The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH

ONE ASHBURTON PLACE, ROOM 1819

BOSTON, MASSACHUSETTS 02108

TEL. (617) 727-6200

A. JOSEPH DeNUCCI

AUDITOR

No. 2008-0206-4T

OFFICE OF THE STATE AUDITOR'S REPORT ON THE EXAMINATION OF INFORMATION TECHNOLOGY-RELATED CONTROLS AT THE UNIVERSITY OF MASSACHUSETTS LOWELL

July 1, 2006 through January 31, 2009

OFFICIAL AUDIT REPORT

SEPTEMBER 22, 2009

TABLE OF CONTENTS

INTRODUCTION

The University of Massachusetts Lowell (UML) is a Massachusetts Institution of Higher Education offering bachelors, masters, and doctoral degrees, as well as certificate programs, on a full-time and part-time basis. UML was established in 1975, upon the merger of the Lowell Technical Institute and Lowell State University. In 1991, the UML campus became part of the Massachusetts State College System under Chapter 15A, Section 5, of the Massachusetts General Laws. A Board of Trustees, that establishes general policies for the campuses, governs the University of Massachusetts System. Under the direction of the President, who oversees the five-campus system, each campus is under the leadership of a chancellor who is responsible for carrying out the policies set by the Board.

The University of Massachusetts Lowell's mission is to enhance the intellectual, personal, and cultural development of its students through excellent, affordable educational programs. The University consists of three campuses, North, South, and East, and occupies 125 acres in Lowell, Massachusetts. It is comprised of 38 buildings that provide student housing, classrooms, laboratories, libraries, administrative offices, and athletic facilities. UML has a combined student population of approximately 12,000 full-time and part-time students. At the time of our audit, the University employed 1,575 full-time and part-time faculty, administrators, and staff members and was supported by a fiscal year 2009 budget of $137,739,000.

UML's administrative operations and academic missions are supported by the automated services provided by UML's Information Technology (IT) Department. The IT Department's mission is to serve the campus faculty, staff, and students in an effort to provide them with quality technology solutions and services. The IT Department is comprised of six groups: IT Security, Network Services, Enterprise System Services, Project Management, Reporting, and Training and Communication. At the time of our audit, the IT Department consisted of 38 full-time staff members. Each of the six groups has a director/manager who is under the direct control of a Chief Information Officer who, reports directly to UML's Chancellor. The IT Department provides assistance and guidance to administrative staff, faculty, and students regarding the use of IT resources, including the use of administrative computer systems, Internet portal support, personal computer maintenance, web hosting services, print servers, and e-mail.

Computer operations are supported by 66 file servers located in the Olsen Data Center on the UML campus, two file server rooms, and 3,997 workstations that are configured to gain access to UML's local area network (LAN). In addition, UML maintained 1,533 laptop computers that were distributed to departments throughout the campus for use by faculty, staff, and administrators. Of the 3,997 workstations, 2,655 were assigned to administrative staff and faculty and 1,342 were assigned to 81

computer laboratories and classrooms. UML's file servers were connected through a wide area network (WAN) to the Commonwealth's state-wide WAN, which provides access to the Human Resources Compensation Management System (HR/CMS) and the Massachusetts Management Accounting and Reporting System (MMARS). In addition, UML is connected to the WAN used by the University of Massachusetts, which is the Massachusetts Information Turnpike Initiative (MITI). The private MITI network links Massachusetts' public higher education in support of administrative applications, distant learning, video services, and electronic communications.

From an administrative perspective, UML utilizes "PeopleSoft" software, a product acquired and further developed by Oracle, Inc., to run the University's business and academic systems, which included Human Resources, Financials, and a Student system known as the Intercampus Student Information System (ISIS). ISIS contains student records on admissions and recruiting, academics, student financial aid, other student financials, as well as for alumni contributor relations. The various applications are maintained by the University Information Technology Services, consisting of a staff of 120 people, located in Shrewsbury, Massachusetts, and managed by the President's Office. Presently, ISIS is a centralized collaborative effort at UML that combines Boston, Dartmouth, and Lowell campuses in its operations.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

In accordance with Chapter 11, Section 12, of the Massachusetts General Laws, we performed an information technology (IT) general controls examination of IT-related activities at University of Massachusetts Lowell (UML) for the period of July 1, 2006 through January 31, 2009. The audit was conducted from May 23, 2008 through January 31, 2009. Our audit scope included an examination of IT-related general controls pertaining to organization and management, physical security, environmental protection, system access security, inventory control over IT equipment, disaster recovery and business continuity planning, on-site and off-site storage of backup copies of magnetic media, and IT-related contract management. In addition, our scope included a review of the University's control practices regarding the Criminal Offender Record Information (CORI) and Sexual Offender Record Information (SORI) background checks required for certain individuals who have the potential for unsupervised contact with children, the disabled, or the elderly. We reviewed UML's approach to comply with Payment Card Industry (PCI) standards set forth by members of the banking industry in setting the University's credit card policies and procedures. We also reviewed UML's policies and procedures to protect and maintain confidentially of personally identifiable information as required by Chapter 93H of the Massachusetts General Laws, regarding the protection of sensitive agency information.

Audit Objectives

Our primary audit objective was to determine whether the University's IT-related internal control environment, including policies, procedures, practices, and organizational structure, provided reasonable assurance that control objectives would be achieved to support UML's business functions. In this regard, we sought to evaluate whether adequate controls were in place to provide reasonable assurance that IT resources would be safeguarded, properly accounted for, and available when required.

