A. JOSEPH DeNUCCI
AUDITOR

The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH
ONE ASHBURTON PLACE, ROOM 1819
Boston, MASSACHUSETTS 02108
TEL. (617) 727-6200

No. 2006-0197-4T

OFFICE OF THE STATE AUDITOR'S REPORT
ON THE EXAMINATION OF
INFORMATION TECHNOLOGY CONTROLS
AT MASSASOIT COMMUNITY COLLEGE

July 1, 2004 through June 23, 2006

OFFICIAL AUDIT REPORT
NOVEMBER 30, 2006

TABLE OF CONTENTS

INTRODUCTION

The Massasoit Community College (MCC) is a two-year, public college that provides affordable, higher education primarily to residents of the City of Brockton and surrounding communities. The College's main campus is located in the city of Brockton, and a satellite campus is located in the town of Canton. The College, which is authorized under Massachusetts General Laws Chapter 15A, Section 5, operates under the auspices of a 12-member Board of Trustees that monitors compliance with policies and procedures established by the Commonwealth. The College offers associate degree programs in the arts and sciences, as well as one-year certificate programs in a variety of liberal arts, allied health courses, engineering technologies and business. During the time of our audit, there were approximately 2,800 full-time students and 3,700 part-time students. The College received approximately $18.3 million in state appropriated funds for fiscal year 2006.

The College's administrative and academic mission and operations are supported by information technology services provided by the Office of Information Technology (OIT). The OIT is comprised of 21 full-time staff members, including a Chief Information Officer who reports to the Vice President of Administration and Finance. The OIT operates both the administrative and academic data centers.

A private vendor, SunGard Higher Education Corporation, developed the College's primary application, named BANNER. The BANNER application serves as the College's primary financial management, administrative, admissions, registration, financial aid, human resources, student receivables, billing and work-study payroll systems. The BANNER application resides on five file servers utilizing an Oracle database application system.

At the time of the audit, MCC was using approximately 1,400 microcomputers configured in a local area network (LAN) to support administrative and academic functions. The administrative functions were supported by 661 microcomputers, and the academic computing consists of 744 microcomputer workstations situated in classroom and lab locations. Additionally, at the time of our audit, the College had 166 laptop computers, of which students in a classroom setting use 27 and faculty and administrators use the remainder. The College also utilizes the statewide WAN to allow certain administrators access to the Massachusetts Management Accounting and Reporting System (MMARS), the Human Resources Compensation Management System (HR/CMS), and the Commonwealth Information Warehouse (CIW) for payroll and business purposes.

The Office of the State Auditor's examination focused on an evaluation of IT-related general controls over MCC's computer operations.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

We performed an audit of selected information technology (IT) related controls at the Massasoit Community College (MCC) from February 13, 2006 to June 23, 2006 covering the period of July 1, 2004 through June 23, 2006. The scope of our audit included an evaluation of IT-related controls pertaining to organization and management, physical security, environmental protection, system access security, inventory control over computer equipment, on-site and off-site storage of backup copies of magnetic media, and disaster recovery and business continuity planning.

Audit Objectives

The primary audit objective regarding the examination of IT-related controls was to determine whether the IT environment was sufficiently controlled to support its automated systems and to safeguard computer equipment. We sought to determine whether the IT-related internal control framework, including policies, procedures, practices, and organizational structure, provided reasonable assurance that IT-related control objectives would be achieved to support administrative and academic functions. We sought to determine whether adequate physical security and environmental protection controls were in place and in effect to prevent unauthorized access, damage to, or loss of computer equipment. The areas reviewed were the MCC's administrative offices at both the main campus in Brockton and the satellite campus located in Canton. We also reviewed the file server room as well as certain academic classrooms containing computer equipment, certain telecommunication closets and on-site and off-site storage areas. We sought to determine whether adequate controls were in place to prevent unauthorized access to systems and data residing on MCC's workstations. Further, we sought to determine whether management was actively monitoring password administration.

