The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH

ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108

A. JOSEPH DeNUCCI
AUDITOR

TEL (617) 727-6200
FAX (617) 727-5891

No. 2010-0197-7T

OFFICE OF THE STATE AUDITOR'S REPORT ON THE EXAMINATION OF INFORMATION TECHNOLOGY-RELATED CONTROLS AND THE USE OF AMERICAN RECOVERY AND REINVESTMENT ACT FUNDS AT MASSASOIT COMMUNITY COLLEGE

January 1, 2007 through June 22, 2010

OFFICIAL AUDIT REPORT

DECEMBER 17, 2010

TABLE OF CONTENTS

INTRODUCTION

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. MCC's main campus is located in the City of Brockton and a satellite campus is located in the town of Canton. MCC, 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. MCC 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 our audit, MCC's annual enrollment was approximately 3,600 full-time students and 4,300 part-time students. MCC received $20 million in state-appropriated funds for fiscal year 2008, $19.2 million for fiscal year 2009, and $15.6 million for fiscal year 2010. In addition, MCC received $4.5 million in federal stimulus funding for fiscal year 2010.

MCC's administration, academic mission and operations are supported by information technology services provided by the Office of Information Technology (OIT). The OIT is comprised of 23 full-time staff members, including a Chief Information Officer who reports to the Senior Vice President and Vice President of Faculty and Instruction. A private vendor, SunGard Corporation, developed MCC's primary software application, BANNER. The BANNER application provides MCC with financial management and administrative, admissions, registration, financial aid and human resources services. The BANNER application system, which is supported by an Oracle database system, resides on five file servers located at MCC.

At the time of the audit, MCC was using 1,282 workstations configured in a local area network (LAN) to support administrative and academic functions. The administrative functions were supported by 494 workstations and the academic functions were supported by 788 workstations in classroom and lab locations. Additionally, the OIT supported 194 notebook computers that were available for administrative staff, faculty, and student use. MCC's file servers provide connectivity to the statewide wide area network (WAN) allowing 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 OSA's audit was limited to an examination of certain IT-related general controls over and within the MCC's IT environment and a review of controls over personal information and federal stimulus funds received by MCC.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

In accordance with Chapter 11, Section 12, of the Massachusetts General Laws (MGL), we performed a follow-up audit of certain information technology (IT) general controls at the Massasoit Community College (MCC). Our audit, which was conducted from March 29, 2010 through June 22, 2010, covered the period of January 1, 2007 through June 22, 2010. The scope of the audit consisted of an evaluation of the status of prior results in our audit report, No. 2006-0197-4T, issued November 30, 2006, regarding system access security, password administration, compliance with MGL Chapter 647 reporting requirements, and disaster recovery and business continuity planning. Furthermore, we determined whether the MCC had appropriate policies and procedures in place regarding the protection of personal information. In addition, we performed a review of selected controls related to funding received at MCC from the American Recovery and Reinvestment Act (ARRA).

Audit Objectives

The primary objective of our audit was to determine whether corrective action had been taken with respect to our prior IT audit results and to assess the adequacy of selected IT general controls. Our objective regarding system access security was to determine whether adequate controls were in place and in effect over user account management, including activation and deactivation procedures, to provide reasonable assurance that only authorized users were granted access to the BANNER application system. A further objective was to determine whether passwords to the BANNER application system were being properly controlled and monitored.

We sought to determine whether adequate controls were in place and in effect to provide reasonable assurance that MCC was aware of the provisions in Chapter 647 and that they had complied with reporting requirements regarding lost or stolen equipment.

We sought to determine whether MCC had in place adequate disaster recovery and business continuity plans to provide reasonable assurance that computer operations would be regained within an acceptable period should a disaster render MCC's computerized functions inoperable or inaccessible. A further objective was to review MCC's policies and procedures associated with the protection of personal information and the compliance requirements set forth through MGL Chapter 93H. In addition, we sought to determine the adequacy of controls at MCC to account for the funds received through the ARRA and compliance with reporting requirements as mandated in the Interdepartmental Service Agreement between MCC and the Commonwealth of Massachusetts Department of Higher Education.

Audit Methodology

To determine whether corrective action had been taken to address the recommendations presented in our prior audit report, No. 2006-0197-4T, we performed pre-audit work that included gaining an understanding of MCC's mission and business objectives, and reviewing prior audit workpapers and the current IT environment. To obtain an understanding of the internal control environment, we reviewed the MCC's organizational structure, primary business functions, and relevant policies and procedures, and interviewed MCC management and staff. Based on our pre-audit work, we confirmed our audit scope and objectives for performing the follow-up audit.

