The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH

ONE ASHBURTON PLACE, ROOM 1819

BOSTON, MASSACHUSETTS 02108

TEL. (617) 727-6200

A. JOSEPH DeNUCCI

AUDITOR

No. 2006-0196-4T

OFFICE OF THE STATE AUDITOR'S
REPORT ON INFORMATION TECHNOLOGY CONTROLS
AT MASSACHUSETTS BAY COMMUNITY COLLEGE

July 1, 2004 through March 22, 2006

OFFICIAL AUDIT REPORT

SEPTEMBER 14, 2006

2006-0196-4T

TABLE OF CONTENTS

INTRODUCTION

Massachusetts Bay Community College (MassBay), which was established in 1963, is a Massachusetts institution of higher education offering associate degree and certificate programs. MassBay also offers continuing education programs on a full-time and part-time basis. Chapter 15A, Section 5, of the Massachusetts General Laws created the Massachusetts State College System, of which Massachusetts Bay Community College is a member.

Massachusetts Bay Community College's mission is to provide a student-centered learning environment in which a diverse student body explores, develops, and achieves educational goals; to serve many of the economic and cultural needs for the citizens of the Metro-West and greater Boston regions of the Commonwealth; and advance business, education, public service, and health care by emphasizing technology and health care programs and offering strong transfer programs in the liberal arts and business. The College's main campus is an 84-acre facility located on Oakland Street in Wellesley Hills, with an additional campus located on Flagg Drive in Framingham and a satellite facility on Eliot Street in Ashland.

At the time of our audit, MassBay had a combined student population of 5,700 full-time and part-time students and the College employed 653 full-time and part-time faculty, administrators, and staff members. The College was supported by a fiscal year 2005 budget of approximately $32 million.

Massachusetts Bay Community College's administrative and academic mission and operations are supported by information technology services provided by the College's Office of Information Technology (OIT). According to the College, the OIT provides a stable technology infrastructure for electronic communications, delivery of student services and course content, and the gathering of information to report on the College's operations. The OIT is comprised of four groups: Administrative Application Services, Desktop/Client Services, Academic Technology Services, and Telephone/Network Services. At the time of our audit, the OIT was comprised of 14 full-time staff members, with each of the four groups having a manager under the direct control of a Chief Information Officer, who reports directly to the College's President. The OIT provides assistance and guidance to administrative staff, faculty, librarians, and students regarding the use of IT resources including the use of administrative computer-systems, Internet support, computer maintenance, web hosting services, print servers, and e-mail.

The Office of Information Technology also supports a campus-wide network and client infrastructure (MassBay network), consisting of 43 servers that are configured on a Windows 2000 local area network (LAN) for use throughout the College, including the 18 computer labs and classrooms.

Upgrades to the College's network infrastructure within the past year now allow users more bandwidth and wireless network connectivity in selected areas within the campus. According to the College, they have more than 1,000 workstations, including 42 notebook computers.

From an administrative perspective, IT-related systems are used to process the College's financial management, administrative, and student information activities. In this area, the primary application is the Peoplesoft system. This system functions as MassBay's database and application server for administrative systems, including admissions, student and administrative financial accounting, and enrollment. The Financial Aid Department uses the federally-supplied software, EdExpress, which processes financial aid-related information internally. Then, using a dedicated dial-in modem, the Financial Aid Department uploads this data to the federal Department of Education. The College also has access to the state Human Resources Compensation Management System (HR/CMS) and the Massachusetts Management Accounting and Reporting System (MMARS).

The Office of the State Auditor's examination focused on an evaluation of selected IT-related general controls over MassBay's IT environment.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

In accordance with Chapter 11, Section 12, of the Massachusetts General Laws, we performed an information technology (IT) general controls examination of IT-related activities at the Massachusetts Bay Community College (MassBay) for the period of July 1, 2004 through March 22, 2006. The audit was conducted from October 31, 2005 through March 22, 2006. Our audit scope included an examination of IT-related controls pertaining to organization and management, physical security, environmental protection, system access security, inventory control over IT equipment, disaster recovery and business continuity planning, on-site and off-site storage of backup copies of magnetic media, and IT-related contract management.

Audit Objectives

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

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

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

With regard to inventory control over IT equipment, including notebook computers, we sought to determine whether control practices regarding the accounting for computer equipment were adequate, including whether an annual physical inventory and reconciliation was conducted and whether inventory controls met Chapter 647 Reporting Requirements.

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

Regarding IT-related contract management, we sought to determine whether contractual relationships with third-party, IT-related service providers were covered by written contracts, whether the contract agreements sufficiently detailed services or deliverables to be provided, and whether the contracts were properly signed and dated. We sought to determine whether third-party contracts contained standard terms and conditions as promulgated by the Operational Services Division and whether incorporated vendors were properly registered with the Office of the Secretary of State. In addition, we evaluated whether the College had implemented adequate controls with regard to IT contract management to provide reasonable assurance that IT contracts executed were being properly initiated and sufficiently documented to conform to relevant state laws and regulations.