We sought to determine whether adequate controls were in place and in effect to provide reasonable assurance that IT-related equipment was properly accounted for, recorded, and safeguarded against unauthorized use, theft, or damage. In addition, we sought to determine whether there were adequate procedures for on-site and off-site storage of backup media to support system and data recovery objectives. Further, we determined whether the MCC had a formal, documented and tested business continuity plan that would provide reasonable assurance that mission-critical and essential IT-related operations could be regained within an acceptable period of time should a disaster render the College's computerized functions inoperable or inaccessible.

Audit Methodology:

To determine the audit scope and objectives, we conducted pre-audit work that included obtaining and recording an understanding of relevant operations, performing a preliminary review and evaluation of certain IT-related internal controls, and interviewing MCC senior management. To obtain an understanding of the IT internal control environment, we reviewed the College's IT organizational structure and primary business functions for selected IT activities. We performed a high-level risk analysis and assessed the strengths and weaknesses of the internal control system for selected activities and upon completion of our pre-audit work, we determined the scope and objectives of the audit.

Regarding our examination of IT organization and management, we interviewed senior management; obtained, reviewed, and analyzed existing IT-related policies, standards, and procedures to determine their adequacy; and assessed IT-related management practices. To determine whether IT-related job descriptions and job specifications were up-to-date and reflected current responsibilities and technical knowledge requirements, we obtained a current list of the personnel employed by the OIT and a copy of IT-related job descriptions and job specifications and reviewed and compared the job descriptions and job specifications to current IT-related assignments and responsibilities.

To evaluate physical security on the Brockton and Canton campuses, we interviewed management and security personnel, conducted walk-throughs, observed security devices, and reviewed procedures to document and address security violations and/or incidents. Through observation, we assessed the adequacy of physical security controls over areas housing computer equipment. We examined the existence of controls, such as office door locks, keypad locks, remote cameras, and intrusion alarms and compared a list of individuals authorized to access the file server room to a current payroll listing.

To determine the adequacy of environmental controls at both campuses, we conducted walk-throughs and evaluated controls in selected areas to assess the sufficiency of documented control-related policies and practices. We examined the file server room and administrative office areas housing computer equipment to determine whether IT resources were subject to adequate environmental protection. Our examination included a review of general housekeeping; fire prevention, detection, and suppression; heat detection; uninterruptible power supply; emergency lighting and shutdown procedures; water detection; and humidity control and air conditioning. Audit evidence was obtained through interviews, observation, and review of relevant documentation.

To determine whether the College's control practices regarding system access security adequately prevented unauthorized access to automated systems, we reviewed policies and procedures used to authorize, activate, and deactivate access privileges to the MCC file servers through the microcomputer workstations. To determine whether only authorized employees were accessing the automated systems, we obtained a system-generated user list from MCC for individuals granted access privileges to the BANNER application and compared it to a current personnel listing at the College. We reviewed control

practices regarding logon ID and password administration by evaluating documented policies and procedures provided to MCC personnel. To determine whether the administration of logon ID and passwords was being properly carried out, we reviewed and evaluated selected control practices regarding system access to network resources and reviewed the security procedures with the security administrator responsible for access to the automated systems on which the College's application systems operate. We determined whether all employees authorized to access the automated systems were required to change their passwords periodically and, if so, the frequency of the changes.

To determine whether adequate controls were in place and in effect to properly safeguard and account for computer equipment, we initially reviewed inventory control policies and procedures and obtained the College's inventory system of record for computer equipment. We reviewed the system of record, as of February 14, 2006, to determine whether it contained appropriate data fields to identify, describe, and indicate the value, location, and condition of the computer equipment. We further examined the MCC inventory record for tag numbers and acquisition dates. To determine whether the system of record for computer equipment was current, accurate, and valid, we used Audit Command Language (ACL) to select a sample of 72 computer equipment items and compared the information from the items selected to information contained in the master inventory record. We confirmed the inventory tags, serial numbers, description, and location of the hardware items selected in our sample and listed on the inventory record to information on the actual equipment on hand. We also judgmentally selected a floor to list sample of 106 items and traced information from the items to information contained in the master inventory list.

