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. 2004-0184-4T

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

July 1, 2002 through March 8, 2005

OFFICIAL AUDIT REPORT

MARCH 6, 2006

2004-0184-4T

TABLE OF CONTENTS

INTRODUCTION

Salem State College (hereinafter referred to as SSC or the College) was established in 1854 as a publicly funded institution dedicated to training teachers. Over the past century and a half, SSC has developed into a comprehensive, public college providing, through the schools of Arts and Sciences, Business and Economics, and Human Resources, undergraduate, graduate, and continuing education programs on a full and part-time basis. The College is a member of the Massachusetts State College System and is regulated by Chapter 15A, Section 5 of the Massachusetts General Laws. The College is situated on 109 acres in Salem, Massachusetts and is comprised of 34 buildings, including the Cat Cove Laboratory and the O'Keefe Athletic Center, located on the North, Central, and South Campuses.

According to SSC's Web site, the College's primary mission is "to educate the residents of northeastern Massachusetts and the Commonwealth and to use its intellectual, scientific, and technological resources to support and advance the economic and cultural life of the region." At the time of our audit, the SSC had 8,349 graduate and undergraduate students in a variety of graduate and undergraduate programs. The SSC is composed of a President, four Vice Presidents, and 1,157 faculty, administrators, and staff. Information technology (IT) positions include Chief Information Officer (CIO), Director of Management Information Services (MIS), Director of Networking Services and 29 IT staff. The College received operating revenue of approximately $37.09 million, including $19.93 million from student tuition and fees and $17.16 million from sources, such as federal, state, and local grants and contracts for the 2004 fiscal year. In addition, the College received a state appropriation of approximately $41.48 million, of which approximately $2.79 million was designated for the operations of the Information Technology Section for fiscal year 2004.

At the time of our audit, SSC's computer operations were assisted by the Information Technology Section which was responsible for the "planning, delivery, and operations for all computing, telecommunications, media, and data administration resources for the College." Further, the IT Section provided assistance and guidance to all College administrative staff, faculty, librarians, and students regarding the use of administrative computer systems, computer maintenance, Web hosting services, print servers, and e-mail. The IT Section comprises two departments: Management Information Systems (MIS) and Network Services. Management Information Systems supported the College's administrative and business operations, including logon ID and password administration, academic and administrative computing, and activities related to work-study programs and student internships. User Support Services (USS), which is a work group within MIS, is responsible for installing computer equipment, training IT staff, maintaining and updating the hardware and software inventory records, and operating the "help desk." Network Services is responsible for maintaining the College's network resources, including wiring infrastructure, telecommunications, data center operations, backup of magnetic media, network

security, e-mail services, and Internet connectivity. The directors of MIS and Network Services report to the College's CIO.

Computer operations were supported by 82 file servers and approximately 1,934 microcomputer workstations configured in a local area network (LAN). Of the 1,934 workstations, 1,508 were assigned to administrative staff and faculty and 426 were assigned to student computer laboratories and classrooms. The file servers were connected through a wide area network (WAN) to the Commonwealth's Information Technology Division (ITD) mainframe, which provides connectivity for access to the Web-based Human Resources Compensation Management System (HR/CMS) and the Massachusetts Management Accounting and Reporting System (MMARS), the Commonwealth's accounting system. In addition, SSC maintained 115 notebook computers that were distributed to 36 departments throughout the College.

The primary software used by SSC to support its business functions was PeopleSoft. PeopleSoft, implemented in 2001, is an enterprise-wide application for client/server environments which has specific suites, such as Student Administration tools used by the Registrar's, Bursar's, and Financial Aid offices. Further, PeopleSoft includes a suite of financial tools comprising the general ledger, accounts payable, accounts receivable, purchasing, and billing. As of January 2005, the College had completed an upgrade to Version 8 of PeopleSoft that encompassed Student Administration. At the close of our audit, the College was continuing to implement the upgrade of the suite of financial tools. In addition, the College performed its administrative functions using business-related applications, such as word processing.