Our audit objective regarding IT organization and management was to determine whether IT-related roles and responsibilities for IT staff were clearly defined, points of accountability were established, appropriate organizational controls were in place, and IT-related policies and procedures adequately addressed the areas under review. We sought to evaluate whether UML had implemented IT-related strategic and tactical plans that help direct the use of technology to fulfill the UML's mission and goals. We also sought to establish whether adequate physical security controls were in place and in effect to restrict access of IT resources to only authorized individuals in order to prevent unauthorized use, damage, or loss of IT-related assets. We sought to determine whether sufficient environmental

protection controls were in place to prevent and detect damage or loss of computer equipment and data residing on UML's system.

Our objective regarding system access security was to verify whether adequate controls had been implemented to provide reasonable assurance that only authorized users were granted access to UML's application systems and data files. We also sought to evaluate whether PeopleSoft system data was sufficiently protected against unauthorized access, and whether UML was actively monitoring password administration.

Our review and evaluation of inventory control over computer equipment was to determine whether control practices were in place regarding the accounting for computer equipment. In addition, we sought to determine whether an annual physical inventory and reconciliation was conducted, and whether inventory controls met Chapter 647 reporting requirements.

With respect to the availability of automated processing capabilities and access to IT information resources, we sought to ascertain whether business continuity strategies would provide reasonable assurance that mission-critical and essential computer operations could be regained within an acceptable period of time should computer systems and supporting technology be rendered inoperable or inaccessible. In addition, we sought to determine whether UML had adequate control procedures for the generation and storage of on-site and off-site backup copies of magnetic media to support system and data recovery objectives.

We sought to evaluate whether UML had implemented adequate controls with regard to IT contract management to provide reasonable assurance that contract monitoring and evaluation were being performed. We sought to verify whether contractual relationships with third-party IT-related service providers were covered by written contracts, and whether the contract agreements sufficiently detailed services or deliverables to be provided, and were properly signed and dated. We also sought to determine whether third-party contracts contained standard terms and conditions as promulgated by the Operational Services Division and whether incorporated vendors were registered with the Office of the Secretary of State.

We also sought to determine whether selected laws, regulations, and control practices regarding the completion of CORI and SORI background checks and the submission of supporting documents were performed prior to an individual's employment, changes in position, or acceptance into a specific academic program at UML for individuals dealing with unsupervised contact with vulnerable populations such as students, children, handicapped, or the elderly.

We sought to determine whether UML was in compliance with Payment Card Industry (PCI) standards as set forth by members of the banking industry regarding the use of credit cards at the University. In addition, we sought to determine whether UML has controls for transaction data that must be protected if they are stored, processed, or transmitted through any network component, server, or application that is included in, or connected to, the cardholder data environment.

We also sought to evaluate whether there were adequate controls in place to protect personally identifiable information and to determine whether UML's control policies and procedures were adequate to comply with the Commonwealth's data breach notification requirements. Personally identifiable information consists of information that can potentially be used to uniquely identify individuals.

Audit Methodology

To establish the audit scope and objectives, we performed pre-audit steps, which included obtaining and recording an understanding of relevant operations, including the IT infrastructure and software applications, reviewing documentation and interviewing staff regarding UML's mission, operations, and IT organization and management. We interviewed the Chief Information Officer, Directors of Enterprise Systems Services and Network Services, Security Specialist, IT Project Manager, administrative staff, and other IT staff to gain an understanding of how the primary business functions were supported by UML's automated systems, IT infrastructure, and the information technology control environment. We also obtained information regarding the organizational structure of UML's IT Department, and the "University System" in general.

To accomplish a preliminary review of the adequacy of general controls over IT-related functions and assets, we evaluated the degree to which UML had documented, authorized, and approved IT-related control policies and procedures. We documented the significant functions and activities supported by the automated systems and reviewed automated functions related to operations designated as mission-critical by UML.

We determined whether the policies and procedures provided management and users with sufficient standards and guidelines to comply with statutes, regulations, and policy directives related to inventory control, physical security, environment protection, and disaster recovery and business continuity planning. To assess the adequacy of general controls regarding IT-related operations, we also interviewed University of Massachusetts Internal Audit management, observed operations, and performed selected audit tests.

Regarding our review of IT organization and management, we interviewed senior management, completed questionnaires, and analyzed and reviewed the organizational structure and reporting lines of UML's IT Department. We obtained, reviewed, and analyzed the adequacy of IT-related policies and procedures, as well as IT strategic and tactical plans. To evaluate whether UML's IT-related job descriptions and job specifications were up-to-date and reflected current responsibilities and duties, we obtained a current list of the personnel employed by the IT Department, including their duties and job descriptions, and sought to compare the list to the IT Department's organizational chart and each employee's day-to-day IT-related responsibilities. In addition, we reviewed documents such as the network configuration, internal control plan, and various documentation related to business continuity planning.

To evaluate physical security, we assessed whether procedures were in place and in effect to help prevent unauthorized persons from gaining access to computer facilities and selected areas housing IT resources and whether authorized personnel were specifically instructed in physical security policies and procedures. Moreover, our review included the completion of a risk analysis questionnaire and interviews with UML's senior management who are responsible for physical security for areas housing IT computer equipment. We also evaluated UML's physical security to determine to what extent physical access was restricted for areas housing IT computer equipment by conducting a walkthrough of the Olsen Data Center, server rooms, classroom laboratories, business offices, on-site storage areas, and selected telecommunication closets. We also examined the existence of controls, such as locks, motion detectors and intrusion alarms.

