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. 2008-0210-4T

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

July 1, 2005 through October 10, 2008

OFFICIAL AUDIT
REPORT
MAY 14, 2009

TABLE OF CONTENTS

INTRODUCTION

The University of Massachusetts-Dartmouth (UMD) is one of the five public institutions of higher education within the University of Massachusetts system. The University of Massachusetts is governed by a single Board of Trustees comprised of 19 voting members and three non-voting members. In addition, a President oversees the five-campus system, with Chancellors located at each University of Massachusetts campus. The Board of Trustees provides oversight for each of the five university campuses within the University of Massachusetts system. UMD offers undergraduate and graduate degree programs in arts and sciences, business and industry, engineering, nursing, and visual and performing arts.

At the time of our audit, UMD had an enrollment of 7,199 full-time and 1,881 part-time and continuing education students. The UMD received an appropriation of state funds totaling approximately $71.1 million in fiscal year 2008 and employed 1,004 full-time and part-time faculty, administrators, and staff members. The University's facilities consist of a main campus located in North Dartmouth and six satellite campuses located in New Bedford, Fall River, and Fairhaven.

The UMD's Computing and Information Technology Services (CITS) Department is responsible for managing all technology requirements for the University. The CITS Department provides assistance and guidance to administrative staff, faculty, librarians, and students regarding the use of IT resources, including the use of administrative computer systems, Internet portal support, personal computer maintenance, web hosting services, and e-mail. The CITS Department is comprised of approximately 43 full-time employees, including an Associate Vice-Chancellor for Information Technology, who reports to the Vice Chancellor for Library Services, Information Resources, and Technology.

The University's primary administrative application is a vender-developed product named PeopleSoft. The centrally managed PeopleSoft application serves as the primary financial management system for billing, receivables, payables, financial aid, registration, admissions, human resources, and student information, including grades. At the time of our audit, computer operations for UMD were supported by 43 file servers and 926 workstations configured in a local area network (LAN). The UMD is connected through the University of Massachusetts President's Office to the Commonwealth's Information Technology Division (ITD) mainframe through a wide area network (WAN), which provides connectivity for Virtual Private Network (VPN) access to the Massachusetts Management Accounting and Reporting System (MMARS).

The Office of the State Auditor's examination was limited to an examination of certain IT general controls over and within the University's IT environment.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

In accordance with Chapter 11, Section 12, of the Massachusetts General Laws, we performed an audit of selected information technology (IT) controls at the University of Massachusetts-Dartmouth (UMD) for the period of July 1, 2005 through October 10, 2008. The audit was conducted from December 17, 2007 through October 10, 2008. The audit scope included an examination of IT-related general controls pertaining to IT organization and management, physical security, environmental protection, system access security, inventory control over computer equipment, UMD's disaster recovery and business continuity planning, generation of backup copies of magnetic media for on-site and off-site storage, and on-site storage of backup copies.

Audit Objectives

Our primary objective was to determine whether IT-related controls were in place and in effect to support the University's IT processing environment. In this regard, we sought to determine whether the internal control environment, including policies, procedures, practices, and organizational structure for IT functions, provided reasonable assurance that control objectives would be achieved to support business functions.

Our audit objective regarding organization and management was to determine whether IT-related roles and responsibilities for staff were clearly defined, points of accountability were established, appropriate organizational controls were in place, and whether IT-related policies and procedures adequately addressed the areas under review. We also sought to determine whether UMD had implemented IT strategic plans that would help direct the use of technology to fulfill the University's mission and goals. We determined whether adequate physical security controls were in place and in effect to restrict access to IT resources to only authorized individuals in order to prevent unauthorized use, damage, or loss of IT resources. We also determined whether sufficient environmental protection controls were in place to provide an appropriate IT processing environment and to prevent and detect damage to, or loss of, computer equipment and data residing on the systems as well as copies of magnetic media for on-site storage.

Our objective regarding system access security was to determine whether adequate controls had been implemented to provide reasonable assurance that only authorized users were granted access to UMD's application system and data files. We evaluated whether procedures were in place to prevent unauthorized user access to automated systems and IT resources through the local area network (LAN) file servers and workstations. In addition, we determined whether the data residing on the PeopleSoft application was sufficiently protected against unauthorized access, modification or deletion, and whether UMD was actively monitoring password administration.

We sought to determine whether adequate controls were in place and in effect to provide reasonable assurance that computer equipment was properly recorded and accounted for in the inventory system of record and safeguarded against unauthorized use, theft, or damage. In addition, we determined whether an annual physical inventory and reconciliation was conducted and whether inventory controls met Chapter 647 reporting requirements.

We determined whether adequate disaster recovery and business continuity plans were in place to provide reasonable assurance that mission-critical and essential IT system capability could be regained within an acceptable period of time should a disaster render the IT functions inoperable or inaccessible. Furthermore, with respect to on-site and off-site generation of backup media to support system and data recovery operations, we sought to determine whether adequate policies and procedures were in place to assist in recovery efforts.

Audit Methodology

To determine the audit scope and objectives, we performed pre-audit steps, which included obtaining and recording an understanding of UMD's relevant operations and information technology control environment. To obtain an understanding of the internal control environment, we reviewed UMD's primary business functions, IT operations and organizational structure, and relevant policies and procedures. We performed a high-level risk analysis and assessed the strengths and weaknesses of the internal control system for selected activities. Upon completion of our pre-audit work, we determined the scope and objectives of the audit.

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 the CITS Department. We obtained, reviewed, and analyzed relevant IT-related policies and procedures to determine their adequacy. With respect to IT strategic planning, we determined whether IT incentives were adequately documented in an IT strategic plan. To determine whether selected IT-related job descriptions and job specifications were up-to-date and reflected current responsibilities, we obtained a current list of CITS personnel and reviewed duties and job descriptions for selected staff, and their stated day-to-day IT-related responsibilities.

To evaluate physical security, we identified areas housing computer equipment, such as the data center, selected computer labs, telecommunication closets, and business offices. We then interviewed senior IT management and UMD's Department of Public Safety, conducted physical inspections, observed security devices, and reviewed procedures to document and address security violations and/or incidents. Our review included the completion of questionnaires and interviews with appropriate personnel responsible for providing security throughout the University. We assessed physical security controls and determined the extent to which physical access was restricted for the data center, selected computer labs, telecommunication closets, and business offices. We examined the existence of controls, such as locks, motion detectors, and intrusion alarms. Regarding controls over individuals possessing access keys to UMD facilities, we interviewed the individual responsible for maintaining the system of record and distributing all access keys. To determine whether appropriate controls for the management of brass keys was in place, we interviewed facility management and staff and requested a master listing of current brass and electronic key holders. We compared the listing of current brass and electronic key holders to a UMD employee listing and verified that the individuals listed as brass key holders were current employees.

