Commonwealth of Massachusetts
Office of the State Auditor
Suzanne M. Bump

Making government work better

Official Audit Report – Issued February 22, 2012

University of Massachusetts Dartmouth

For the period July 1, 2009 through February 28, 2011

TABLE OF CONTENTS/EXECUTIVE SUMMARY

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 composed of 19 voting members and three non-voting members, a President who oversees the five-campus system, and 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's facilities consist of a main campus located in North Dartmouth; six satellite campuses located in New Bedford (three campuses), Fall River (two campuses), and Fairhaven; and the University of Massachusetts School of Law-Dartmouth. During our audit period, UMD's annual enrollment consisted of approximately 7,000 undergraduate, 1,349 continuing education, and 1,198 graduate students. At that time, UMD employed 1,513 full-time and part-time faculty, administrators, and staff members. UMD received state-appropriated funds totaling $47 million in fiscal year 2010 and $48 million in fiscal year 2011. In addition, UMD received $19 million in federal stimulus funding in fiscal year 2011.

The scope of our audit consisted of an evaluation of the status of the issues disclosed in our prior audit report, No. 2008-0210-4T, issued May 14, 2009, regarding inventory controls over computer equipment, compliance with Chapter 647 reporting requirements, management of keys for physical security, user account management for UMD's network and PeopleSoft application system, and business continuity and disaster recovery planning for application systems housed at UMD.

Based on our review we have concluded that, as of the period ended February 28, 2011, UMD had resolved two of our five prior audit issues. Specifically, although UMD had adequately addressed the prior audit issues relating to compliance with Chapter 647 of the Acts of 1989 and user account management controls, the prior audit issues relating to inventory controls over computer equipment, management of keys for physical security, and disaster recovery and continuity planning remained unresolved.

AUDIT RESULTS

Our prior audit disclosed that inventory controls over computer equipment needed to be strengthened to ensure that information technology (IT) resources would be properly accounted for in UMD's inventory system of record for property and equipment.

Our current audit revealed that although UMD had addressed certain weaknesses since our prior report, adequate controls were not in effect to ensure that a current, accurate, and complete perpetual inventory record of computer equipment (valued at $13,043,600) was being maintained. Specifically, our audit tests revealed that 38 of 73 items selected from the inventory list could not be physically located at UMD. An additional audit test to trace IT-related equipment from its location to the inventory record revealed that 23 of the 60 items tested were not included in the inventory record. Our audit test of UMD's computer laptop inventory revealed that 31 of 60 items selected from the inventory list could not be located with the employee to which they were assigned. Furthermore, our tests revealed that of the 31 missing laptop computers, 19 did not have off-campus form documentation, as required by UMD's internal control policies and procedures.

Our prior 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, UMD's controls over keys to office areas housing computer equipment needed to be strengthened.

Our follow-up review found that management controls still needed to be strengthened to ensure that only authorized individuals had keys to UMD facilities. Specifically, UMD did not maintain written policies or procedures for the distribution and return of physical access keys and was not reconciling the list of keyholders on a perpetual basis. Moreover, our random sample of 60 of the total population of 4,414 authorized keyholders indicated that 45 individuals were no longer employed by UMD but still possessed keys that could potentially allow access to UMD facilities, including computer labs and areas housing personal information.

Our prior audit found that UMD 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 Internet services could be regained effectively and in a timely manner should a disaster render automated systems inoperable and that specific formal arrangements had not been made to provide for an alternate processing site should UMD's network or systems become unusable or inaccessible.

Our follow-up audit disclosed that disaster recovery and business continuity planning still needed to be strengthened for application systems housed at UMD, including campus network, e-mail, and Internet services for faculty, staff, and students. Specifically, although UMD had developed a strategic plan for addressing disaster recovery and business continuity issues, it had not developed a documented and tested plan to address the applications housed at UMD.