To assess the adequacy of business continuity planning, we determined whether any formal planning had been performed to resume computer operations should the network application systems 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. Furthermore, to evaluate the adequacy of controls to protect data files through the generation and on-site and off-site storage of backup copies of magnetic media, we interviewed management regarding the generation and storage of backup copies of magnetic media. We also reviewed the physical security and environmental protection controls in place and in effect over areas for on-site and off-site storage of backup copies of magnetic media We also examined the delivery logs to determine whether the tapes were being transferred to and from the off-site location on a consistent basis.

Our audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) issued by the Comptroller General of the United States and generally accepted industry practices. Audit criteria used in the audit included management policies and procedures and control guidelines outlined in Control Objectives for Information and Related Technology (CobiT), as issued by the Information Systems Audit and Control Association, July 2000.

.

AUDIT CONCLUSION

Based on our audit at the Massasoit Community College (MCC), we determined that internal controls in place provided reasonable assurance that IT-related control objectives pertaining to organization and management, physical security, environmental protection, and on-site and off-site storage of backup computer media would be met. However, our audit revealed that controls pertaining to business continuity planning and disaster recovery, system access security, and inventory control for computer equipment needs to be strengthened.

Our examination of IT-related organization and management controls 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 IT management and staff were well aware of their responsibilities, and that IT-related job descriptions and job specifications reflected current responsibilities and required technical knowledge and skills. Our review of IT-related internal control policies and procedures indicated that the College had developed and documented policies and procedures for IT-related functions for the selected control areas we reviewed.

Our audit found that physical security and environmental protection controls were in place and in effect to provide reasonable assurance that MCC's IT resources would be protected and were operating in a controlled environment at both campus locations. Our examination of physical security controls confirmed that the file server room was locked and the College maintained a list of authorized individuals having keys to the file server room. The MCC has full-time campus police on duty 24 hours, seven days a week at both campuses. We found that the administrative offices and the computer labs were equipped with motion detectors and intrusion alarms. In addition, we found that the computer labs were locked and equipped with intrusion devices.

Our evaluation of environmental protection controls over the administrative office areas and file server room indicated that policies, procedures, and appropriate control mechanisms were in place and in effect over the processing environment. Specifically, we found that control objectives related to air conditioning, fire prevention and detection, emergency power and lighting, and emergency shut down would be met. We also observed the presence of handheld fire suppression devices and an automatic fire suppression system throughout both campuses. The administrative offices and classroom labs housing computer equipment that we observed were found to be clean and environmentally protected. Our audit revealed that general housekeeping controls over the file server room needed to be strengthened. Specifically, we observed the presence of excess computer supplies and surplus equipment in the file server room and recommend that the room not be used for storage.

Our audit indicated that access security controls needed to be strengthened to ensure timely deactivation of user privileges for those individuals no longer requiring access to the BANNER

application system. Although we found that appropriate policies and procedures were documented, security administration had been assigned, rules for user access activation were in place, and security requirements had been established, 14 user accounts should have been deactivated. Our tests of authorized users of the BANNER system revealed that 14 (5%) out of 277 users could not be identified on the MCC's May 12, 2006 payroll record. Furthermore, with regard to password administration, although MCC had policies for password length and composition, a mandatory timeframe for changing passwords had not been established for access to the BANNER application. As a result, passwords had not been changed on a regular basis since the BANNER application became fully operational in July 2004.

With respect to inventory control of computer equipment, we found that the MCC was adhering to the policies and procedures promulgated by the State Comptroller's Office requiring annual physical inventories. Our tests of the MCC's hardware inventory revealed that items were properly accounted for, locatable, and tagged. We believe that including acquisition dates and historical cost figures for all equipment would allow proper accounting for computer equipment and would enhance the IT-related inventory record. The College should also consider expanding the data fields to include equipment condition, targeted replacement, and maintenance status to support IT configuration objectives.