To gain an understanding of procedures regarding key management at UML, we interviewed the individuals responsible for maintaining records of administrators, faculty, and staff who were issued keys, both electronic and standard metal, for locks located at various locations throughout the campus. We requested a master listing of current electronic key holders. We then compared this listing to a UML current employee listing. We verified that the listing of electronic key holders contained only the names of those who were current employees. We then requested a second listing of current metal key holders from three separate departments for the purpose of comparing it to the current UML employee listing obtained from the Human Resources Department.

To determine whether adequate environmental controls were in place to properly safeguard automated systems in the Olsen Data Center and areas housing workstations from loss or damage, we conducted walkthroughs and checked for the presence of smoke and fire detectors, fire alarms, fire suppression systems (i.e., sprinklers and fire extinguishers), an uninterruptible power supply (UPS), and emergency power generators and lighting. To determine whether proper temperature and humidity controls were in

place, we inspected the datacenter to ensure the presence of appropriate dedicated air conditioning units and/or HVAC systems. In addition, we reviewed environmental protection controls related to general housekeeping procedures in the Olsen Data Center, server rooms, computer classrooms, telecommunication closets, and selected areas housing workstations.

To verify whether adequate system access security controls were in place, we reviewed and evaluated the administration of logon IDs and passwords and selected control practices regarding system access to network resources. We also reviewed the UML's access security procedures with the security administrators responsible for access to UML's network, application programs, and data files.

To determine whether all users with active privileges were current employees, we obtained the list of faculty and staff granted access privileges to the Active Directory Account, which includes e-mail accounts and network access, and a list of personnel with access to the business-related applications of PeopleSoft, and compared all users with active access privileges, as of June 11, 2008, to the University's list of current employees, including faculty, administrative staff, and outsourced staff. To determine that access privileges were disabled in a timely manner, we also compared the active network user listing to UML's listing of former employees. Furthermore, we reviewed whether all persons authorized to access the automated systems were required to change their passwords periodically and, if so, the frequency of the changes.

To evaluate whether the University complied with Commonwealth of Massachusetts regulations for fixed-asset accounting, we reviewed evidence supporting UML's performance of an annual physical inventory and reconciliation of the inventory record of IT assets. To determine whether adequate controls were in place and in effect to properly account for UML's computer equipment, we reviewed inventory control policies and procedures and requested and obtained UML's inventory system of record for computer equipment. We reviewed the current system of record, dated June 13, 2008, valued at $19,635,200 to determine whether it contained appropriate data fields to identify, describe, and indicate the value, location, and condition of the computer equipment. We also performed a data analysis on the inventory and made note of any unusual distribution characteristics, duplicate records, or unusual or missing data elements. To verify whether the system of record for computer equipment was current, accurate, complete, and valid, we used audit sampling software to select a statistical sample of 72 items, valued at $65,490. To evaluate whether the system of record accurately and completely reflected the items of computer equipment, we confirmed the location, description, inventory tags, and serial numbers of the hardware items listed on the inventory record to the actual equipment on hand. To further verify the accuracy and completeness of UML's system of record for IT resources, we randomly selected 72

additional computer hardware items from the floor, valued at $94,919 in adjacent locations and determined whether they were properly recorded on UML's inventory record.

To validate whether selected computer hardware purchased in fiscal years 2007 and 2008 were accurately listed, we tested 45 invoices comprised of 338 items, valued at $1,402,117, and verified whether the items and amounts recorded on the UML's purchase orders and invoices were properly recorded on the inventory system of record. To determine whether UML had appropriate control practices in place and in effect to account for and safeguard computers not on campus, we interviewed representatives from the IT and facilities department, reviewed the control form used by each department regarding computer equipment loan policies for employees, and reviewed UML's documented policies and procedures to control the assignment and use of these computers.

To determine whether UML complied with the Commonwealth of Massachusetts' regulations for the disposal of surplus property, we reviewed records and supporting documentation for IT equipment disposed of during the audit period. Finally, to ascertain whether UML was in compliance with Chapter 647 of the Acts of 1989 reporting requirements, we reviewed incident reports for missing or stolen IT-related equipment for the audit period and confirmed whether these incidents were reported to the Office of the State Auditor.

To assess the adequacy of disaster recovery and business continuity planning, we reviewed the level of planning and the procedures to be followed to resume computer operations in the event that the automated systems become inoperable or inaccessible at the UML campus for an extended period. We interviewed UML management to determine whether the criticality of application systems had been assessed, whether risk analysis to computer operations had been performed, and whether a written business continuity plan was in place, and if so, whether it had been adequately tested. In addition, we reviewed the status of management's efforts to designate a potential alternate processing site to be used in case of an extended disruption of system availability.

To determine the level of business resumption planning in place at the University of Massachusetts Data Center in Worcester, which supports the UML administrative functions on the PeopleSoft applications, we reviewed the report issued by the University's internal audit department in reference to this issue. We also interviewed UML's IT Audit Manager to obtain the current status of UML's Disaster Recovery Plan.

As part of our review of the adequacy of generation and storage of backup copies of magnetic media, we assessed relevant policies and procedures, as well as the adequacy of physical security and environmental protection controls for on-site storage of magnetic media. We interviewed the Director of Enterprise Systems who is responsible for the automated full backup of all mission-critical applications and

associated data files and reviewed the current backup procedures in place for their adequacy and completeness. We also inspected the on-site daily backup copies of computer media to review the provisions for storage, frequency of backup, and adequacy of controls in place to protect backup media. Further, we interviewed responsible personnel to determine whether they were formally trained in the procedures of generating backup copies and were aware of the procedures for on-site and off-site storage of magnetic media and the steps required ensuring the protection and safety of the backup copies. In addition, we interviewed UML IT department personnel to determine whether they were cognizant of, and trained in, all procedures required to restore systems via backup magnetic media under disaster or emergency circumstances.