Our prior audit disclosed that, contrary to Chapter 647 of the Acts of 1989, UMD management did not report to the Office of the State Auditor the thefts of 20 IT items valued at an estimated $38,175. Our follow-up review revealed that UMD had implemented new policies and procedures to report all missing and stolen equipment to the Office of the State Auditor in accordance with Chapter 647. Moreover, we noted that UMD had reported to the University of Massachusetts Internal Audit

Department the thefts of 41 computer equipment items from October 2008 to October 2010 totaling $53,184 and that the Internal Audit Department had complied with Chapter 647 by reporting all 41 items to the Office of the State Auditor. In addition, we confirmed that UMD had integrated Chapter 647 requirements into its internal control plan.

Our prior audit noted that although access security controls were generally in place and in effect for UMD's mission-critical application and network systems, controls related to the termination of user privileges for UMD staff no longer employed by UMD needed to be strengthened. Specifically, we noted instances in which action had not been taken to remove expired, terminated, or suspended user accounts from PeopleSoft and UMD's network systems. Our follow-up review revealed that UMD had strengthened controls for the deactivation of user accounts for individuals no longer requiring access to both the network and the PeopleSoft application system. Our tests of authorized users of the network also revealed that all of the 1,720 user accounts could be identified as individuals currently associated with UMD. In addition, our examination of the PeopleSoft application system revealed that all 1,419 user accounts could be identified as authorized individuals on the official personnel system of record.

INTRODUCTION

Background

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 composed of 19 voting members and three non-voting members, a President who oversees the five-campus system, and Chancellors located at each University of Massachusetts campus. The Board of Trustees provides oversight for each of the five university campus locations within the University of Massachusetts system. UMD's facilities consist of a main campus located in North Dartmouth; six satellite campuses located in New Bedford (three campuses), Fall River (two campuses), and Fairhaven; and the University of Massachusetts School of Law-Dartmouth. During our audit period, UMD's annual enrollment consisted of approximately 7,000 undergraduate, 1,349 continuing education, and 1,198 graduate students. At that time, UMD employed 1,513 full-time and part-time faculty, administrators, and staff members. UMD received state-appropriated funds totaling $47 million in fiscal year 2010 and $48 million in fiscal year 2011. In addition, UMD received $19 million in federal stimulus funding in fiscal year 2011.

UMD's Computing and Information Technology Services (CITS) is responsible for managing the information technology requirements for UMD. CITS provides assistance and guidance to students, faculty, and staff regarding the use of IT resources, including the use of Enterprise Resource Planning (ERP) network services and enterprise systems, Internet portal support, computer maintenance, Internet hosting services, and instructional development. CITS is composed of 44 employees, including a Chief Information Officer/Associate Vice Chancellor of Information Technology, who reports to the Vice Chancellor of Administration and Finance.

UMD's primary application is PeopleSoft, a vendor-developed ERP product that supports the following systems: financial (e.g., payables, receivables, purchasing), human resources, and student administration (e.g., admissions, student records, financial aid). At the time of our audit, computer operations for UMD were supported by file servers and workstations configured in a local area network. UMD is connected through the University of Massachusetts President's Office to the Commonwealth's Information Technology Division (ITD) through a wide area network, providing connectivity to the Massachusetts Management Accounting and Reporting System.

Audit Scope, Objectives, and Methodology

In accordance with Chapter 11, Section 12, of the Massachusetts General Laws, we performed a follow-up audit of selected information technology- (IT) related controls at UMD for the period of July 1, 2009 through January 31, 2011. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Our audit was also conducted in accordance with 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. Furthermore, we assessed UMD's compliance with the requirements of Chapter 647 of the Acts of 1989 for reporting missing or stolen equipment, and of the Commonwealth of Massachusetts regulations for accounting of assets as required by 802 Code of Massachusetts Regulations (CMR), as promulgated by the Office of the State Comptroller.

