

Item for Information

Subject: Report of University Internal Audits
July - September 2011

Background:

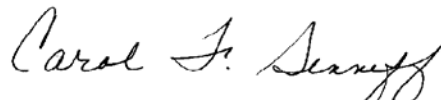
This is the report of the Office of University Audits activities for the period **July – September 2011**. The summaries of audits contained in this report were previously reported to members of the Regents' Finance, Audit, and Investment Committee and included in discussions at Committee meetings.

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, 2011**.

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

Respectfully submitted,



Carol F. Senneff, Executive Director
University Audits

ORIGINAL REPORTS

Campus

Service Unit Billing

#2011-104

Report issued July 26, 2011

Service Unit Billing (SUB) is the primary method for payments between University units. It was developed as a substitute for journal entries to provide a faster and more efficient process for inter-department transfers of funds. In 2006, ITS and Procurement Services updated the SUB model to allow users to directly upload their SUB data through M-Pathways, creating a more user-friendly interface. Many administrative units on campus are involved in SUBs, including Procurement Services, Financial Operations - Accounting Services, Information and Technology Services (ITS), and the Office of Financial Analysis.

SUB activities are categorized as either recharge or rebill expenses. Recharge expenses are charges for goods sold or services performed by a unit. University units authorized as recharge centers (also termed service units) may directly bill other University units for these goods or services. Charges appear on the billed unit's Statement of Activity report. Rebill expenses are pass-through transfers of funds or an allocation of charges.

Examples of Common Recharges:

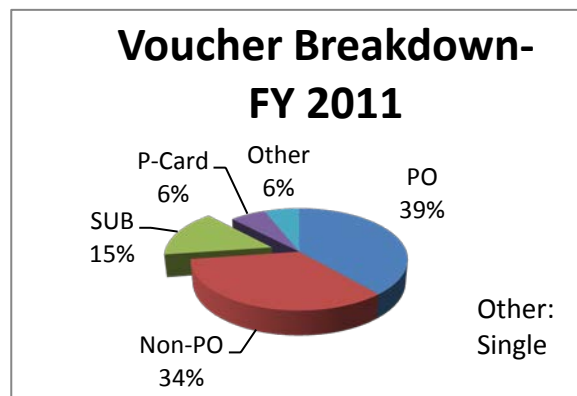
- University Unions caters a department's annual employee luncheon.
- ITS Comm provides local and long distance phone service to University units.

Examples of Common Rebills:

- Three departments consolidate orders of lab supplies in order to achieve a cheaper rate and then divide the final cost.
- A building with three departments assigns one department to purchase cleaning and lavatory supplies, and expenses are divided between all three departments.

Units submit SUB expenses using either an ITS-supported Excel upload template controlled by users' M-Pathways security profile or a File Transfer Protocol (FTP) connection that requires separate levels of authentication.

SUB activity, compared to other voucher types, is represented by the graph. This data is based on vouchers entered between July 1, 2010, and June 19, 2011 (the most recent data available), representing nearly a complete fiscal year. At present, SUB transactions account for 15% of voucher activity on campus, a far higher percentage than our peer institutions per discussions within the Administrative Transformation Services project on campus.



This audit examined high-level procedures for entering and managing SUB activity along with the detailed information technology systems that are used to process SUBs. Items considered during the audit included:

- University policies and procedures to control SUB processes
- Data analysis methods available to aid in review of SUB activity, for both units that charge and those that receive SUB charges
- Recharge information management
- Access restrictions to data and systems
- Configuration and change management processes
- System and information integrity controls to ensure data accuracy

In performing this evaluation, University Audits met with central administrative units on campus that have responsibility over various portions of the SUB process. This included Financial Analysis, ITS, Accounting Services, and Procurement Services. In addition, individual units on campus that perform SUB activity were assessed to determine how those departments manage their SUB operations. Units were selected to ensure that both high and low volume SUB users were included. Some units were also selected to determine their general understanding of analyzing SUB charges being billed to their departments. Units chosen for review were:

- ITS Communications Systems and Data Centers (ITS Comm)
- Pharmacy Services
- Inglis House
- Kipke Conference Center
- University Unions
- Facilities-Maintenance
- North Campus Research Center

Representatives from UM-Flint and UM-Dearborn were interviewed to obtain a general understanding of SUB processing on those campuses but only UM-Ann Arbor units were selected for testing. Finally, data analysis was performed on SUB activity and internal vendor information.

Audit observations related to SUB risks are discussed below.

Risk and Control Discussion

- Ownership of SUB Process - Ownership of the SUB process has not been formally established. The technical component, driven by ITS through control of the uploader template and FTP accounts, has very different requirements and needs than the financial component, where the movement of funds is monitored and tracked. Without a clear owner, it is difficult for departments to make recommendations regarding desired features or services of the SUB process. For example, Accounting Services would like additional fields on the uploader template to be required in order to provide more information to units reviewing their Statement of Activity. However, this change would require authorization from a process owner.

A clear process owner could also better publicize the proper procedure for units who use recharge rates externally. Discussions may involve several units, including the Tax Department, Division of Research Development and Administration, or Procurement Services, but a consistent message should be communicated to University departments for such situations.

Management Plan - The Financial Operations Accounting Services Customer Service Team will take leadership as the SUB process owner, working with the Office of Financial Analysis. These groups will review the entire SUB process to clarify who has responsibility over

individual components of the process and determine if there are any opportunities to streamline operations. An online information portal or FAQ page will be developed to ensure SUB information is consolidated into one location, including policy statements on appropriate recharge and rebill activity. Imbedded web links will direct units to other departments for questions related to those areas. This will ensure users with SUB questions receive consistent information and are aware of appropriate contacts for additional questions.

- **Identifying Recharge Activity** - There is no method to identify units performing unauthorized recharge activity. In the past, these units could have been identified by Comprehensive Rate Reviews performed by Financial Analysis. These reviews were of a limited scope to identify department IDs with recharge revenue (money deposited into fund 52000) that were not included in Financial Analysis' tracking database of authorized recharge units. However, if a unit were to apply unapproved recharge revenue to a general fund revenue account, Financial Analysis would be unable to identify them using this process. The Comprehensive Rate Reviews have not been performed for several years due to resource constraints. It is not feasible to simply review units processing SUB charges, since rebill expenses, which have no restrictions, are charged using the same SUB process and appear no different from recharge expenses. University Audit's review identified two units that were billing without a Financial Analysis-approved recharge rate. One of those units receives federal funds and could have additional compliance risks.

Management Plan - Financial Operations will work with ITS and Vendor Maintenance to modify internal vendors into three types - 1) Rebill, 2) Recharge with Rate Approval Letter, and 3) Recharge - Other. Financial Operations will continue to review activity processed outside SUB and transition those users to the SUB process. Financial Analysis will continue to ensure that all recharge activities with approval letters are reviewed at least bi-annually.

When data becomes available on other Recharge users, Financial Analysis will initially review the list of users processing recharge transactions without authorization letters to ensure that some other method of review and approval is in place. New requests for SUB access without specific approved rates will require Financial Analysis to review for appropriateness and to ensure that follow-up review procedures can be implemented.

In addition, ongoing education opportunities will be conducted to better educate units as to permissible and appropriate use of the SUB process, including incorporating a policy statement on recharge and rebill activities on the web portal along with pertinent examples.

- **Inactive Recharge Information** - Units may cease recharge operations and send recharge rate cancellation requests to Financial Analysis. The unit has the responsibility to forward vendor ID and shortcode termination requests to Accounting Services. Of the four sampled Termination Requests within the past year, all still had active vendor IDs and/or shortcodes.

Accounting Services does not proactively terminate shortcodes to allow a department time to move payroll or other recurring expenses to a different account. Internal vendor IDs are not deactivated after a period of inactivity, as external vendor accounts would be. If both the vendor ID and the shortcode are available, units could continue to perform recharge billings after informing Financial Analysis the activity has stopped.

There should be a process to work with units who have not submitted vendor ID and shortcode terminations within 90 days of the Termination Letter's issuance.

Management Plan - Financial Analysis will send recharge Termination Request letters to Accounts Payable/Vendor Maintenance for immediate deactivation of the vendor ID. Vendor Maintenance will modify their processes to include deactivation of internal vendors after a set period of inactivity. In addition, Financial Operations will create a log to check recharge shortcodes three months after receipt of a Termination Letter to determine if the shortcode has been closed.

- **FTP Account Management** - Units processing SUB expenses via File Transfer Protocol (FTP) or Secure File Transfer Protocol (SFTP) accounts require coordination from ITS to ensure proper access control and secure configurations of the interfaces. Best practice opportunities exist to strengthen controls over FTP/SFTP account management.
 - Unsuccessful login attempts to an SUB FTP account are not controlled. These accounts could be configured to disable after a predetermined number of failed login attempts. Without proper account lockout policies enforced, unauthorized users could gain system access via repeated login attempts.
 - ITS procedures require the use of SFTP rather than FTP. SFTP is a more secure protocol to transfer data, while FTP has no security features to prevent unauthorized disclosure. In addition, authorization must be obtained from the Security and Network Services (SNS) team within ITS for units that are unable to support SFTP (e.g., due to IT limitations within the account holder's department). Unsecured FTP accounts were created prior to these procedures and there appears to be no attempt to identify, document, or justify the use of FTP instead of more secure protocols.
 - There is no process to identify inactive accounts assigned to the SUB FTP directories. Unnecessary accounts increase the risk of unauthorized access and potential loss, compromise, and/or destruction of University information.