Audit Methodology

To determine our audit scope and objectives, we first obtained an understanding of MassBay’s mission, organizational structure, and primary business functions. We conducted pre-audit work, which included obtaining and recording an understanding of relevant operations, performing a preliminary review and evaluation of IT-related internal controls, and interviewing senior management to discuss the College’s control environment. We documented the significant functions and activities supported by the automated systems and reviewed automated functions related to operations designated as mission-critical or essential. We performed a preliminary walkthrough of the data center and selected administrative offices within the College’s main campus. We performed a high-level risk analysis of selected IT functions in order to identify vulnerabilities and select areas to be reviewed.

Regarding our review of IT organization and management, we interviewed senior management, completed questionnaires, and analyzed and reviewed the organizational structure and reporting lines of the College's Office of Information Technology (OIT). We obtained, reviewed, and analyzed relevant IT-related policies and procedures, strategic and tactical plans, and reviewed steering committee meeting minutes to determine their adequacy. To determine whether MassBay's job descriptions and job specifications for IT staff were updated and reflected current responsibilities, we obtained a current employee list and job descriptions of the personnel employed by the OIT. We then compared the personnel list to the OIT's organizational chart, and each employee's job descriptions to their day-to-day IT-related responsibilities.

To evaluate physical security, we determined whether procedures were in place and in effect to help prevent unauthorized persons from gaining access to computer facilities and selected areas housing IT resources, and whether authorized personnel were specifically instructed in physical security policies and procedures. Our review of physical security of IT computer equipment included the completion of a risk analysis questionnaire and interviews with responsible parties, including the College's senior management and the MassBay Department of Public Safety, referred to as Campus Police. We assessed the College's physical security program and determined the extent to which physical access was restricted for areas housing computer equipment by conducting a walkthrough of the data center, classroom labs, business offices, on-site storage areas, and selected telecommunication closets. We examined the existence of controls, such as motion detectors and intrusion alarms. Regarding key management at the College, we interviewed the individual responsible for maintaining records of administrators, faculty and staff who were issued brass key sets for the administrative offices within the College. Further, we obtained a listing of current brass keyholders and compared it to a MassBay employment listing to verify that all identified keyholders were current employees of the College.

To determine whether adequate environmental controls were in place to properly safeguard automated systems in the data center and areas housing workstations from loss or damage, we conducted walkthroughs and checked for the presence of smoke and fire detectors, fire alarms, fire suppression systems (e.g., sprinklers and fire extinguishers), an uninterruptible power supply (UPS), and emergency lighting. To determine whether proper temperature and humidity controls were in place, we reviewed the presence of appropriate air conditioning units in the data center. In addition, we reviewed environmental protection related to general housekeeping procedures in the data center, selected areas housing workstations, computer labs, and telecommunication closets.

With respect to system access security, our audit included a review of access privileges of those employees authorized to access the network and associated workstations. To determine whether the

College's control practices regarding system access security adequately prevented unauthorized access to automated systems, we initially sought to obtain policies and procedures regarding system access and data security. We reviewed security practices with the Chief Information Technology Officer and the security administrator and evaluated selected access controls to the network and the PeopleSoft application. We determined whether MassBay's internal control documentation included control practices, such an acceptable use policy for IT resources and a formal security statement.

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. We reviewed the security procedures with the security administrator responsible for access to the automated systems on which the College's application systems operate. In addition, we reviewed control practices used to assign MassBay staff access to the application programs and data files. To determine whether adequate controls were in place to ensure that access privileges to the automated systems were granted only to authorized users, we reviewed and evaluated procedures for authorizing, activating, and deactivating access to application software and related data files. To determine whether all users with active privileges were current employees, we first obtained the list of individuals granted access privileges to e-mail accounts and other business-related applications, such as PeopleSoft. We then compared all the users with active access privileges, as of November 14, 2005, to the personnel roster of current employees, including faculty, administrative staff, and third party providers. We determined whether all persons authorized to access the automated systems were required to change their passwords periodically and, if so, the frequency of the changes.

To determine whether adequate controls were in place and in effect to properly account for MassBay's computer equipment, we reviewed inventory control policies and procedures and requested and obtained the College's inventory system of record for computer equipment. We reviewed the College's most current system of record, provided during the course of our audit, to determine whether it contained appropriate data fields to identify, describe, and indicate the value, location, and condition of the IT-related fixed assets. We also performed a data analysis on the inventory and made note of any distribution characteristics, duplicate records, unusual data elements, and missing values. To determine whether the most recent system of record for computer equipment was current, accurate, and valid, we used Audit Command Language (ACL) to select a statistical sample of 85 items, as well as all known 42 notebook computers, out of a total population of 1,893 items in order to achieve a 95% confidence level. We traced the inventory tags and serial numbers of the hardware items listed on the inventory record to the actual equipment on hand.