Our tests of system access security included a review of policies and procedures to authorize, activate, and deactivate access privileges to the BANNER application system. We reviewed control practices regarding logon ID, password administration, and password composition by evaluating the appropriateness of documented policies, procedures, and guidance provided to personnel. We reviewed training instruction manuals given to users who were granted access privileges to the BANNER application and sought to confirm that each user had acknowledged an understanding of the security requirements for using the application. We determined whether all individuals authorized to access the BANNER application were required to change their passwords periodically and, if so, the frequency of the changes. In order to verify that all users of the BANNER application were either full-time or part-time employees, we obtained a system-generated user list containing 230 user accounts as of April 13, 2010. We compared the user account list to an MCC employee listing, dated April 14, 2010, which consisted of 380 full-time employees and 821 part-time employees. We developed an exception list consisting of any user accounts that could not be reconciled to the employee list. Our audit did not include an examination of controls over network security.

To determine whether the MCC was in compliance with the reporting requirements of Chapter 647 of the Acts of 1989, we interviewed management and staff regarding their awareness of the Chapter 647 reporting requirements. Furthermore, we examined incident reports for missing or stolen IT-related equipment for the audit period and verified whether all incidents were reported to the Office of the State Auditor.

To assess the adequacy of business continuity planning, we determined whether MCC had performed any formal planning to resume IT operations should the automated systems be rendered inoperable or inaccessible. In addition, we determined whether risks or exposures to computer operations had been evaluated and conducted interviews with management as well as a cross-section of support staff to determine the business impact to users should the automated systems be unavailable. In addition, we reviewed the status of MCC's efforts to designate an alternate processing site to be used in case of an extended loss of the current operational facility and disruption of computer system availability.

To determine whether MCC was in compliance with the requirements associated with the protection of personal information and those set forth through MGL Chapter 93H, we determined whether documented policies and procedures were in place regarding the protection of sensitive data, whether relevant hard copy files were safeguarded, and whether appropriate controls were in place regarding system access security to the BANNER application system. We also determined whether MCC had documented breach notification procedures.

To determine the nature and extent of ARRA funding received by MCC, we obtained and reviewed the Interdepartmental Service Agreements (ISA) between the Massachusetts Department of Higher Education and MCC. We examined the agreements to determine the specific areas that the ARRA funds were to be expended. Furthermore, we obtained MCC payroll records for the periods of December 5, 2009, December 19, 2009, January 2, 2010, and January 16, 2010 and compared these records to Massachusetts Management Accounting and Reporting System (MMARS) reports during this period to verify the number of employees compensated by ARRA funds as well as the total amount of ARRA funds expended by MCC. We examined appropriation codes in the MMARS reports to verify that the ARRA expenditures were properly accounted for. We also obtained and reviewed employment reports verifying the number of positions retained at MCC as a result of ARRA funding. To determine that MCC was complying with reporting requirements, we verified that quarterly reports were submitted by the Massachusetts Department of Higher Education on behalf of MCC detailing the amount of funds expended and the number of positions retained through March 31, 2010, the last reported quarter of our audit period. Furthermore, we sought to determine whether there were any funds appropriated and expended for non-payroll purposes, and to what extent and purpose those funds were expended. We requested and reviewed a sample of purchase orders, purchase requisitions, and invoices for the installation of a telecommunications and security system. We verified that the appropriate MMARS accounting codes were used, that the appropriated funds were paid, and that the proper signatures for approval were in place. We also tracked these expenses to the ARRA reporting documents issued by the Department of Higher Education.

Our audit was conducted in accordance with generally accepted government auditing standards issued by the Comptroller General 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

Our examination of the status of audit results from our prior audit report No. 2006-0197-4T, issued November 30, 2006, confirmed that corrective action had been taken to address control objectives regarding the MGL Chapter 647 reporting of lost or stolen equipment and disaster recovery and business continuity planning. However, our audit tests revealed that user account management for the BANNER application system needed to be strengthened for part-time employees.

Our audit confirmed that MCC had implemented policies and procedures to report all missing and stolen equipment to the Office of the State Auditor in accordance with Chapter 647. We found that MCC had reported to the Office of the State Auditor the thefts of five items of computer equipment from January 2007 to April 2010 totaling $4,900. Our audit confirmed that MCC had integrated Chapter 647 requirements into the MCC internal control plan.