The review of IT-related contracts with third-party service providers was accomplished by analyzing UML's policies and procedures used to help ensure that contracts were initiated and processed in compliance with state regulations. For the period of July 1, 2006 through June 30, 2008, we reviewed all five IT vendor service contracts for fiscal years 2007 and 2008. Regarding contract documentation, we reviewed the selected contracts to ascertain that the contracts contained the original signature pages with corresponding proper signatures to ensure compliance with standard terms and conditions as promulgated by the Operational Services Division. We evaluated contract documentation provided to us to determine whether contract provisions were sufficient to hold the third-party service providers accountable for delivering quality services. This was accomplished by interviews with project managers, and review of project documentation and UML's policies and procedures which helped to ensure that the contracts were initiated and processed in compliance with standard terms and conditions as promulgated by the Operational Services Division.

To assess compliance with laws, rules, policies, and procedures of UML as they pertain to the Criminal Offender Records Information (CORI) and Sexual Offender Record Information (SORI) background checks, we analyzed and tested actions taken by UML for prospective and current employees, as well as for those students involved in programs requiring a CORI. In this regard, we reviewed and analyzed Executive Office of Health and Human Services' 101 Code of Massachusetts (CMR) 15.04-Criminal Offender Record Checks. We compared required information outlined within 803 Code of Massachusetts (CMR) 3.05 Sections 1 and 2, with UML's CORI Request Forms and CORI Applicant Files of all new hires since January 1, 2008 including faculty, administrators and staff. We also conducted interviews with the UML Human Resources Assistant Director to ascertain information regarding the CORI and SORI background checks and analyzed all program specific documentation.

To determine the status of the UML's ability to meet compliance with Payment Card Industry standards and to ensure control mechanisms were in place to protect personally identifiable information, we

reviewed the PCI Industry's data security standards, evaluated UML's PCI self-assessment questionnaire provided by the Office of the State Comptroller, and interviewed senior management. We also reviewed policy and guidance issued by the Commonwealth's Information Technology Division through Chapter 93H of the Massachusetts General Laws regarding the protection of sensitive agency information and the University's policies and procedures to safeguard personally identifiable information. In addition we also performed walk-throughs of areas containing sensitive information and interviews with key UML management.

Our audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) issued by the Comptroller General of the United States of America through the U.S. Government Accountability Office and generally accepted industry practices. Audit criteria used in the audit included management policies and procedures and control guidelines outlined in Control Objectives for Information and Related Technology (CobiT), as issued by the Information Systems Audit and Control Association in 2007.

AUDIT CONCLUSION

Based on our audit at the University of Massachusetts Lowell, we found that adequate controls were in place to appropriately safeguard and account for the University's information technology resources. We found that high level control objectives for physical security and environmental protection over IT resources would be met, except where certain control practices need to be strengthened. We also found that internal controls in place provided reasonable assurance that IT-related control objectives would be met with respect to IT organization and management, system access security, hardware inventory control, third-party provider IT service contracts, Payment Card Industry Standards, and management controls over personally identifiable information. Regarding business continuity planning, we determined that although UML had documented important controls, sufficient control practices were not in place to provide reasonable assurance that normal business operations could be restored in a timely manner should automated systems be unavailable for an extended period. In addition, we found that UML needed to expand its monitoring and evaluation of Criminal Offender Record Information background checks to include information from other states when individuals reside outside Massachusetts prior to the individual's employment or acceptance into a specific academic program.

Our review of IT management and organizational controls indicated that UML had an appropriate and defined organizational structure and chain of command for the IT Department with assigned reporting responsibilities and documented job descriptions. UML had documented a variety of IT-related strategic and tactical plans that identified business goals and address risks to the IT environment and mission-critical applications. The strategic plan strengthened business requirements to help ensure that control practices, such as system access security and hardware inventory controls, would be adequately communicated and administered.

Our audit found that adequate physical security controls were in place over and within the administrative offices of the IT department, the Olsen Data Center, server rooms, and selected computer laboratories and telecommunication closets. Controls were found to be in place for the on-site storage area for copies of magnetic media to provide reasonable assurance that access to IT resources would be restricted to only authorized persons and that IT assets would be safeguarded from damage or loss. We confirmed that the controls included surveillance cameras, locked doors, intrusion detection devices, and motion detectors. However, our audit revealed that management controls for door keys needed to be strengthened to assure that only authorized employees could access offices housing computer equipment. We found that there is no central record maintained by the UML locksmith or by a designated department over the distribution

and return of metal door keys. As a result, UML cannot properly account for the number of keys available for use and to whom keys have been distributed.

We found that adequate environmental protection controls, such as smoke detectors and fire alarms, were in place throughout the building housing the Olsen Data Center and campus buildings housing computer laboratories, telecommunication closets, and server rooms. We determined that fire extinguishers were installed in the areas reviewed, and that there were separate temperature controls and an uninterruptible power supply (UPS) in the Olsen Data Center to permit a controlled shutdown and prevent a sudden loss of data. UML had installed backup generators for the building housing the Olsen Data Center. Our audit also disclosed that the data center was neat and clean, general housekeeping procedures were adequate, and humidity levels were automatically controlled. However, environmental protection controls would be improved in the Olsen Data Center by replacing the water sprinkler system with an inert fire suppression system.