To verify the relevance and completeness of MassBay's system of record for IT-related equipment, we randomly selected 55 additional computer hardware items in adjacent locations and determined whether they were properly recorded on MassBay's inventory record. To determine whether selected computer hardware purchases in fiscal years 2005 and 2006 were accurately listed, we randomly selected 99 items, valued at $55,763 and verified whether the amounts recorded on MassBay's purchase orders and invoices were accurately recorded on the inventory system of record. To determine whether MassBay had appropriate control practices in place and in effect to account for and safeguard notebook computers we interviewed OIT representatives, reviewed the control form used by each area regarding their computer equipment loan policies for employees, and reviewed MassBay's documented policies and procedures to control the assignment and use of notebook computers.

To determine whether the College complied with Commonwealth of Massachusetts regulations for fixed-asset accounting, we reviewed evidence supporting MassBay's performance of an annual physical inventory of IT assets. Further, to determine whether MassBay complied with Commonwealth of Massachusetts regulations for disposal of surplus property, we reviewed records and supporting documentation for IT-related equipment disposed of during the audit period, as well as IT-related equipment that the College planned to request Commonwealth approval to dispose of as surplus. Finally, to determine whether MassBay was in compliance with Chapter 647 of the Acts of 1989 reporting requirements, we determined whether incident reports for missing or stolen IT-related equipment for the audit period existed, and verified whether all incidents were reported to the Office of the State Auditor.

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

As part of our review of business continuity planning, we assessed the adequacy of generation and storage of backup copies of magnetic media. We assessed the adequacy of physical security and environmental protection controls for on-site storage of magnetic media. We interviewed the Senior Systems Administrator responsible for the automated online full backup of various MassBay servers connected to the Windows 2000 network, and we reviewed the current backup procedures in place for their adequacy and completeness. The review of the backup operation included the mission-critical

PeopleSoft application. We also inspected the on-site daily backup copies of computer media to determine the provisions for storage, the frequency of backup, and the adequacy of controls in place to protect backup media. We interviewed personnel responsible for generating and storing backup copies of electronic media to determine whether they had been formally trained in their duties, including securing and protecting media, and were aware of procedures for on-site and off-site media storage. We further sought to determine whether Office of Information Technology personnel were aware of, and trained in, all procedures required to restore systems via backup media that would be required under disaster or emergency circumstances. Also, we examined the on-site storage facility that was located in another building within the campus to determine whether the area had adequate physical security and environmental controls. We reviewed the condition of the fireproof safe being used to store on-site backup media to determine whether it would help ensure that backup media would remain machine-readable for a limited period of time. In addition, we evaluated the process for the generation of off-site backup of magnetic media, but did not review the off-site storage location.

The review of IT-related contracts with third-party service providers was accomplished by analyzing the policies and procedures used to help ensure that contracts were initiated and processed in compliance with state regulations. For the period of July 1, 2004 through March 1, 2006, we reviewed five IT vendor service contracts for fiscal year 2005 and four IT vendor service contracts for fiscal year 2006. The Commonwealth's Secretary of State's Office was consulted to determine whether the incorporated vendors selected were properly registered with the Commonwealth. Regarding contract documentation, we reviewed selected contracts to ascertain that the contracts contained the original signature pages with corresponding proper signatures to ensure compliance with applicable state laws and regulations. We evaluated contract documentation provided to us by the College to determine whether contract provisions were sufficient to hold the third-party service providers accountable for delivering quality services and whether payments were made properly. Further, start dates for work under contract were verified according to dates of contract signature and compliance with contract terms.

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 Massachusetts Bay Community College (MassBay), we found that internal controls in place provided reasonable assurance that IT-related control objectives would be met with respect to IT organization and management, physical security, environmental protection, system access security, on-site and off-site storage of backup copies of magnetic media, and third-party provider information technology (IT) service contracts. However, our audit revealed that controls needed to be implemented and monitored to provide reasonable assurance that MassBay's IT environment would include controls to properly record, account for, and reconcile computer equipment to a formal system of record. In addition, the College needed to develop and implement a disaster recovery and business continuity plan to ensure system availability when required.

Our review of IT management and control indicated that management was aware of the need for internal controls, had an appropriate and defined organizational structure for the Office of Information Technology (OIT), clear reporting lines and points of accountability, appropriate span of control and oversight, and documented job descriptions for IT staff. The College also had documented IT strategic and tactical plans that address the College's IT environment with regard to infrastructure, active directory domain health, imaging and software updates/management, hardware, backup/disaster recovery, communication, and issues related to the PeopleSoft application. The College also had a steering committee, for which minutes were maintained, that assisted in overall long and short term IT initiatives and direction. With respect to the use and the safeguarding of information technology, we determined that formal policies and procedures were in existence, but needed to be updated to more accurately reflect the current IT environment for physical security and system access security. In addition, the College needs to implement and develop policies and procedures for inventory control over computer equipment and business continuity planning. Having appropriate and well-documented policies and procedures reduces the risk that desired control practices would not be adequately communicated, administered, or enforced.