Management Plan

- The ability to limit the number of unsuccessful login attempts is likely something that would have to be set globally on the FTP server, which would impact all internal and external interfaces to the University, not just SUB interfaces. Given this, ITS does not believe this change can be implemented at this time. It should be noted that only eleven service units on campus use the system-to-system FTP method.
 - ITS reviewed all SUB FTP accounts several years ago and worked with the units to transition them to SFTP. For those SUB accounts that were unable to make the change at that time, ITS will follow up again and if they are still unable due to IT limitations, we will document the exception and reasons for permission from SNS.
 - ITS believes that all FTP account holders are aware of their responsibility to notify the Accounts Office when an account is no longer used. We will, however, begin an annual review of the SUB FTP accounts by contacting the account holder and requiring confirmation that the account is still in use. If that confirmation is not received, the account will be disabled.
- **Reporting Options** - Reporting capabilities for reviewing SUB activity are limited to specific point-in-time analysis. Units can review, for example one month's worth of SUB charges billed to or from their department. However, there are no reports that provide a lengthier review, such as year-to-date or month-over-month. Trend analysis can be an effective oversight technique to identify inappropriate activities or business processes that need to be addressed. Without centrally supported reporting tools, some larger units have turned to internally developed applications to better serve their needs. Other units, lacking the financial or technical resources, have no alternative.

Management Plan - ITS has identified several reports that could be modified to provide broader review possibilities for SUB transactions. Financial Operations will list all SUB-related reports on the SUB portal/FAQ page.

SUB represents an effective and efficient method for inter-department billings on campus. Financial Analysis is currently tracking 144 department IDs with over 300 recharge rates. A formal follow-up to the outstanding issues will be conducted during the third quarter of fiscal year 2012.

[Department of Geological Sciences Camp Davis Rocky Mountain Field Station](#)

#2011-813

Report issued July 28, 2011

Camp Davis Rocky Mountain Field Station is a teaching facility owned and operated by the University of Michigan and managed by the Department of Geological Sciences, within the College of Literature, Science, and the Arts (LSA). The University of Michigan has been operating Camp Davis each summer since 1929. Camp Davis offers undergraduate courses in geology, environmental science, and the humanities.



Camp Davis is located approximately 30 miles south of Jackson, Wyoming. Situated on 120 acres of University owned property, Camp Davis abuts the Hoback River¹ and the Bridger Teton National Forest. Camp Davis' remote location and relative close proximity to exposed geological features and Grand Teton and Yellowstone National Parks make it an ideal learning environment for students of geological sciences.

Camp Davis is usually open June through August each year. There are typically six or seven courses offered for credit each summer at Camp Davis. Students from U-M as well as other colleges and universities are invited to attend. Maximum enrollment is 24 students per class, with approximately one-third of the students coming from out of state and five to ten percent from other colleges. The following

Course Title	Sessions
GEOSCI 116 - 5 credits Introductory Geology	Session 1: June 26 - July 26, 2011 Session 2: July 22 - August 21, 2011
GEOSCI 202 - 4 credits Introductory Environmental Science in the Rockies	June 3 - June 28, 2011
GEOSCI 341 - 5 credits Ecosystem Science in the Rockies	July 7 - August 7, 2011
GEOSCI 440 - 5 credits Geology Field Course	July 14 - August 16, 2011
AMCULT 301/ENGLISH 317 - 3 credits History and Literature of the Rockies	June 26 - July 17, 2011

¹The Hoback River is an approximately 55 mile-long tributary of the Snake River in Wyoming. It rises in the southern Rocky Mountains of Wyoming and flows northeast through the Teton National Forest, before turning northwest to join the Snake just downstream of Jackson Hole, near the head of the Snake River Canyon and near the town of Hoback.

The Camp Davis facility is also used for other purposes:

- Academic conferences - This year, the National Science Foundation will hold a two-week conference at the end of August.
- Alumni gatherings - Once every three years, Geological Sciences hosts an event for alumni at the site to raise awareness of Camp Davis and other Geological Science programs and to increase donations to support them.
- Guest universities and colleges - Groups from other colleges or universities may camp for a day or two on the grounds. On occasion, they will use the cabins.

External groups are charged a per person fee designed to cover costs, not generate profit.

During the off-season, when the camp is closed, Camp Davis contracts with two local individuals to perform weekly maintenance and security checks of the grounds and to plow snow from the main roads at the site. Facilities at Camp Davis include a kitchen, a small camp store, cabins where students and staff reside, a game/recreational building, garage storage, several classrooms, shower buildings, and a central office.

In an ongoing effort to maintain and improve Camp Davis, the Geological Sciences Department, in conjunction with the LSA Facilities Team and U-M Facilities and Operations, completed a major capital improvement project. To support recent growth in course offerings and student enrollment, new cabins were added to the east wing of the camp. The pictures below show the west wing (older cabins) and the east wing (new cabins) of Camp Davis. This is where faculty, staff, and students reside while at Camp Davis.



West Wing



East Wing

The purpose of this audit was to evaluate the adequacy of Camp Davis processes over the following key areas:

- Safety of faculty, staff, students, and visitors
- Maintenance and security over the camp grounds and facilities
- Management and tracking of equipment
- Security and management of computer systems, electronic data, and networks
- Use of Camp Davis facility by other groups

Audit objectives also included review of fiscal responsibility areas for Camp Davis, such as, managing restricted funds, cash handling, budgeting, awarding financial aid scholarships, payroll processing, and procurement.

Auditors spent a few days onsite while the Introductory Environmental Science in the Rockies course was in session to walk through the various buildings, review documentation and tools relative to the audit objective areas, and observe the maintenance of the grounds and activities at the camp.

Risk and Control Discussion

- **Fire Safety and Inspections** - A local health inspector inspects the kitchen two times during the summer. These inspections are required to maintain the camp's Wyoming Food License. The fire extinguishers are inspected annually. The most recent fire inspection of Camp Davis was completed by a U-M Fire Marshal in 2005. Camp Davis leadership applied many of the recommendations in the fire inspection report, focusing on the highest risk areas and those required by local ordinance. Due to limited resources, several recommendations have not been implemented, for example:
 - Carbon monoxide detectors in the buildings that have fireplaces
 - Monthly testing of all smoke detectors
 - Annual inspections of fireplaces, water heaters, and other fuel fired appliances
 - Emergency spill containment kit for the vehicle motor fuel-dispensing facility located on Camp Davis property
 - Replacement of older mattresses with ones that are flame resistantCamp Davis staff currently does not receive fire extinguisher training.

Management Plan - In response to the 2005 U-M Fire Marshal's report, we removed the wood burning stoves from all cabins in 2006. We have recently purchased and installed carbon monoxide detectors in the two buildings that have fireplaces. We will immediately test and repair or replace, if necessary, all smoke detectors and have all fuel fired appliances inspected. We will immediately post fire safety information in each building and emergency contact information near all hard-wired telephones.

Beginning with the 2012 camp season, we will institute the following:

- Include fire safety instructions in our camp orientation for all faculty, students, and staff.
- Train all custodial and kitchen staff in the proper use of fire extinguishers.
- Test all smoke detectors and have all fuel fired appliances inspected at the beginning of each camp season.

We will reassess other outstanding recommendations from the 2005 U-M Fire Marshal's inspection to determine additional fire safety measures that are required by local ordinance and develop cost estimates for implementation.

- **Documented Policies and Procedures** - There is a general lack of documented policy and procedures for operations of the camp. One individual is responsible for several critical processes involved with managing Camp Davis. Documented procedures promote consistent practices and efficiency, and provide employees a point of reference for decision making and training.

In many cases, procedures can be as simple as a checklist. Key operational processes that should be documented include, but are not limited to:

- *Information Technology* - Document contact information for computer issues and procedures for setup and take-down of PCs and laptops. Implement an acceptable use policy for computers at Camp Davis and instruct users not to store data locally on computers.
- *Building and Grounds Maintenance* - Document procedures/checklists for ensuring the grounds and buildings are properly maintained and secured. Specific checklists that could be created include season opening procedures, performance of nightly checks, and regular maintenance.

- *Staff Orientation and Training* - Document orientation and training procedures for faculty and staff, such as kitchen prep and safety and maintaining pertinent medical information while out in the field.
- *Safety Measures* - Document additional measures taken to ensure the safety of students, such as not allowing students to drive on certain roads after it has rained.
- *Tracking Students* - Formalize and document procedures for tracking student whereabouts while at the camp. Require documentation of head counts performed while traveling to the site and during fieldwork or trips.
- *Budget Process* - Document the processes required to create the Camp Davis budget and review financial activity.
- *Scholarships* - Document the process for awarding scholarships to students, including coordination efforts with the Office of Financial Aid.
- *Repair Processes* - Document standard procedures used for regular repairs around the site.