Regarding system access security, we found that appropriate control practices were in place regarding the authorization of faculty and staff to be granted access to network resources, activation of access privileges, and deactivation of access privileges. We also found controls were in place to help ensure that access privileges would be appropriately modified, should UML faculty or staff terminate employment or incur a change in job requirements. Access privileges to network resources were managed by the security officer at UML. We found that all 1,315 faculty and staff user accounts tested for access to the network were assigned current employees. Regarding PeopleSoft, the University's primary application, only business departments were authorized to grant access privileges to specific modules, such as financial operations and human resources. Our tests confirmed that 594 users granted access to PeopleSoft were UML employees. We confirmed that a security officer was designated, policies and procedures were documented, and UML faculty and staff were required to participate in formal security training and sign a formal security statement regarding password protection and confidentiality. We determined that adequate control practices, including policies and procedures, were in place for password formation, use, and frequency of change.

With respect to inventory control over computer equipment, we found that UML's control practices provided reasonable assurance that IT resources were properly accounted for in the inventory system of record. We determined that the inventory system of record for computer equipment, as of June 13, 2008, could be relied upon as a current, accurate, complete, and valid record of computer equipment installed at UML. Our review of compliance with Chapter 647 of the Acts of 1989 reporting requirements for missing or stolen Commonwealth assets revealed that UML staff responsible for inventory were aware of

the requirements and that UML had properly reported occurrences of missing or stolen computer equipment during the audit period. Our test of 45 invoices of hardware purchased in fiscal years 2007 and 2008, comprised of 338 items valued at $1,402,117, indicated that all purchases in our sample were properly listed on the inventory of record.

Regarding the availability of mission-critical and essential systems at UML, we noted that a recently drafted "Enterprise Systems Services Disaster Recovery Plan", which applies to the Olsen Data Center, needed to be strengthened if it were to be referred to in the event that IT resources at the data center were rendered inoperable or inaccessible. UML should address the implementation of an alternate processing site(s), periodically test the plan, modify the plan as needed, and train the staff in the plans use to provide reasonable assurance that normal business operations could be regained within an acceptable period. However, we determined that UML had not documented a business continuity plan to access PeopleSoft should the application be unavailable for an extended period. PeopleSoft is installed at the Worcester Data Center and maintained by the University Information Technology Services (UITS). We acknowledge that UML IT-related business continuity planning is dependent on the UIT's disaster recovery planning regarding these automated systems. It is our understanding that UITS had documented a plan to restore the PeopleSoft application. UML should develop user area plans for PeopleSoft student and financial applications in conjunction with UITS.

Regarding IT-related contracts for fiscal years 2007 and 2008 with third-party contractors, we found that UML exercised adequate management control over the contracts to provide reasonable assurance that contract monitoring and evaluation were being performed. We found that the contract agreements sufficiently detailed services or deliverables to be provided to adequately measure results against stated goals and scheduled timelines for completion dates, and that the contracts were properly signed and dated. We also determined that the third-party contracts contained standard terms and conditions as promulgated by the Operational Services Division and the incorporated vendors were registered with the Office of the Secretary of State.

We found that the Human Resources Department, which conducts background checks on students and employees when required, is following the current UML management policies and procedures for background checks. UML needs to more effectively evaluate whether Criminal Offender Record Information (CORI) background checks are being consistently performed prior to an individual's employment or acceptance into an academic program requiring background checks. The current system used to identify potential employees or students who would not be acceptable at UML is not

comprehensive, as the process of background checks does not currently review out of state criminal record information. Also the background checks do not include a check of the Massachusetts Sexual Offender Registry (SORI), nor does UML ensure that vendors under state contract conduct background checks as required. As a result, the current criminal record check used by UML may not identify a sex offender from Massachusetts or another state who is working with students or possible patients since the entire criminal background of an individual may not be available under current procedures. UML should continue to improve its background checks by: expanding background checks to include additional federal and/or out-of-state information; expanding background checks to include checks to identify a person who has committed sexual offenses in Massachusetts or other states; and ensuring that college vendors conduct CORI checks.

Our review of Payment Card Industry (PCI) data security standards indicated that adequate controls were in place to provide for the security of payment cardholder information. We verified that UML does not store credit card information and that transmission of sensitive cardholder data is not passed through the UML network. Based on our review of UML's response to the Office of the Comptroller and Information Technology Division questionnaire, dated May 16, 2008, we found that UML stated that UML is in compliance with the PCI data security standards concerning Service Set Identifier (SSI) Broadcast and PCI vulnerability scans. We determined that UML performs scheduled quarterly vulnerability scans. We also found that UML had policies and procedures for antivirus and firewall protection, access security controls, and encryption of confidential data.

Our review of controls over personally identifiable information determined that UML had adopted the controls set forth in the Family Educational Rights and Privacy Act (FERPA) and Health Insurance Portability and Accountability Act (HIPPA) to protect electronic and hardcopy information that can potentially be used to uniquely identify an employee or student of UML. We also determined that user access to the system to add, update, and electronically view sensitive information is monitored and approved by the appropriate offices' managers, as well as the PeopleSoft security administrator. We determined that each office is responsible for overseeing access rights within their respective areas. Our audit included a review of personally identifiable information in UML's Student Health Services Department where we determined that electronically stored personally identifiable information was maintained in a secured manner as well as health forms containing personally identifiable information.

AUDIT RESULTS

1. Physical Security and Environmental Protection

With respect to physical security and environmental protection, our audit revealed that although certain controls were in place and in effect at the Olsen Data Center, file server rooms, classroom laboratories, business offices, the on-site storage area, and selected telecommunication closets, we found that physical security and environmental protection controls needed to be strengthened to adequately safeguard UML's IT-related assets. Currently, UML does not provide reasonable assurance that computer equipment will be safeguarded from unauthorized use, damage, loss, or theft.

