background:

This is the report of the Office of University Audits activities for the period **September through November 2010**. The summaries of audits contained in this report were previously reported to members of the Regents' Finance, Audit and Investment Committee and included in discussions at Committee meetings.

Included in this report:

- Summaries of each audit report issued during the period, including Management's Plan to enhance specific control processes discussed with the audit client and presented in the report.
- Summaries of follow-up review reports issued during the period, including the actions taken by Management. Follow-up reviews are designed to give assurance that Management's Plan for corrective action has been implemented and controls are working appropriately.
- A report on the status of follow-up reviews as of **November 30, 2010**.

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

Respectfully submitted,

Carol F. Senneff, Executive Director
University Audits

University Audits
September - November 2010
Summary of Reports Issued

## ORIGINAL REPORTS

### *Campus*

University of Michigan-Flint Genesee Early College Program #2010-114
Report issued October 1, 2010

In 2006, Michigan Governor Jennifer Granholm and the Michigan Department of Education unveiled grants that would allow high school students the opportunity to pursue careers in health professions in a collegiate environment. The following year, UM-Flint partnered with the Genesee Intermediate School District (GISD), a regional service agency that supports students and schools in Genesee County's twenty-one school districts, to establish the Genesee Early College program (GEC) as a recipient of the State's grants. UM-Flint provides financial, academic, and administrative support for GEC students.

The GEC is a five-year program (grades nine through thirteen). In grades nine and ten, students take classes from GEC teachers in dedicated GEC classrooms on UM-Flint's campus. Starting in the eleventh grade, students enroll in general UM-Flint courses, intermingled with the regular student population. Upon completion of the program students will have not only their high school diploma, but up to 60 college credits. GEC is managed by the GISD Superintendent and a Principal, assigned by GISD. A K-12 Coordinator, located in UM-Flint's Office of the Associate Provost and Graduate Programs, serves as the liaison between the GEC and UM-Flint.

The GEC program is now in its third year and has graduated 38 of the original 39 eleventh graders who started the program. Each year the GEC has expanded enrollment to additional grade levels and is now enrolling ninth graders. Capacity for the program has been established at a maximum of 80 students in each grade level.

The purpose of this audit was to evaluate UM-Flint's processes that support the GEC program. Specifically, the review of the GEC included:

- Access to UM information systems and technology
- Student safety
- Admissions and enrollment to UM-Flint for GEC students
- Legal obligations
- Program metrics and reporting
- Financial oversight

**Risk and Control Discussion:**

1. Updating Formal/Informal Agreements - **T**here is no approved agreement documenting the partnership between UM-Flint and the GISD; the agreement is still in draft form. Certain provisions were omitted or may have changed. For example,
    - The draft agreement states the GEC will not receive keys for UM facilities, but the Associate Provost now authorizes key access for the GEC classrooms in the William White building.
    - There is no clear definition of the "underserved" qualifier for GEC enrollment.
    - There is no requirement for consultation from both the GISD and UM-Flint on any proposed modifications to GEC procedures.

- There is no provision allowing both parties to review any advertisements regarding the GEC program prior to print and distribution.
- The roles and responsibilities of the GEC Advisory Board are not documented.

**Management Plan -** The K-12 Coordinator will oversee creation of additional language and/or attachments for inclusion in the agreement. These will describe duties or responsibilities of the parties in specified areas not addressed in the draft agreement:

- Coordination of advising roles - The Advising Director will convene a meeting to include GEC personnel for the purpose of creating an advising flowchart for GEC students.
- Management of UM-Flint student employees assigned to GEC - An Administrative Specialist within the Associate Provost's Office will work with the GEC to develop a flowchart describing responsibilities and time frames.
- Mutual right to preview documents - Management has prepared language for the agreement that describes the rights of both parties to preview any GEC documents for clarity and factual accuracy. The language has been approved by the Associate Provost and the GEC Principal and inserted into the draft agreement.
- GEC will be responsible for issuing and collecting UM-keys through management of their employee turnover (UM-Flint DPS tracks keys issued to GEC, but not individuals).

The updated agreement will be forwarded to the Office of the General Counsel for review prior to obtaining signatures from UM-Flint and GISD officials. In addition, the Associate Provost and the GISD Superintendent met mid-September. As part of this meeting, a process for systematic communication and review of the quality of the program between the GISD and UM-Flint's top leadership will be discussed.

2. Reportable Data and Metrics - Employees from both GISD and UM-Flint have expressed satisfaction with the GEC program and believe it is achieving the original partnership's goals. However, there is a need for reporting that validates these achievements.

   **Management Plan -** The K-12 Coordinator will facilitate a series of meetings to identify required or desired data needs and develop a long-range plan for data maintenance and analysis. These meetings will include appropriate representation from the GISD, the GEC, and relevant UM-Flint offices and academic divisions. As an outcome of these sessions, a leadership team (including representation from GISD and UM-Flint) will be identified and empowered to study various options, identify cost implications, and develop a feasible plan of action. This leadership team will work in consultation with pertinent advisory boards and administrators. In addition to considering local data analysis options, the leadership team will explore data analysis services available via the Middle College National Consortium, and determine what role that organization might play in GEC data analysis. The leadership team will submit a draft of the final proposed plan, including cost implications, to the Provost and GISD superintendent or designees for approval.

3. Information Technology Management
   3.1 Approval for UM Access - Non-UM employees have been given access to Banner, the University's system for student records management. UM-Flint's Associate Provost originally approved access specifically for one GEC employee to facilitate the process of adding and removing registration holds on GEC student accounts. These holds freeze a student's account to ensure students do not enroll in non-GEC approved courses and must

be lifted and re-added during each semester's registration process. When UM-Flint ITS received approval to give this access, they created a GEC department classification within the Online Access Request System and listed the GEC Principal as the department head. Using that authorization, the Principal approved Banner access for two other GEC employees. Only UM employees should authorize access to UM systems.

In addition, one employee was given access to Banner as a secondary back-up and has not yet needed to use that access. This suggests access may be unnecessary.

**Management Plan -** The ITS Director has changed the department head within the access request system. The Associate Provost is now designated, for ITS purposes, as the department head of GEC.

Management will review all GEC employees with Banner access; the secretary's access to Banner will be evaluated. The UM-Flint Advising Office will be contacted to determine if they would be a feasible back-up for modifying student holds.

3.2 Monitoring Banner Activity - Some GEC employees have been given access to student records in Banner, which was approved by the Associate Provost. Nevertheless, it is unusual for an external organization to have this type of access. An increased monitoring of GEC employees' activity within Banner would provide assurance that access is used only as intended.

UM-Flint ITS can activate a detailed audit log for each GEC employee with Banner access. This log will capture all records accessed by the GEC employees and can be e-mailed to the Provost's Office or designee.

**Management Plan -** ITS will be requested to enable Banner tracking for GEC employees and provide audit logs at three-month intervals. The Associate Provost will review the log to ensure appropriate use of Banner, and will sign and date the report as evidence of the control. The logs will be stored in the Office of the Associate Provost.