The scope of our audit consisted of an evaluation of the status of the issues disclosed in our prior audit report, No. 2008-0210-4T, issued May 14, 2009, regarding inventory controls over computer equipment, compliance with Chapter 647 reporting requirements, management of keys for physical security, user account management for UMD's network and PeopleSoft application system, and business continuity and disaster recovery planning for application systems housed at UMD.

The primary objective of our audit was to determine whether corrective action had been taken with respect to the prior audit issues. Our objective regarding inventory controls over computer equipment was 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, damage, or theft. In addition, we determined whether an annual physical inventory and reconciliation had been conducted. Our objective regarding the reporting of lost or stolen items was to determine whether UMD was in compliance with the requirements of Chapter 647 by reporting all losses or thefts to the Office of the State Auditor.

We determined whether adequate controls over management of keys for physical security were in place and in effect to provide reasonable assurance that IT-related assets would be protected from unauthorized access, use, damage, or theft.

Our objective regarding user account management was to determine whether adequate controls were in place and in effect to provide reasonable assurance that only authorized users had access to UMD's network and the mission-critical PeopleSoft application system.

We also determined whether adequate disaster recovery and business continuity plans were in place to provide reasonable assurance that application systems housed at UMD, including campus network, e-mail, and Internet services for faculty, staff, and students, could be regained within an acceptable period of time should a disaster render the IT functions inoperable or inaccessible.

To determine whether corrective action had been taken to address the issues noted in our prior audit report, we performed pre-audit work that included gaining an understanding of UMD's mission and business objectives and reviewing prior audit workpapers and UMD's current IT environment. To obtain an understanding of the internal control environment, we reviewed UMD's IT structure, primary business functions, and relevant policies and procedures and performed a risk analysis, including a brainstorming session identifying areas of potential fraud and abuse. Furthermore, we conducted interviews with UMD management and staff. Based on our pre-audit work, we determined our audit scope and objectives for performing the follow-up audit.

To evaluate inventory control over computer equipment, we obtained and reviewed the inventory system of record for computer equipment, dated October 13, 2010. We reviewed inventory control policies and procedures to determine whether UMD was in compliance with the Office of the State Comptroller's regulations regarding fixed asset control. We reviewed the inventory record, consisting of 6,006 items of computer equipment with a stated total value of $13,043,600, and determined whether inventory records contained appropriate data fields to identify, describe, and indicate the value, location, and condition of the equipment. To confirm the existence and assess the proper recording of computer equipment, we performed a statistical sample of 73 of the 5,059 IT-related items (excluding laptop computers) listed on the inventory record. We tested whether the information for identification tag numbers, location, description, and serial numbers were accurately and completely recorded on the system of record. We performed an additional statistical test by selecting 60 items from their physical locations and determining whether they were accurately recorded on the inventory system of record. Regarding our examination of UMD's inventory of laptop computers, we statistically selected 60 items out of a total population of 947 to determine whether the equipment could be located and whether the required documentation had been completed and filed with the Property Control Department as required by UMD's policies and procedures.

To evaluate whether UMD was in compliance with the reporting requirement of Chapter 647 regarding the reporting of lost or stolen equipment, we verified the existence of all incident reports from October 2008 to October 2010. We determined whether the lost or stolen items had been reported to the Office of the State Auditor and whether policies and procedures had been followed to report the items to the University of Massachusetts Internal Audit Department. Furthermore, we determined whether the missing equipment had been removed from UMD's inventory record.

To determine whether appropriate controls for the management of physical access keys were in place, we interviewed facility management and staff, determined whether policies and procedures were in place, and requested a master listing of current keyholders. In order to verify that UMD had adequate controls in place regarding the management of physical access keys, we performed a statistical sample, selecting 60 key holders of a population of 4,414 and comparing it to the UMD employee listing and verifying whether the individuals listed as keyholders were current employees.