Regarding physical security, we found that UML needed to strengthen controls over the management of metal key sets for all areas throughout the three UML Campuses. Regarding environmental protection, the water sprinkler system, if activated in the Olsen Data Center, could seriously damage the unprotected file servers residing there.

The physical security controls in place and in effect included surveillance cameras, locks, keypad access, electronic key access, intrusion alarms, and motion detectors to prevent and detect unauthorized physical access. However, from a key management standpoint, we found that adequate controls were not in effect to ensure that only authorized individuals had keys to areas where computer equipment was installed. Currently, UML does not have appropriate monitoring controls over the issuing or return of keys on a by-department basis. The University could not clearly identify what metal key sets were outstanding and, therefore, could not ensure adequate security over areas where IT-related assets are located. If, for instance, someone left or retired and did not turn in their key, neither security nor the locksmith would be aware of this occurrence. Currently, key control is within the purview of the University's facility management with administrative information maintained by the Commonwealth Administration Management Information Systems (CAMIS).

Lack of key management controls for the return of keys from transferred or terminated employees increases the risk of unauthorized entry to restricted areas, including computer laboratories and telecommunications closets. As a result, UML's assets, including computer equipment and data, are placed at risk of potential loss. Although UML's Campus Police maintain policies that include provisions for checking physical security of the data center, server rooms, computer laboratories, and telecommunication closets, we found that there are no policies and procedures for the distribution and return of keys for the interior or exterior doors for all of the buildings. These policies and procedures for the distribution and return of keys should be part of UML's Internal Control Plan. We acknowledge that

UML is in the process of making changes to CAMIS that would automatically show the room, building and name of the person to whom the key was assigned.

Our review of environmental protection revealed that certain controls were in place and in effect. We found that fire extinguishers were installed throughout UML. They were placed in strategic areas within reach of the telecommunication closets. We also found that the Olsen Data Center contained separate automatic temperature and humidity controls, as well as an uninterruptible power supply and back-up generators. The telecommunication closets, file server rooms, and the data center were neat and clean. We found the presence of smoke and fire detectors, as well as a water sprinkler fire suppression system. However, adequate environmental controls were not in effect to ensure the protection of the file servers from water damage in the Olsen Data Center. There are water sprinklers directly over the file servers and there is no protection for the servers in the event of activation.

Generally accepted computer industry standards and practices indicate that appropriate physical security and environmental protection controls should be in place to ensure that IT resources operate in a secure processing environment that is protected from unauthorized access, use, damage, or theft.

Recommendation

Regarding physical security, we recommend that UML reconcile the metal key sets distributed to current employees to ensure that appropriate access privileges have been granted. UML should also attempt to retrieve keys from terminated employees or consider re-keying locks to designated secure areas. In addition, UML should enhance the documented procedures for managing the metal key sets and including the establishment of a central register for recording the distribution and return of metal keys. The procedures should require periodic reconciliation of the metal key sets to current employees and a return of all keys upon employment termination.

Regarding environmental protection controls we recommend that UML establish adequate controls to prevent water damage to computer equipment in the Olsen Data Center. In addition, UML should install water detection devices and consider the installation of a raised floor within the data center to help ensure the safeguarding and protection of computer equipment. UML should also consider the purchase of plastic covers for critical IT equipment, such as the file servers, to help provide some level of protection against the risk of water damage from either the floors above, or from the water sprinklers, if activated. We further recommend that UML conduct an inspection of all their computer laboratories to ensure that they contain easily accessible fire extinguishers. To further support the safeguarding of equipment, we suggest that UML maintain a floor plan of the server rooms and wiring closets indicating the location of equipment, power sources, and physical security and environmental protection controls.

We further recommend that UML define and ensure that staff have an adequate understanding of the control objectives to physical security and environmental protection. Policies, procedures, and responsibilities for physical security and environmental protection should be written, reviewed, approved, and distributed to all appropriate staff members. UML should assign a single point of accountability regarding physical security and environmental protection for the server rooms, wiring closets, and computer labs. The assigned responsibilities should be comprehensive, understandable, and properly communicated. UML should also establish adequate mechanisms to monitor and evaluate the effectiveness of physical security and environmental controls. Monitoring mechanisms should include formal reporting of any incidents or lapses in security, adherence to established procedures, and identification of security and environmental problems along with their resolutions.

Auditee's Response

Key Control Update

The University has begun to capture detailed key control information into Excel files and has begun to load the data into CAMIS. The campus has started with all new ASSA – keyed locks and is assessing the costs in time, human and financial resources necessary to capture all information for the approximately 3,000 locks throughout the building inventory. The University will begin to re-key certain secure areas where sensitive information technology equipment is located as part of a larger effort to replace locks in a systematic way.

Once the data are loaded, and following staff training, (generally less than a week), the CAMIS Key Control module will be made operational. The campus is reviewing the appropriate office (s), staff and procedures to oversee key issuance and monitoring including enhancing documentation procedures, retrieving keys from employees that leave University employment and disaster recovery/business continuity planning.

Olsen Hall

The University has replaced the Olsen Hall Server Room old "wet" type fire protection system with a Novec-1230 clean agent fire suppression system. Clean agent type fire protection systems suppress fire through the use of "dry" chemicals. Clean agent chemicals are specially formulated so as not to cause damage to server room equipment.

To comply with 780 CMR, the new Olsen Hall system is being provided with a "back-up" preaction type, water-based fire protection system. In this application, preaction type protection will prevent accidental discharge due to mechanical failure and will limit-exposure-through-false-detection by requiring activation of multiple detection devices.