3.3 Access to ITS Computer Lab - GEC was issued a sub-master key for their classrooms in the William White building. This sub-master also opens two doors to an ITS-managed student computer lab, located near the GEC classrooms. There is no business purpose for GEC administrators to have access to this lab.

**Management Plan -** A DPS administrator will issue a work order to eliminate GEC access to the computer lab in question. At the same time, a new key will be issued that will open the principal's office only, in order to have the work order address all key-related GEC requests.

*Auditor's Note: GEC administrators were unaware their key could open the ITS lab. The discovery was made by verifying key codes with DPS for the keys issued to GEC.*

3.4 GEC Access to Student Passwords - GEC administrators collect their students' passwords for the Student Information System (SIS). SIS is a UM system used by students to monitor their academic progress, including registration and enrollment, transcripts, and current course syllabi. GEC administrators keep these passwords for access to student records during the students' advising appointments as a precautionary measure, in case the students

forget their password. Sharing of passwords is against the UM-Flint IT access policy and a violation of UM's Student Rights and Responsibilities.

**Management Plan -** UM-Flint and GEC officials recently outlined a process by which forgetful GEC students can quickly establish a new PIN without the need to postpone a scheduled counseling/advising session in order to report in person to ITS. A more detailed description will be prepared by UM-Flint and forwarded to GEC. There is an additional option being considered; whereby a student can authorize access by others to specific sections of SIS. UM-Flint officials will verify with ITS how this access can be granted. Both solutions will be reviewed by the K-12 Coordinator, in concert with GEC representatives, to determine the ultimate resolution.

*Auditor's Note: GEC administrators were shredding stored passwords at the end of each academic year.*

3.5 GEC Sign-off on Access and Compliance Form - As non-UM employees, GEC employees with access to UM systems are less likely to be aware of changes to UM's IT security policies or other UM security best practices. This may increase the risks of inadvertent disclosure of sensitive information. Any GEC employee with access to UM systems should review and sign UM-Flint's IT Access and Compliance Form, annually. The forms can be maintained in the Provost's Office or other designated area.

**Management Plan - GEC** leadership has reviewed the IT security policy and agreed this would not impose an administrative burden. Each September, a list of GEC employees will be provided to the Associate Provost's Office. An administrator will prepare a personalized copy of the security policy form and forward them to GEC. Signed forms will be returned for filing in the Associate Provost's Office.

4. Employment Controls for Student Temporary Employees - The GEC and UM-Flint share supervisory tasks for UM-Flint student employees working as GEC tutors. University Audits reviewed the employment process and noted the following:
    - The GEC has been delegated the responsibility to collect timesheets for the student employees; however the actual timesheets are not retained. An administrator in the Associate Provost's Office receives a summarized spreadsheet to enter the student employees' time into M-Pathways. The spreadsheet is also used to reconcile the Gross Pay Register by an accountant in the Provost's Office.
    - SPG Section 201.24*, Employment of Students*, requires that an applicant's student status be verified before offering student employment. Currently, no one is verifying the enrollment status for student employees working as GEC tutors.

**Management Plan -** The GEC will send original signed timesheets to the Associate Provost's Office via interdepartmental mail. If signed timesheets are unable to be delivered timely, the office will accept faxed copies of signed timesheets and the originals will then be mailed. The original timesheets will be retained in compliance with University policy.

An administrator in the Associate Provost's Office will verify the enrollment status of proposed student tutors during the hiring process each fall. Enrollment status will be re-verified at the beginning of the winter semester.

These procedures will be included in the flowcharts used to document GEC processes.

5. University Obligations for K-12 Students - There are many state and federal laws that apply to K-12 educators, but possibly not to higher education institutions (e.g., criminal background checks for educators). It is critical that administrators at UM-Flint have a clear understanding of any legal obligations that pertain to the education of GEC high school students. It is important that UM-Flint seek guidance from the Office of the General Counsel regarding responsibilities and restrictions under federal and state K-12 laws, and determine if any additional safeguards or legal measures should be taken.

   **Management Plan** - The Associate Provost will contact the Office of the General Counsel to discuss dual-enrolled students and how best to mitigate related risks.

The Genesee Early College (GEC) program, a collaboration between the University of Michigan-Flint and the Genesee Intermediate School District, was designed as an alternative high school that would encourage students to pursue careers in medical fields. GEC caters to students who are not currently well-served in their home district, either due to economic or social restraints.

As the program is growing in enrollment, this is an opportune time to evaluate the partnership. Clarifying some aspects of the arrangement, in addition to documenting routine business procedures, will allow both UM-Flint and the GISD to have a clear understanding of their roles and responsibilities. University Audits will evaluate the status of these procedures during a follow-up review, scheduled for the third quarter of fiscal year 2011.

Division of Research Development and Administration Export Controls Compliance #2010-402
Report issued October 21, 2010

**Background on Export Controls**
Export controls are federal laws that regulate the export of strategically important technology, services, and information. These regulations were instituted for reasons of United States foreign policy, national security, anti-terrorism, and non-proliferation. Export control rules have existed for decades, but the level of awareness and federal regulatory focus has increased since September 2001. The emergence of intensified technological development programs in countries that are not traditional United States allies has also increased public awareness.

The term "export" applies not only to the shipping or hand carrying of materials, products, or funds to overseas locations, but also to the transmission of technological knowledge, information, data, or computer software to foreign nationals. A foreign national is defined as any person who is not a lawful citizen or permanent resident of the United States, any foreign corporation or other entity or group that is not incorporated or organized to do business in the United States, and any foreign government. Transmission of items or information to foreign nationals on U.S. soil is also deemed to be an export.

**Regulatory Framework**
There are three primary sets of export control regulations:

- *International Traffic in Arms Regulations (ITAR)*[1]. ITAR is administered by the Department of State and controls the export of defense articles, defense services, and related technical data listed on the United States Munitions List. Military technology includes weapons, explosives, chemical and biological agents, military vehicles, missiles, aircrafts, and associated equipment, and satellites.

[1] U.S. Department of State, Regulations and Laws, International Traffic in Arms Regulations, http://pmddtc.state.gov/regulations_laws/itar_official.html (accessed September 29, 2010).

- *Export Administration Regulations (EAR)*[2]. EAR is administered by the Department of Commerce and controls the export of non-military technologies and commercial items that may have potential military applications, otherwise known as "dual-use" technology.
- *Office of Foreign Assets Control (OFAC)*[3]. OFAC, a federal agency under the Department of the Treasury, administers and enforces economic trade sanctions, boycotts, and embargoes against targeted foreign countries, entities, and individuals. OFAC may prohibit travel to, and other activities with, embargoed countries and individuals even when ITAR and EAR regulations do not apply.

In addition to the above regulations, there are some other federal agencies that regulate the export of specific items or materials. They include the Department of Energy and the Nuclear Regulatory Commission, among others. However, ITAR, EAR, and OFAC are the key regulations of federal export control legislation.