Management Plan - We will develop and document policies and procedures for Camp Davis operations that include important timeframes, as well as a process for reviewing and updating documented procedures. We will begin this process as time allows during the current season, but we will not be able to complete the process until the off-season period.

- Inventory Management - A large amount of equipment, tools, vehicles, and appliances are housed at Camp Davis. Many buildings at the camp are used to store these items. There is currently no list of equipment or inventory owned by and located at Camp Davis. A sign-out sheet is used for linen, rock hammers, and compasses. Faculty, staff, and students are not required to sign-out any of the other equipment. Also, there are no documented procedures for performing and tracking preventative maintenance on equipment such as the camp's truck and lawn mower.

Management Plan - We will develop a policy for inventorying, records maintenance, sign-out procedures, and preventative maintenance tracking for camp property and equipment. We will complete an initial inventory of higher value items by the end of the 2011 camp season.

- Documented Emergency Plans - Several documented safety plans, rules, and regulations are provided to students and staff at Camp Davis. There is also a documented flowchart for general evacuation and informal agreements with surrounding neighbors for temporary boarding in the event of an emergency. For example, Camp Davis property has a bridge crossing the river allowing access to the main road, as does the neighboring property. Both parties have agreed to allow each other usage of the bridge on their property in emergency situations. There are no formally documented emergency procedures for specific disasters that may occur.

To further improve safety and emergency preparedness, consider potential threats to Camp Davis and formally document emergency plans for incidents such as a fire at Camp Davis, fire on a neighboring property, earthquake, flood, or gas spill.

Rules and regulations could be expanded to include the informal safety practices already in place at the camp, such as citing specific dangerous locations that are forbidden and stating the requirement to sign-out when walking offsite for activities such as swimming in the river or horseback riding while on free time.

Management Plan - Camp Davis management prioritizes the safety and welfare of our students, faculty, and staff above all. We will review and revise our existing emergency plans and documents to ensure that they encompass as many potential risks as possible.

- **Cash Handling** - Students enrolled in Camp Davis courses pay regular U-M tuition, which is processed through their student accounts like the rest of their University courses. They also pay a course fee, which helps cover costs for transportation, meals, lodging, and other operational expenses. Geological Sciences collects and deposits course fees from the students before they travel to Wyoming. Students' total balances due are tracked and logged on a spreadsheet, but there is no log of actual checks received. Checks are not restrictively endorsed "for deposit only" at the time of receipt. There is no reconciliation of the amount collected for course fees to the amount deposited per the Statement of Activity.

Management Plan - We will immediately begin restrictively endorsing and logging checks upon receipt and discontinue the practice of copying of checks. We will evaluate, revise, and document our cash and check handling procedures for course fees to improve internal controls. We will investigate the feasibility of billing course fees through the University to improve efficiency and controls.

- **External Entities** - The Camp Davis facility is open to academic conferences and guest universities and colleges. Usage of the site and services vary. External entities are charged a fee to use the facility. There is no signed agreement between these external entities and the University.

Management Plan - We will consult with the Office of the General Counsel on the requirements for a formal agreement to be used with external entities and, if required, develop a standard agreement. We will continue to review Camp Davis operational activities with Risk Management. We will consult with the Tax

Department to ensure potential unrelated business income taxes are handled appropriately, if applicable.



Overall, processes for managing Camp Davis operations are strong in the areas reviewed. Formalizing and documenting these processes will help solidify camp operations. Procedures for ensuring fiscal responsibility for Camp Davis business operations are adequate. Students are provided a significant amount of information to help prepare for their experience and ensure safety during the course. Detailed driving instructions and requirements are given to students to promote safe travels to the site. While onsite, auditors observed that Camp Davis' grounds are clean and well maintained. A fence outlines the property. While there are no mountains or forest terrain on actual campgrounds, students often use the mountains and forest trails on the neighboring properties during class and free time. The Camp Davis Rules, Regulations, and Safety Procedures manual given to students covers several important safety measures, such as, never hiking alone or at night, wearing an orange safety vest during roadside

fieldwork, and precautions for potentially hazardous wildlife encounters with bears, moose, elk, bison, and snakes. Expanding this manual to include all existing safety procedures and requirements, such as signing out when walking off the site during free time, will promote increased awareness of and compliance with all safety rules.

University Audits will follow-up during the fourth quarter of fiscal year 2012 to assess progress made on corrective action plans.

Information Technology

College of Literature, Science, and Arts Information Technology Asset Management

#2011-311

Report issued July 22, 2011

Information Technology Asset Management (ITAM) is a process that consists of business practices that combine financial, contractual, and inventory functions to support information technology life cycle management and strategic decision-making. LSA Software Licensing (SWL²) and the University of Michigan Information Technology Asset Management Consortium (UmichITAM)³ provide access to software for faculty, staff, and students of LSA as well as sixteen other schools, units, and departments across the University.

Goals

UmichITAM's goals are to reduce software costs and ensure proper compliance with software license agreements. The program exists to distribute software resources and costs across multiple units within the University to increase the return on investment on software, reduce the total cost of ownership of software through management of licensing and monitoring capacity, create a consolidated repository of software assets, and maintain compliance with licensing agreements. UmichITAM manages a common budget used to acquire a portfolio of shared software for its members. UmichITAM charges all participating members a fixed amount per Full Time Equivalent (FTE) employees. In 2010, this charge was \$98.12 per FTE.

Services

The shared software portfolio includes all applications licensed by LSA (including applications shared with the College of Engineering Information Technology (CAEN) and Information and Technology Services (ITS)). Microsoft products, anti-virus software, and Apple Mac OS X are not included in this software portfolio. These products are managed by ITS and charges for these licenses are billed directly to departments.

Services provided by SWL and UmichITAM include:

- Research and negotiation of software licenses
- Reduction of departmental operational costs by consolidating/renegotiating current department software contracts
- Management of software compliance to mitigate costly external reviews and fines
- Provision of software usage reports and statistics
- Maintenance of communication with UmichITAM users on current software acquisition projects, updates and negotiations
- Education of users on software licensing compliance and related legal issues

² SWL is part of LSA Security, which is part of LSAIT.

³ For the purposes of this report, the term ITAM will be used when referring to the process of managing information technology assets, while UmichITAM will be used when referring to the consortium at UM.

- Creation and distribution of media
- Maintenance of an inventory of licensed software

SWL tracks and maintains approved software that has an associated cost and software with no associated cost (but licensing requirements). SWL maintains a list of approved software on the UmichITAM website.

Compliance

Compliance with software license requirements is a complex process. There are no overall guidelines on what constitutes compliance and it can be different for each publisher. Each publisher defines compliance for his or her own products. Proofs of purchase and certificates of authenticity are generally viewed to be evidence of compliance. However, each publisher must be contacted to determine their definition of compliance.

SWL manages compliance using KeyServer⁴ to ensure that the terms and conditions of each licensing agreement are enforced to mitigate the risks of audits and fines from software publishers and software watchdog groups such as the Software Business Alliance (SBA) and the Software and Information Industry Association (SIIA). This software manages applications on sixteen thousand machines.

Adding Software

Applications are added to the portfolio if funding is available, a cost saving is achievable through inclusion, and the use of such software spans multiple independent units. UmichITAM processes and funds software that meets these acquisition requirements. If insufficient demand exists for a specific title, SWL puts it into a queue until sufficient interest is demonstrated. At that point, SWL will request a quote from the publisher or vendor.

Software must be used primarily for administrative or instructional use to be added to the UmichITAM portfolio. The costs of research software must come from departmental or grant funds. LSA departments may work with SWL to negotiate licenses with vendors even if the acquired software is not shared with other UmichITAM members. SWL charges such software directly to the requesting department.

Consolidating Software

UmichITAM consolidates licenses for software titles already purchased by members. This can result in a cost savings due to volume discounts. SWL collects and redeploys abandoned licenses in an effort to forestall the need for acquiring additional licenses when unused capacity exists. Additionally, this process helps eliminate spending on obsolete software. Use of concurrent licenses helps minimize the need for license harvesting⁵. However, there are still several titles that are licensed on a per-install basis.

The objective of the audit was to assess UmichITAM's ability to reduce member software costs while ensuring compliance with applicable licensing provisions by using effectively controlled processes and a secure processing environment. University Audits reviewed the following SWL processes:

- Distributing software resources and costs across multiple units within the University to increase the return on investment on software

⁴ KeyServer is a license control product from Sassafra Software designed to allow a network administrator to centrally control access to any Windows or Macintosh application running anywhere on (or off) the network. KeyServer limits launches of each application to the legal number available and can control access to a given program by any combination of criteria such as network location, time of day, name/password etc.

⁵ Harvesting is the process of identifying copies of software licenses that are underused and making those copies available to other individuals or environments to avoid the cost of an additional license to support the genuine need.