The University will also inspect computer labs to ensure that fire extinguishers are accessible.

Auditor's Reply

We commend the actions being taken by UML to improve physical security controls for the University campus. The University's implementation of a key record tracking system and control module, CAMIS, should be helpful in maintaining an accurate record of who has been assigned keys and to what areas they have been granted access. The University should identify the essential data elements necessary to be gathered and stored in CAMIS to support the management of physical security throughout the whole campus. If an adequate reconciliation of keys can not be performed, the re-keying of sensitive areas may be a sound approach to strengthening security. Understandably, the installation of other types of locking devices may be an option. Continuous monitoring, maintenance and reconciling of the data in CAMIS is also essential. The University's actions with regard to physical security will enable UML to reduce the risk of unauthorized access to areas housing computer equipment that could lead to property damage, vandalism or theft.

We also commend The University's quick action over environmental controls in correcting the risk of potential water damage from the water sprinklers located in the Olsen Data Center. Continuous monitoring to ensure proper environmental protection controls is essential for all areas housing sensitive computer equipment.

2. Disaster Recovery and Business Continuity Planning

We determined that UML did not have a comprehensive disaster recovery plan and business continuity plan to provide for the timely restoration of mission-critical and essential business functions should IT systems be rendered inoperable or inaccessible. Although certain controls over the information technology systems ensuring the continuance of essential business functions were found to be in place and in effect in the event of a disaster, our audit disclosed that comprehensive UML user area plans for the PeopleSoft student and financial applications needed to be developed in conjunction with University Information Technology Services (UITS), located in Shrewsbury. The user area plans then need to be incorporated in a complete disaster recovery and business continuity plan that has been formally documented and tested. Disaster recovery and business continuity planning for UML needs to be in alignment with "Business Resumption Planning" at UITS that, in turn, provides up-to-date specific instructions for various courses of action to address different types of disaster scenarios at the Worcester Data Center.

We acknowledge that UML's IT-related business continuity planning is dependent on the University's disaster recovery planning regarding automated systems. We further acknowledge, based on information

received through interviews with staff in the University's Internal Audit Department, that UITS maintains adequate on-site and off-site storage for the University's mission-critical and essential applications accessed by the Lowell Campus (Human Resources, Financial, and Student).

Regarding the availability of mission-critical and essential systems at UML, we note that a recently drafted "Enterprise Systems Services Disaster Recovery Plan", which applies to the Olsen Data Center, located on the Lowell Campus, needed to be strengthened if it is to be referred to in the event that IT resources at the data center are rendered inoperable or inaccessible. The University needs to address the implementation of an alternate processing site, periodic testing of the plan, and the training of staff in the plan's use in order to provide reasonable assurance that normal business operations can be regained within an acceptable period. We found that UML's draft disaster recovery plan had policies and procedures to support the recovery of UML's mission-critical systems and included background information for each system, system dependencies, support information, back-up procedures, recovery steps, and data loss risk assessment. Our audit indicated that although UML would be able to access backup magnetic media for their LAN-based system/applications, UML had not designated or tested an alternate-processing site to support recovery efforts should a disaster render the University's LAN-based computer system unavailable or inaccessible. A significant disaster impacting UML's LAN-based computer system, could seriously impact daily operations of the Lowell Campus.

Disaster recovery planning identifies the manner in which essential services are provided without full use of the computer facility or network communications and, accordingly, the manner and order in which processing resources are restored or replaced. The plan identifies the policies and procedures to be followed, detailing the logical order for restoring critical data processing functions, either at the original site or at an alternate processing site. In addition, the plan describes the tasks and responsibilities necessary to transfer and safeguard backup copies of data files, program software, and system documentation from off-site storage to the site being used for restoration efforts. Given the absence of a complete and approved IT disaster recovery plan, a significant disaster impacting all of the computer systems and associated applications, could seriously effect, or even hinder daily business operations. Without a comprehensive, formally documented, and tested IT recovery and business continuity plan, UML's ability to regain mission-critical processing capabilities and access to information related to its various application systems would be impeded, or worst case scenario, come to a halt. Business resumption planning has assumed added importance given the potential processing disruptions that could be caused by man-made events. Generally accepted practices and industry standards for computer operations support the need to have an ongoing business resumption planning process that assesses the

relative criticality of information systems and business operations, as well as develops and maintains appropriate business continuity and recovery plans.

Without sufficient IT disaster recovery planning, a possible long-term loss of the UML's computer operations could hinder access to processing capabilities, electronic data needed to perform essential business functions, and to critical communications systems across the campus. Under the disaster scenario of being unable to conduct business at the Olsen Data Center, UML has not formally designated an alternate processing site for various disaster scenarios for the campus' critical systems. Although UML's IT Department has on-site and off-site storage of backup magnetic media available for recovery efforts, they have not formalized an agreement with an alternate processing site that would be available to regain computer operations should the data centers be damaged or inaccessible for an extended period of time. According to UML management, they are confident that they would be able to conduct business, regardless of the location of the University's IT systems, within 48 hours of a disaster that results in a total shutdown.