Our tests of user account management included a review of policies and procedures to authorize, activate, and deactivate access privileges to UMD's network and the PeopleSoft application system, which resides on the University of Massachusetts' Information Technology Services file servers. In order to verify that all users of the network and PeopleSoft application system were current UMD employees, we obtained a system-generated listing containing 1,720 network user accounts and 1,419 PeopleSoft user accounts as of October 6, 2010. We compared these system-generated user account lists to a current UMD employee list.

To assess the adequacy of disaster recovery and business continuity planning for application systems residing at UMD, we determined whether a formal disaster recovery plan had been developed and tested. Furthermore, we determined whether UMD's strategic plans regarding business continuity planning had addressed the resumption of computer operations should these application systems be rendered inoperable or inaccessible.

Based on our review we have concluded that, as of the period ended February 28, 2011, UMD had resolved two of our five prior audit issues. Specifically, although UMD had adequately addressed the prior audit issues relating to compliance with Chapter 647 of the Acts of 1989 and user account management controls, the prior audit issues relating to inventory controls over computer equipment, management of keys for physical security, and disaster recovery and continuity planning remained unresolved.

AUDIT RESULTS

1. PRIOR AUDIT RESULTS UNRESOLVED

a. Inventory Controls over Computer Equipment

Our prior audit disclosed that inventory controls over computer equipment needed to be strengthened to ensure that information technology (IT) resources would be properly accounted for in UMD's inventory system of record for property and equipment. Specifically, 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 also 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, which 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 follow-up audit revealed that UMD had addressed certain weaknesses over inventory controls, such as the appointment of individuals responsible for reporting changes of all equipment assigned to their department. In addition, UMD has implemented the installation of tracking software, Computrace, on newly purchased high-risk IT-related computer equipment to aid in the recovery of stolen assets. However, we determined that adequate controls were not in effect to ensure that a current, accurate, and complete perpetual inventory record of computer equipment, with a stated value of $13,043,600, was being maintained.

According to UMD's system of record, dated October 13, 2010, there were 6,006 items of computer equipment located throughout UMD, including the satellite campus locations. Our audit tests revealed that 38 items identified from a statistical sample of 73 (52%) could not be physically located at UMD. The stated value of the missing items is $88,170. A second test to trace IT-related equipment from its location to the inventory record revealed that 23 of the 60 items (38%) tested were not included in the inventory record.

Our audit test of UMD's laptop computers revealed that 31 of 60 statistically selected laptop computers could not be located with the employee identified on the inventory record and are presumed missing. Of these 31 missing laptop computers, we verified that 19 (61%) did not have the required off-campus forms. All individuals who are assigned a laptop are required to sign an acknowledgement that they have received the laptop computer, per the UMD Inventory Control Policy.

Our examination of UMD's system of record revealed that critical data fields of information were missing. We found that information relating to purchase order numbers, cost information, equipment condition, and custodian were missing. The inclusion of the missing information would help ensure that UMD's IT equipment would be properly accounted for during the physical inventory. The integrity of the system of record for computer equipment could not be determined due to the missing or inaccurate information contained in the inventory data fields.

We determined that the policy regarding on-campus location changes, such as equipment transfers to other departments, rooms, or building locations, was also not being followed. Our test of relocated assets determined that only three of eight assets tested had been updated with the new location on the system of record. Furthermore, UMD reported 41 items as missing or stolen from October 2008 through October 2010. However, our audit test revealed that eight such items had not been removed, resulting in inaccuracies to the system of record.

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.

Our audit testing revealed that UMD management cannot be adequately assured that its computer equipment is properly accounted for and that the inventory record is accurate, complete, up-to-date, and valid. The absence of a sufficiently reliable inventory of computer equipment, as determined by our audit, hinders UMD's ability to properly account for IT resources, evaluate the allocation of equipment, identify missing equipment, and meet IT configuration management objectives. Overall, we believe the following systemic problems contributed to the deficiencies noted above: (a) lack of monitoring procedures and management oversight to ensure that an annual physical inventory and reconciliation is conducted; (b) limited property control staffing; and (c) insufficient oversight regarding the inventory system of record.