To determine whether adequate environmental controls were in place to properly safeguard automated systems in the data center and selected areas housing computer equipment 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 lighting. To determine whether proper temperature and humidity controls were in place, we inspected the data center and selected areas housing computer equipment to ensure the presence of appropriate dedicated air conditioning units and/or heating, ventilation, and cooling systems (HVAC). In addition, we reviewed environmental protection controls related to general housekeeping procedures in the data center, computer labs, and telecommunication closets. Audit evidence was obtained through interviews, observation, and review of relevant documentation.

Our tests of system access security included a review of policies and procedures to authorize, activate, and deactivate access privileges to UMD's network and the PeopleSoft application. The PeopleSoft application system, which resides on the University of Massachusetts's Information Technology Services file servers, is accessed through workstations that are located at UMD. We reviewed control policies regarding logon ID and password administration and password composition, evaluated the appropriateness of documented policies and guidance provided to the UMD personnel, and interviewed employees from the CITS Department responsible for system access security. To determine whether adequate controls were in place to ensure that access privileges to the automated systems were granted to only authorized users, we reviewed and evaluated procedures for authorizing, activating, and deactivating access to application software and related data files. We determined whether all individuals authorized to access system applications were required to change their passwords periodically and, if so, the frequency of the changes. In addition, we reviewed selected access user privileges, access logs, and evidence that passwords were required to be changed on a pre-determined basis. In order to verify that all users of the LAN and PeopleSoft application system were current UMD employees, we obtained a LAN account listing containing 1,556 user accounts and PeopleSoft user accounts totaling 1,207 as of May 30, 2008. We compared the system-generated user account lists for LAN access and the PeopleSoft application to a current UMD employee list and developed an exception list of those individuals no longer requiring access privileges to either the LAN or the PeopleSoft application.

To determine whether adequate controls were in place and in effect to properly account for UMD's computer equipment, we reviewed inventory control policies and procedures and requested and obtained the inventory system of record for computer equipment, dated January 11, 2008. We reviewed UMD's inventory system of record for computer equipment, consisting of 4,620 items of computer equipment, with an estimated value of $10,220,510 to determine whether inventory records contained appropriate data fields to identify, describe, and indicate the value, location, and condition of the computer equipment. We also conducted data analysis on the inventory records by performing an examination of distribution characteristics, duplicate records, unusual data elements, and missing values. To determine whether the inventory system of record for computer equipment was current, accurate, and valid, we used a random number generator to select a statistical sample of 73 items out of the total population of 4,620 items. We traced the inventory tags, serial numbers, and locations of the hardware items listed on the inventory record to the actual equipment on hand. Furthermore, we judgmentally selected an additional 27 computer items in adjacent locations and determined whether they were properly recorded on UMD's inventory record.

To evaluate the completeness of the inventory record, we determined whether the 1,148 computer hardware items, purchased from July 1, 2005 through December 31, 2007, with a total value of $3,619,633, were accurately recorded on the inventory system of record. We obtained a system-generated listing of the IT purchases from UMD's Administrative Services Department and compared the detailed information to the inventory system of record.

To assess the adequacy of inventory control procedures for computer equipment, we conducted an examination of UMD's inventory to determine whether controls were in place and in effect to properly account for and safeguard IT resources. We reviewed policies and procedures regarding inventory control for fixed assets to determine whether UMD was in compliance with the Office of the State Comptroller's (OSC) regulations regarding fixed asset control. In addition, to determine whether UMD was in compliance with Chapter 647 of the Acts of 1989 reporting requirements, we verified the existence of incident reports for missing or stolen computer equipment for the audit period, and verified whether all incidents were reported to the Office of the State Auditor. We also reviewed the University's policies and procedures for complying with Commonwealth of Massachusetts regulations for the disposal of surplus property.

To assess the adequacy of disaster recovery and business continuity planning, we determined whether any formal disaster recovery or contingency planning had been performed and whether a formal disaster recovery plan had been developed and tested by UMD to resume computer operations should the network or application systems housed at the UMD campus be rendered inoperable or inaccessible. In addition, we determined whether the criticality of application systems had been assessed, and whether risks and exposures to computer operations had been evaluated. To determine whether backup copies of application systems and data files would be available for the recovery of IT operations, we determined whether on-site and off-site backup copies of media were generated on a scheduled basis. We also determined whether on-site tapes were stored in a secure location, but we did not review the off-site storage location. We examined the on-site storage facility location to determine whether the area had adequate physical security and environmental protection controls. Although we determined whether procedures were in place for the generation of off-site backup copies of media, we did not evaluate the physical security and environmental controls at the off-site storage location.

Our audit was conducted in accordance with generally accepted government auditing standards (GAGAS) issued by the Comptroller of the United States 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 version 4.1), as issued by the Information Systems Audit and Control Association, July 2007.

AUDIT CONCLUSION

Based on our audit at the University of Massachusetts-Dartmouth (UMD), we found that internal controls were in place to provide reasonable assurance that IT-related control objectives would be met with respect to information technology (IT) organization and management, environmental protection, generation and storage of on-site backup, copies of magnetic media, and generation of backup copies for off-site storage. However, our examination found that control practices needed to be strengthened for inventory control over computer equipment, management of brass keys for campus physical security, system access security, and disaster recovery and business continuity planning for systems residing at the UMD campus.

Our examination of organization and management controls related to IT organizational structure revealed that there was an established chain of command, adequate level of oversight, segregation of duties, and clear points of accountability regarding IT functions. We found that management and staff were well aware of their responsibilities, and that IT-related job descriptions and job specifications reflected current responsibilities. Our review found that UMD had developed and documented policies and procedures for certain IT-related functions and that appropriate IT strategic planning initiatives had been formulated. However, policies and procedure needed to be strengthened regarding certain aspects of physical security, system access security, inventory control over computer equipment, and disaster recovery and business continuity planning.

We found that UMD had adequate physical security controls in place and in effect over the data center, CITS Department offices, computer labs, IT classrooms, and telecommunication closets. We determined that the controls included surveillance cameras, locks, intrusion alarms, and motion detectors to prevent and detect unauthorized physical access. However, from a facilities management standpoint, we found that physical security controls needed to be strengthened over office areas containing computer equipment. Our audit indicated that adequate controls were not in effect to ensure that only authorized individuals had keys to office areas where computer equipment was installed. We found that UMD did not maintain written policies or procedures regarding key management and were not reconciling the list of brass key holders to a current authorized employee roster. As a result, management could not account for every key distributed and could not provide adequate assurance that only authorized employees could gain access to UMD office areas housing computer equipment.