- Reducing the total cost of ownership of software through management of licensing and monitoring capacity
- Creating a consolidated repository software assets
- Maintaining compliance with licensing agreements
- Co-locating⁶ of a K2 Shadow on each subnet

This audit examined the effectiveness of controls over the shared portfolio including all software applications licensed by LSA (including applications shared with CAEN and ITS). The applications managed by ITS and subject to direct billing such as Microsoft products, Anti-Virus software and Apple Mac OS X were excluded.

Risk and Control Discussion

- Use of the K2 Client - SWL uses Sassafras K2 KeyAuditor and KeyServer to manage compliance and ensure that the terms and conditions of the licensing agreements are enforced. A K2 client represents a vital part of this monitoring process. Failure to deploy this software on all relevant machines makes it difficult to monitor software usage and control compliance with licensing agreements. Although most LSA machines use the client, including an increasing number of LINUX machines, accurate license monitoring requires that the client be deployed on all machines in LSA and those housed in other UmichITAM partners. University Audits recommends that use of the K2 client on each workstation participating in the UmichITAM program be made mandatory.

Management Plan - A policy will be drafted regarding the K2 Client for LSA units. A Service Level Agreement with this requirement for non-LSA UmichITAM partners will be created. A process will be created to measure that the K2 client has been installed on all IT assets.

- Firewalling License Servers - UmichITAM's license servers are open to the internet. This means that anyone who knows the names of these license servers could potentially use the University's licenses. SWL indicated that they have seen faculty/staff leave campus and still access the license servers and use UM software licenses. This unauthorized use could result in violation of licensing agreements with potential fines or other penalties.

Management Plan - SWL will create a project to communicate and educate end users regarding the impact of this change. Due to the current expectations of software availability off campus, we will need to ensure adequate communication has been made, as well adequate education so faculty will know how to access software managed by license servers from off campus. Changes in infrastructure may also be necessary in order to allow the current VPN solution to work with network-licensed software.

- Changing and Deleting Users - UmichITAM user IDs are issued to Department System Administrators (DSA) who are privileged users. Many of these DSAs work in areas outside of LSA. Deleting system access as a result of employee transfers and terminations represents a problem for any system administrator. Unless those running the system have a mechanism for identifying transferred or terminated employees, users with no business reason for access continue to retain system access. Although SWL effectively administers IDs for users in LSA departments, LSAIT currently does not have a procedure for eliminating non-LSA DSAs from the system when they transfer or terminate.

⁶ Co-location allows a department to place their servers on someone else's network and/or in their facility. Co-location facilities have better outage protection.

Management Plan - The SWL group will create a procedure for non-LSA partners. This procedure will also be added to the SLA as an UmichITAM requirement.

- **Key Process Areas** - Twelve Key Process Areas (KPA) designed to ensure that software assets are managed properly constitute the UmichITAM program.
 - Acquisition management
 - Asset identification
 - Compliance management
 - Communication and education management
 - Disposal management
 - Documentation management
 - Financial management
 - Legislation management
 - Policy management
 - Project management
 - Program management
 - Vendor management



UmichITAM Roadmap 2011,
issued December 2010

The UmichITAM Roadmap 2011, which describes ITAM procedures, discusses these processes. Not all process documentation is complete and up-to-date.

Management Plan - Some of the processes associated with the KPA's have been modified on the SWL Sharepoint site. The SWL group will update the Roadmap based upon training that the Software Asset Manager recently attended. He will incorporate what he learned into the document.

- **Project Management** - A formal project management process does not exist within UmichITAM. LSAIT does not have a set of guidelines for project management. Lack of a formal methodology can make it difficult to prioritize projects and ensure that adequate resources are available for completing high priority projects.

Management Plan - The Software Asset Manager will develop the foundation for project management for the ITAM program. Since project management is a KPA of ITAM, this will remain an area of focus for the short and long term.

- **Disaster Recovery and Business Continuity Plans Testing** - Review of the disaster recovery plans for the license servers and the business continuity plan for the K2 Server revealed these documents are well written and comprehensive. The plans address a number of scenarios that potentially threaten the resources and processes for software licensing. However, there is no provision for periodic testing of the plans. Conducting mock disaster exercises makes it easier to discover gaps and inconsistencies that could limit plan usefulness in the face of an actual disaster.

Management Plan - The LSAIT Security Manager will update the disaster recovery plan with rules for testing. Testing will subsequently be performed.

- **Management of Copyrighted Software** - Standard Practice Guide (SPG) sections related to software are outdated. *SPG Section 601.03-0 Ownership and Use of Computer Software* has not

been updated since 1979 and *SPG Section 601.03-1 Management of Copyrighted Software* has not been updated since 1993 and refers to methods of purchasing software that are no longer in practice at the University of Michigan.

Management Plan - We will form a committee to develop new policy verbiage. The committee will consist of members of Office of the General Counsel, Office of the CIO, the UM Copyright Office, and others who would add value to the discussion.

- **Licensing Processes** - SWL monitors the KeyServer on an ongoing basis. They track usage patterns over time to ensure that demand and supply of software are balanced. UmichITAM uses KeyServer usage data to make software provisioning decisions. However, department IT staff are not notified which specific software is needed by individual faculty for classroom teaching. This creates the problem of wasteful spending by staff deploying several software titles to machines where the software will not likely be used. This lack of communication also increases the risk that software licensed for administration and teaching is used for research, which may violate certain software licenses.

Management Plan - We will form a Steering Committee to discuss possible solutions. The Steering committee will consist of stakeholders from areas that will be impacted by this project.

- **Maintenance of Access Control Lists for the KeyServer** - SWL had not removed access to the export file on the KeyServer for a temporary employee who is no longer with LSAIT SWL. Access to the export file is needed for part of SWL's maintenance processes. Export files can also be used to create a data mirror⁷ for more advanced reporting.

Management Plan - LSAIT Software Licensing group immediately revoked access and will perform regular reviews of access.

Software asset management is an important business process that has the potential to provide the University substantial cost savings through better utilization of existing licenses and stronger negotiating positions on future software purchases. In 2010, LSAIT estimated a Total Portfolio Cost Avoidance/Savings from ITAM of approximately eleven million dollars. ITAM provides effective compliance with software licenses to help eliminate losses due to fines. The need for software management is a growing one. As copyright laws become more restrictive, there is the potential for an increase in liability if the University does not manage software correctly. It appears that real opportunities exist for better monitoring of compliance and conserving resources through license consolidation by extending the ITAM program to the University as a whole. ITAM is integral to keeping costs under control and identifiable. Hardware Asset Management and Software Asset Management are both key to ITAM. Management should consider performing a cost benefit analysis for extending the ITAM model throughout the University.

Based on the audit work conducted, it appears that controls are in place and provide a level of assurance that UmichITAM is able to reduce member software costs while ensuring compliance with applicable licensing provisions using effectively controlled processes and a secure processing environment.

The SWL group in LSAIT Security effectively administers ITAM. They have well documented processes for managing software that include robust controls over purchasing and access management, and proactive monitoring of licensing provisions.

⁷ A copy of data made from one location to a storage device in real time. Because the data is copied in real time, the information stored from the original location is always an exact copy of the data from the production device.

UmichITAM has performed a risk assessment, defined incident response procedures, and created a security plan in accordance with University of Michigan's Information and Infrastructure Assurance (IIA) guidance.

University Audits will conduct a formal follow-up to the outstanding issues during the third quarter of fiscal year 2012.

[UM-Flint Business Continuity](#)

#2011-303

Report issued August 12, 2011

Based on University Audits University-wide annual risk assessments, a review of UM-Flint Business Continuity Planning was conducted. Best business practice indicates that proper business continuity management (BCM) and planning is essential to a large organization such as UM-Flint. The goal of BCM is to enable the University to restore critical processes after a disaster.

Key departments have incorporated business continuity into their operations and preparedness planning. Campus discussions of continuity planning have occurred dating back to 2000. UM-Flint is currently part of a multi-year FEMA hazard mitigation planning initiative. An independent consultant is reviewing University property and operations, conducting a thorough risk assessment, hazard and vulnerability analysis, and evaluation and prioritization of mitigation strategies. Management implemented focused initiatives to improve crisis communication among leadership on campus, for response and preparedness planning drills and exercises, and training for enhancing students, faculty, and staff understanding of their roles before, during and after an emergency.

The primary objective of this audit was to verify that a comprehensive continuity plan for UM-Flint includes the following components:

- Risk Assessment and Risk Mitigation –Identifies potential risks and determine their probability and potential impact
- Business or University Impact Analysis (BIA/UIA) - Identifies business processes that are integral to keeping the University functioning in a disaster and to determine how soon these integral processes should be recovered following a disaster
- Business Recovery and Continuity Strategy - Addresses the actual steps, people, and resources required to recover a critical business process
- Maintenance - Ensures that the Business Continuity Plan (BCP) remains effective and aligns with University priorities
- Exercises and Training - Educates personnel and identifies potential shortfalls of the BCP

University Audits conducted interviews with Flint's Chancellor, Provost, Environmental Health and Safety Manager, Registrar, and Library Director. This audit did not involve an in-depth review of departmental continuity plans, but did include a brief review of the Registrar's Office and UM-Flint Library's continuity plans to evaluate the processes used to develop and the information gathered while establishing the BCP.