Recommendation

UMD should:

- Strengthen its inventory controls to ensure the integrity of the system of record for computer equipment.
- Strengthen its current practices to comply with the Office of the State Comptroller's requirements to conduct an annual physical inventory to ensure the proper accounting for, and disposal of, property and equipment.
- Conduct a reconciliation of IT resources to ensure that accurate, complete, and valid inventory records are being maintained.
- Continue its training efforts for assigned individuals with responsibilities for points of contact to ensure that any changes to a department's IT inventory are communicated to UMD's Property Control Officer.
- Maintain its inventory system of record on a perpetual basis to reflect any changes to computer equipment locations or custodian.
- 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. Staff should be required to complete sign-out forms before equipment is distributed to them, and users should be made aware of and acknowledge acceptable use policies.

Auditee's Response

> *The University agrees with the need to improve controls by expansion of responsibility to other core departments (Facilities, Computer and Information Technology Services, Procurement and Property Control) over the inventory process for computer equipment. We will continue to perform a biennial physical inventory and reconciliation to comply with University-wide policy.*

Specific action items are as follows:

Action Item: *UMass Dartmouth will review, improve and document its physical inventory and reconciliation procedures; provide enhanced training to all departments; expand review and control oversight to Facility and CITS department, and review system field use to strengthen controls over our inventory process.*

Expected Completion: March 15, 2012

Responsible Person(s): Assistant Vice Chancellor of Administrative Services and Controller

***Action Item**: The Facilities Department will be required, prior to closing out of a work order for department or individual moves, to confirm that change in location for trackable assets has occurred with Property control.*

Expected Completion: April 1, 2012

Responsible Person(s): Associate Vice Chancellor of Administrative Services and Assistance Vice Chancellor of Administrative Services

Action Item: *CITS Department, as the department responsible for administering and maintaining University IT assets, will on a continual basis confirm IT equipment location and custodian prior to providing any support services to the University community.*

Expected Completion: February 15, 2012

Responsible Person(s): Associate Vice Chancellor of Information Technology

Action Item: *All IT assets will be delivered to CITS for imaging and activation of electronic tracking software prior to delivery to individuals within the community. Any and all required property control forms will be received prior to release to community.*

Expected Completion: July 31, 2012

Responsible Person(s): Associate Vice Chancellor of Information Technology, Assistant Vice Chancellor of Administrative Services and Associate Vice Chancellor of Administrative Services.

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: January 31, 2012

Responsible Person(s): Assistant Vice Chancellor of Administrative Services and Controller

Auditor's Reply

We believe that controls to ensure adequate accounting of computer equipment will be strengthened by 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. Maintenance of a perpetual inventory, coupled with routine reconciliation, should also improve the detection and subsequent accounting for any lost, stolen, or surplused equipment. Strengthening inventory control procedures will improve the integrity of the system of record regarding computer equipment and assist UMD in making IT infrastructure and configuration management decisions.

b. Management of Keys for Physical Security

Our prior 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, controls over the management, distribution, and return of keys to office areas housing computer equipment needed to be strengthened.

Our follow-up review found that management controls needed to be strengthened to ensure that only authorized individuals had keys to UMD facilities. Specifically, UMD did not maintain written policies or procedures for the distribution and return of physical access keys and was not reconciling the list of keyholders to a current authorized employee roster. As a result, management could not provide adequate assurance that only authorized individuals could gain access to UMD facilities housing computer equipment.

At the time of our audit there were a total of 4,414 individuals listed on UMD's system of record as authorized keyholders. Our random sample of 60 out of the total population of authorized keyholders indicated that 45 individuals were no longer employed by UMD, but still possessed keys that could potentially allow access to UMD facilities, including computer labs and areas housing personal information. We also found that the record did not adequately identify individuals for whom keys were distributed through departmental managers and supervisors. Our review of the system of record used for maintaining assigned keys revealed that the record was not current, complete, accurate, or maintained on a perpetual basis.