In August 2010, the White House administration announced a major step forward in the efforts to fundamentally reform the United States export control system. An interagency review of the current federal export control system determined that the existing system is overly complicated, contains redundancies, and may not properly focus efforts on the most critical national security priorities. The administration expressed plans to restructure the control lists, simplify policies, improve coordination between agencies, and eliminate gaps and duplications.[4]

**Impact on Research**

University of Michigan (U-M) conducts its research activities in an open environment. The Regent's Policy Concerning Research Grants, Contracts, and Agreements states:

> *"The mission of the University is to generate and disseminate knowledge in the public interest. Essential to this mission are two fundamental principles: open scholarly exchange and academic freedom."*

Consistent with this policy, U-M is committed to the principle of freedom of access by all interested parties to the data, the processes, and the final results of research. U-M generally does not accept research agreements that limit publication of results or the participation of researchers on the basis of nationality. At the same time, U-M is fully committed to complying with all applicable export control laws and regulations that pertain to the conduct and dissemination of research and its products. Researchers at U-M may conduct research that involves advanced, cutting-edge technology. Therefore, they may from time to time intersect with federal regulations that impose access, dissemination, or participation restrictions on the transfer of items and information.

The export regulations have a variety of exemptions and exclusions, otherwise known as "safe harbors." The most important one for universities is the "Fundamental Research" exclusion, which applies to ITAR and EAR. This exclusion covers the information that results from basic and applied research in science and engineering, conducted in accredited U.S. institutions of higher learning, the results of which ordinarily are published and shared broadly within the scientific community. Other exclusions result

---

[2] U.S. Department of Commerce, Bureau of Industry and Security, Policies and Regulations, http://www.bis.doc.gov/policiesandregulations/index.htm (accessed September 29, 2010).
[3] U.S. Department of Treasury, Office of Foreign Assets Control, http://www.ustreas.gov/offices/enforcement/ofac/ (accessed September 29, 2010).
[4] The White House, Office of the Press Secretary, "President Obama Lays the Foundation for a New Export Controls System To Strengthen National Security and the Competitiveness of Key U.S. Manufacturing and Technology Sectors," August 30, 2010.

from use of publically available information, scientific journals, and other public information. Except in very limited circumstances, most research conducted at the University qualifies for this exemption from export control regulations.

There are limited circumstances where some activities within a research project may be restricted by export regulations. An example is space exploration technology; certain aspects of projects that involve research on space instruments may be sensitive and under export controls.

**Fines and Penalties**
Violations of export control regulations can be prosecuted under criminal law, civil law, or both. Penalties and fines may be large, both for the individual researcher and for the involved university. Criminal penalties can reach up to ten years imprisonment and one million dollars per violation. Civil penalties may be from $120,000 up to $500,000 per violation in cases involving national security. In addition, individuals and institutions found guilty can be debarred from federal grants and contracts and may lose future export privileges.

**Export Control Compliance at the University of Michigan**
The University's export compliance efforts related to research activities are coordinated through the Division of Research Development and Administration (DRDA). The Executive Director of DRDA is the designated institutional official for export controls matters. An Export Compliance Officer at DRDA assists the research community with export issues and provides guidance on and interpretation of federal regulations. The Export Compliance Officer also consults on export issues in areas outside of the research environment, including procurement, property disposition, and technology transfer. DRDA has formed an Export Compliance Committee, composed of DRDA leadership and selected senior project representatives. Project representatives at DRDA serve as liaisons between the researchers and the sponsoring agencies and assist the research community with the administration of research activities. This committee provides oversight and guidance to researchers on projects with export controlled technology.

Project representatives work with researchers to identify and address issues that might involve export statutes and regulations. They are assisted, as needed, by the Export Compliance Officer and the DRDA Export Compliance Committee. Where possible, the University negotiates the terms of agreements and statements of work to minimize or eliminate export control compliance requirements. The project representative and researcher, with assistance as needed from the Export Compliance Officer, prepare a Technology Control Plan describing how access to information, materials, equipment, or computer software will be controlled. Beyond this point, it is the responsibility of the individual researchers and their support staff to ensure compliance with federal regulations.

University Audits performed a review of export control compliance to identify risks, controls, and best practices to ensure compliance with federal regulations. The scope included University research activities subject to export controls and research management at the University, college, department, and principal investigator level. Other areas outside of research, where export controls could apply, including procurement, treasury, and property disposition functions, were outside the scope of this review.

University Audits selected a sample of faculty members who have multiple export controlled activities and conducted interviews to obtain an understanding of the export control environment within their specific research areas. Physical and IT controls were also reviewed to determine how well export controlled technology is protected. Based on the review, individual researchers have strong knowledge of export control regulations, take appropriate precaution, and take the regulations seriously. While the level and types of controls vary among researchers, no instances of non-compliance were observed.

A summary of observations and best practices that would strengthen processes is listed below.

- Training and Education - DRDA has developed thorough educational materials on export controls which are available on the DRDA website. DRDA-led educational sessions have also occurred at research units with potential export controlled research. To aim training and education effort at researchers with known export controls activity, consider individual or small group sessions with these individuals. University Audits recommends expanding training and education programs to include research staff and administrative personnel to further raise awareness in the organization. Consider developing a module similar to the web-based Program for Education and Evaluation in Responsible Research and Scholarship (PEERRS) regarding export controls.
- Export Control Identification - Emerging technologies may inadvertently trigger export control regulations. The regulations are complex and require specialized knowledge and training. While identifying when and how to apply export controls can be complicated, it is important that common red flags are universally recognized by the project representatives and principal investigators. University Audits recommends developing some practical tools and reminders to further assist the research community in identifying and referring potential export control situations to the Export Compliance Committee and/or Export Compliance Officer.
- Technology Control Plans - Technology Control Plans define specific technologies and indicate how they will be controlled. Monitoring compliance with these plans on an ongoing basis, implementing a single repository system, and sharing relevant information with the research community will further mitigate export compliance risks.
- Information Technology Controls - Varying levels of IT controls are used throughout the research community to ensure export controlled assets are protected. When IT staff at the department or lab level assist researchers with installation of electronic software or data, they ensure best practices and security guidelines are implemented. IT staff should be consistently included in the development of the Technology Control Plans.
- Technology Disposition - Export controlled technology should be properly disposed of at project end. Clear definition and guidance on technology disposition at the end of the projects should be provided to principal investigators. Establishing a follow-up process to ensure proper disposition will further mitigate the risk.

**Management Plan** - DRDA is exploring how we can cost effectively supplement existing training. Our experience is that it is often difficult to get faculty to participate and college and departmental leadership will need to encourage participation. As indicated, we do provide information via our website to faculty, and we are creating additional web-based tools to help faculty self-identify when they need assistance and support with export control issues. An extensive set of self-directed solutions is not viable due to the complexity of issues, but knowing when to reach out for help is critical. A PEERRS module would be helpful; DRDA will need assistance from the research community in determining how to identify who is required to take this training, as a small percentage of projects involve export controls.