We found that adequate environmental protection controls, such as fire prevention and detection devices, automated fire suppression systems, smoke detectors, alarms, and fire extinguishers were in place in areas housing computer equipment. In addition, we found that the University had backup generators and an uninterruptible power supply in place for the technology housed in the data center and computer labs. Our audit disclosed that the data center was neat and clean, general housekeeping procedures were adequate, and temperature and humidity levels within the computer room were appropriate.

Our review of password administration revealed that the processes for authorizing, granting, and activating logon IDs and passwords were appropriate for both access to the network and the PeopleSoft application. However, we found that UMD needed to strengthen controls regarding the termination of user privileges once a user is no longer authorized or requires access to UMD's network or IT systems. Our examination of the initial network logon indicated that employees were required to change passwords every 180 days for the LAN, and that passwords were required to have a minimum of ten alphanumeric characters, and be case sensitive. Moreover, we found that additional password composition rules were in place, such as passwords could not contain any portion of the user's name. We recommend that UMD consider requiring that users change their passwords on a more frequent basis for access to sensitive IT systems.

Our audit revealed, with respect to user account management, that controls needed to be strengthened for the deactivation of user accounts no longer needed for the PeopleSoft application. Our examination of the PeopleSoft application revealed that 15 out of 1,207 user accounts could not be identified on the official personnel record. Of these user accounts, some had been active for an extended period of time for former or retired employees who had termination dates going back to June 2004. In addition, our tests of authorized users of the LAN also revealed that 11 out of 1,556 user accounts could not be identified as individuals currently associated with the University. We acknowledge that the majority of users accounts to the PeopleSoft application had been appropriately deactivated during our audit period.

Our audit revealed that UMD could not provide reasonable assurance that the system of record for computer equipment could be relied upon since a complete annual physical inventory and reconciliation had not been performed during the audit period to assist in verifying the accuracy and completeness of the inventory record. The absence of a reliable inventory of computer equipment hinders UMD's ability to properly account for IT resources, evaluate the allocation of equipment, identify missing equipment, and meet IT configuration management objectives. Our analysis disclosed that the inventory record was missing essential information regarding serial numbers, cost, assigned custodian, and purchase order number for many of the computer-related items. We also found that the inventory system for computer equipment did not include a data field for condition or asset status for IT configuration management purposes. Our audit test of the inventory record disclosed that of the 73 randomly selected items of computer equipment, 58 items could not be located in the recorded location. We selected 27 items at adjacent locations and found that 20 of the items were not accurately recorded on the inventory system. We found that controls need to be strengthened to record and account for IT equipment when received; to maintain a system of record with appropriate and complete data; and to provide prompt notification and update of the inventory record when equipment is relocated, disposed of, lost, or stolen. In addition, inventory records did not appear to be adequately reviewed for accuracy and completeness, and an appropriate level of reconciliation was not in place. As a result, UMD could not provide reasonable assurance of the integrity of its inventory system of record for computer equipment.

Our audit also revealed that UMD was not in compliance with the Office of the State Comptroller's reporting requirements regarding stolen or lost assets; in part due to the condition of the inventory system of record. At the time of our audit, UMD had not notified the Office of the State Auditor in a timely manner of nine incidents of theft of computer equipment valued at $38,175. We found that the UMD management lacked sufficient guidance concerning the reporting requirements of Chapter 647 of the Acts of 1989.

We found that disaster recovery and business continuity planning needed to be strengthened for mission-critical and essential systems that were housed at UMD. We found that controls at UMD needed to be strengthened to ensure continued processing of UMD application systems for the campus network, e-mail, and web services should IT systems be rendered inoperable or inaccessible. To assist in UMD's recovery efforts, our review indicated that UMD had appropriate procedures for the generation of on-site and off-site backup copies of magnetic media and that UMD utilized a fireproof safe for on-site storage and a private vendor (Iron Mountain) for its off-site storage facility for backup copies. We also found that UMD had performed a risk assessment and analysis, established a disaster recovery team and contact information, and had identified mission-critical and essential IT systems. However, our audit disclosed that a formal, tested disaster recovery and business continuity plan was not in place for the timely restoration of computer operations with regard to the UMD's automated systems. Without sufficient business continuity planning, a possible loss of UMD's computer operations could hinder processing capabilities needed to perform business functions related to the use of the campus network, email, and UMD web services. Our audit did not include a review of the disaster recovery plan for the centralized PeopleSoft application housed at the University of Massachusetts Information Services of the UMass President's Office in Shrewsbury.

AUDIT RESULTS

1. Inventory Control over Computer Equipment

Our audit disclosed that inventory controls over computer equipment needed to be strengthened to ensure that IT resources would be properly accounted for in the UMD's inventory system of record for property and equipment. We determined that adequate controls were not in effect to ensure that a current, accurate, and complete perpetual inventory record of computer equipment, valued in excess of $10 million, was being maintained. We found that controls needed to be strengthened to record and account for IT equipment when received, to maintain a system of record with appropriate and complete data, and to provide prompt notification and update of the inventory record when equipment is relocated, disposed of, lost, or stolen. In addition, inventory records did not appear to be adequately reviewed for accuracy and completeness, and an appropriate level of reconciliation had not been performed. As a result, the integrity of the inventory system of record for computer equipment could not be adequately assured. The absence of a sufficiently reliable inventory of computer equipment hinders the UMD's ability to properly account for IT resources, evaluate the allocation of equipment, identify missing equipment, and meet IT configuration management objectives.

Although we determined that the UMD had documented internal controls regarding the purchase, receipt, and the surplus of IT resources, we found that documented policies and procedures needed to be enhanced regarding the recording, maintenance, compliance monitoring, and reconciliation of the system of record for IT resources. For example, although documented procedures were in place requiring that a perpetual inventory be conducted, documentation could not be provided to support that an annual physical inventory and reconciliation was being performed. Moreover, although the UMD had policies and procedures for Chapter 647 requirements, they were not being followed, as evidenced by the UMD's failure to submit required Chapter 647 reports to the Office of the State Auditor, as further discussed in Audit Result #2.