Generally accepted computer industry practices indicate that appropriate physical security controls should be in place to ensure that IT resources are protected from unauthorized access, use, damage, or theft. The control measures need to include preventive controls, such as developing a process for authorizing key issuance, maintaining a system of record for key holder information, and the implementation of a formal policy for the return of keys from individuals no longer associated with UMD. We believe that UMD will strengthen its physical security controls by actively monitoring the management of keys.

Recommendation

UMD should develop, document, and implement policies and procedures for managing the distribution and return of all physical access keys to all UMD facilities housing IT resources. In addition, UMD should perform an immediate reconciliation of the system of record of authorized keyholders to a current employee roster and attempt to retrieve keys from individuals who are no longer associated with UMD. Also, UMD should ensure that the policies, procedures, and responsibilities for key management are reviewed, approved, and distributed to all appropriate staff members and that the record of authorized keyholders is maintained on a perpetual basis.

Auditee's Response

> *The University agrees with the need to improve key management and plans to formalize written policies and procedures and strengthen controls for the distribution and return of physical access keys. The University will also begin an annual reconciliation to insure that key management documentation is not only accurate, but also complies with University-wide policy.*
>
> *Specific action items are as follows:*
>
> ***Action Item:*** *UMass Dartmouth will perform a complete reconciliation of the key management database. The reconciliation with make sure all paper transactions are recorded into the database and all key holders are currently authorized by the University to possess keys. Every measure will be taken to gain possession of keys from unauthorized individuals.*
>
> *Expected Completion: August 31, 2012*
>
> *Responsible Person(s): Associate Vice Chancellor of Administrative Services and Director of Facilities*
>
> ***Action Item****: UMass Dartmouth will revise the Key Policy and include in the revision specific language concerning fines and penalties that will be levied in the event that keys are not returned. Language will also include steps to follow to replace or rekey locks that are compromised by lost or stolen keys.*

Expected Completion: August 31, 2012

Responsible Person(s): Associate Vice Chancellor of Administrative Services and Director of Public Safety/Chief of Police

Action Item: *UMass Dartmouth will begin the implementation of "smart" card access for its buildings and high security spaces. The smartcard will allow computerized control over access by giving the University the ability to shutoff access at anytime to any card. Individuals who become separated from the University will simply have their cards turned off. The University will begin to issue smartcards to a select test group during the summer of 2011. All students, faculty, and staff will have smartcard identification cards within three to four years.*

Expected Completion: August 31, 2015

Responsible Person(s): The Access Committee - includes members from CITS, DPS, Campus Services, and Facilities.

Auditor's Reply

We reiterate our concerns regarding the risks associated with unauthorized individuals having access keys to UMD facilities and recommend that that UMD management perform an immediate reconciliation of the system of record of authorized key holders to a current employee roster.

c. Disaster Recovery and Business Continuity Planning

Our prior audit found that UMD 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 Internet 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.

Our follow-up audit disclosed that UMD 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 Internet services could be regained effectively and in a timely manner should a disaster render automated systems inoperable. UMD's Strategic Plan for Information Technology 2010-2015 states its objective to "forge strategic alliances in the University at large, community, and peers in the region and expand interconnectedness, establish a 'safe harbor' for disaster recovery and business continuity, and utilize UMD's FCC licensed broadband spectrum." 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.

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's business continuity efforts.

The Fair Information Practices Act, Chapter 66A of the General Laws, requires state entities to "take reasonable precautions to protect personal data from dangers of fire, identity theft, theft, flood, natural disaster, or other physical threat." In addition, generally accepted business practices and industry standards for computer operations support the need for 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.

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

Recommendation

UMD should 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 network 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 also recommend that the updated plan be reviewed by UMD senior management and, if deemed appropriate, be approved and adopted by UMD. The plan should then be tested, 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.