We determined that adequate physical security controls were in place and in effect within MassBay's buildings that house the data center, computer labs, and selected telecommunication closets. Our examination also disclosed that these areas have restricted key access to only approved individuals. We reviewed the College's management of keys and found that all identified holders of brass keys were current employees of the College. In addition, visitors are escorted when accessing the data center to minimize the risk of damage and/or theft of computer equipment. Our review of selected areas housing workstations disclosed that on-site Campus Police make periodic rounds nightly to verify that all office doors are locked and that all campus buildings are secure. However, documentation of stated control practices with respect to policies and procedures for physical security needed to be enhanced to more accurately reflect the current IT environment for physical security.

We found that adequate environmental protection, such as fire prevention and detection controls, smoke and fire detectors, fire extinguishers, and fire alarms were in place throughout the MassBay campus. In addition, we found that an uninterruptible power supply was in place for the data center, computer labs, and selected telecommunication closets housing IT resources to help prevent damage to, or loss, of computer equipment. Our audit disclosed that the data center was neat and clean, general housekeeping procedures were adequate, and temperature levels within the room were appropriate. However, we determined that the data center did not have in place an automated fire suppression system, such as a wet or dry sprinkler system and humidity detection equipment.

With respect to logon ID and password administration, we determined that adequate controls were in place to provide reasonable assurance that the College had granted access privileges and activated user access to authorized persons. Appropriate procedures were in place regarding authorization to access network resources and activation/deactivation of access privileges. Policies and procedures regarding network security and IT security management had been issued. Access levels were assigned to staff by the employee’s manager based upon job duties. Staff were required to sign a formal security statement regarding password protection and confidentiality. According to IT management, security logs, including access logs, were periodically reviewed by the security administrator. Our tests revealed that all PeopleSoft and network users were current employees. However, we found that policies and procedures needed to be strengthened regarding the frequency of required password changes. We determined that MassBay management did not require a mandatory timeframe for changing passwords. We recommend that passwords for all systems be changed at least every sixty days and that access security controls be monitored for compliance.

Our audit revealed that MassBay could not provide reasonable assurance that the inventory system of record for computer equipment could be relied upon, since the system of record lacked adequate integrity. In addition, an annual physical inventory and reconciliation was not being performed to assist in verifying the accuracy and completeness of the inventory record. We determined that 90 of the 99 IT purchases made during fiscal years 2005 and 2006 were not included in the inventory system of record and could not be found by the College. Our data analysis of the entire population of 1,893 IT hardware items indicated that there were missing fields of information with respect to historical cost and acquisition date. Since historical cost was not maintained for the computer equipment, the inventory system of record could not be used by the College to provide the value of IT resources under their charge.

Our inventory test of 85 items selected from the College's system of record indicated that 25 pieces of computer equipment were not recorded on the inventory record. In addition, a test of 55 hardware items that were traced from multiple physical locations back to the inventory listing indicated that 22 pieces of computer equipment were not recorded on the inventory record. Furthermore, an inventory test of 42 notebook computers indicated that 18 notebook computers could not be located. The College indicated that the 18 notebook computers had been stolen. We found that MassBay did not adequately maintain its records for computer equipment loaned to administrators and faculty.

Regarding surplus property and equipment, our audit revealed that MassBay was aware of and in compliance with Operational Services Division's policy and procedures. Although MassBay's Internal Control Manual included control and reporting requirements set forth in Chapter 647 of the Acts of 1989, our audit revealed that the College did not comply with the requirements of Chapter 647 of the Acts of 1989 since MassBay had failed to notify the Office of the State Auditor of approximately $24,750 of stolen computer equipment.

Although we determined that procedures regarding the generation of back-up copies of magnetic media for on-site back-up media and the storage of the back-up media at a secure on-site location was adequate, our review indicated that the level of disaster recovery and business continuity planning needed to be strengthened. Our audit disclosed that the College did not have a comprehensive disaster recovery and business continuity plan to provide reasonable assurance that mission-critical and essential data processing operations for administrative and academic functions could be regained effectively and in a timely manner should a disaster render automated systems inoperable. We also found that although a potential alternate processing site had been selected, user area plans had not been established to document the procedures required to regain business operations in the event of a disaster.

Regarding IT-related contracts with third-party vendors, we found that the College exercised adequate management oversight to hold contracted parties sufficiently accountable for their performance and delivery of services. We found that IT-related contracts with third-party service providers were initiated and processed in compliance with state regulations pertaining to contract authorization and vendor corporate registration. Regarding contract documentation for our selected test sample of five Fiscal Year 2005 and four Fiscal Year 2006 IT vendor service contracts, we found all original signature pages contained only authorized signatures as well as compliance with all applicable state laws and regulations. In addition, our audit disclosed that all of the vendors that we tested for corporate registration were registered with the Office of the Secretary of State to conduct business within the Commonwealth, as required by Massachusetts General Laws (MGL), Chapter 181, Section 4, which requires the registration of foreign corporations within ten days of commencing business within the Commonwealth. Although we found the College to have adequate information regarding IT contract deliverables and milestones, the College should have vendors more specifically identify deliverables and clearly specify milestones and contract completion timelines.