Our analysis of the UMD's inventory system of record confirmed that certain required data fields, including description, identification tag, user name, serial number, cost, and location, were present. However, we found that the IT inventory listing did not include a data field for condition or asset status. We found that the system of record lacked integrity, since the total population of 4,620 records indicated that information related to certain data fields was either missing or contained incorrect information for purchase order number (3,603 items), cost (1,126 items), custodian (764 items), and serial number (68 items). The inclusion of the missing information would help ensure that the UMD's IT equipment would be properly accounted for during the physical inventory. Although the UMD provided an inventory system of record that listed IT-related assets as of January 11, 2008, we were unable to determine the integrity of the system of record for computer equipment due to the missing or inaccurate information in certain data elements as well as the failure to reconcile the inventory system of record.

With respect to the recording of IT-related assets, we found that the UMD lacked appropriate and adequate assurance mechanisms to ensure that computer equipment is entered into the inventory system when received and accepted, and that the inventory record is updated accordingly as equipment is assigned. Our tests indicated a significant error rate and inconsistency in data recorded by UMD staff on the computer hardware inventory. Specifically, our audit tests comparing data supplied by UMD for purchased computer equipment to the UMD inventory listing indicated that 566 new purchases were missing from the inventory in our sample, or an error rate of 49% in the recording of 1,148 tested hardware items encompassing all purchases for fiscal years 2006 and 2007. We then tested 45 items out of the 566 new purchases missing from the inventory listing and were not able to locate 28 items, or 62%, of the sample drawn. Due to the condition of the inventory record, additional testing was not practical. UMD should improve its monitoring of information in the system of record to ensure the accuracy and completeness of the information contained in the inventory database. Because of the rate of errors in entering new purchases and inadequate management of the system of record, an acceptable level of data integrity did not exist for the UMD's inventory system of record for IT equipment at the time of our audit.

Our inventory tests were conducted on the total population of 4,620 items of computer equipment listed on the UMD's inventory record. Based on a statistical sample of 73 items, we verified by inspection the tag number and the system of record location of the computer equipment. We found that 58 of the 73 items were not at the locations indicated on the inventory system of record. Furthermore, to verify the integrity and completeness of the inventory system of record, we judgmentally selected 27 additional IT-related items in adjacent locations to verify that the items were correctly recorded on the system of record. Although our audit test indicated that seven of the 27 IT-related items selected were recorded on the inventory system of record, we determined that 20 of the 27 items were not recorded on the UMD's listing of inventory computer equipment. Because the inventory did not distinguish laptops from other items of computer equipment, UMD could not provide us with a complete and properly classified inventory list of laptop computers. After reviewing the UMD inventory database and interviewing the Information Systems/Procurement Reporting Manager, we determined that an accurate laptop test would be difficult to conduct because segregating laptop computers out of the general computer inventory population was not possible since the inventory system of record had no specific laptop identifier field. The problem existed because the only common laptop identifier was located in the description field and these fields can identify the unit by various names including laptop, desktop, notebook, ThinkPad, or by a specific vendor model name or number such as Latitude d620.

We determined that the UMD maintained a policy that required individuals who are assigned a laptop to sign an acknowledgement that they have received the laptop computer; however, we found that UMD was not following the policy and was not reconciling signed acknowledgments to a laptop inventory system of record. The UMD Inventory Control Policy states that "All laptops, because of portability, must have an off campus form filed with Property Control." We reviewed the University's "Off Campus Form" for comprehensiveness and requested a complete list of the University’s completed "Off Campus Forms" during our audit period to establish a population and draw a sample of assigned laptop computers. A senior member of the Property Control Department stated that the paper trail was not reliable because the information in the records was not up to date. The same individual stated that the “Off Campus Forms” were infrequently completed and were being performed on a voluntary basis. Our review of completed Off Campus Forms indicated that only a dozen or so had been returned, although several hundred laptop computers had been assigned.

The UMD inventory had several systemic problems that included the lack of monitoring procedures to ensure that an annual physical inventory and reconciliation would take place, limited property control staffing, and insufficient oversight regarding the inventory system of record. Without formal, documented, and tested procedures for performing an annual physical inventory count and reconciliation of the inventory record to purchase or lease documentation and surplus equipment records, UMD management cannot be adequately assured that their computer equipment is properly accounted for and that the inventory record is accurate, complete, up-to-date, and valid. In addition, a periodic comparison of the computer equipment and the recorded accountability of the computer equipment will reduce the risk of unauthorized use, loss, or theft of computer equipment. We believe that the weaknesses in inventory control were the result of a lack of adequate inventory assignment of control responsibilities and insufficient monitoring and management oversight. We found that responsibilities for tagging the equipment, maintaining and reconciling the inventory system of record, and completing a physical inventory were not clearly defined or delineated.

Generally accepted industry standards and sound management practices advocate that adequate controls be implemented to account for and safeguard property and equipment. In addition, Chapter 647 of the Acts of 1989, states, in part, that “the agency shall be responsible for maintaining accountability for the custody and use of resources and assign qualified individuals for that purpose, and periodic comparison should be made between the resources and the recorded accountability of the resources to reduce the risk of unauthorized use or loss and protect against waste and wrongful acts.” Sound management practices and generally accepted industry standards for IT installations advocate that a perpetual inventory record be maintained for all computer equipment and that sufficient policies and procedures be in effect to ensure the integrity of the inventory record.

Recommendation:

The UMD must strengthen its inventory controls to ensure integrity for the system of record for computer equipment. The UMD should also strengthen its current practices to comply with the Office of the State Comptroller's requirements that each state agency conduct an annual physical inventory to ensure the proper accounting for, and disposal of, property and equipment, and that IT resources are adequately maintained and safeguarded. The UMD should conduct an annual physical inventory and reconciliation of IT resources to help ensure that an accurate, complete, and valid inventory record is being maintained.

We recommend that UMD consider reallocating staff assignments to accomplish the maintenance, physical counting, and reconciliation of the inventory system of record on a perpetual basis instead of on an annual basis. UMD should specifically assign responsibilities for maintaining the inventory system of record through the financial and accounting functions at the University.

We recommend that the UMD enhance its inventory control policies and procedures related to the receiving function by increasing supervision and oversight to help ensure that the University properly records all received items of computer equipment on the inventory system of record. The University should segregate the functions of receiving, tagging, recording, and distribution of assets to reduce the risk of undetected data entry errors, unrecorded items, and loss of IT-related equipment. A member of the IT staff should continue to assist in the verification of equipment deliveries and the subsequent tagging of equipment.

With respect to IT configuration management, the UMD should expand the inventory data fields to include data elements related to the condition or asset status. In addition, the University should update missing information in its inventory data fields with specific attention to serial number, purchase order number, cost, and custodian. We recommend that the University's inventory records reflect any changes to computer hardware items, including location or status, for both deployed equipment and items held in storage.