Auditee's Response

> *UMass Dartmouth recognizes the need to develop a formal DR/BC plan for IT. Beginning in FY12, the University will identify and commence a phased approach to put in place a formal DR/BC Plan.*
>
> *Although UMass Dartmouth does not have a formal DR/BC plan, a number of steps have been taken and are underway to maintain access to systems in the event of an emergency.*
>
> *Document critical systems. This working document identifies individuals/departments responsible for the business operation and those responsible for the systems administration for its critical systems. The UMass Ready system, a system for documenting business processes and procedures, is being implemented as a component of the DR/BC plan.*
>
> *In line with optimizing a disaster recovery operation, UMass Dartmouth has invested in virtualizing its systems which allows for immediate failover for UMass Dartmouth systems where the failure and downtime are unnoticed by the end user.*
>
> *A generator is installed for the data center that only operates when there is no power on campus. UMass Dartmouth backs up all mission-critical systems on a consistent basis in line with the pre-determined criticality of those systems.*
>
> *UMass Dartmouth is in discussion and planning with UMass Worcester to establish a "safe harbor" for critical systems and data at the new data center in Shrewsbury. Additionally, UMass Dartmouth, together with the UMass President's Office, established a redundant network link to the internet that will maintain network connectivity in the event that one of the 2 links is down. As part of the OSHEAN BTOP stimulus grant, UMass Dartmouth*

will receive fiber [optic cabling] to the main campus and 3 satellite campuses over the next 18 months that will further solidify redundant network connectivity.

The UMass Central Office has recently hired a certified Emergency Planning and Business Continuity Manager, and the campus is currently working with this individual develop an integrated business continuity strategy for all UMD systems and applications.

Action Item: *Over the next year, UMass Dartmouth plans to establish a "safe harbor" for critical data and critical systems [in conjunction with] UMass Worcester [at the new] data center in Shrewsbury. This will allow for automatic failover for critical systems in case of a disaster on campus. Once the "safe harbor" has been established the Campus will document the environment and develop formal Disaster Recovery and Business Continuity plans. The campus will then test the plans annually, amending and enhancing the plans as testing dictates.*

Estimated Completion: July 2013

Responsible Person(s): Associate Vice Chancellor for Information Technology

Auditor's Reply

A comprehensive and well-documented business continuity and contingency strategy is essential to ensure timely recovery of mission-critical and essential business functions and systems. Until appropriate disaster recovery and continuity plans are completed, UMD needs to continue to focus on risk management and contingency planning.

2. PRIOR AUDIT RESULTS RESOLVED

a. Compliance with Chapter 647 of the Acts of 1989

Our prior audit disclosed that, contrary to Chapter 647 of the Acts of 1989, UMD management did not report to the Office of the State Auditor the thefts of 20 IT items valued at an estimated $38,175. Our follow-up review determined that UMD had implemented new policies and procedures to report all missing and stolen equipment to the Office of the State Auditor in accordance with Chapter 647. Moreover, we noted that UMD had reported to the University of Massachusetts Internal Audit Department the thefts of 41 items of computer equipment from October 2008 to October 2010 totaling $53,184 and that the Internal Audit Department had complied with Chapter 647 by reporting all 41 items to the Office of the State Auditor. In addition, our follow-up review confirmed that UMD had integrated Chapter 647 requirements into UMD's internal control plan.

b. User Account Management Controls Improved

Our prior audit noted that although access security controls were generally in place and in effect for UMD's mission-critical application and network systems, controls related to the termination of user privileges for UMD staff no longer employed by UMD needed to be strengthened. Specifically, we noted instances in which action had not been taken to remove expired, terminated, or suspended user accounts from PeopleSoft and UMD's network systems. Our follow-up audit revealed that, with respect to user account management, controls had been strengthened regarding the deactivation of user accounts no longer needed for the PeopleSoft application system. Our examination of the PeopleSoft application revealed that all 1,419 user accounts could be identified on the official personnel record. In addition, our tests of authorized users of the network also revealed that all 1,720 user accounts could be identified with individuals currently associated with UMD.