Risk and Control Discussion

- University Impact Analysis - University of Michigan-Flint has effectively identified risks and corrective actions. The next step in the impact analysis process would be analyzing business process and prioritizing them at a UM-Flint-wide level. Although discussions related to this topic have occurred both as part of the Campus Hazard Mitigation Planning Process and during the All Hazard Planning Team meetings, a more formal and documented evaluation of these

campus-wide business processes discussions would help to elevate the UM-Flint campus continuity planning to the next level. At this point, UM-Flint would benefit from a formal, campus-wide impact analysis. Such an impact analysis involves identifying business processes and workflow that are integral to keeping the University functioning at the University, college, and department level. An impact analysis also establishes the priority of restoration for critical processes. Recovery Time Objectives (RTOs)⁸ and Recovery Point Objectives (RPOs)⁹ of each critical business processes are also determined during the impact analysis. At UM-Flint, individual units are required to identify the business processes that are critical to local operations, prioritize them, and develop continuity plans. However, these critical processes are not evaluated and prioritized at the University level.

Management Plan - We believe that significant and sustained all hazards business continuity planning has been, and continues to be, an integral aspect of our ongoing preparedness planning for the campus. The Executive Officers (EOs) support the recommendation to conduct a business impact analysis by first identifying and prioritizing critical business operations and processes for each of their respective EO areas. Furthermore, the EOs will establish a small team representing academic and non-academic operations with assistance of an external consultant (due to limited staffing resources) that will evaluate these critical business processes and conduct a business impact analysis of these critical processes/operations on the Flint campus. This team will report to the EOs on the action plan and progress. Assembly of the work group to address this recommendation will take place in fall of 2011.

- **BCP Standard Template** - UM-Flint uses a standard template for business continuity planning. The continuity plans developed using this template address only the assumptions of reduced staffing levels and undamaged facilities. This set of assumptions is characteristic of pandemic planning. The template adequately addresses pandemic planning but does not address other scenarios.

Additionally, the business continuity template does not force users to document certain information required to resume business operations after a disaster. Along with the information already requested in the template, other areas typically addressed in a business continuity plan include staffing recovery activities, provision of alternate office or facility spaces, and identification of information technology dependencies and significant procedural changes that could occur during the contingency. As currently constituted, the standard template will not result in a plan comprehensive enough to provide the ability to successfully restore University operations if a disaster occurs.

Management needs to address the following areas in the standard template:

- The business continuity template needs to expand beyond pandemic planning
- The section of the template titled “Action Plan to Continue Essential Operations/Service” should include more detail such as:
 - Identification of process dependencies such as Financial Aid Office processes that are critical to Payroll processes and Payroll processes that are dependent on Financial Aid processes
 - IT dependencies such as online forms, databases, and websites
 - RTOs and RPOs
- Processes need to be identified for different types of events such as loss of facilities, resources, or personnel

⁸ RTO is duration of time within which a process must be restored to avoid unacceptable consequences.

⁹ RPO is the amount of data that can be lost if a disaster destroys the information systems.

- The template needs to identify whether critical processes can operate under reduced capabilities and document those capabilities
- A section to document contracts or agreements with other department, facilities, and/or campuses showing established arrangements to share staff, facilities, and/or other resources in the event of a contingency
- The BCP should also include procedures on how to return processes to normal operation once all contingencies are over and operations under reduced capabilities are no longer necessary

Management Plan - We agree that the existing University of Michigan business continuity planning template is in need of updating to better reflect the ongoing all hazards continuity planning that is occurring at the Flint campus. Environmental Health and Safety is planning on reviewing and updating the instruction narrative located in the beginning of the document, adding sections to assist units in identifying and communicating their departmental specific ITS and Facilities related needs, and ultimately, if feasible, to explore creating a web-based process so completing the BCP template and performing the annual updating is easier. A web-based process would also facilitate processes for units involved in reviewing and prioritizing needs across the campus allowing for robust evaluation of departmental plans in relationship with other plans. Upgrading the general template will be relatively straightforward. Moving it from a paper system to a web-based system will be more involved and require further expertise and assistance from a person/consultant with previous knowledge and skills in successfully developing such a program.

We will begin to reformat the template in the fall of 2011. Discussions with a consultant to investigate the feasibility of a web-based approach to BCP will begin following the completion of our FEMA Hazard Mitigation Plan in 2012.

- **Business Continuity Testing** - Not all units are fully testing their Business Continuity Plans. When exercises are conducted, the focus centers on Emergency Response to the event rather than how to restore the business process at alternate sites, with reduced personnel, and/or lack of IT assets once the emergency is over. Exercising and testing of the BCP is the most effective way to identify gaps within the plan and help identify areas that need to be updated due to changes in the business process or personnel. Various exercises can be conducted such as desk checking, walkthroughs, tabletop exercises, and complete end-to-end testing.

Management Plan - We agree that departments should test their BCPs and by doing so will further strengthen our campus preparedness and overall ability to restore our critical business operations. Environmental Health and Safety will further promote additional testing of select continuity plans in spring/summer 2012.

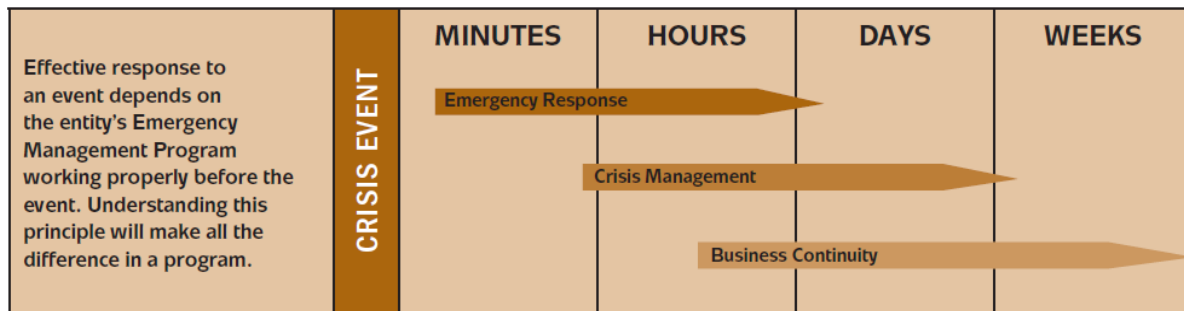
- **Disaster Recovery Plan** - Critical business processes have not been identified at U-M Flint as a basis for ITS' Disaster Recovery Plan (DRP). UM-Flint ITS developed a DRP in the absence of a formal BIA. Failure to base a DRP on an effective BIA can compromise the DRP's effectiveness. Disaster recovery planning done to restore information technology capabilities is an element of the BCP and should support restoring operations critical to the resumption of business. These IT capabilities include regaining access to data, communications, and other business processes after a disaster. Backup schedules and restoration priorities should be designed to meet the University's needs set forth by the BIA.

Management Plan - Over the past five years, ITS has pursued working with units at the University of Michigan Ann Arbor campus, as well as other public higher education institutions

in Michigan, as partners to create offsite disaster recovery options. ITS has been proactively working with ITS Ann Arbor and others internal/external to the campus in further developing, testing, and enhancing the DRP. A great deal of effort has been focused on addressing the needs of providing timely restoration for critical network systems and data storage for the campus based on information received from key departments on campus. Partnerships have been, and continue to be, explored for off-site backup with University of Michigan Ann Arbor and University of Michigan Dearborn campuses. ITS will continue efforts to enhance a process that encourages individual departments and ITS to work more closely together to determine and prioritize critical business operations that rely upon key IT systems and network availability as well as providing the needed support in identifying, supporting remote and alternate work locations.

University of Michigan-Flint has been proactive in creating emergency preparedness and response procedures. These efforts at evaluating and identifying hazards, determining probability, and mitigation strategies help minimize the impact of a disaster. By reducing the impact of the disaster, business processes are more sustainable during and after a crisis.

Working with a third-party consulting firm, UM-Flint is in the process of developing a FEMA Approved Hazard Mitigation Plan. Identifying and mitigating the hazards UM-Flint faces is a key portion of the BCP. However, further action, as discussed above, needs to take place to ensure the University can sustain business operations both during and after a disaster. Business Continuity is not “Emergency Response” or “Crisis Management.” Each one of these is an important part of emergency management but each has a different focus and separate goals from continuity planning. Each of these areas need to be addressed to ensure the immediate response to a disaster, the management of the crisis, and the resumption of business operations are effectively coordinated.



Source: Global Technology Audit Guide, Business Continuity Management, Institute of Internal Auditors, David Everest, Key Bank; Roy E. Garber, Safe Auto Insurance Co.; Michael Keating, Navigant Consulting; Brian Peterson, Chevron Corp

University Audits will conduct a follow-up of management’s progress on action plans in the third quarter of fiscal year 2012.

[University of Michigan Health System Level 2 Identity Management](#)

#2011-306

Report issued August 26, 2011

Medical Center Information Technology (MCIT) creates and maintains digital identities for more than 30,000 users within the University of Michigan Health System (UMHS) and other segments of U-M’s HIPAA¹⁰ covered entity. The identity management system, through which these credentials are defined and stored, provides authentication, authorization, and role management for the UMHS Exchange email

¹⁰ Health Insurance Portability and Accountability Act

system, workstation logon, file storage, UMHS web sites, and applications such as MLearning, CareWeb, and UM-CareLink, and is planned for use with MiChart¹¹.