To ensure safeguarding of laptop computers, we recommend that the UMD implement improved identification of laptops on the inventory system of record. Once the laptops have been properly identified and recorded in the system of record, the University must set up assurance mechanisms that monitor and evaluate the assignment and return of laptop computers. In addition, to ensure the integrity of the laptop computer inventory list, we recommend that UMD strengthen its controls to maintain complete and up-to-date signed acknowledgements that users have received or returned their laptop computers, thereby reducing the risk that laptops may be lost or stolen. We recommend that staff be required to sign sign-out forms before equipment is distributed to them. This will also provide an opportunity to ensure that acceptable use policies are signed off as well.

Auditee's Responses:

The University agrees with the need to improve controls over the inventory process for computer equipment. We perform a biennial physical inventory and reconciliation to comply with University-wide policy.

Action Item: UMass Dartmouth will review, improve and document its physical inventory and reconciliation procedures, provide enhanced training to all departments, and review system field use to strengthen controls over our inventory process.

Action Item: We will complete our current physical inventory and reconciliation and make necessary changes to ensure the integrity of data within the system record.

Expected Completion: June 30, 2009

The following paragraphs describe specific areas that we are addressing to improve controls:

Training Corrective Actions

In the last 6 months the University has implemented a requirement that all departments have an inventory Point of Contact (POC) that will be the primary liaison between the department and Property Control for all inventory matters. Dean's and department inventory POC's have been trained on the appropriate safe keeping of assets and responsibility of the departments regarding timely notification of moves and changes to an assets inventory record. Forms used to ensure timely notification of changes have been updated to make them more user friendly, in an effort to facilitate compliance. The POC primary responsibilities are as follows.

- *Assist in the maintenance of inventory controls over equipment in their areas with the direct support of the Property Office.*
- *Works to ensure integrity of inventory system and safe keeping of University Assets by submitting appropriate forms to insure perpetual inventory.*
- *Keeper of Accurate Department Inventory Records.*

A second training has been provided to all University staff responsible for the data entry of requisitions within PeopleSoft regarding appropriate inventory account codes and descriptions. This was done to address the issue of errors caused at the source, the creation of a requisition which ultimately feeds to the inventory control system. Additionally, there are multiple checks to insure that purchases are appropriately coded and identified for either tagging as a fixed asset or trackable item. The first review is done at the department level, when the requisition is reviewed and approved by the department budget manager, next the purchasing staff reviews all purchase transactions to determine if it should be a fixed asset or taggable item and finally Property Control reviews all items identified as taggable, validating it is an item that is to be recorded as inventory. The performance of the community will be monitored and additional training *will be provided as required to specific departments and staff that continually make errors within these areas.*

Finally, training will be provided to departments and locations that do not use UMD's central CITS computer technicians for their IT Services. These locations have their own technicians that are required to ensure compliance with University Policy, Procedures and Standards regarding IT equipment and Inventory. The training will specifically address obtainment of Off Campus Forms for laptops prior to release of equipment to a custodian, submittal of appropriate perpetual inventory forms for moves, disposals and when inventory is being decommissioned for spare parts. Their performance will be monitored and additional training will be provided, as required, to specific departments and staff that are not compliant.

Expected Completion: March 30, 2009

Property Control Manual

Action Item: The University will create a Property Control Manual to be made available to the community and used as the basis of training and compliance management.

Expected Completion: May 30, 2009

Reallocating Staff Assignments

Action Item: UMD has assigned the responsibility of maintaining and physically counting inventory items to the Property Control staff. The reconciliation is managed by the Information Systems / Procurement Reporting Manager within Administrative Services, with the assistance of the Dean's and their department inventory POC's. The Dean's and their staff are required to address and document the status of any inventory item with a reconciliation issue. Once completed, it will be reviewed and approved by the Controller and Assistant Vice Chancellor of Administrative Services. UMD will review the operations staffing requirement and make any adjustments that it feels will improve the Property Control Function.

Expected Completion: July 31, 2009

Enhance Inventory Control Policies and Procedures

It is currently UMD's policy to receive all items that have an account code reflecting equipment within PeopleSoft that is to be inventoried and tagged. The functions of receiving, tagging, recording and distribution of assets are segregated at the University. Two (2) separate departments, Property Control (Tags, records and Maintains Inventory records) and Receiving (Centrally receives and distributes all equipment) with mutually exclusive staff and functions. In addition, UMD's receiving personnel scan every package that is delivered to its Pitney Bowes arrival system, a separate system from PeopleSoft, and obtains electronic signature of delivery of all packages that go through receiving.

Action Item: We will review these functions to ensure that appropriate segregation exists, provide training to staff as required and develop receiving and property control procedures for new equipment to be inventoried.

Expected Completion: July 31, 2009.

IT Configuration Management

Currently, there is a status field in the inventory system that indicates the item is either in service or disposed. The university will review the feasibility and value of expanding information within this field to include other status or condition descriptors. The critical fields that UMD will focus on updating are Custodian and Location.

Action Item: Once the current physical inventory and reconciliation is completed, Location and Custodian will be updated. All new asset records will have Serial # (if applicable), PO # (If applicable), Cost, Custodian and Location information when a record is created.

Expected Completion: May 30, 2009.

Safeguarding of Laptop Computers

UMD has created an inventory profile specifically for identifying laptops within the inventory system to facilitate the monitoring, managing and accountability of these assets.

Action Items: To strengthen its controls over laptops UMD will implement the following:

- *All custodians of Laptops will be required to complete an Off Campus Authorization that will confirm receipt of laptops. This is in conjunction with training to be provided.*
- *On an annual basis, a reconciliation between the inventory system records and forms will be performed with the requirement of updating/refreshing the off campus authorization form.*
- *When an employee leaves employment at the University, an inventory report will be run for assets that have the departing individual listed as custodian. It will be confirmed that all University assets assigned to the individual as the custodian are accounted for. The inventory record will be updated accordingly.*

Expected Completion: July 31, 2009

Auditor's Reply:

We commend the actions initiated by UMD to improve fixed-asset inventory controls. We believe that a single comprehensive inventory control system for all fixed assets located throughout the University is an important ingredient for the University's overall internal control structure. Strengthening inventory control procedures will improve the integrity of the system of record regarding fixed assets and assist the University in making IT infrastructure and configuration management decisions. We believe that controls to ensure adequate accounting of fixed assets will be strengthened by perpetually updating the inventory record when changes in status or location occur and then routinely, or on a cyclical basis, reconciling the physical inventory to the system of record. Supporting documentation for a biennial physical inventory and reconciliation were not provided for the audit period. To perform the tasks associated with maintaining a complete, valid, accurate, and reliable inventory may require management to identify and assign additional resources.