DRDA will be meeting with the College of Engineering and other research leadership to identify the best way to share relevant information on export controls. DRDA generally relies on faculty to engage relevant IT staff when export controlled information or data is stored on any computer. In the future, we will ensure that relevant IT staff be included in developing the Technology Control Plan. With support from research leadership, IT staff in areas with more than one Technology Control Plan per year will be targeted for additional training and discussion. These additional activities related to export controls will require additional resources.

**Summary**
Export control regulations present unique challenges to universities requiring a balance of national security and U.S. economic vitality concerns with traditional concepts of unrestricted academic freedom and dissemination of research findings and results. University researchers and administrators need to be aware that these laws may apply to research, though in most cases the regulations do not affect normal University activities. The research community is proactively taking measures to ensure compliance with federal regulations. Opportunities exist for improving some of the supporting infrastructure related to training and education, communication, information technology, and disposition of controlled technology. University Audits will perform a follow-up review during the fourth quarter of fiscal year 2011.

***Information Technology***

Plant Operations – Facilities Maintenance Building Automation Systems #2010-311
Report issued September 8, 2010

The Building Automation System (BAS) is part of the University of Michigan's Facilities Maintenance department within Plant Operations. BAS is tasked with monitoring environmental control systems in nearly all of the University's General Fund buildings and some non-General Fund buildings (for a fee). BAS implements schedule and operational changes for various types of equipment and monitors alarm conditions and energy efficient system operation. BAS staff work closely with building managers in each of the monitored buildings to effectively provide services and ensure quick response to anomalies and alarms.

BAS monitors and controls the environmental condition in buildings utilizing data input[5] and output points, which are located on building mechanical systems and throughout the facility. Input points feed information into the buildings' digital control panels. Using locally running computer programs, the panels evaluate the input information and calculate the appropriate output signal to send to control devices such as damper or valve actuators, fan motors, and lighting circuits. This evaluation occurs several times per second, allowing for quick, precise control of environmental conditions.

BAS operates 24x7x365 with ten full time utility system technicians to maintain this coverage. They continuously monitor roughly 120 facilities with 13,081,694 square feet of space. This process is accomplished using over 180,000 data points. These devices connect to 6,761 controllers and actuators that are administered by 548 building control panels. These panels connect with six scanning PCs and 45 micro servers, to monitor 392 networks of building support systems data.

Each input point monitors multiple types of environmental data using multiple data points. For example, one data point may track temperature while another tracks air flow, and a third humidity. Within the panels, set points are designated for specific data points. The set point is the reading a data point is expected to provide to the panel. In the case of a temperature data point, a set point may be 68 degrees. The data point is also assigned an allowable tolerance. In the case of a temperature point, the allowable tolerance may be ± 3 degrees. This means that as long as the temperature is within 3 degrees of the set point of 68° (71° at the high end and 65° at the low end), everything is satisfactory.

To keep the data point within the allowable range, the panels also connect to various actuators within the buildings. These controls may open or close a damper, adjust the speed of a fan, turn an air handler on or off, or trigger an adjustment on a humidifier. All of these events happen automatically and are

[5] A data input point is a sensor that detects and reports on a certain condition e.g., temperature, valve positioning, humidity.

monitored by the staff at BAS. If a data point's reading is outside of the allowable tolerance levels, an alarm is triggered at the panel and alerts BAS monitoring staff.

All panels are connected to a central BAS server. Panels send data to the server in a number of different ways:

- Via dedicated circuits
- Via the campus Ethernet backbone
- Via remote monitoring stations
- By a combination of those methods

Despite the variety of systems and networks data must traverse, alarms reach BAS almost instantaneously. BAS utility systems technicians review and verify each alarm as soon as it comes in. If service is needed, the technicians create a work order within the Plant Operations system. If the alarm is critical in nature, such as the temperature in a vivarium, BAS notifies the appropriate facility managers and immediately dispatches maintenance personnel. BAS also utilizes the capability of remote alarm notification, where building personnel who are responsible for critical building systems are notified via computer server using "text to talk" software. In these cases, the central BAS server verbally relays critical alarm information to the responsible individual. Alarms are logged to help staff identify problem areas and/or faulty data points.

This audit included an examination of BAS, the processes directly affecting that system, and the implementation of that system at a number of locations. This audit does not address the security of the systems that interface with BAS.

The following criteria were used for choosing installations for review. The locations reviewed during this audit are listed along with the reason for their inclusion:

- School of Education Building (SEB)
    - Complexity of main hub location
    - Connected via dedicated line
- Medical Science II (Med Sci II)
    - Connected via Ethernet
- Life Sciences Building, Central Chiller Plant
    - Critical systems
- Hill Auditorium
    - High profile venue
- Rackham Graduate School
    - Mix of old and new technology
- Stockwell Hall
    - Modern installation
- Mendelssohn Theater
    - Little or no problems
- Power Center for the Performing Arts
    - Unique Installation

The objective of the audit was to ensure the security, availability, and reliability of BAS by performing the following:

- Assessing the processes surrounding creation of, changes to, and removal of user access privileges
- Assessing the security of the BAS servers
- Assessing the security of the BAS data points

Failure to effectively manage risk within BAS could result in:

- Failure of critical building support systems
- Destruction of sensitive University property
- Damage to sensitive University property
- Costly repairs and replacements
- Negative publicity for the University

**Risk and Control Discussion**

BAS currently communicates with the monitored buildings across a combination of dedicated phone lines and the University's Ethernet backbone. Although it does not represent a specific security risk, the model of using dedicated lines is outdated. New hardware, though backwardly compatible, is designed to leverage the speed of Ethernet technology as its primary source of network communication. The amount of data a dedicated line can carry is severely limited. BAS is using converters in places where new hardware must communicate via dedicated lines, but this limits the amount of information the new hardware will be able to provide and the speed at which it can be provided. Because of the shift in technology and the increasing amounts of data transmitted, BAS needs to transition from the dedicated lines to an all Ethernet connection model to gain the most benefit from the newly installed equipment. This change will improve system performance and better position BAS for the future. It will, however, change their risk profile since Ethernet networks are subject to security concerns that do not affect dedicated phone lines. Because of this, in the near future, BAS is moving towards a secured, isolated network.

- Open Ports on Monitoring Devices - Data points throughout buildings connect to panels. These panels then connect to the BAS central server via a variety of methods. There are two types of panels that have the ability to connect directly to the University network and deliver data across it. Other types must connect through intermediate devices; one of which utilizes the University network. University Audits performed a vulnerability assessment on these network connected devices and found multiple unnecessarily open ports. Network connected devices use ports to communicate. Each open port is an open doorway into the device. An unused, open port provides an unnecessary point of access to the device and could provide an avenue for inappropriate or malicious access. Results of our testing were provided to BAS management.

  **Management Plan** - BAS management has obtained a list of ports our panels use to communicate from the vendor. We will work with the vendor, as part of our service agreement, to find a solution to closing unnecessary ports on the monitoring devices.