UMHS uses levels to distinguish between campus-issued and UMHS-issued computer accounts. The term Level 1 describes the username and UMICH Kerberos password issued by Information and Technology Services (ITS) to all University of Michigan employees. The Health System issues Level 2 accounts to more closely control and monitor access to electronic PHI¹². To comply with the HIPAA Security Rule for remote access, Level 1 is used to connect remotely to the UMHS network, and Level 2 is used to access UMHS systems, providing a second layer of authentication and authorization. University Audits conducted a review of Level 2 identity management within UMHS.

Effective identity management is essential to ensure the confidentiality, integrity, and availability of UMHS patient, faculty, staff, and student data. Careful management of identities significantly reduces the risk of inappropriate use, damage, or theft of University resources and helps mitigate the risk of penalties for failing to comply with a wide range of local, state, and federal regulations enacted to protect information resources.

The primary objectives of this audit were to assess the effectiveness of policies and procedures and to verify adequate controls are in place for the Level 2 identity management system. University Audits evaluated the following components:

- Lifecycle of Level 2 accounts
- Username management
- Configuration and management of Level 2 passwords
- Verification that Level 2 identity management systems are considered for use in future UMHS IT systems

Risk and Control Discussion

- **Password Distribution** - Level 2 password distribution methods are not in accordance with UMHS Information Security Supplement and Requirements. MCIT Identity Management Team (IDMT) members currently print a "User Information" sheet containing a list of users including each person's full name, username, UMID and a PIN number. The IDMT member also prints a "UMHS Access Information" card containing the PIN number and the user's Level 2 password, and then places a scratch-off sticker over the password. The PIN number allows support staff to associate the two separate cards as part of its distribution to the user. This distribution method appears to work well but requires human intervention, enabling one individual to see a username and password prior to placing the sticker on the card. Information Security Supplement and Requirements V.D.2(a) states, "If there is human intervention, besides the user, the password must be expired and reset by the user prior to use on an ePHI system." The "UMHS Access Information" card advises users to change their passwords and instructs them how to do it, but the system does not require them to do so. This practice is contrary to UMHS policy.

Management Plan - The identity management team will request a meeting with the Compliance Office to review options and define next steps. The options include:

- Approval to continue current practice
- Forcing customers to reset passwords during initial authentication, which would negatively impact on-boarding of large groups at MTV (Michigan Traditions and Values), house officer, medical student, and nursing student on-boarding events

¹¹ MiChart is a multi-year clinical system implementation providing an integrated suite of applications that support patient care.

¹² Protected Health Information

- Development of off-site password self-service portal mimicking the current process used by Campus to set the user's initial Level 1 (UMICH) password
- Other possible solutions yet to be identified

Existing controls over the lifecycle of a Level 2 account are sound. Automated procedures are used to establish and remove Level 2 accounts and create user names. Password criteria are stringent, and Level 2 is included during the Request for Proposal (RFP) phase of new projects. By implementing the recommended changes, MCIT IDMT and Level 2 will strengthen the already well controlled environment.

The Level 2 identity management system is attentively and proactively managed by MCIT IDMT. Policy, procedures, and flowcharts documenting system configurations were readily available for review. MCIT IDMT is exploring new technologies to enhance the security provided by Level 2, such as using mobile phones/smartphones as an additional authentication factor in highly sensitive systems. MCIT IDMT sets goals for improving identity management in additional ways, including:

- Reducing the number of special processes used to create accounts, cutting down on manual data entry, and speeding up the delivery of credentials
- Collecting information required to support role-based access control and ensure proper privileging
- Categorizing users to streamline the delivery of applications, services in accordance with compliance requirements
- Understanding the relationships between a user/role and the services and applications to which they have access
- Reducing manual workloads and ensuring compliance requirements

MCIT IDMT is also actively involved with the MiChart project, ensuring the Level 2 identity management system is well integrated with new systems. The replacement of legacy systems with MiChart throughout UMHHC will increase and enhance utilization of the Level 2 identity management system.

University Audits will conduct a follow-up review during the third quarter of fiscal year 2012 to assess the effectiveness of improvements implemented by management.

[Information and Technology Services CTools Software Development Processes](#)
Report issued August 29, 2011

#2011-808

CTools is an open source, web-based, course and collaboration environment. It provides a set of tools designed to help instructors, researchers, and students create course and project websites. These CTools sites allow faculty and students to communicate about course requirements, assignments, projects, and more.

Students are given access to the CTools site for classes in which they are registered. Using a web browser, faculty choose from the many options in CTools and combine them to create a site that meets their course needs. Faculty post assignments, required materials, and syllabi to these sites, and expect students to regularly review the materials. Additionally, CTools is the course management system used to deliver online courses at the University of Michigan and in the College of Arts, Sciences, and Letters at the University of Michigan-Dearborn.

The Sakai Foundation is a community of academic institutions, commercial organizations, and individuals who work together to develop a common a Collaboration and Learning Environment (CLE).

CTools is the University of Michigan's implementation of the Sakai Project's CLE software. Information and Technology Services (ITS) is responsible for managing CTools at U-M. This includes management of the multiple software environments (development, test, load, and production) and the hardware on which they run.

Sakai CLE is an open source project. Sakai Project's CLE continues to be developed by multiple people from multiple institutions. All work done on the project by individuals is made available to the group. CTools is running code developed here and elsewhere as part of the CLE project. This relationship allows the University to leverage not only our own developers, but that of the entire Sakai community to improve and advance CTools. To ensure this is done safely, both Sakai and ITS have implemented rigorous review and testing processes on all new code.

CTools version 2.7.1 was released to the U-M community on December 28, 2010. This version represents a significant upgrade from 2.7 and includes new features in existing tools, improvements in ease-of-use and navigation, and bug fixes.

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

- Assessing the management of CTools hardware in terms of:
 - Consistency between environments
 - Ability to handle user load
 - Change management procedures
 - System inventory and documentation
 - Access control
- Assessing the management of CTools software related to:
 - Version control
 - Code classification
 - Change management procedures
 - Code migration processes and procedures
 - Access control
 - Assessing updates and backups that affect security and availability

Failure to effectively manage risk within CTools could result in:

- Failure of critical academic support systems
- Loss of academic data
- Negative publicity for the University

This audit included an examination of the management of the CTools system and the processes, policies, and procedures that directly affect it. Security was only reviewed as affected by system updates and backups.

Risk and Control Discussion

- Documentation - Proper documentation of a complex system like CTools is essential to continued success in administering and managing the service. Having documentation detailing processes and procedures helps ensure that they are done correctly and are easily repeatable. University Audits noted the following areas either are not documented or have out of date documentation:
 - End-user service level expectations such as user data retention and restoration, maintenance windows, system availability, support availability, maintenance and other notices of changes

- Service Level Agreements (SLA) with data center providers
- Hardware inventory
- Sakai application update processes such as the release process, new version evaluation and product planning, and security issue procedures
- Server Operating System update process
- Radmind software use
- User access reviews (i.e., How usage data is used to inform product and infrastructure planning)
- Growth planning process
- Hardware management processes (i.e., installation, repair, change, removal)

Management Plan - We agree and will take measures to ensure the documentation, SLAs, and Operating Level Agreements mentioned above are created and maintained into the future. Many of these items will be addressed as part of the ITS CTools Infrastructure Rationalization priority project.

- Backups - A well thought out and properly implemented backup strategy is a key component of any successful computing system. Ensuring the integrity and availability of data is necessary with a system as important as CTools. The system is currently backed up using a variety of methods managed by different individuals. The processes, as implemented, have been successful thus far.

CTools management should review all backup processes currently in use for locally managed systems and decide upon a coordinated backup process. Implementing a unified backup strategy would ensure no gaps in the data being preserved. It would also allow for quicker recovery, easier testing, and a single upgrade path. Implementation of this single process across the platform will simplify the process and provide for improved controls and performance.

Management Plan - We agree with this recommendation. Coordinated, synchronized backups of infrastructure components that must be kept in sync will be addressed as part of the ITS CTools Infrastructure Rationalization priority project.

- Use of wush.net - Code developed for CTools is stored within the Subversion¹³ code management system. This helps ensure that code is properly backed up and revisions are appropriately tracked. The CTools group also purchases space with online storage vendor wush.net. Space on wush.net was previously used for code that was deemed to have “secret” information in it. This information included hardcoded passwords. Coding practices have changed within the CTools group and no “secret” information is included in code anymore. This renders the wush.net repository redundant and unnecessary for the CTools product. The ITS Teaching and Learning will retain a wush.net account but only use it for non-CTools code and other activities (e.g., issue tracking).

Management Plan - We agree and will take steps to remove any CTools specific code from the wush.net repository and document guidelines for the appropriate use of wush.net for non-CTools related activities.