AUDIT RESULTS

1. Inventory Control over Computer Equipment

Our audit disclosed that as a result of weak or nonexistent inventory control practices over IT resources, MassBay did not properly account for computer equipment in the College's inventory system of record for property and equipment. We determined that adequate controls were not in effect to ensure that a current, accurate, and complete perpetual inventory record of computer equipment was being maintained. We found that controls needed to be strengthened to provide prompt notification and update of the inventory record when equipment is acquired, relocated, disposed of, lost, or stolen. In addition, inventory records did not appear to be adequately reviewed for accuracy and completeness, and an appropriate level of reconciliation was not being performed. As a result, the integrity of the inventory system of record for computer equipment could not be adequately assured. The absence of a sufficiently reliable inventory of computer equipment hinders the College's ability to properly account for IT resources, evaluate the allocation of equipment, identify missing equipment, and support IT configuration management objectives.

Although we determined that the College had documented internal controls regarding the purchasing of IT resources, we found that documented policies and procedures needed to be implemented or enhanced regarding the maintenance, compliance monitoring, and reconciliation of the inventory system of record for IT resources. We also found that the College had not performed annual physical inventory and reconciliation of the inventory system of record. In addition, there were inadequate controls on the recorded allocation of notebook computers for faculty and staff, and not all computer equipment on hand was properly recorded on the inventory. We found that a significant portion of a sample of computer equipment drawn from the inventory record could not be found.

Our inventory tests of the College's system of record provided to us during the course of our audit, which included 1,893 IT-related assets, disclosed that controls over the recording of, and accounting for, IT-related equipment needed to be strengthened. Our analysis of MassBay's inventory system of record indicated that although most of the appropriate data fields, such as description, identification tag, user name, serial number, and location, were present, the listing lacked data fields for historical cost and acquisition date. Recording historical cost and acquisition date in inventory systems of record is required by Commonwealth of Massachusetts regulations for all departments to provide a comprehensive, auditable inventory record of fixed assets. By failing to record the historical cost of purchased computer hardware items and their purchase dates on MassBay's inventory system of record, MassBay was also not in compliance with the Office of the State Comptroller's 2005 fiscal year fixed-asset requirements and

Office of the State Comptroller (OSC) Memorandum No. 313A. In addition, inventory valuation for computer equipment could not be analyzed and evaluated.

With respect to the recording of IT-related assets acquired by the College, we found that MassBay lacked appropriate and adequate senior management oversight to ensure that the recording of all necessary identifying data for received computer equipment would be entered into the inventory system of record free of errors or omissions. Adequate controls were not in place to prevent or detect data entry errors or omissions. Our tests indicated a significant error rate and inconsistency in identifying data recorded by staff on MassBay’s computer hardware inventory listing. Specifically, our audit tests were performed on 99 computer hardware purchases consisting of 81 computer processing units, five monitors, four servers, four printers, three uninterruptible power supply, and two notebook computers valued at $55,763 selected from fiscal year 2005 and 2006 invoices. Our audit revealed that 90 of these items, an error rate of 91%, were not included in the College’s system of record. Because of the rate of data input errors, failure to record asset costs and acquisition dates, and inadequate management of the system of record, an acceptable level of data integrity did not exist for MassBay’s inventory system of record for IT equipment at the time of our audit. MassBay needs to ensure that appropriate controls are in place and in effect for data entry and improve its monitoring and validating of information contained in the system of record to ensure the accuracy and completeness of the information contained in the inventory database.

Based on a statistical sample of 85 pieces of computer equipment selected from the inventory record, we verified by inspection the existence and the recorded location of the computer equipment as listed on the College’s inventory record. We found that 25, or 29%, of the 85 items that were selected from the system of record, were not at the locations indicated on the inventory record and could not be found by the College. Of the 60 items from the 85 items that were selected from the system of record, all were properly tagged, and the inventory system of record correctly listed tag and serial numbers, and manufacturer. Furthermore, to verify the integrity and completeness of the inventory system for computer equipment, we selected 55 additional pieces of computer equipment and determined whether the equipment was properly recorded on the College’s inventory system of record. We found that of the 55 items selected, 22, or 40% of the selected items, were not recorded on the inventory record. MassBay’s lack of a complete hardware inventory listing hinders the College's ability to properly account for available hardware systems and undermines its ability to detect missing or stolen equipment.

Our audit further indicated that MassBay’s monitoring of computer equipment needed to be strengthened. Specifically, the College could also not provide verification records supporting any annual physical inventory or a reconciliation of computer equipment to MassBay’s inventory system of record for at least four years. The absence of documented policies and procedures regarding inventory verification hindered MassBay's ability to ensure the integrity of its inventory system of record as it pertained to computer equipment.