Our review of disaster recovery and business continuity planning indicated that MCC had taken corrective action by developing a formal, documented business continuity plan to restore automated systems should computer operations be rendered inaccessible or inoperable. Our audit indicated that certain tests of the recovery plan had been conducted on-site, and the results had been incorporated into the current disaster recovery plan, dated March 2010. We found that the plan provided sufficient disaster recovery strategies to regain computer operations in a timely manner should a catastrophic event render IT systems inoperable. In addition, we found that MCC had entered into formal reciprocal agreements with five surrounding area state colleges to further assist in recovery efforts.

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 our audit revealed 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, we found that three user accounts for part-time employees should have been deactivated. Our tests of authorized users of the BANNER application system revealed that three out of 230 users could not be identified on the MCC's April 14, 2010 payroll roster. The three users were part-time employees with access to the BANNER application system which contains sensitive data including social security numbers and financial-related information. The individuals had terminated their employment on June 30, 2008, March 30, 2009, and September 28, 2009, respectively. We determined that although access privileges were granted on a read-only basis for two of the individuals and limited data entry privileges regarding student registration for the third user, we found that the user accounts had access to personal and sensitive information. Our additional audit test confirmed that the user accounts were immediately deactivated by MCC management when brought to MCC's attention. We acknowledge that MCC had implemented controls restricting access for user accounts that did not have activity after a predefined period. Regarding password administration, we found that there were policies for password length and composition, mandatory timeframes had been established for changing passwords for access to the BANNER application, and that users were prompted to change passwords on a regular basis.

Regarding our review of controls over personal information, we found that the MCC had policies and procedures in place and in effect to comply with the requirements of Massachusetts General Law Chapter 93H regarding protection of personal information and notification requirements for a breach of confidential data. We found that MCC had developed documented procedures to prevent, detect, and mitigate theft of personal information as part of MCC's operations and accounting system. The procedures, approved and implemented by MCC's Board of Trustees on April 8, 2009, follow the guidelines of protecting personal information against identity theft as detailed in the Federal Fair and Accurate Credit Transactions Act of 2003.

Regarding our review of ARRA funding received at MCC, we determined that MCC had controls in place and in effect to properly report on the accounting of federal stimulus expenditures. Our audit tests of the accounting of federal stimulus expenditures, as outlined in the Inter-Departmental Agreement between the Department of Higher Education and MCC, indicated that all expenditures were correctly charged to the appropriate expenditure account for job retention under the agreement. We found that MCC had expended $2,287,965 for payroll with an average of 250 jobs retained through March 31, 2010. Regarding our examination of non-payroll stimulus funds, we found that MCC had expended $807,000 in federal stimulus funds for security and telephone systems through the last reported quarter, March 31, 2010. We verified these expenditures by reviewing purchase orders and approved invoices and tracing the expenses to the sub-recipients' quarterly reports. Through our examination and review of sub-recipient quarterly reports and MMARS reports, we determined that MCC had conformed to the requirements as stipulated in the inter-departmental agreements. Furthermore, we verified that the required quarterly reports were filed by the Massachusetts Department of Higher Education and reviewed by MCC management to provide accurate data relative to the number of positions that MCC had retained as a result of the federal stimulus funding.

AUDIT RESULTS

1. Prior Audit Results Unresolved - User Account Management and Password Administration

Our prior audit report indicated that 14 (5%) out of 277 authorized users of the BANNER system could not be identified on MCC's payroll record. The prior audit indicated that termination dates for the active user accounts of individuals no longer employed at MCC exceeded 24 months.

Our current audit found that although access security over the MCC's network appeared to be appropriate, controls needed to be strengthened to ensure that all users who are no longer authorized to access the mission-critical BANNER application system are deactivated in a timely manner. Although we found that adequate controls were in place to authorize and activate user accounts to the BANNER application, controls needed to be strengthened to ensure timely deactivation of access privileges for users no longer authorized to access to the application.

Our tests of user account management for the BANNER application system indicated that three of 230 user accounts had not been deleted for individuals who were no longer employed by the MCC. Our audit disclosed that the three user accounts were for part-time employees who had terminated employment at MCC as far back as June 2008 and that the user accounts remained on the active BANNER user list. Moreover, our audit revealed that there were no formal policies and procedures in place requiring notification from the Human Resources Department to the Office of Information Technology to initiate the removal of access privileges of part-time individuals who terminate employment with MCC. Our audit evidence confirmed that a reconciliation of the user account list to authorized employees was being conducted for full-time employees on a pre-defined basis, but that a reconciliation of user accounts for part-time employees was not being conducted.

Our audit revealed that an increase in the monitoring of user accounts associated with the part-time employees is required to evaluate user account access and identify user accounts that should be deactivated. The failure to deactivate or delete user accounts in a timely manner places automated systems at risk of unauthorized access or having an individual gain higher access privileges than currently authorized. As a result, certain information residing on the BANNER application system could be vulnerable to unauthorized access.