Our audit revealed that MCC was not in compliance with Office of the State Comptroller's reporting requirements regarding stolen equipment. We found that the College did not comply with the requirements of Chapter 647 of the Acts of 1989 for instances that had occurred during our audit period since the College had failed to notify the Office of the State Auditor of stolen computer equipment. According to the College the estimated value of the stolen equipment was $1,400.

Our audit disclosed that MCC did not have a formal, tested, disaster recovery plan to provide reasonable assurance that mission-critical and essential data processing operations could be regained effectively and in a timely manner should a disaster render automated systems inoperable. We determined that procedures regarding the generation of backup copies of magnetic media were being performed on a consistent and timely basis. We also found that backup media was stored at secure and environmentally protected on-site and off-site locations and that logs of backup media were being appropriately maintained.

AUDIT RESULTS

1. Disaster Recovery and Business Continuity Planning

We found that Massasoit Community College did not have a formal disaster recovery and business continuity plan to provide reasonable assurance that data processing for administrative and academic functions could be regained effectively and in a timely manner should a disaster render automated systems inoperable. Although backup copies of mission-critical and essential software and data were being generated on a consistent basis and properly stored, specific formal arrangements had not been made to provide for an alternate processing site should the LAN be unusable or inaccessible. Our audit also revealed that system users had not developed user area contingency plans to address a potential loss of their automated processing. Based on our interviews with College management and staff, we found College management had not assessed the relative criticality of their automated systems and had not conducted a risk analysis to determine the extent of potential risks and exposures to IT operations.

We acknowledge that the College had an informal draft business continuity plan, but the plan had not been formally documented and approved by the President of the College or the Board of Trustees. The informal draft plan had never been tested. We also found that a reciprocal agreement to provide temporary processing services and facilities between MCC and Bristol Community College had been drafted, but by the conclusion of our audit, the agreement had not been formally approved and adopted by the institutions.

As a result of the weaknesses noted, if a disaster were to occur, the automated systems, including the functional capabilities of the Banner application supported by the OIT, could not be restored within an acceptable period of time, thereby jeopardizing essential College operations. The lack of a detailed, tested plan to address the resumption of processing by 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 its application systems, the College would be hindered in re-establishing the processing of mission-critical functions, such as admissions, registration, financial aid, human resources, student receivables, billing, and work-study payroll systems 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 the MCC'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. Generally accepted business practices and industry standards for computer operations support the need for the MCC to have an ongoing business continuity planning process that assesses the relative criticality of information systems and develops appropriate contingency and recovery plans. To that end, MCC 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 MCC establish a framework of procedures to ensure that the criticality of all automated systems is evaluated and that business continuity planning is assessed for the LAN. We recommend that senior management and key users review the information technology environment and perform a criticality assessment and risk analysis of their automated systems. Based on the results of the assessment, MCC should proceed with the development of a written business continuity plan for their mission-critical and essential functions.

We recommend that the updated plan be reviewed by the President and the Board of Trustees and if deemed appropriate be approved and adopted by the College 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 MCC management to complete their assessment of the proposed reciprocal agreement and finalize the agreement as soon as possible.

Auditee Response:

> *While there is no formal tested Disaster Recovery Plan, there is an existing Disaster Recovery Plan that was developed in 2004 by Collegis consultants in response to an earlier audit. This plan is reviewed and updated as vendor contract information changes, and is annually reviewed within IT for general currency and accuracy. The plan, however, lacks detailed scenarios and recovery plans that would help prevent delays in the reestablishment of mission critical systems. The plan also lacks formal test procedures and has not been reviewed by senior management and/or the Board of Trustees.*
>
> *To address the deficiencies in the existing plan we propose to expand the specific responses for each of the disaster scenarios to include responsible staff, specific stepwise actions to be taken, and include a proposed test plan for each scenario. We are also developing questionnaires and checklists for areas of critical concern; standards, servers, network, identification management, operations and physical access, and personnel, that will allow an internal review of these areas on an annual basis.*
>
> *It is expected that a draft of the revised plan and the results of the questionnaires will be available for senior management review by December 15, 2006. The draft plan and questionnaire results should provide the means for an effective assessment of preparedness for disaster and a risk assessment profile.*
>
> *Additionally, we will continue to pursue the reciprocal agreement between Massasoit Community College and members of CONNECT towards a formal, signed arrangement that will provide a recovery site in the event of a worst case disaster*