Our examination of one occurrence of computer equipment that had been designated as surplus property and disposed of indicated that the College had complied with the Commonwealth of Massachusetts regulations for the disposal of surplus equipment. Adequate documentation was in place to support the disposal of equipment as indicated in the initial request to obtain approval from the State Surplus Property Officer. However, our audit revealed that the College had not complied with Chapter 647 of the Acts of 1989 by failing to submit reports to the Office of the State Auditor of lost or stolen equipment. (Please refer to audit finding #2)

A primary contributory factor to the control weaknesses in inventory control and the accounting of IT resources area was the result of no clear assignment of responsibility for the maintenance, monitoring, and reconciliation of the inventory system of record. Senior management did not appear to rate inventory control as a high enough priority nor adequately identify inventory control as an administrative management function, as evidenced by the repetitive nature of this issue in prior audit reports.

Recommendation:

We recommend that senior management promptly develop and then implement internal control policies, procedures, and practices regarding inventory control of IT resources in the areas of recording and inventory verification to help ensure that the College properly accounts for its computer equipment. The College should implement appropriate assurance methods, such as independent verification, physical inspection, reconciliation and oversight, to ensure that inventory controls are in place and in effect. We recommend that procedures be established to ensure that the inventory record for IT resources is maintained on a perpetual basis allowing management to use the inventory for accounting and IT configuration management purposes.

We recommend that the MassBay adapt its current control guidelines to comply with the Office of the State Comptroller's "Internal Control Guide for Departments" regarding asset management. We also recommend that the College benchmark its policies and procedures to generally accepted control practices for IT configuration management. Once senior management has approved the policies and procedures, the policies and procedures should be distributed and instructed to the appropriate staff.

We recommend that inventory control policies and procedures linked to the receiving function be enhanced by increasing the level of required supervision and oversight to help ensure that all items of computer equipment received are properly recorded on the College's inventory list in a timely manner and adequately safeguarded. The College should enter all IT-related equipment on the inventory system of record when received, taking into account any necessary acceptable procedures. We recommend that a member of the OIT staff assist in the verification of equipment deliveries and the subsequent tagging of equipment.

With respect to IT configuration management, we recommend that the data fields in the IT inventory be expanded to include the condition and status of the computer equipment. In addition, data fields may include information related to hardware or software maintenance. We recommend that all material IT resources be included on the inventory to support IT configuration management objectives.

The College should implement these control procedures to help ensure that all IT-related equipment is recorded on the inventory record in a complete, timely, and accurate manner so that the College can generate a complete record of all IT-related equipment on a perpetual basis. The College's inventory records should reflect any changes to computer hardware items, including location or status, for both deployed equipment and items held in storage.

With respect to the recording of IT-related equipment, we recommend that the College should develop procedures for independently validating the information recorded on the inventory system of record for newly-received computer equipment. In addition, the College should perform an annual physical inventory and reconciliation of the inventory system of record. The perpetual inventory record of IT resources, including computer equipment and software, should be periodically verified through reconciliation to computer equipment acquisition, records of lost or stolen equipment, and disposal records.

With respect to MassBay's monitoring of its IT-related equipment, the College should improve documentation supporting the annual physical inventory, including a reconciliation of the physical inventory to the College's inventory records, and documentation of acquired or disposed of items. This improved documentation will help ensure the integrity of MassBay's perpetual inventory system of record for IT-related assets, provide reasonable assurance that the College's inventory records can be effectively used to support IT configuration management, and help safeguard computer equipment. To maintain proper internal control, the staff who perform the periodic reconciliation should not be responsible for maintaining the College's system of record for fixed-assets. We also recommend that the College consider migrating its inventory data to a fixed-assets module within the PeopleSoft application that can be integrated with the College's automated accounting information system.

Auditee's Response

> *The College agrees with these recommendations and will implement internal control policies, procedures and practices regarding inventory control of all material IT assets. Once these have been implemented the College's Internal Control Manual will be updated to comply with the Office of the State Comptroller.*

Auditor's Reply:

We are pleased that the College has agreed to take appropriate corrective action. A comprehensive inventory control system requires a detailed process that encompasses receiving, managing, accounting and disposing of IT resources. We are pleased that the College is taking steps to strengthen the integrity of the fixed-asset inventory record. We believe a comprehensive inventory control system for all fixed assets, including IT resources, is an important ingredient for your overall internal control structure. Strengthening inventory control procedures will improve the integrity of the inventory system of record and enhance knowledge of the IT infrastructure management capabilities.