- System Maintenance - BAS utilizes computers running the Windows XP operating system for monitoring and interacting with the central server and data collection devices. The central server also has a Windows-based operating system. These computers, like any other, require regular maintenance and upgrades to their operating systems to continue to perform smoothly and securely. Currently, there is no regular maintenance plan for these systems nor is there an IT professional assigned to them.

  **Management Plan** - BAS has recently developed a highly productive relationship with Plant Operations IT. As part of this relationship, we have created a stock of backup monitoring PCs to use in the event of systems crashing in the field. We will continue to work with Plant Operations IT to establish a formalized maintenance agreement for the remainder of our systems.

- User Access - When dealing with highly sensitive systems such as the BAS central server, it is important to control who has access to the system. Only users with a documented business need should have access. Restricting user access is problematic in complex environments such as U-M since users can gain access to systems because of their membership in certain user groups. This situation is most common with users who are members of administrator-level groups. University Audits found users with access to the central server who had no business need to access the server.

  **Management Plan** - BAS and the Plant Operations IT department are working collaboratively through weekly working meetings to address user and computer access issues. We have begun the process of removing unnecessary accounts from our workstations and servers. BAS is also setting up a regular access review process to ensure user access stays appropriately restricted.

- Network Security - BAS's central server is critical to building monitoring. It acts as the clearing house for all monitor and alarm information coming in from all of the data points across campus. Currently, no one has been assigned to manage network security risks on the central server.

  **Management Plan** - BAS has begun working with Plant Operations IT to address known security vulnerabilities. We will establish a relationship with the Business and Finance Information Security Officer for assistance in continuing this work.

- Network Isolation - BAS building panels and monitoring systems are connected using dedicated lines, the University's data network, or a combination of the two. Newer panels and devices are designed to work over a data network. As BAS has grown and upgraded equipment, more and more of their devices have moved to the University's data network. As this transition has taken place, BAS has utilized existing network hardware and connections resulting in devices using multiple networks across campus. Some of these networks are unsecured and are not controlled by BAS or Plant IT. For example, the general network at the School of Education Building is unsecured for ease of use. While this arrangement works well for its intended purpose, it leaves the BAS system potentially vulnerable. This configuration has caused outages on the BAS system and puts the sensitive devices on these networks in a potentially vulnerable position.

  **Management Plan** - In conjunction with Plant Operations IT, BAS has secured a cache of dedicated IP addresses. This will allow us to better isolate our network traffic. Plant Operations is in the process of installing its own network hardware to support card reader systems. Wherever feasible, BAS will use these devices for our network connections. In other areas, BAS will employ private networks and VLANS for improved security. We will also develop relationships within ITSComm and MCIT to assist us in further isolating and securing our network connections.

- Local User Access - The BAS monitoring office consists of five workstations used by the current shift of Utility System Technicians. Because of staffing levels, these machines are not usually all occupied at once. Non-BAS Physical Plant staff occasionally use unoccupied systems to check e-mail and browse the web. Allowing unauthorized users access to these machines creates an increased potential for them to be compromised.

**Management Plan** - BAS will make this office policy and inform Utility Systems Technicians through our existing regular one-on-one meetings. A memo will also be distributed reflecting the new policy.

The BAS system has become much more complex since its initial installation. Due to the increased complexity of the technical environment supporting BAS, there is a need for more technical personnel to support the system and eliminate the control deficiencies identified during this audit. The staff at BAS are very good at what they do but are not IT professionals. The recommendations made in this report reflect a need for more IT involvement.

The close relationship with its vendors has contributed to the success of BAS. The University has committed to using a single, internationally recognized vendor for front end devices, including direct digital control panels, in all of their General Fund facilities (other equipment such as valves, dampers, actuators, and sensors are competitively bid under normal University guidelines). This has afforded the BAS staff the ability to create lasting relationships with vendor engineers and product developers. Plant Operations now employs some former employees from this vendor. These relationships have put the University in a unique position. Because of this expertise with the vendor's systems and the incredible variety of installations, the Ann Arbor campus is regularly used as a test bed for the latest technology. This gives BAS staff a preview of new developments and a head start in knowing how to use them. U-M has also been given unprecedented access to some aspects of the vendor's systems to help them troubleshoot in a live environment. This access and experience is invaluable to the University.

A formal follow-up to the outstanding issues will be conducted during the fourth quarter of fiscal year 2011.

University of Michigan Dearborn Information Technology Services Data Center at Fairlane Center
Original report issued November 18, 2010 #2010-309

Dearborn's Information Technology Services (ITS) is responsible for the IT infrastructure at University of Michigan – Dearborn (UM-D). ITS controls the day-to-day operations and management of the Fairlane Data Center.

The Fairlane Data Center is located in the Fairlane Center North Building. University of Michigan purchased the Fairlane Center in 2003 from Ford Motor Company. The Fairlane Center is comprised of two buildings including the one housing the data center. Ford continues to occupy a portion of the Fairlane Center buildings.

The Fairlane Center has approximately 318,000 gross square feet[6]. UM-D recently renovated room 108 in the North Building to house a data center, which is now the primary data center for the campus. As of October 2010, Dearborn IT staff had migrated approximately 90% of the servers and services to the Fairlane Data Center including Zimbra[7], TouchNet[8], all file servers, DNS[9], DHCP[10], Wireless Network Controllers, RADIUS[11], Campus Routing, web services, and all network/systems monitoring.

[6] http://www.umd.umich.edu/univ/ur/press_releases/may03/ftdc_announce.html
[7] Zimba is third party software used for email and calendaring.
[8] TouchNet is a web based application used to manage student accounts.
[9] Domain Name System is an Internet service that translates domain names into IP addresses.
[10] Dynamic Host Configuration Protocol is a protocol for assigning dynamic IP addresses to devices on a network.
[11] Remote Authentication Dial-In User Service is an authentication and accounting system.

The objective of the audit was to verify that the Fairlane Data Center is safeguarded by reviewing and testing controls over:

- Physical facilities
- Environmental systems
- Emergency power systems
- Incident response procedures
- Disaster recovery plans

Currently, physical security services are provided by a third party contractor, GuardsMark. They will continue to provide security services until September 2011 at which time all Ford tenants will have vacated the building. At that time, UM-D Public Safety will assume security responsibilities for the Fairlane complex. Ford Land Division is currently responsible for building maintenance at the Fairlane Center. Bids are being reviewed from the Ford Land Division and UM-D Plant Operations to determine who will maintain the building once Ford vacates the center.

**Risk and Control Discussion:**

1. Disaster Recovery Plan - A disaster recovery plan (DRP) provides guidance on how to maintain essential business functions during a crisis. A properly documented and executed DRP can minimize the impact of a disaster on IT systems and services. UM-D does not have a disaster recovery plan that covers the Fairlane Data Center. To ensure success in the planning and implementation of a DRP, UM-D IT should categorize the level of impact the crisis will have on data and proper training of personnel for disaster response.