Our Office's examination focused on selected general controls, such as physical security and environmental protection, system access security, inventory control over IT-related resources, and business continuity planning, including on-site and off-site storage of magnetic media.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

In accordance with Chapter 11, Section 12 of the Massachusetts General Laws, we performed an audit of selected information technology (IT) related controls at Salem State College (SSC) for the period July 1, 2002 through March 8, 2005. The audit was conducted from March 30, 2004 to October 28, 2004 and from February 21, 2005 to March 25, 2005. The scope of our audit included a review of the organization and management of IT operations. We examined control practices, procedures, and devices regarding physical security and environmental protection controls over and within selected administrative offices, computer laboratories, and network closets located at the College's central and north campuses and the data center housing the file servers. We reviewed and evaluated system access security to SSC's automated systems, including access to file servers and microcomputer workstations. In addition, we examined inventory control practices for computer equipment and software.

Regarding system availability, we reviewed business continuity planning for the daily administrative and financial operations processed through the automated systems. With respect to the normal business functions, we reviewed the adequacy of formal policies and procedures regarding business continuity planning, including the provisions for on-site and off-site storage of backup copies of magnetic media. In conjunction with our audit, we reviewed IT-related formal policies and procedures for the areas under review.

Audit Objectives

Our primary audit objective was to determine whether adequate controls were in place to provide reasonable assurance that IT resources would be safeguarded, properly accounted for, and available when required. We sought to determine whether appropriate security controls were in place and in effect to provide reasonable assurance that only authorized parties could access IT-related resources and that system information was sufficiently protected against unauthorized disclosure, change, or deletion. We sought to determine 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. In addition, we sought to determine whether adequate controls had been implemented to provide reasonable assurance that only authorized users were granted access to network resources, PeopleSoft, the College's primary application used to process SSC's administrative and financial activities, and other business-related office applications, and that procedures were in place to prevent and detect unauthorized access to automated systems. We determined whether sufficient environmental protection controls were in place to provide a proper IT environment and to prevent and detect damage or

loss of IT resources. Another objective was to review and evaluate control practices regarding accounting for computer equipment and software.

We sought to determine whether adequate business continuity planning had been performed and whether recovery plans were in place to restore mission-critical and essential business operations in a timely manner should the automated system be unavailable for an extended period. Further, we determined whether adequate control procedures were in place regarding on-site and off-site storage of backup copies of computer-related media.

Audit Methodology

To determine our audit scope and objectives, we initially obtained an understanding of SSC's mission and business objectives. Through pre-audit interviews with the managers and staff and reviews of the College's enabling legislation, Website and selected documents, such as the College's IT-related policies and procedures, we gained an understanding of the primary business functions and the automated systems that support them. We documented the primary functions and activities supported by the automated systems and reviewed automated functions related to operations designated as mission-critical or essential. We interviewed management to discuss internal controls regarding physical security and environmental protection over and within the data center housing the file servers, administrative offices and computer laboratories housing microcomputer workstations, network closets located throughout the three campuses, and the on-site and off-site storage areas. We performed a preliminary walk-through of the data center and selected administrative offices at the Central Campus. Further, we reviewed relevant documents, such as the business continuity plan, and performed selected preliminary audit tests.

As part of our audit work, we reviewed and evaluated the organization and management of IT operations at the College. In that regard, we reviewed relevant policies and procedures, reporting lines, and IT job descriptions. In addition, we reviewed committee notes, documented from March 2004 to October 2004, related to the modification of the PeopleSoft application. In conjunction with our audit, we determined whether written, authorized, and approved policies and procedures had been implemented for control areas under review. We determined whether the policies and procedures provided management and users sufficient standards and guidelines to describe, review, and comply with statutes, regulations, and policy directives, such as network security and generally accepted control objectives for IT operations and security.