2. Chapter 647 Reporting Requirements

Our audit disclosed that UMD management did not report to the Office of the State Auditor (OSA) the thefts of 20 information technology items that the University estimated to be valued at $38,175. Chapter 647 of the Acts of 1989, An Act Relative to Improving the Internal Controls within State Agencies, requires agencies to immediately report unaccounted-for variances, losses, shortages, or thefts of funds or property to the OSA. Since UMD's inventory system of record for IT-related assets could not be relied upon, we believe that the potential of additional losses could be significant. Once brought to UMD management's attention, the thefts of computer equipment that occurred within the audit period were ultimately reported to the Office of State Auditor.

Our audit revealed that although the UMD Department of Public Safety internally documented the thefts and reported them to the UMD Controller and Property Control Manager on a timely basis, the appropriate reporting documentation was not forwarded to the Office of the State Auditor and the State Comptroller as required by Chapter 647 of the Acts of 1989. Although UMD had policies and procedures in place and in effect to ensure that incidents of thefts or lost equipment would be reported to the O`SA and the State Comptroller, we found a lapse in the reporting of IT equipment thefts due to time and resource constraints.

Listing of Stolen Items

Month of Theft	Description	Number of Stolen Items	Cost Per Item	Total Cost
December 2007	Dell Latitude D600 LT	1	$1,570	$1,570
	Gateway Solo 5300 LT	1	$1,520	$1,520
	Kodak Easyshare 7300 D/camera		$89	$89
	Sony Mavica D/camera	1	$200	$200
	Projector (Toshiba Infocus Mach)	1	$2,600	$2,600
	Microphone	1	$150	$150
January 2008	Imac	1	$1,400	$1,400
	Imac Dsktp	1	$2,000	$2,000
	Imac	1	$2,097	$2,097
April 2008	Hard Drive	1	$500	$500
	Dell hard drives	3	$600	$1,800
	Samsung TV	1	$2,400	$2,400
	Computer	1	$1,000	$1,000
	Apple G5	1	$2,299	$2,299
June 2008	IMAC	3	$4,000	$12,000
	Hard Drives			
September 2008	IMAC	1	$2,583	$2,583
	Power Mac G5	1	$3,967	$3,967
Total		**20**		**$38,175**

Recommendation:

The University should more closely monitor compliance with policies and procedures with regard to reporting requirements set forth in Chapter 647 of the Acts of 1989. Although UMD did file reports on the stolen items during our audit period, UMD should immediately report all instances of unaccounted for variances, losses, and thefts of funds or property to the OSA. The University should communicate requirements for all internal and external notifications of thefts to a designated staff member. Furthermore, the University should investigate how these thefts occurred and try to establish controls to minimize the risk of reoccurrence.

Auditee's Response:

> *The Chapter 647 reporting is now current and processes have been put into place to continue timely reporting. Procedures have been documented that inform all departments to report thefts and losses to the Campus Police Department. The Campus Police are sending Incident Reports to both the Controller and Property Control Offices. Chapter 647 filing information is sent to University Internal Audit for submission to the Office of State Auditor. In addition, it is the responsibility of the department to complete the Lost or Stolen Equipment Report; it must be completed and approved by both the property custodian and the Department Chairperson/Administrator, and returned to the Property Control Office. This form is now available on line via our Property Control website.*

Auditor's Reply:

We are pleased that UMD has familiarized management and staff with the requirements stipulated under Chapter 647. The objectives of Chapter 647 not only include notification of lost or stolen equipment or assets to the OSA, but also require state agencies to review and evaluate their internal controls. Safeguarding and reporting on the loss of computer equipment is critical not just because of the loss of the hardware, but also more importantly because of the data that may be stored on the equipment. Maintenance of a perpetual inventory, coupled with routine reconciliation, should improve the detection and subsequent accounting for any lost, stolen, or surplus computer equipment.

3. Management of Keys for Physical Security

Our audit revealed that although UMD had controls over physical security in place for selected areas housing computer equipment, controls over keys to office areas housing computer equipment needed to be strengthened. Our audit revealed that UMD had appropriate physical security controls, including intrusion alarms, surveillance cameras, motion detectors, keypad access, and electronic key access to prevent and detect unauthorized physical access to the data center, computer labs, IT classrooms, and telecommunication closets. However, at the time of our audit, control over the management, distribution, and return of brass keys at the University needed to be strengthened. Although UMD had key request forms that appeared to be adequately composed and contained applicable information that was necessary to track the brass key sets and electronic keycards, our audit revealed that University management had not established written physical security policies and procedures for issuing and returning brass key sets for office areas housing computer equipment. We found that the brass key sets were originally issued to authorized University personnel. However, since the University had not established appropriate monitoring controls, prior employees who had left UMD employment had not returned brass key sets. Although the University indicated that certain locks had been re-keyed in order to prevent physical access, UMD could not clearly identify what brass keys sets were outstanding and therefore could not ensure adequate physical security over office areas where workstations are located. As a result, the level of security may be jeopardized from an IT- and facilities-management perspective.

Our audit revealed that the University did not maintain documented policies and procedures with respect to brass keys. We also found inadequate database guidelines for the various individual listings of key holder information; inadequate separation of duties or cross training for facilities management staff responsible for maintaining the system of record for brass key holders; and no formal documented policy for the collection of keys from retiring or terminating employees. Furthermore, we found that the lists that contained key holder information were being stored only on a flash memory stick. As a result, physical security controls may not be adequate for office areas housing computer equipment. The University needs to enhance its physical security policies and procedures, and the controls over the database that contain information on key holders, to ensure that only authorized individuals have access to office areas housing computer equipment and to prevent loss, damage, or theft of IT resources. To ensure that UMD has a comprehensive physical security process, the University should establish different levels of security for various areas housing IT resources and monitor more closely the controls over the distribution and return of brass keys.

The University maintained a spreadsheet that was used to track the issuance and return of all brass key sets. The lists contained data fields that included information identifying who the key was assigned to, the type of key, what the key would open, the employment position of staff individual assigned the key, and the request and allocation date. Although the spreadsheet had a data field outlining the return of brass key sets for employees that had left or changed positions within the University, the field was rarely completed even though the number of outstanding keys as of our audit date totaled 15,815 assigned to 3,800 individuals. Our judgmental sample of 69 key holders out of a total population of 3,800 outstanding key holders at the time of our audit indicated that 21 of the individuals were no longer associated with the University, but still maintained keys that could potentially allow access to office areas housing computer equipment. The spreadsheet did not identify a complete list of brass key set holders, returned keys were not frequently updated on the list, and the list was not maintained on a perpetual basis. Our review of the spreadsheet used for maintaining assigned brass key sets revealed that the record was not current, complete, or accurate.