   **Management Plan -** ITS has developed a working document that outlines plans and personnel to address disaster recovery for systems maintained in the Fairlane Data Center. The department is continuing to expand and refine this plan.

2. Visitor Control - The security company, GuardsMark, allowed contractors access to the data center without obtaining required permission from ITS or Facilities Management. UM-D procedures indicate that contractors are to report to either ITS or Facilities Management to obtain permission to enter the data center. Once permission is granted, ITS or Facilities Management calls the GuardsMark security desk, located at Fairlane Center, to inform the guard that the contractor has permission to enter the data center. In situations when contractors go directly to the Fairlane Center, the guard should contact ITS or Facilities Management to ensure the contractors have appropriate permission to access the data center.

   **Management Plan -** ITS has worked with UM-Dearborn Department of Public Safety to confirm the following procedure for access to Fairlane Data Center. Entry to the data center will be handled in one of two ways:

   - Those individuals that have authorization to enter the data room (e.g., ITS personnel, designated facilities management personnel, public safety) have an encoded UM-D identification card that allows that person access via a card swipe reader on the door.
   - Contractors and all others individuals will be required to report to the main campus and receive specific authorization along with a temporary ID from Facilities Management during regular business hours and Public Safety after hours.

   Fairlane Center security personnel will not admit anyone to the data room without first verifying that the individual has signed-in by calling Public Safety for final authorization to allow entry.

Public Safety will meet with the Fairlane Center building manager and GuardsMark security director to confirm agreed upon procedures. ITS will review visitor logs quarterly.

University Audits will conduct a follow-up of management's progress on action plans in the fourth quarter of fiscal year 2011.

**Follow-up Reviews**

CTSA (Clinical and Translational Science Award) Michigan Institute for Clinical Research and Health Research (MICHR) Operational Review #2009-106
Original report issued November 30, 2009 Follow-up report issued September 30, 2010

University Audits recently conducted a follow-up review to assess the status of management's corrective action plans. See summaries below for additional information. **This audit is closed.**

- Non-Certified Effort Reporting - All key personnel supported by the CTSA grant and a sample of MICHR staff have now certified effort for fiscal year 2009. MICHR should continue to look for ways to transfer funds in a timely manner between the cost-share portion and the grant to avoid affecting the certification status of employees who have certified before the funds are transferred.

- Grant Adjustments - Late adjustments have decreased greatly from 2009 and MICHR streamlined their financial monitoring processes to avoid substantial late adjustments.

- Veterans Administration (VA) Hospital Appointments - Sponsored Programs held training for applicable MICHR employees that included a section on training awards. MICHR employees found the training to be helpful in reminding them of unique NIH (National Institutes for Health) CTSA requirements. MICHR employees are aware of the need to obtain approval from NIH if scholars also have a VA appointment.

- Expense Classification - MICHR reassigned the monthly Statement of Activity reviews to each unit manager. Unit managers are more familiar with the financial activity and can better identify potential issues. Each manager initials and dates the statements as evidence of their review.

- Compliance with P-Card Guidelines - A higher administrative authority now approves all P-Card statements. The cardholder and reconciler functions are separated; after the P-Card holder reconciles the account, the reconciliation is reviewed by a second party, and then a higher administrative authority performs a final review and sign-off on the report.

- Business Continuity Plans - MICHR has completed their Business Continuity Plan. High priority portions of the plan, such as the phone tree, have been tested.

University of Michigan Hospitals and Health Centers (UMHHC) Payroll and Timekeeping Processes #2008-110
Original report issued January 30, 2009 First follow-up report issued February 26, 2010
Second follow-up report issued September 30, 2010

University Audits performed a second follow-up to review open audit issues and corresponding action plans.

Management addressed the remaining open issues by implementing continuous monitoring activities that enhance existing controls. These improvements are discussed below. **This audit is closed.**

- Human Resource Management System Access Controls - A single unit liaison was responsible for monitoring human resource system access rights for all UMHHC employees. UMHS Human Resources increased management awareness of employee access to sensitive human resources and employment data by distributing Information Technology Services (ITS) security reports to department administrators. These security reports allow local administrators to monitor access roles assigned to staff.

- Systematic Data Integrity Controls - Department supervisors use time off awards (TOA) to reward and recognize employees who exceed performance expectations and take on additional duties. UMHS guidelines recommend limiting employee TOA awards to 24 hours per year, but in special circumstances awards can be up to 40 hours per year. Prior to the audit, a lack of systematic reporting and monitoring of TOAs resulted in awards exceeding the 40 hour per year limit. In January 2010, UMHS HR began sending TOA data reports to departmental human resource consultants to ensure consultants are aware of TOA usage in their respective areas. In fall 2010, UMHS HR management began actively monitoring TOA activity to ensure consultants contact supervisors and recommend alternate ways to reward or recognize employees who are near or over award limits.

University of Michigan-Dearborn School of Education #2010-205
Original report issued April 26, 2010 Follow-up report issued October 1, 2010

University Audits has performed a follow-up review to assess plans to address issues identified during the audit. Management has made progress on many items that are now closed. One open issue remains and will be reevaluated during a second follow-up review scheduled for the third quarter of fiscal year 2011.

- Agreements with External Entities - The Dearborn School of Education (School) has agreements with many external entities. University Audits observed that formats varied widely, terms had changed but were not updated in the agreement, or the agreements were not authorized by the appropriate level of University leadership. The School's leadership planned to update agreements, create a master spreadsheet to track agreements, and create a variety of standard templates (based on the type of arrangement) for future use. Due to turnover in the Dean and both Associate Dean roles, this item has not yet been addressed.

- Information Technology Risk Assessment - The School has implemented policies regarding two of the issues identified in their 2006 IT risk assessment. They have also received a one-time fund allocation to upgrade computers to address the third issue, with the understanding that a catastrophic failure of equipment would likely be covered by their insurance policy (if due to flood damage, theft, etc.). In addition, UM-Dearborn Information Technology Services is conducting a high-level information technology assessment to strengthen information technology controls campus-wide. **Closed**.

- Documentation for Purchase Exceptions - The School has a departmental purchasing policy that is more restrictive than the general University policies. The Dean's approval is now documented when an exception to the School's purchasing policy is granted. **Closed.**

- Conflict of Interest Contact Information - The Dean's Office utilizes a hiring and termination checklist, which now includes a requirement to notify the conflict of interest database manager of changes in the dean's role. **Closed**.

- Check Copying Practice - The School has updated their policies to prohibit copying checks. Employees are aware of the policy and have destroyed any previously held copies. **Closed.**

- Use of Signature Stamps - The School destroyed signature stamps previously used for the Dean. A new policy was created to allow electronic signatures on informational or promotional materials only; they are not used for any financial or business transactions. **Closed.**

William L. Clements Library #2008-202
Original report issued January 26, 2009 Follow-up report issued November 9, 2010

University Audits conducted a follow-up review to assess management's progress in mitigating identified risks.