Additional controls recommended by the CobiT control framework include having procedures to ensure timely action for suspending and closing user accounts, having a control process to periodically review and confirm access rights, and regularly performing scheduled comparisons of resources with recorded accountability to help reduce the risk of errors, fraud, misuse, or unauthorized change. 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 functions.

Regarding our examination of password administration for the BANNER application system, our prior audit indicated that passwords had not been changed on a regular basis since the application became fully operational in July 2004 and that a mandatory timeframe for changing passwords had not yet been established. Our current audit revealed that management had taken corrective action by establishing mandatory timeframes for changing passwords and strengthening controls over password composition by adopting security standards as promulgated by the Commonwealth's Information Technology Division.

Recommendation

We recommend that management develop written policies and procedures requiring timely notification to the security administrator of any changes in both part-time and full-time employee status that could warrant change or deactivation of access privileges to the BANNER application system. We also recommend that the MCC implement preventive and detective control mechanisms, such as vigilant monitoring of access accounts, to ensure that only authorized individuals have appropriate levels of access to IT resources.

Auditee's Response

> *In response to the earlier audit with findings on the deactivation of Banner accounts Massasoit had implemented an automatic email notification of responsible IT staff when individuals terminated employment at the college. With this audit, it was discovered that the auto-notify emails triggered by termination activity in the human resources department are only triggered for full- time employees. The accounts that were found to be active inappropriately with this audit were all part-time employees who had terminated employment.*
>
> *There are two means by which we hope to address this persistent problem. First, Massasoit has contracted with an outside vendor, Interview Exchange, to develop and implement a paperless system for processing all personnel transactions. The first phase of this process was the conversion of all job postings and the process of application and candidate review to a shared electronic format. This conversion was completed on August 20, 2010. The next phase of the implementation, taking place in September 2010, will be the conversion of all paper transactions for personnel actions to electronic forms. Each of these electronic requests will automatically be forwarded to the CIO. So, all hiring, termination, suspension, and transfer activity processed by Human Resources regardless of whether an employee is full time, part time or temporary, will be electronically transmitted to the CIO for the appropriate response. This will eliminate any need for manual reminders or periodic cross-communication between IT and the payroll or human resource departments.*

> *Also, IT is in the process of designing a system for auto-provisioning of Active Directory accounts, email accounts, and Banner personnel records from HR/CMS entries by the Human Resources staff. Some relatively simple additional coding will be able to provide reporting to IT of any termination entries made to HR/CMS by the Human Resources staff that may elude the personnel data form process. This additional procedure will serve as a cross-check of the Interview Exchange system being implemented.*
>
> *We feel strongly that these two measures will close any loophole in existing procedures and practices that allows accounts for Banner and any other IT administered accounts to remain active inappropriately.*

Auditor's Reply

We acknowledge MCC's action for addressing the security concerns related to user account management. We believe that efforts to improve communication regarding changes in access privileges for part-time employees will strengthen security and enhance user account management. In addition, the timely reconciliation of full-time and part-time employee user accounts to currently authorized users will strengthen security controls and help prevent unauthorized access to sensitive information.

2. Prior Audit Results Resolved

a. Chapter 647 Reporting Requirements

Our prior audit disclosed that MCC did not report to the Office of the State Auditor (OSA) the thefts of two laptop computers which MCC had estimated were valued at approximately $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 current audit determined that the MCC was aware of the reporting requirements and has implemented policies and procedures to report all missing and stolen equipment to the Office of the State Auditor in accordance with Chapter 647. We found that MCC had reported the thefts of five items of computer equipment from January 2007 to April 2009 totaling $4,900 to the OSA as required by Chapter 647. According to MCC management, these were the only thefts of IT equipment during our audit period.

b. Disaster Recovery and Business Continuity Planning

Our prior audit revealed that MCC 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. The audit had revealed that system user departments had not developed user area contingency plans to address a potential loss of their automated processing. The audit had also found that management had not assessed the relative criticality of MCC's automated systems and had not conducted a risk analysis to determine the extent of potential risks and exposures to IT operations.

Our current audit determined that the MCC has performed a criticality assessment of the automated systems and has developed a formal disaster recovery and business continuity plan for restoring mission-critical systems in a timely manner should a disaster render the automated systems inaccessible or inoperable. Our audit also confirmed that user area plans had been developed to support business continuity planning. Our audit evidence revealed that MCC has reciprocal agreements in place and in effect with three community colleges and two four-year state colleges to assist in providing alternative processing capabilities and to assist in recovery efforts.