To determine whether physical access over IT-related resources, including computer equipment, was restricted to only authorized users and that the IT resources were adequately safeguarded from loss, theft or damage, we performed audit tests at the data center, including the file server room, selected administrative offices and computer laboratories housing microcomputer workstations at the Central Campus, six (13.6%) of 44 network closets located throughout the College, and the on-site and off-site

storage areas. We reviewed physical security and environmental protection over IT-related equipment through inspection and interviews with management and staff. To determine whether adequate controls were in place and effect to prevent and detect unauthorized access to the data center and areas housing IT resources, we inspected physical access controls, such as locked entrance and exit doors, presence of a receptionist at the entrance to the IT Section offices, cameras installed at entrances to buildings, and the issuance of identification cards to staff, faculty, and students. We reviewed additional physical security control procedures, such as maintaining a list of staff authorized to access the data center and the file server room, and the card-key access and punch keypad systems used to access administrative offices and classrooms. Further, we reviewed controls over physical keys used to access the file server room, computer laboratories, administrative offices, and network closets.

To determine whether adequate environmental protection controls were in place to properly safeguard automated systems from loss or damage, we checked for the presence of smoke and fire detectors, fire alarms, fire suppression systems (e.g., sprinklers and inert-gas fire suppression systems), an uninterruptible power supply (UPS), surge protectors for automated systems, and emergency power generators and lighting in the data center, administrative offices, and computer laboratories. We reviewed general housekeeping procedures to determine whether only appropriate office supplies and equipment were placed in the file server room, network closets, or in the vicinity of computer-related equipment. To determine whether proper temperature and humidity controls were in place, we reviewed for the presence of appropriate dedicated air conditioning units in the data center and the file server room. Further, we reviewed control procedures, such as sensors placed under the floor to detect water in the file server room and to prevent water damage to automated systems and backup copies of computer-related media stored on site.

With respect to system access security, our audit included a review of access privileges of those employees authorized to access the network and associated microcomputer 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 Officer, Director of Management Information Systems, and the Director of Network Services and evaluated selected access controls to the network and the PeopleSoft application. We determined whether SSC'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 Director of MIS responsible for access to the automated systems on which the College's application systems operate. In addition, we reviewed control practices

used to assign SSC 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 obtained the list of individuals granted access privileges to e-mail accounts other business-related applications, such as PeopleSoft, and compared all users with active access privileges, as of July 28, 2004, to the personnel roster of current employees, including faculty, administrative staff, and outsourced staff. 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.

With respect to the granting of access to e-mail accounts, we obtained from the Director of Network Services a list of users with active e-mail accounts, as of July 2004, and compared the list to SSC's official personnel roster. We determined that of the 1,275 users with active e-mail accounts, 770 employees or outsourced staff were listed on the official personnel roster and 505 users were not recorded on the official roster. We then selected a judgmental sample of 76 (15%) of the 505 users with active e-mail accounts for further review. Regarding the granting of access to the PeopleSoft application, we obtained a list of users granted access to the application, as of July 2004. We selected a statistical sample of 379 (32.8%) of 1,157 users granted access to PeopleSoft and compared the list to the official personnel roster, as of July 2004. We determined whether all users with active access privileges were listed on the College's official personnel roster.

Regarding inventory control over IT-related resources, we gained an understanding of the role of the Director of User Support Services regarding accounting for computer equipment and software. To determine whether IT-related resources were being properly safeguarded and accounted for, we reviewed inventory control procedures with the Director of USS. During our audit period, we obtained the hardware inventory record, as of June 30, 2004, from the Director of USS. We determined whether computer equipment installed at selected buildings located at the College's North, South, and Central campuses was tagged with state identification numbers and whether the College's inventory records accurately reflected the tag numbers and equipment serial numbers. We reviewed the inventory record to determine whether appropriate "data fields," such as state identification number, manufacturer's model number, acquisition date, serial number, location, and cost were included for each piece of equipment listed on the record and provided sufficient information to identify and monitor IT-related pieces of equipment. Further, we determined whether appropriate information, such as version number and cost were listed on the software inventory record.