Generally accepted computer industry practices indicate that appropriate physical security controls should be in place to ensure that IT resources operate in a secure operating processing environment and that IT-related resources be protected from unauthorized access, use, damage, or theft. Those control measures need to include preventive controls, such as developing a process for authorizing brass key issuance to locked areas, maintaining a system of record for key holder information, and implementing a formal policy for the return of keys from retired or terminated University employees. The review of brass key sets relies on certain elements of authentication. By more closely monitoring the validity of brass key set access, the University will strengthen its authentication controls in this area.

Recommendation:

We recommend an immediate reconciliation of all brass key sets to current employees to ensure that only appropriate physical access privileges have been granted. The University should also attempt to retrieve keys from terminated employees on locks that have not been re-keyed and extend the process of re-keying locks to designated office areas. In addition, the University should develop, document, and implement policies and procedures for managing the brass key sets. The procedures should require periodic reconciliation of brass key sets to current employees and a return of all keys upon employment termination. In addition, the lists of brass key holders should be combined into a single database and should be maintained on the University's network. We recommend that the University define and ensure that the staff has an adequate understanding of the control objectives regarding physical security. The policies, procedures, and responsibilities for key management should be reviewed, approved, and distributed to all appropriate staff members and monitored by facilities.

Auditee's Response:

> *The University of Massachusetts Dartmouth recognizes the importance of improved security and access control for all of its buildings and for the protection of its assets, staff and students. The current keying systems are difficult to manage when employees leave the employ of the University. It is not cost effective to rekey buildings if a critical key is not returned. As part of its capital requests for the Federal Stimulus Funding, the university has requested funds to develop a card key access system for all of its buildings. This type of system will allow for the immediate elimination of building access once an employee leaves the University or if a key card is lost or stolen. In the event the Federal Stimulus funding is not forthcoming, the University will budget for this project through its capital project funding process.*

Action Item: Moving forward immediately, the University will develop a key policy that will require Management approval for the issuance of any key, Senior Administration approval for the issuance of any Master Key and a requirement to return keys upon the departure from the campus.

Expected Completion: March 13, 2009

Action Item: In order to protect the integrity of the database that tracks the distribution of keys on campus, the database will be placed in a secure, limited access drive on a network server. This will give the current database custodian access to a secure file that is backed up regularly. It will also prevent loss of the database should the current flash drive be lost or damaged.

Expected Completion: May 1, 2009

Action Item: Facilities will work with Human Resources and IT personnel to identify current employees in the database that currently have keys, in order to reconcile that only appropriate physical access privileges were granted. In addition, Facilities will work with IT to alter the current key tracking system; so that, the database also captures ID numbers, ensuring our ability to properly track individuals that have been assigned keys.

Expected Completion: June 30, 2009

Auditor's Reply:

We are pleased that UMD will develop and implement enhanced physical security policies and procedures over IT resources and establish a formal process for key distribution and collection. We commend the University for the corrective measures to be taken to improve physical security by developing and implementing the recommended policies and procedures regarding brass key sets. The University should continue to evaluate potential physical security risks of outstanding keys and ensure that appropriate assurance procedures are in place to sufficiently monitor compliance with the established security requirements and standards. Since some areas house hardcopy files and computer equipment, a facility management team should assess various potential risk factors in tandem with improvements in physical security.

4. User Account Management

Although access security controls were generally in place and in effect for UMD's mission-critical application and network systems, controls related to termination of user privileges for UMD staff no longer employed by the University needed to be strengthened. We found that access security policies and procedures were documented, security administration had been assigned, appropriate rules for user access activation were in effect, and requirements for password composition and frequency of change were in place. However, there were no written procedures in place requiring department heads and UMD Human Resources to inform the Computing and Information Technology Services (CITS) Department when an employee terminates employment or services. Our audit revealed instances when action had not been taken to remove expired, terminated, or suspended user accounts from PeopleSoft and UMD's network systems.

Our tests of system access security for the PeopleSoft application indicated that, contrary to sound access security practices and internal security policies, there were active user accounts that had not been deleted for individuals who were no longer affiliated with the University. The University maintains a separate listing for LAN users throughout the campus, while PeopleSoft use is for administrative staff. Our review of the 1,207 PeopleSoft user accounts indicated that 15 of these accounts should have been deactivated or disabled, but the CITS Department was not being informed on a consistent basis of changes in user status (resignations, terminations, name changes) by Human Resources. We found that the 15 deactivated users had access to UMD's Human Resource files, Student Account files, and Financial Modules. Our tests of authorized user accounts through the University's LAN indicated that of the 1,556 user accounts, 11 were no longer employed at the University. These user accounts should have been disabled or terminated on a timely basis, but instead remained active for periods ranging from one to five years. We verified that these user accounts were subsequently disabled by UMD when we brought the matter to the CITS's attention.

Our audit revealed that the UMD had not developed a formal access security policy for deactivation or deletion of user accounts. To ensure that only authorized access privileges are maintained, timely notification should be made to the Access Management Manager of the CITS Department of any changes in user status that would impact the level of authorized access privileges. The failure to deactivate user accounts in a timely manner may place UMD at risk of unauthorized access or use of established privileges. As a result, certain information residing on the UMD's network, including the PeopleSoft application, could have been vulnerable to unauthorized access and disclosure.

The Control Objectives for Information and Related Technology (CobiT), issued by the Information Systems Audit and Control Association, is a generally applicable and accepted standard for IT security and control that provides a control framework for management, business process owners, and IT users. Additional controls from the CobiT control framework include establishing procedures to ensure timely action relating to requesting, establishing, issuing, suspending, and closing of user accounts; establishing a control process to review and confirm access rights periodically; and performing regularly scheduled comparisons of resources with recorded accountability to help reduce the risk of errors, fraud, misuse, or unauthorized alteration.

Recommendation:

We recommend that UMD more closely monitor compliance with policies, procedures, and IT management controls regarding the disabling and termination of user accounts for employees no longer requiring access to UMD's network and application systems. We recommend that the policy include written notification from the UMD department heads or Human Resources Department to the CITS Department of any changes in personnel status. We further recommend that the CITS, in conjunction with department heads, review the levels of authorized privileges and perform routine reconciliations to help ensure that only authorized users have access to UMD systems.