CTools is one of the most used and most popular applications at the University. This service has become a must use tool for faculty and students alike, and has become critical to the academic and research

¹³ Subversion is a version management software application provided by the Sakai Foundation to member institutions.

missions of the University. Over 80% of the courses offered by U-M have a CTools component. Its feature set and reliability have ensured quick adoption and continued usage. It is estimated that every student will have used CTools in some capacity before graduation.

Much of this is possible because CTools is well managed. The development process has a series of checks to make sure code meets the high standard of functionality that has come to be expected. The development team utilizes built in checkpoints in the development process to double check each other's work and ensure proper functionality. Hardware is properly administered ensuring availability and performance. The service, as a whole, is well run.

While CTools is being properly managed, there is still room for improvement. Many of the processes and procedures that are the key to its continued success are undocumented. This creates a high potential for institutional knowledge loss. It also increases the potential for deviation from these proven practices.

A formal follow-up to the outstanding issues will be conducted during the third quarter of fiscal year 2012.

Follow-up Reviews

[U-M Dearborn ITS Data Center at Fairlane Center](#)

#2010-309

Original report issued November 18, 2010

Follow-up report issued July 13, 2011

The original audit report contained two open action items. A follow-up review was recently performed by University Audits. Both of the open items have been addressed. **This audit is closed.**

- Disaster Recovery Plan - Dearborn Information Technology Services (ITS) developed a "Disaster Recovery, Initial Plan and Outline" that addresses the control recommendations from the audit. The purpose of this document is to define, at a high level, steps needed to be implemented in a disaster scenario and continuity strategies in the event of a failure at the Fairlane Data Center. Key infrastructure components have been identified along with responsible personnel. ITS Dearborn is continuing to expand and refine this plan. University Audits has reviewed this plan and determined that it effectively addresses the recommendation.
- Visitor Control - As of June 1, 2011, the University of Michigan-Dearborn Public Safety (DPS) Office took over responsibilities for security at the Fairlane Center. University Audits reviewed the memo indicating the transfer of security responsibility from Guardsmark to DPS. Updated procedures now include the requirements for contractors working in the Fairlane Data Center to follow sign-in procedures. ITS has worked with DPS to confirm the procedures for data center access are followed.

[University Press](#)

#2008-203

Original report issued January 30, 2009

Follow-up report issued July 27, 2011

In January 2009, University Audits conducted an audit focused on the processes associated with recording inventory and accounts receivable balances for University Press (UPress). The audit included review of:

- Policies and procedures for recording inventory and accounts receivable
- Contract with Perseus¹⁴ Distribution Systems (PDS)

¹⁴ Perseus Distribution has been providing warehousing, fulfillment, and distribution services to UPress since 2006.

- Business office and accounting procedures
- Management reporting

At the time of the audit, it was determined that controls were not in place to provide an acceptable level of assurance that the accounts receivable and inventory balances for UPress are properly stated in the financial records of the University of Michigan. The processes used to produce these balances were not consistent or well controlled.

University Press enlisted the assistance of Financial Operations and requested advice from University Audits to ensure that their business decisions and processes are based on accurate, timely, and consistent financial reporting.

In September 2009, UPress transitioned from an auxiliary unit reporting to Rackham Graduate School to a department reporting to University Libraries. To address the issues raised during the audit, and to place UPress accounting and financial analysis on a stronger foundation, a temporary controller was hired and consultants engaged to analyze all accounting processes at UPress.

- University Press Business Office and Accounting Practices - The initial audit identified control weaknesses related to producing and analyzing financial data and reports at UPress.

Recommendations included:

- Instituting high-level accounting reviews
- Ensuring that UPress closes the financial books regularly and reconciles financial information between M-Pathways, UPress financial statements, and the distributor's records
- Streamlining the process for booking adjusting entries
- Formalizing and documenting accounting policies and procedures

The following controls have been instituted to address these recommendations.

- The UPress Director and Library Chief Operating Officer (COO) perform a high-level review of the balance sheet and income statement on a quarterly basis. The Director and Library COO sign the reports as evidence of review.
- Controls were instituted to help UPress close the financial books on a timely basis, including a closing checklist.
- The UPress Business Office created and maintains a monthly and annual closing checklist that specifies who is to perform each task.
- UPress has worked with an outside consultant and developed documented accounting policies and procedures.
- UPress management implemented a process to reconcile their internal financial statements to M-Pathways.
 - UPress extracts financial and business information from M-Pathways (the University's official book of record) and other systems.
 - Spreadsheets are used to compile the information and create final financial statements.
 - University Audits reviewed the reconciliation process and noted that UPress financial statements agree to M-Pathways when reconciling items are considered. Reconciling items include minor adjustments and a monthly receivable entry not made in M-Pathways.
 - University Audits recommends that UPress analyze the reconciling items each month to identify process changes that could reduce, with a goal to eliminate, reconciling items. Minimum dollar thresholds could be established to dictate when adjustments outside of M-Pathways are

made, and the monthly receivable entry should be reflected in M-Pathways. Since a monthly reconciliation is performed and discrepancies are identified and explained, the risk of producing final financial statements that materially differ from M-Pathways is low.

- Manual reconciliation processes, noted in the original audit, have been eliminated or streamlined and documented.
- Relationship with Perseus Distribution - University Audits examined the agreement between UPress and PDS during the original audit and noted that UPress did not exercise financial oversight over PDS on an ongoing basis. UPress did not receive appropriate management information from PDS, especially in the areas of uncollectible accounts, obsolete inventory, and comparative analysis. University Audits recommended that UPress evaluate the value of additional information from PDS against the cost benefit of obtaining that information and that UPress confirm the accuracy of data and reports from PDS on a regular basis. To address the risks identified:
 - UPress performed a benchmarking study of nine university presses, which included a review of fulfillment and distribution.
 - The UPress Logistics Manager reviews the PDS Cycle Count Report on a monthly basis to substantiate PDS data and reports.
 - The UPress Business Manager reviews the Monthly Inventory Error Report, which identifies missing receipts by comparing the International Standard Book Numbers (ISBNs) and inventory quantities.
- Inventory Valuation - At the time of the audit, it was determined that an accurate inventory valuation was necessary to properly analyze inventory costs, understand exposure to various valuation issues, and price and market UPress publications. University Audits recommended that UPress work with Financial Operations to determine proper costing method and valuation for inventory. Several implemented procedures address this issue.
 - UPress management and the University Controller reviewed the accounting treatment of plant costs, copyediting, and production costs and treatment of complimentary books for appropriateness.
 - UPress inventory database was examined and refined.
 - An obsolescence reserve has been established.
 - Monthly obsolescence adjustments are made based upon a formal UPress write-off policy, which is reviewed on an annual basis.
 - Unit costs at PDS are reviewed monthly and reconciled by UPress on an annual basis.
 - Work in process costs are reconciled to M-Pathways on a regular basis.
 - Procedures for inventory management have been documented.
- Accounts Receivable Valuation - Previously, the accounts receivable value for UPress was recorded from numbers provided directly from the PDS reports. Other observations noted that UPress accounting personnel had direct access to the PDS financial system, there was a lack of bad debt analysis, and an absence of a reserve for book returns. To address these observations:
 - UPress reconciled the PDS statement to the Perseus data warehouse and to sales, inventory, and cash transactions in the general ledger. The UPress Business Manager reconciles the PDS statement on a monthly basis.
 - The UPress Logistics Manager conducts physical inventory cycle counts at the Perseus Jackson, TN location on an annual basis. Investigations of discrepancies are done for ISBNs that have a variance percentage more than 2% or 100 units.
 - A process has been created for estimating bad debts.

- UPress now prepares an allowance for doubtful accounts on an annual basis in accordance with Generally Accepted Accounting Principles.
- The UPress Business Office prepares an annual customer return analysis to create a reserve for returns.

University Press has made significant progress in improving its inventory and accounts receivable processes. Controls have been implemented to provide reasonable assurance that the accounts receivable and inventory balances for UPress are properly stated in the financial records of the University of Michigan. The processes used to produce these balances are formally documented and reviewed on a regular basis. University Audits verified the regular reconciliation of UPress data to M-Pathways and assessed the processes, controls, policies, and accounting procedures instituted by UPress to mitigate risks identified during the initial audit. UPress should continue to evaluate related risks and modify or refine these processes and procedures for appropriateness and effectiveness. **This audit is now closed.**

Unauthenticated Wireless Access

#2010-312

Original report issued December 22, 2010

Follow-up report issued September 2, 2011

- CALEA Compliance - Based on the presence of unauthenticated wireless services at U-M, University Audits recommended that Information and Technology Services (ITS) work with the Office of the General Counsel (OGC) to identify and implement the steps necessary to assure that U-M remains compliant with the Communications Assistance for Law Enforcement Act (CALEA). CALEA obligates Internet access providers to make it possible for law enforcement agencies to perform surveillance of Internet traffic.

OGC has performed additional research into the University's obligations under CALEA. Based on this research, they identified two separate elements.

First, U-M must be CALEA compliant by ensuring it can provide law enforcement timely access to U-M networks through a specialized interface. Merit Network provides this service to U-M as the University's Internet access provider. In OGC's opinion, U-M is therefore CALEA compliant.