- Grant Related Compliance - Clements Library management had not filed an annual report on the project accomplishments and expenditures for 2007 and 2008, which is required by a major grant. The report, including the last three fiscal year activities and a letter of explanation written by the Director, was mailed to the McGregor Fund in January 2009.

- Endowment Agreement Execution - Written and properly executed agreements were not available for all Clements Library endowments. Clements Library management has obtained appropriately executed endowment agreements from donors where possible. These agreements are now documented and stored in a common location. University Audits has reviewed this documentation.

- Deaccession Policies and Procedures - The Clements Library occasionally deaccesses (i.e., disposes of) some duplicate collection items, as well as gift items received where donor intent states that the Clements Library is to sell the gift items and use the proceeds to enrich the collection. At the time of the audit, Clements Library did not have any documented deaccession policy. A formal deaccession policy was completed and was reviewed by University Audits.

- Documented Collection Policy - To facilitate the overall mission of the Clements Library, a reevaluation of current collection policies and documentation of a new collection policy was required. Clements Library Management is holding regular meetings to draft a collection policy. Clements Director is also working with other special collection libraries around campus (e.g., Bentley and Hatcher) to coordinate collection policies.

- Missing Collection Items - At the time of the audit, there was no process in place for Clements Library management to identify or find items from the collection that are stolen or lost. Clements management has created written procedures addressing this issue, which University Audits has reviewed.

- Collection Management Policies and Procedures - Policies and procedures for key collection management processes performed by Clements Library staff (i.e., reporting and handling of missing collection items, filing of gift and purchase related documents, separating collection items that need conservation, and loan of items from the library collection) were not formally

documented. Consistent procedures and standard forms have been implemented for key collection management policies.

- Clements Library Collection Insurance - The Clements Library collection is very valuable and much of it is irreplaceable. At the time of audit, the only insurance coverage Clements Library had for their collection was the $120,000,000 standard university-wide Fine Arts Policy. The Clements' Director has worked with Risk Management and the University Fine Arts underwriter to ensure that the Clements collection is adequately insured. Coverage under the Fine Arts Policy has been increased to one billion dollars.

- Willow Run Facility - A small part of Clements Library collection is stored at the Willow Run facility. The stored items that Clements Library management considers valuable were not reported to Risk Management for coverage under the University-wide fine arts insurance policy. Risk Management assured Clements management that collection items housed at the Willow Run storage facility are now covered under University's Fine Arts Policy.

- Collection Management at Willow Run - University Audits recommended that the portion of the collection stored at Willow Run be reevaluated to determine which items are critical for the overall collection and to catalogue/access these items. The portion of the collection stored at Willow Run has been reviewed and duplicates and items not meeting the collection policy have been deaccessed and sold. The remaining collection items will be moved to shared storage.

- Department of Public Safety Fire Inspection Report - The fire inspection report issued by Department of Public Safety on March 30, 2007, recommended that the electric stove in the tea room in the Clements Library should be removed and replaced with a non-heat producing induction unit to avoid fire hazard. The stove has been removed.

- Statement of Activity (SOA) Reconciliation - Clements Library personnel responsible for the reconciliation or review of the Statement of Activity did not formally document the review and reconciliation. The Clements Library Business Manager worked with ITS staff to develop a report that lists total monthly revenues and expenses for all library funds/accounts. Clements Director reviews, signs, and dates this monthly report. The Director reviews the detail SOA reports when more detail information is required.

- Internal Recharge Rate - Clements Library occasionally rents out space to other business units within the University. Clements Library staff have worked with the Office of Financial Analysis and obtained an approved recharge rate for their internal customers (University units).

- Procurement Observation - Clements Library personnel often use Non-PO vouchers to acquire collection items when vendors do not accept payments via P-Card and/or the payment amount is over $5,000. University of Michigan policy requires that any purchase over $5,000 must have approval from a buyer in Procurement Services and a purchase order. Procurement is drafting a Performance Agreement, which would authorize the library to execute Non-PO vouchers of $5,000 or more that are for collection-related purchases without use of a purchase order or sign-off of a Procurement Services buyer. The Agreement should soon be finalized. In the meantime, a Senior Purchasing Agent in Procurement is reviewing Clements purchases done on non-PO vouchers that are greater than $5,000.

Management has taken appropriate corrective action on all audit recommendations and improved internal controls. **This audit is closed.**

School of Kinesiology Fiscal Responsibilities #2009-203
Original report issued April 14, 2009 First follow-up report issued February 25, 2010
Second follow-up report issued November 10, 2010

One item had not been fully addressed at the time of the first follow-up review and was recently evaluated as part of a second follow-up review. This item has been satisfactorily addressed and the audit is now closed.

Health Management Research Center (HMRC) HIPAA Compliance

- A fully executed Business Associate Agreement has been signed by the HMRC's third party data center and has been received by U-M Procurement Services. This updated agreement includes provisions to comply with the HITECH Act of February 2009, which is related to the use of electronic health records.
- Previously, HMRC employees only completed HIPAA training as new hires. All HMRC employees have now completed an updated HIPAA training online. This will be an annual requirement for all HMRC employees going forward.

In addition, the Kinesiology Dean's Office has appointed the Business Administrator Associate as a liaison between the HMRC and the UMHS Compliance Office. This will allow a single point of contact for the Compliance Office to update the HMRC of necessary training, updates, or other compliance matters. The Compliance Office intends to develop an in-depth HIPAA training specific to the unique needs of the HMRC, and this training should be coordinated with the Business Administrator Associate.

NCAA Compliance Review – Complimentary Tickets #2010-401
Original report issued June 28, 2010 Follow-up report issued November 19, 2010

University Audits reviewed the process for providing complimentary tickets to student-athletes, prospects, and non U-M coaches as part of a broader review of key National Collegiate Athletic Association (NCAA) compliance areas. During the audit, sample testing revealed that the Ticket Office inadvertently provided a high school coach with three complimentary tickets, when the NCAA limit is two. A follow-up review was performed to assess the progress on the Ticket Office process improvements to ensure consistency with NCAA complementary ticket limits.