2. Noncompliance with Chapter 647 Reporting Requirements

Our audit disclosed that Massachusetts Bay Community College did not report to the Office of the State Auditor (OSA) the theft of 18 notebook computers valued at $24,750, as required by Chapter 647 of the Acts of 1989. 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. The College did not report the following incidents to the OSA:

Item/Description	**Historical Cost**	**Type of Incident**
12 Gateway Notebook Computers	12 @ $1,500 totaling $18,000	Theft
3 IBM Notebook Computers	3 @ $850 totaling $2,550	Theft
1 Toshiba Notebook Computer	$1,500	Theft
1 Compaq Notebook Computer	$1,300	Theft
1 Dell Notebook Computer	$1,400	Theft
18 Notebook Computers	**Approximate Total: $24,750**	

According to the College, the thefts of the 18 notebook computers probably occurred between fiscal years 2002 and 2005. The primary contributing factor leading to the thefts was that the College had not developed a comprehensive inventory control system for computer equipment and had not developed formal policies and procedures regarding the distribution and return of notebook computers from faculty and administrative staff. The College was not monitoring the assignment, use, and return of notebook computers and had not implemented a process to periodically monitor the status and the need for the notebook computers distributed to personnel.

Chapter 647 of the Acts of 1989 requires that access to resources be limited to authorized individuals and that the restrictions on access to resources depend on the vulnerability of the resources and the perceived risks. Since the College did not have a clear record of assigned notebook computers, there is a risk and significant vulnerability of the loss of confidential or sensitive information contained in the hard drives of the missing computers as well as the value of the equipment. Information such as social security numbers and health information of students, student grade information, and College business information, such as tuition payment information, may all be vulnerable.

MassBay's Internal Control Plan does document the Chapter 647 reporting requirements to the Office of the State Auditor (OSA) for unaccounted for variances, losses, and shortages or thefts of funds or property. Although we were able to locate completed 647 reports outlining other incidents of thefts within MassBay, the College did not comply thoroughly with the requirements as these specific incidents of theft should have been reported immediately and investigated by the OSA as prescribed by law, to ensure full and proper disclosure, resolution, and corrective action to help preclude their recurrence.

Sound management practices advocate that a comprehensive inventory control system be implemented, maintained and properly monitored. Specific control policies and practices should be formulated regarding the distribution and return of notebook computers from individuals to ensure the appropriate safeguarding and use of these potentially vulnerable assets. Control procedures should include written instructions regarding distribution and return of equipment, sign-out and sign-in forms, supervisory approvals, signed user agreements, and periodic monitoring of the status of assigned computers.

The absence of consistent policies and procedures, a comprehensive process and formal set of documented sign-out and sign-in forms, and a schedule for the periodic monitoring of notebook computers hindered designated managers responsible for safeguarding computers and monitoring their use. Management did not make staff, to whom notebooks had been assigned, aware of their responsibilities regarding appropriate safeguarding and use of the equipment. Further, due to the lack of appropriate recordkeeping procedures, notebook computers were placed at increased risk of theft.

Recommendation:

The MassBay should formulate, maintain and monitor a comprehensive inventory control system 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. In addition, the College should document a formal process for the assignment and return of notebook computers. Users should be required to formally sign-out and sign-in each notebook computer and record the actual date of transfer of responsibility. The College's designated fixed-asset manager for IT resources should periodically review the status of notebook computers, especially those that have been signed out. In addition, given that MassBay has notebook computers signed out to employees to assist them in their work, we recommend that, on at least a quarterly basis, MassBay perform a file comparison of the list of individuals to whom computer equipment has been assigned to the master list of current College employees. This would serve as a detective control to identify any instances when IT-related resources have not been returned to MassBay upon employee termination, transfer or leave of absence. Further, once the IT resource has been transferred to another party, MassBay should require that the transfer be formalized by the completion of a new sign-out form.

Auditee's Response

> *The College agrees with these recommendations. The implementation of a comprehensive inventory control system will comply with Chapter 647 of the Acts of 1989, so that all instances of unaccounted for variances, losses and thefts of funds or property are reported to the Office of the State Auditor. The 647 report for these specific items has been reported to the State Auditors Office. To date three of the eighteen notebooks have been located and the College is committed to locating the remaining fifteen.*
>
> *It should be noted that all loaned notebook computers contain only standard issue Microsoft Office and web browser software. These notebooks would not contain sensitive information or passwords, which would enable an unauthorized user to access such information.*

Auditor's Reply:

We commend the College for initiating corrective action in a timely manner. We are pleased that the College is taking steps to strengthen the integrity of the fixed-asset inventory record and to include the requirements set forth in Chapter 647 of the Acts of 1989 in its inventory control system. We believe control over laptop computers at the college was weak and may have lead to the missing equipment. Since the College has not managed these resources adequately, we feel the potential for information breaches through lost or stolen laptops remains a possibility, and therefore controlling these assets is critical. Given that notebook computers are more likely to be stolen than desktops, the College should develop a process to ensure that confidential or sensitive data stored on assigned notebooks is encrypted and that restricts users from storing sensitive or confidential information on notebooks.