Second, U-M may register itself with the Federal Communications Commission (FCC) as an Internet access provider under CALEA. Based on extensive inquiries and consideration, OGC's opinion is that registration is not appropriate for U-M. OGC noted that few post-secondary institutions have registered themselves. Michigan State University registered, but indicated to OGC that in hindsight registration was not helpful and was unnecessary. Many organizations in the educational community (i.e., American Council on Education, EDUCAUSE) recommend that compliant organizations such as U-M forgo registration. In addition, U-M faces no penalty for not registering, should the FCC later determine that registration is necessary.

Based on OGC's considered opinion, **this item is closed.**

- Unauthorized Access to Licensed Content - University Audits recommended that the unauthenticated wireless network services should not provide, either directly or through address translation, any network address contained in the Library's file of address ranges authorized to access licensed content.

ITS Comm presented a proposal for unauthenticated wireless access to the Unit IT Steering Committee in July 2011. The Unit IT Steering Committee accepted the option in which ITS

Comm develops and deploys MGuest, an unauthenticated Wi-Fi network. This option includes using an IP address block that is not in the Library's file of IP ranges authorized to access licensed content.

ITS Comm is working to finalize the configuration of MGuest and deploy the service on campus during the fall semester. ITS Comm is also working to assist the small number of current providers of unauthenticated wireless access in adopting this approach. Based on the demonstrated progress toward resolving the issue, **this item is closed.**

This audit is now closed.

[UMHS Portable Electronic Devices](#)

#2009-305

Original report issued August 26, 2010

Follow-up report issued September 8, 2011

The original audit report contained four open action items. University of Michigan Health System (UMHS) Medical Center Information Technology (MCIT) is in the process of hiring a Business Systems Analyst. Responsibilities of this job include support for Portable Electronic Devices (PED) along with handling technical documentation and training materials. UMHS MCIT has indicated that the candidate hired for the Business Systems Analyst position will be responsible for addressing the issues identified during the Portable Electronic Devices audit, which include:

- Proper Use Standards: The new hire's responsibilities will include developing a Proper Use Standard
- Exposure Based on Standard Configuration: Current plan is to implement the Microsoft ActiveSync® policy on the Blackberry Enterprise Server (BES) during the Outlook Phase 2 Project
- Mobile Devices Policy: MCIT is still working to deploy a solution to address the conflicting UMHS and MCIT policies
- Access Control: The new hire's responsibilities will include developing a documented procedure to ensure disabled, inactive, and unnecessary accounts on the BES are removed

University Audits will follow-up with UMHS MCIT in December 2011, by which time management anticipates filling this open position and addressing these issues.

Open Audits Follow-up Table
September 30, 2011

Audit Title	Report Date	Issues	Expected Completion
Portable Electronic Devices UMHS 2009-305	8/26/10	Proper use standards; standard configurations; mobile devices policy; access control	First Follow-up September 2011 <hr/> December 2011
Plant Operations - Facilities Maintenance Building Automation Systems 2010-313	9/08/10	Open ports of monitoring devices; network security; network isolation	First Follow-up April 2011 <hr/> December 2011
Information and Technology Services Shared Desktop 2010-315	2/28/11	Included software; shared desktop program; disaster recovery plan; Windows @7 security/configuration design; updates(patch level)	November 2011
CAC and ITS Use of Federal Hardware in the Flux HPC Cluster 2011-810	4/12/11	Transitory oversubscription of federal hardware	First Follow-up June 2011 <hr/> June 2012
UMHS UM-CareLink Provider Order Entry System 2010-304	3/30/11	Access controls; incident response and escalation; change control	October 2011
UM-Flint Business Continuity 2011-303	8/12/11	University impact analysis; BCP standards template; business continuity testing; disaster recovery plan	March 2012
UMHS Level 2 Identity Management 2011-306	8/26/11	Password distribution	March 2012
ITS CTools Software Development Processes 2011-808	8/29/11	Documentation; back-ups; Use of wush.net	March 2012
College of Literature, Science, and Arts Information Technology Asset Management 2011-311	7/22/11	Use of the K2 Client; Firewalling License Servers; Changing and Deleting Users; Key Process Areas; Project Management; Disaster Recovery and Business Continuity Plans Testing; Management of Copyrighted Software; Licensing Processes; Maintenance of Access Control Lists for the KeyServer	March 2012

College of Literature, Science, and Arts Research Computing 2010-809	7/26/11	Security plan template; Data classification; Make available data storage; Centrally provided back-ups; Training; Anti-virus software; Disaster recovery plans; physical security	November 2011
Information and Technology Services eResearch Proposal Management 2010-304	6/27/11	Contractual restrictions on vendor access; "Site Manager" access	December 2011
Center for Human Growth and Development 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 <hr/> October 2011
University of Michigan Center for Statistical Consultation and Research (CSCAR) 2010-809	6/23/10	Recharge rates and workshop fees, segregation of duties, reconciliations, supplemental systems, policies/procedures	October 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	First Follow-up June 2011 <hr/> March 2012
University of Michigan Museum of Art 2010-201	12/17/10	Budget monitoring; collections inventory management; Museum Store inventory management; payroll processes; statement of activity reconciliation - system access; documented procedures	November 2011
UM-Flint School of Health Professions and Studies 2010-209	1/25/11	Segregation of duties; faculty and staff certifications; privacy and data security; policies and procedures; p-card controls; conflict of Interest and conflict of commitment management; affiliate payment processing	January 2012
University of Michigan-Flint Educational Opportunity Initiatives 2010-201	2/18/11	Strategic oversight and guidance; campus support and collaboration; budget and financial management; staff management; time reporting and payroll; event management; cash handling; business continuity; documentation of policy and procedure	December 2011

Conference Services 2010-102	2/25/11	Contract compliance; department accounting and reporting; billing and payment accuracy; payroll and time reporting; statement of activity reconciliation; background check verification; client management	October 2011
Division of Student Affairs Recreational Sports - Club Sports 2010-816	3/2/11	Sponsored student organizations; guidance; financial management; practice, game, and fitness space; medical support; property	December 2011
Division of Student Affairs Recreational Sports 2010-816	3/2/11	Revenue management; information technology; procurement; employment; cash handling; Outdoor Adventure Center process documentation; business continuity	October 2011
University of Michigan Flint Cashier's Office 2011-804	3/22/11	Vault balance; accuracy of cash; petty cash reimbursement; deposit delays; segregation of duties; collection process efficiency; security and access; policies, procedures, and training	December 2011
Office of the Vice President and General Counsel 2010-207	4/22/11	Physical and electronic document security; conflict of interest/conflict of commitment; monitoring matters requiring retention of outside counsel; document management; expense reimbursements; OGC procedures; annual certification and controls assessment	March 2012
Financial Analysis - Management of Asset Data, Space Data, and University Surplus 2010-111	5/10/11	Staff oversight; capital asset inventory management; government-titled assets; asset tagging; data security; outside trucking; sale of goods; physical security of assets; system access/data integrity; space survey submissions; building phase definitions	December 2011
College of Literature, Science, and the Arts Center for Afroamerican and African Studies 2010-820	6/1/11	Cash handling; travel advance procedures; purchasing review; P-Card/Concur process; conflicts of interest; payroll records; CAAS equipment; study abroad program administration; storage of business critical data	December 2011
Emergency Loans in Financial Aid 2010-112	6/7/11	Inconsistent processing; regulatory compliance; policies and procedures;	December 2011
Leased Employees 2011-112	6/7/11	Central process owner; identification of leased employees; U-M guidance; contracts	March 2012

University Unions 2011-814	6/15/11	General control environment; financial monitoring and oversight; purchasing management; human resource management; building renovation and maintenance	March 2012
Financial Considerations for International Activity 2011-101	6/30/11	Coordination of effort; documented policies and procedures; currency exchange; cash purchases; international bank accounts	March 2012
UM-Dearborn Office of the Provost 2011-210	6/30/11	Segregation of duties; timekeeping; policies and procedures; Fairlane Center procedures; collections and exhibitions	March 2012
Service Unit Billing 2011-104	7/26/11	Ownership of SUB Process; Identifying Recharge Activity; Inactive Recharge Information; FTP Account Management; Reporting Options	March 2012
Department of Geological Sciences Camp Davis Rocky Mountain Field Station 2011-813	7/28/11	Fire Safety and Inspections; Documented Policies and Procedures; Inventory Management; Documented Emergency Plans; Cash Handling; External Entities	May 2012
UMHS Professional and Hospital Customer Service Charity Care Policy 2011-107-1	6/21/11	Policy reforms needed due to the Patient Protection and Affordable Care Act (PPACA)	March 2012
UMHS Staff Licensure/Certification/ Registration Policy Review 2011-107-2	6/30/11	Documentation of required certifications; handling of credentialing time extensions; annual review and updating of licensure matrix	March 2012
UMHS Michigan Health Corporation 2011-	6/30/11	Assess effectiveness of JV compliance programs; standardized management analysis and operational reporting; streamline consolidation accounting; update COI policy; documentation of board deliberative process	June 2012