The Compliance Services Office self-reported the secondary violation to the NCAA on June 18, 2010. Management implemented the following corrective actions:

- Addressed the violation and related corrective actions during the annual rules education session for regular, full-time Ticket Office staff
- Provided both Ticket Office windows in Yost Arena with a list of complimentary ticket recipients and their affiliation, along with a job aid documenting NCAA ticket limits
- Improved communication between the ticket windows and the supervisor for the event through use of Yost Arena's two-way radios
- Restricted access to additional complimentary tickets to the supervisor(s)
- Reinforced the requirement for supervisors to approve any additional or last minute complimentary ticket requests and document their approval

These improvements will help ensure the University provides the appropriate number of complimentary tickets to recipients. **The audit is closed.**

**Open Audits Follow-up Table**
**November 30, 2010**

| Audit Title | Report Date | Issues | Expected Completion |
|---|---|---|---|
| Information Technology Central Services<br>2009-838 | 12/02/09 | Inventory management; billing for services; monitoring services quality and demand; financial monitoring; human resources processes; facilities; procurement | First Follow-up June 2010<br>December 2010 |
| Wire and ACH Transfer Process<br>2009-112 | 1/06/10 | Authorized user list; transaction limits; wire transfer policy | First Follow-up August 2010<br>December 2010 |
| University of Michigan Video Surveillance Systems<br>2009-311 | 4/14/10 | Network connectivity; unnecessary ports, services, and shares; video quality; video handling; video storage; process documentation; cross-training | December 2010 |
| Dearborn Office of Cashiers/Student Accounts TouchNet<br>2010-303 | 6/3/10 | Application hosting; application vulnerabilities; change control; user roles | December 2010 |
| Medical Center Information Technology Michigan PGIP Analytics Collaborative<br>2010-302 | 7/16/10 | Risk assessment of local data workspace; project governance; time limit for reporting breaches; control of data use/access disclosure | March 2011 |
| College of Literature, Science & the Arts Research Computing<br>2010-809 | 7/26/10 | Security policy; data classification; data storage; backups; training and guidance; antivirus; disaster recovery plan; physical security | January 2011 |
| Portable Electronic Devices UMHS<br>2009-305 | 8/26/10 | Proper use standards; standard configurations; mobile devices policy; access control | March 2011 |
| Plant Operations – Facilities Maintenance Building Automation Systems<br>2010-311 | 9/08/10 | Open ports of monitoring devices; system maintenance; user access; network security; network isolation | June 2011 |
| University of Michigan Dearborn Information Technology Services Data Center at Fairlane Center<br>2010-309 | 11/18/10 | Disaster recovery plan; visitor control | June 2011 |
| University of Michigan Hospitals and Health Centers Cashier's Office<br>2008-206 | 10/17/08 | Segregation of duties; bank statement reconciliation and check writing practices; follow-up of outstanding vouchers; duplicate facility refunds | First Follow-up June 2009<br>January 2011 |
| Medical School Administrative Internal Control Review<br>2008-208 | 1/30/09 | IT strategic planning; reconciliations; gift fund usage; IT security; fire drill regulations | December 2010 |

| | | | |
|---|---|---|---|
| University of Michigan Health System<br>Office of the Executive Vice President for Medical Affairs Operational Review<br>2009-205 | 11/17/09 | Procurement and payroll training; excluded costs; segregation of duties; reconciliations | December 2010 |
| University of Michigan Medical School<br>Internal Medicine, Division of Hematology/Oncology<br>Southwest Oncology Group Review<br>2010-501 | 11/25/10 | Retroactive grant adjustments; detailed financial reconciliations; late submission of timesheets; up-to-date effort certifications | First Follow-up August 2010<br>December 2010 |
| U-M Hospitals and Health Centers<br>Omnicell Pharmaceutical Distribution System<br>2010-305 | 6/16/10 | User access; discrepancy reporting and escalation; patient charges; controlled substance procedures | December 2010 |
| U-M Medical School W.K. Kellogg Eye Center<br>2010-204 | 8/30/10 | Financial monitoring and oversight; procurement and travel; grant management and effort reporting; inventory management; charge capture; payroll; cash management; management structure | March 2011 |
| University Press Inventory and Receivables<br>2008-203 | 1/30/09 | Accounts receivable; inventory (U-Press continues to implement internal controls in many areas, including those noted in the audit report) | January 2011 |
| Chemical Biology Doctoral Program<br>Interdepartmental Degree Program<br>2009-812 | 6/30/09 | Program reporting and oversight; compliance with procurement and hosting guidelines; effort certification; record retention; service level agreement; conflict of interest and conflict of commitment (Follow-up review will be conducted after the new chair is named) | December 2010 |
| University Housing Fiscal Responsibilities<br>2009-814 | 11/9/09 | purchasing; payroll and time reporting, cash operations, internal control gap analysis, business continuity and disaster recovery plans, conflict of interest/conflict of commitment | First Follow-up August 2010<br>December 2010 |
| Center for Human Growth and Development<br>2009-206 | 11/17/09 | Security/maintenance of sensitive data; monitoring grant budgets; imprest cash fund management/subject fee payments; disaster recovery/business continuity planning; statement of activity reconciliation/segregation of duties | First Follow-up August 2010<br>March 2011 |
| School of Art & Design<br>2009-201 | 12/08/09 | International programs; supplemental system; statement of activities reconciliation; P-cards; payroll; cash handling | First Follow-up June 2010<br>December 2010 |

| | | | |
|---|---|---|---|
| Wire and ACH Transfer Process<br>2009-112 | 1/06/10 | Authorized user list; transaction limits; wire transfer policy | First Follow-up August 2010<br>December 2010 |
| University of Michigan Dearborn School of Education<br>2010-205 | 4/26/10 | Agreements with external entities; IT risk assessment; documentation for purchase exceptions; conflict of interest contact information | First Follow-up October 2010<br>March 2011 |
| Matthaei Botanical Gardens and Nichols Arboretum<br>2010-202 | 4/29/10 | Safety and security; cash handling; procurement; inventory; community programs; | January 2011 |
| Office of University Development Life Income Gifts Program<br>2010-806 | 6/11/10 | Unit roles, sharing information, procedural efficiencies, and system opportunities | March 2011 |
| School of Social Work<br>2010-813 | 6/18/10 | Stewardship of gift funds, segregation of duties, signature authority, policies/procedures, inventory management, relationships with central service units, supplemental systems | February 2011 |
| University of Michigan Center for Statistical Consultation and Research (CSCAR)<br>2010-809 | 6/23/10 | Recharge rates and workshop fees, segregation of duties, reconciliations, supplemental systems, policies/procedures | March 2011 |
| Center for AfroAmerican and African Studies<br>2010-820 | 6/25/10 | Significant oversight and other control activities need to be implemented into many processes | December 2010 |
| PeoplePay<br>2010-107 | 7/16/10 | Payroll Office review office; clarification of PeoplePay capabilities; change management | April 2011 |
| U-M Flint Early Childhood Development Center<br>2010-118 | 7/19/10 | Financial decision-making; Kid's Care system; Web camera access; transportation agreements; imprest cash and snack station fund | December 2010 |
| U-M Flint School of Education and Human Services Fiscal Responsibilities<br>2010-812 | 7/19/10 | Financial reporting and budget monitoring; segregation of duties; faculty release time; conflict of interest and conflict of commitment; documented policies and procedures | February 2011 |
| U-M Flint Genesee Early College Program<br>2010-114 | 10/1/10 | Updating formal/informal agreements; reportable data and metrics; information technology management; employment controls; University obligations for K-12 students | March 2011 |

| | | | |
|---|---|---|---|
| Division of Research Development and Administration Export Controls Compliance 2010-402 | 10/21/10 | Training and education; export control identification; technology control plans; information technology controls; technology disposition | June 2011 |