Auditee's Response:

> *UMass Dartmouth has a total of 19,932 user accounts on the campus network with faculty, staff and students who may also have access to the PeopleSoft systems: Human Resources (HR), Financial, or Student Administration. The auditor finding shows a fraction of a percent of the total LAN users and 1% of the PeopleSoft users remained with access even though they were no longer with the University. A monthly HR report of terminated employees with reason codes is distributed by HR. Some reason codes indicate cyclical employment that dictates we not close access (Part Time Lecturers and Coaches) . These individuals do not always "officially" terminate.*
>
> *Action Item: Close access after a determined number of reports with same reason code. CITS will work with HR to establish the appropriate number of monthly reports.*
>
> *Expected Completion: June 1, 2009*
>
> *HR termination reports do not include student employees. Student employees with access to Student Records and their supervisor are required to fill out a FERPA form that designates the supervisor is responsible for notification of departure of student employees.*
>
> *Action Item: newly created descriptor (stuemp) is being placed on ldap account of any student with employee-related access. Semi-annual reviews can be instituted using this descriptor.*
>
> *Expected Completion: July 1, 2009*
>
> *Action Item: CITS will provide Department Heads, Academic Chairpersons and student employment supervisors with a list of access reports for annual review.*
>
> *Expected Completion: July 1, 2009*
>
> *Termination can be difficult to determine as the HR system terminates an employee at contract expiration. Contracts are often extended, but several weeks may pass before all paperwork is processed and the employee is again active in the HR system. Closing IT access during this lapse time would not be beneficial. Therefore, HR reports on a given date may not be a true reflection of the situation.*
>
> *Action Item: In order to tighten the timeframe for closing down accounts for employees, the Human Resource Department, as part of the exit process, will send an email to the System Access and Security Manager in CITS. At that time, the System Access and Security Manager will take the appropriate measure to remove access.*
>
> *Completed: February 6, 2009*

Auditor's Reply:

We acknowledge that the University will take steps to improve controls for system access security, including the enhancement of procedures related to termination of user account privileges. With respect to deactivation policies and procedures, we suggest that requirements be included for notification from user departments when changes in job responsibilities necessitate modification of user access privileges. The latter would pertain to those situations where there is no transfer involved, but rather a change in assigned duties where a different level of access is needed. Furthermore, once the University has formally documented the access security policies and procedures, we suggest that UMD periodically review them to ensure their applicability and that they continually meet the needs of changing IT environments and risk-management objectives.

5. Disaster Recovery and Business Continuity Planning

We found that the University of Massachusetts-Dartmouth did not have a formal disaster recovery and business continuity plan to provide reasonable assurance that data processing for campus network email, Microsoft Office suite, and web services could be regained effectively and in a timely manner should a disaster render automated systems inoperable. We found that backup copies of mission-critical and essential software and data were being generated on a consistent basis and management had assessed the relative criticality of their automated systems, and had conducted a risk analysis to determine the extent of potential risks and exposures to IT operations. However, specific formal arrangements had not been made to provide for an alternate processing site should UMD's network or systems become unusable or inaccessible.

As a result of the weaknesses noted, if a disaster were to occur, the automated applications, e-mail, network, Microsoft Office applications, and web services could not be restored within an acceptable period of time, thereby jeopardizing certain University operations. The lack of a detailed, tested plan to address the resumption of processing through the LAN and microcomputer systems might render data files and software vulnerable should a disaster occur. Without a comprehensive, formal, and tested recovery strategy for University systems, UMD would be hindered in regaining processing capabilities for automated applications, e-mail, network, and web-based services should a disaster occur.

The objective of business continuity planning is to help ensure timely recovery of mission-critical and essential functions, should a disaster cause significant disruption to computer operations. A business continuity plan should document UMD's recovery strategies with respect to various disaster scenarios. Business continuity planning for information services is part of business continuity planning for the entire organization. Although University of Massachusetts (UMASS) Central management staff indicated a comprehensive business continuity strategy exists for UMASS systems that are centrally maintained, such as the PeopleSoft application, these strategies had not been integrated with UMD business continuity efforts. Generally accepted business practices and industry standards for computer operations support the need for the UMD to have an ongoing business continuity planning process that assesses the relative criticality of information systems and develops and maintains appropriate recovery and contingency plans. To that end, UMD should assess the extent to which it is dependent upon the continued availability of information systems for all required processing or operational needs and develop its recovery plans based on the critical aspects of its information systems and supporting technology.

Recommendation:

We recommend that UMD establish a framework of procedures to ensure that the criticality of all automated systems is evaluated and that business continuity planning is assessed for all LAN systems and applications. We recommend that senior management and key users review the information technology environment and then proceed with the development of a written business continuity plan for UMD-housed systems and essential functions. We also recommend that UMD work in conjunction with the UMASS Central office to develop an integrated business continuity strategy for all UMD systems and applications.

We recommend that the updated plan be reviewed by UMD senior management and, if deemed appropriate, be approved and adopted by the University once the plan has been determined to be viable. The plan should then be tested and updated on a periodic basis to conform to changes in technology and communicated to staff. Further, we encourage UMD management to complete its assessment of the proposed reciprocal agreement and finalize the agreement as soon as possible.

We recommend that UMD develop a formal, tested disaster recovery and business continuity plan and that all personnel responsible for business continuity tasks and activities be clearly identified and adequately trained. Further, we recommend that the University develop an agreement with a compatible institution for an alternate processing agreement in case of a disaster.

Auditee's Response:

> *Over the years, it has been difficult to dedicate resources to develop a formal disaster recovery/business continuity (DR/BC) plan. UMass Dartmouth recognizes the need to have a formal plan and will identify this to be considered as an initiative for funding in FY10.*
>
> *Although UMass Dartmouth does not have a formal DR/BC plan, it does document its critical systems. This working document identifies individuals/departments responsible for the business operation and those responsible for the systems administration for its critical systems.*

> *In line with optimizing a disaster recovery operation, UMass Dartmouth has invested in virtualizing its systems. This allows for immediate failover for UMass Dartmouth systems where the failure and downtime are unnoticed by the end user.*
>
> *Action Item: Plans are in process to establish an alternate site for critical systems in fy10. Implementation is contingent on the availability of funding. Establishment of a "hot site" will allow for automatic failover in case of a disaster on campus.*
>
> *Estimated Completion: October 2009*

Auditor Reply:

We are pleased that the University is developing a viable disaster recovery and business continuity plan. However, after the plan is completed it should be reviewed and updated annually, or whenever there is a significant change to the processing requirements, risks, or changes to the University's IT infrastructure. Designation of an alternate processing site and procedures for the generation and secure storage of backup copies of magnetic media are an integral part of any recovery strategy and should be documented, maintained, and appropriately monitored to aide in recovery efforts.