Auditor's Reply:

We acknowledge that the College has made efforts to develop a more comprehensive and current strategy for business continuity planning. Documenting and testing comprehensive business continuity and contingency plans provides a strong basis for regaining mission-critical and essential IT and business operations within an acceptable period of time. The College should conduct a thorough risk assessment as a sound first step. The business continuity plan that is developed should address various disaster scenarios and clearly identify cooperative efforts necessary to assist in recovery efforts. Modeling a business continuity strategy by incorporating generally accepted disaster recovery and business continuity practices and CobiT standards and guidelines should help ensure that all key elements of a comprehensive business continuity strategy are addressed. We encourage the College to continue to pursue designation of an alternate processing site as an integral part of any recovery strategy.

2. System Access Security and Password Administration

Our examination of system access security for the BANNER application that supports administrative and academic operations indicated that access security administration needed to be strengthened. We found that appropriate policies and procedures were documented, security administration had been assigned, and appropriate rules for user access activation and security requirements had been established. However, although there were written policies and procedures in place requiring that the Office of Information Technology (OIT) be informed when an employee terminates employment at the College, we found that written notification was not being provided on a consistent basis by the MCC's Human Resources Department to inform the OIT that certain user privileges to the automated systems needed to be deactivated.

Our tests of access security for the BANNER application system indicated that, contrary to sound access security practices, there were active user IDs and passwords for individuals who were no longer employed by the College. Our tests indicated that 14 (5%) out of 277 authorized users could not be identified on MCC's May 12, 2006 payroll record. Our audit indicated that termination dates for the active user accounts of individuals no longer employed at MCC went back to April 27, 2004.

Access to computer systems, program applications, and data files should be authorized on a need-to-know, need-to-perform, and need-to-protect basis. To ensure that only authorized access privileges are maintained, timely notification should be made to the security administrator of any changes in user status, which would impact the user's level of authorized access. For example, the Human Resources Department should notify the security administrator of changes in employment status so that access privileges may be deactivated in a timely manner for individuals no longer needing access. Although procedures were in place to inform the security administrator of changes in employment status, those procedures were not always followed. As a result, user accounts no longer needed or authorized were not

always removed from the active user list in a timely manner. Consequently, critical information on the BANNER application may have been vulnerable to unauthorized access, alteration, and deletion.

Computer industry standards advocate that policies and procedures for system access security be documented and approved to provide a basis for proper protection of information assets. The policies and procedures should address authorization for system users, activation and deactivation of user accounts and notification of changes in user status.

Our review of password administration of the BANNER application revealed that passwords had not been changed on a regular basis since the application became fully operational in July 2004. Although MCC had policies for password length and composition, our audit revealed that a mandatory timeframe for changing passwords had not yet been established. The failure to change passwords for user accounts on a regular basis places the College at risk of unauthorized use of established privileges or to unauthorized access. Formal policies and procedures should be developed to address password administration requiring system users to change their passwords on a regular basis.

Recommendation:

The College's access security policies and procedures should be amended to include a provision which requires the prompt disabling of employee names from the authorized user list when their active service ends. The College should designate an appropriate official to take responsibility for ensuring compliance with this requirement and monitor results on a regular basis so that the user list is promptly updated and contains only active, legitimately enabled employees.

Regarding password administration, we recommend the College utilize the default mechanisms within its security software to prompt users to change their passwords on a pre-defined basis. The failure to change passwords on a regular basis places the College at risk of unauthorized access to their mission-critical and essential application systems.