Administrative functions on the PeopleSoft applications are accessed, as noted earlier, through the MITI (Massachusetts Information Turnpike Initiative) WAN, as the University of Massachusetts Data Center in Worcester maintains the servers that contain the applications. UML management has plans in place to handle various scenarios dealing with downtime of the administrative functions. A well-documented Human Resource's (HR) disaster recovery plan exists, and a disaster recovery environment warm-site is maintained at the Amherst Campus, geographically removed from the production environment housed at the Worcester Data Center. Payroll checks and advices are also printed at the Amherst site. All University of Massachusetts campuses have participated in an HR payroll disaster recovery test exercise in conjunction with the HR disaster recovery site in Amherst. The next test will be conducted sometime after the central HR applications are upgraded during 2009. On a yearly basis, a disaster recovery payroll print test of checks and advices is performed with internal audit participation to ensure payroll checks and advices can be printed at the back-up payroll print site in Shrewsbury, geographically removed from the Amherst payroll check and advice print production site. A disaster test and recovery environment has been established at the Boston Campus' data center. An extended loss of access to centrally managed financial and student applications could impact essential business functions processed on these PeopleSoft applications.

The objective of business continuity planning is to help ensure the continuation of mission-critical functions should a disaster cause significant disruption to computer operations. Disaster recovery planning for information services is part of business continuity planning for the entire organization. UML should continue to assess the extent to which it is dependent upon the continued availability of

information systems for all required processing or operational needs and should develop its recovery plans based on the critical aspects of its information systems.

The success of the business continuity planning process requires management commitment. Senior management and system users should be closely involved in business continuity planning to help ensure that there is a clear understanding of the entity's information system environment, that determinations of system criticality and the risks and exposures associated with the systems are correct, that appropriate data processing area disaster recovery and business operations user area continuity plans are developed based on the relative criticality and importance of systems, and that adequate resources are available.

Recommendation

UML should continue in its effort to implement procedures to provide reasonable assurance that the criticality of application systems and supporting technology is evaluated, business continuity requirements are assessed on an annual basis, or upon major changes to user requirements or information technology, and that appropriate business continuity plans, as well as work-around plans, are developed for all the applications residing on the computer systems. We recommend that senior management and key users continue to review the computer environment and operations, and perform criticality assessments and risk analysis on the UML's automated systems. Based on the results of the assessment, UML should proceed with further development and strengthening of a written disaster recovery and business continuity plan for its mission-critical and essential functions.

The IT disaster recovery plan should document UML's recovery strategies with respect to various disaster scenarios. The recovery plan should contain all pertinent information needed to effectively and efficiently recover critical operations within the needed time frames. UML should continue the development of user area operations business continuity plans to continue its operations should the computer systems be unavailable. We further recommend that all disaster recovery and business continuity plans be tested, then periodically reviewed and updated when needed, to ensure its viability. UML management and staff should be trained in the execution of the plan under emergency conditions. Sections of the completed plan should be distributed to the appropriate staff members based on their roles in the recovery or planning processes.

Auditee's Response

The University of Massachusetts Lowell has a campus-wide Disaster Recovery/Business Continuity (DR/BC) team with senior management sponsorship and team leadership coming from the financial services and information technology offices. The membership of the team includes staff from the following offices: Registrar, Facilities, Controller,

Public Safety, Enrollment Management (admissions, advising, financial aid), Library and Media Services, Academic Administration (Dean's Offices), Human Resources, Student Affairs and Residential Life.

In May of 2008, the DR/BC team updated the campus Business Continuity Plan "Restarting UML" using the highly regarded web-based planning tool developed by the University of California, Berkeley. The following departments completed business continuity plans at that time and have posted the plans on the campus intranet site: Controller's Office, A/P, A/R and Bursar's Offices, Payroll and Human Resources, Purchasing and Distribution Services. There are a number of departmental business continuity plans that are "in progress" and will be completed as a result of this report. Recent reorganizations in the campus Administration, Finance, Facilities and Technology departments necessitate a full updating of the DR/BC plans which will include an assessment of critical IT systems and operations. All DR/BC plans will be periodically tested, reviewed, and updated.

Auditor's Reply

We note that the University is aware of the need for a comprehensive disaster recovery and business continuity plan to ensure that business operations and IT services can be recovered and maintained in the event of a catastrophic IT systems failure or loss of processing capabilities. We are pleased that UML plans are in place to continue developing a comprehensive disaster recovery and business continuity plan. It should be noted that until the recovery and business continuity plans have been completed and tested, UML remains at risk of not being able to recover IT processing capabilities within an acceptable period of time. The University should also coordinate their business continuity strategy with the University of Massachusetts centralized system.

Glossary

Business Continuity Planning (BCP): Process of developing and documenting arrangements and procedures that enable an organization to respond to an event that lasts for an unacceptable period of time and return to performing its critical functions after an interruption.

Business Impact Analysis: A process designed to prioritize business functions by assessing the potential quantitative (financial) and qualitative (non-financial) impact that might result if an organization was to experience a business continuity event.

Continuity of Operations Plan (COOP): COOP provides guidance on the system restoration for emergencies, disasters, mobilization, and for maintaining a state of readiness to provide the necessary level of information processing support commensurate with the mission requirements/priorities identified by the respective functional proponent. The Federal Government and its supporting agencies traditionally use this term to describe activities otherwise known as Disaster Recovery, Business Continuity, Business Resumption, or Contingency Planning.

Disaster Recovery: The ability of an organization to respond to a disaster or an interruption in services by implementing a disaster recovery plan to stabilize and restore the organization's critical functions. The disaster recovery plan is a management-approved document that defines the resources, actions, tasks and data required to manage the technology recovery effort. Usually the disaster recovery plan refers to the technology recovery effort and is a component of the business continuity management program.

Personal information: Defined under Chapter 93H of the Massachusetts General Laws, personal information is a resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident:

(a) Social Security Number;

(b) Driver's license number or state-issued identification card number; or

(c) Financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.