We reviewed Generally Accepted Accounting Principles (GAAP) Fixed-Asset reporting requirements for Institutions of Higher Education, required by the Office of the State Comptroller (OSC)

as of February 2004, and determined whether the College had complied with the requirements. GAAP Fixed-Assets are comprised of property and equipment, including hardware and software, with an historical cost of $49,999 or more and an economic life of one year or more.

To determine whether the hardware inventory record, as of June 30, 2004, accurately reflected computer equipment purchased during fiscal years 2003 and 2004, we initially selected 1,453 (21%) of the 6,907 pieces of equipment listed on the record. Subsequently, we selected a statistical sample of 73 (5%) of the 1,453 pieces of equipment, including file servers, microcomputer workstations, and printers purchased during fiscal years 2003 and 2004. We compared the tag numbers and serial numbers attached to the 73 pieces of computer equipment to the corresponding numbers listed on the hardware inventory record. Further, we traced serial number, equipment description, and location listed on the record to the actual equipment on hand. In addition, we confirmed a judgmental sample of 36 pieces of computer equipment installed at the Central Campus to the items listed on the record. In another test, we determined whether equipment purchased during fiscal years 2003 and 2004 was listed on the inventory record and could be located at SSC campuses. To perform this test, we confirmed purchase documentation for a judgmental sample of 48 items of computer equipment, with an estimated value of approximately $92,775, to the corresponding items listed on the inventory record and to the actual equipment on hand.

With respect to notebook computers, we initially determined the role of MIS and USS regarding the management and control of the computers. We reviewed control procedures for assigning notebook computers to SSC departments and to faculty and administrative staff. To gain an understanding of control procedures regarding the distribution to and return of the computers from College faculty, we interviewed the Director of MIS and the Director of User Support Services. We reviewed instructions regarding the process of sign-out/in for the notebooks and reviewed a sample of sign-out/in logs provided by USS. We determined whether the College periodically monitored the status of notebooks.

To assess disaster recovery and business continuity planning, we reviewed the adequacy of formal business continuity plans to resume mission-critical and essential operations in a timely manner should the file servers and the microcomputer workstations be inoperable for an extended period. We interviewed the Director of MIS to determine whether the criticality of application systems had been assessed, risks and exposures to computer operations had been evaluated, and a written business continuity plan was in place. We reviewed and evaluated the College’s business continuity plan, as of June 2004.

To determine whether controls were adequate to ensure that software and data files for business applications would be available should the automated systems be rendered inoperable, we interviewed the Director of MIS and Director of Network Services responsible for generating and storing backup copies of magnetic media. Further, we reviewed the adequacy of provisions for on-site and off-site storage of

backup copies of mission-critical and essential magnetic media at the College. To determine whether backup copies of magnetic media were safeguarded and protected from damage or loss, we reviewed the adequacy of physical security and environmental protection controls at the on-site and off-site locations. Further, we reviewed control procedures regarding logs maintained for backup copies of magnetic media transferred to and returned from the off-site storage location. We did not review Executive Office for Administration and Finance's (EOAF) Information Technology Division's (ITD) backup procedures for transactions processed through the Massachusetts Management Accounting and Reporting System (MMARS) and the Human Resources Compensation Management System (HR/CMS).

Our audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) of the United States and generally accepted computer industry control practices and auditing standards.

AUDIT CONCLUSION

Based on our audit at Salem State College, we found that adequate physical security and environmental protection controls were in place and in effect to provide reasonable assurance that automated systems were properly safeguarded and protected from damage or loss. With respect to system access security, we determined that, although important controls were in place and in effect to provide reasonable assurance that only authorized users were granted access to network resources and applications residing on automated systems, certain control practices regarding logon ID and password administration needed to be strengthened and internal control documentation needed to be enhanced. Our audit indicated that control practices over IT resources needed to be strengthened to provide reasonable assurance that IT resources were properly accounted for in College records.