Auditee Response:

> *We had considered that locking an account accomplished the same objective as deleting an account with the advantage that the user's Banner security profile was retained for future reference. Since a locked account can only be accessed after someone with Database Administrator capability unlocks the account, we did not consider the locked account a significant security risk. However, upon the recommendation of the audit team we have deleted the locked accounts from the Banner database.*
>
> *At the time of the audit there was, and still is, an automatic notification of any HR activity to terminate an employee. Therefore IT knows immediately when employee access should be removed. At this notification we had been locking Banner accounts to prevent unauthorized access and deleting other access accounts. From this point forward the procedure for terminated employees will be modified to delete any Banner accounts along with other account access rights such as network and email access.*

The recommendation for aging and expiring Banner passwords is well taken and is being implemented in conjunction with a user awareness effort and publication of a Banner Password Policy and Best Practices for password generation. The recent implementation of Banner 7 (October 9, 2006) and Oracle 9i now allows for the automatic notification of user password expiration that was not available in earlier iterations of these products. Since Banner allows for users to change passwords at any time with a user friendly form, we will be testing the implementation of these security features from within the Banner application. When proven to be fully functional, we will enforce a password minimum length and complexity policy that will create more secure passwords. Password expiration will be set for 60 days, in conjunction with other user account policy on campus. We expect that this change will be met with a degree of resistance and intend to use this audit report to reinforce the importance of this security measure.

Also, the CIO will work with the Human Resources department quarterly to compare a listing of all users with Banner access to a listing of all active employees in an effort to identify and resolve any discrepancies that may still fall through the cracks of the system already in place.

Auditor's Reply

We are pleased that the College is taking steps to strengthen security to its automated systems by reinforcing the existing policies and procedures that require notification to the Network Security Administrator of any change in employee job requirements, transfers, active/inactive status, or termination that would necessitate modification or deactivation of access privileges. We suggest that the notification procedures and subsequent modification or deactivation of user access privileges be more closely monitored. We feel that system defaults requiring change to user passwords on a pre-determined timeframe and a standard for password composition will improve access security controls.

3. Non-compliance with Chapter 647 Reporting Requirements

Our audit disclosed that Massasoit Community College (MCC) did not report to the Office of the State Auditor (OSA) the thefts of two laptop computers which the College estimated the value to be $1,400. 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. Chapter 647 also requires the OSA to determine the internal control weaknesses that contribute to or cause an unaccounted-for variance, loss, shortage, or theft of funds or property; make recommendations to correct the condition found; identify the internal control policies and procedures that need modification; and report the matter to appropriate management and law enforcement officials.

Our audit revealed that the first theft was reported to campus police on April 15, 2005 and the second theft was reported on August 9, 2005. The campus police completed incident reports on both items and forwarded the reports to the Massachusetts State Police. However, since the College was unaware of the

reporting requirements of Chapter 647 involving missing or stolen equipment, a report of the thefts was never filed with the OSA. Subsequent to our discussions with MCC administrators, a written policy and procedure was developed to ensure that any future incidents of thefts or lost equipment would be reported to the OSA in compliance with the requirements of Chapter 647.

Recommendation:

The MCC should maintain policies and procedures that will comply with Chapter 647 of the Acts of 1989 and immediately report all instances of unaccounted for variances, losses, and thefts of funds or property to the OSA. The College should communicate requirements for all internal and external notifications of thefts to a designated staff member. Furthermore, the College should investigate how these thefts occurred and try to establish controls to minimize the risk of reoccurrence.

Auditee Response:

> *The two missing laptops identified during this audit have been reported to the Office of the Massachusetts State Auditor using the Chapter 647 forms.*
>
> *IT has also incorporated Chapter 647 reporting requirements into the procedures to be followed for all stolen equipment. This process will be coordinated with the Comptroller's Office and Campus Police.*

Auditor's Reply

We commend the College for initiating corrective action. We are pleased that the College is taking steps to include the requirements set forth in Chapter 647 of the Acts of 1989 in its inventory control system.