3. Disaster Recovery and Business Continuity Planning

We found that the College had not formulated a comprehensive business continuity planning strategy to address business operations. In addition, although the College had on-site and off-site storage of backup copies of media available for recovery, the College had not formalized their agreement with an alternate processing site to use to regain processing should the data center be damaged or inaccessible for an extended period of time and the College had not developed a disaster recovery plan. Furthermore, 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. The risk analysis, once developed, should identify the relevant threats that could significantly degrade or render the systems inoperable, the cost of recovering the systems, and the likelihood of the threat and frequency of occurrence for each disaster scenario. Additionally, the tasks and responsibilities necessary to carry out the completion of the College's duties and business objectives under various disaster scenarios for all relevant College personnel had not been documented. As a result of the weaknesses noted, if a disaster were to occur, the automated systems, including the PeopleSoft application that is supported by the OIT, could not be restored within an acceptable period of time, thereby jeopardizing essential College operations.

Without a comprehensive, formal, and tested recovery and contingency plan, the College's ability to regain critical processing capabilities and access information related to its various application systems would be impeded. Given the absence of recovery plans, a significant disaster impacting the College's automated systems would seriously affect the College's ability to regain mission-critical and essential data processing operations. Business continuity and contingency planning has assumed added importance given the potential processing disruptions that could be caused by natural disasters or man-made events. Further, the College had not implemented or tested a formal business continuity plan for a timely post-disaster restoration of mission-critical important business functions processed through the local area network servers, or the applications residing on the workstations.

The objective of business continuity planning is to help ensure the continuation of mission-critical and essential functions enabled by technology should a disaster cause significant disruption to computer operations. Generally accepted practices and industry standards for computer operations support the need to have an ongoing business continuity planning process that assesses the relative criticality of information systems and develops appropriate contingency and recovery plans, if required.

An effective disaster recovery plan should provide specific instructions for various courses of action to address different types of disaster scenarios. The plan should identify the ways in which essential services would be provided without full use of the data processing facility or network communications and, accordingly, the manner and order in which processing resources would be restored or replaced. The plan should identify the policies and procedures to be followed, detailing the logical order for restoring critical data processing functions, either at the original site or at an alternate processing site. In addition, the plan should describe the tasks and responsibilities necessary to transfer and safeguard backup copies of data files, program software, and system documentation from off-site storage to the site being used for restoration efforts.

Recommendation:

The College should assess the criticality of automated systems to identify application priorities and critical resources. An analysis should be conducted to identify risks and exposures relating to the College's data processing operations and workstation environment. The College should identify potential processing alternatives and resources to be utilized should a disaster disrupt its data processing or business operations. Based upon these results and input solicited from management and user departments, a documented disaster recovery and business continuity plan should be developed, reviewed, tested to the extent possible, approved by senior management, and implemented.

Senior management should ensure that a written business continuity and contingency plan is developed containing, at a minimum, guidelines on how to use the continuity plan consisting of emergency procedures to ensure the safety of all affected staff members; response procedures meant to bring the business operations back to their prior state before the incident or disaster; procedures to safeguard and reconstruct the primary site; coordination procedures with public authorities; communication procedures with stakeholders (employees, key customers, critical suppliers, and management); and critical information on continuity teams, affected staff, customers, suppliers, public authorities and media.

We further recommend that procedures should be developed to ensure that the criticality of systems is periodically reassessed; that the impact of changes in user needs, automated systems, or the IT environment is evaluated; and that staff are adequately trained in executing recovery plans. Upon a major change to systems or equipment, or at least annually, the disaster recovery plan should be reviewed, updated, and tested to ensure that it is current, accurate, complete, and remains viable. The business continuity plan, or specific sections of it, should be distributed to appropriate personnel and a complete hardcopy and electronic copy of the plan should be stored in a secure off-site location.

Auditee's Response

> *The College agrees with these recommendations. The Office of Information Technology (OIT) and the College are aware of this issue. The PeopleSoft upgrade will provide an opportunity to de-commission server hardware, which can be used to establish an alternate, backup data center on the Framingham campus. OIT will conduct a risk assessment and investigate the costs associated with establishing such as center with appropriate software, such as NeverFail, specifically designed to assure business continuity and disaster recovery for Microsoft Windows 2003 server systems. This is not anticipated to be completed until Fiscal 2008 after the aforementioned PeopleSoft upgrade.*

Auditor's Reply:

Documenting and testing comprehensive business continuity and contingency plans provide a strong basis for regaining mission-critical and essential IT and business operations within an acceptable period of time. Importantly, appropriate controls need to be exercised to also ensure the integrity and security of the system and related IT resources. Well-developed recovery strategies help diminish the time needed to recover processing and network capabilities. In addition to having a documented business continuity plan, the College should ensure that recovery strategies are formally reviewed and periodically tested to ensure their viability. Certainly, conducting a thorough risk assessment is 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.

After the plan's completion it should be reviewed and updated annually, or whenever there is a significant change to the processing requirements, risks, or changes to the College's IT infrastructure. Designation of an alternate processing site and procedures for the generation and secure storage of backup copies of magnetic media are an integral part of any recovery strategy and should be documented, maintained, and appropriately monitored.