Regarding availability of systems, although a business continuity plan had been developed, the College needed to address additional recovery strategies to provide reasonable assurance that normal business operations could be regained in a timely manner. We determined that adequate control practices were in place regarding on-site and off-site storage of backup copies of magnetic media for administrative and academic activities processed at the College.

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 IT Section, assigned reporting responsibilities, and documented job descriptions for IT staff. To strengthen controls regarding IT organization and management, we recommend that IT strategic planning and oversight be expanded to address the entire IT environment in addition to the issues related to the PeopleSoft application, and that internal control documentation regarding physical security, environmental protection, and management and control over IT resources be improved (see Appendix B, page 29).

Our audit revealed that adequate physical security controls were in place and in effect at the locations reviewed to provide reasonable assurance that only authorized persons have access to IT resources and that damage or loss would be prevented or detected. Responsibility for physical security, including key management, had been assigned to the College's Director of Facilities. The controls found in place included foot patrols performed by campus police 24/7 and maintenance of logs of unusual events and unauthorized attempts to enter buildings. Administrative staff, faculty, and students had been issued identification cards and were required to keep them on their persons. According to management, the buildings throughout the three campuses were locked after normal business hours and cameras were installed at the entrances to all buildings. Card-key and punch keypad access systems were installed on a significant number of offices and classroom doors throughout the College. Appropriate control practices regarding the activation and deactivation of card-keys were in place. Our audit disclosed that the data center, including the computer room, was located in a non-public area and a receptionist area was located

at the entrance to the IT Section offices. Upon our recommendation, a punch keypad lock system was installed on the door to the computer room.

To strengthen controls, we recommend that the College pursue the implementation of a card-key access system to replace many physical keys used by faculty, administrative staff, and students. Further, we recommend that to improve key management, an annual reconciliation of card-keys and physical keys be performed and that a formal schedule of periodic changes for card-key and punch-keypad access codes be developed. In addition, we recommend that SSC centralize the distribution and return of any remaining physical keys.

We found that, except for one network closet, adequate environmental protection controls were in place at the locations reviewed, including the data center at the Central Campus. We found that smoke detectors, fire alarms, and sprinkler systems were installed throughout all the buildings reviewed. We confirmed that the fire alarms had been tested on a regular basis and that IT staff had been trained during the prior two years regarding emergency procedures, specifically evacuation plans. Our audit indicated that the data center, including the computer room, was neat and clean, good housekeeping procedures were exercised, and temperature and humidity levels within the rooms were appropriate. A fire suppression system and water detectors were installed in the computer room. We found that uninterruptible power supply (UPS) devices were in place to permit a controlled shutdown and to prevent a sudden loss of data. Upon our recommendation, hand-held fire extinguishers were also installed in the computer room.

Appropriate physical security and environmental controls were in place in all but one of the six network closets reviewed. Our audit revealed that one closet, located in an attic, was accessed by an unstable wooden staircase, floorboards were weak and cracked, temperature and humidity were uncontrolled, and the attic area was littered with debris. SSC management stated that corrective action would be taken to improve environmental protection over the network closet. To ensure that appropriate physical security and environmental protection controls are in effect, we recommend that SSC periodically inspect network closets and take appropriate corrective action when necessary.

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 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 Director of Network Services.

Our audit indicated that the deactivation of access privileges to automated systems needed to be improved. We found that contrary to control procedures documented in the College's "Network Security and Usage Policy," as of June 2003, which generally require the suspension of e-mail access immediately upon termination of employment, 63 (82.9%) of a sample of 76 persons no longer listed on the current personnel roster retained active e-mail accounts. At the time of our audit, one staff who had terminated employment in May 1998 still retained an active e-mail account. However, we found that, with few exceptions, active privileges to the PeopleSoft application were deactivated for persons no longer needing access. According to SSC management, access to e-mail accounts was deactivated for faculty and staff no longer listed on the current personnel roster and logon IDs and passwords were deactivated for five staff no longer needing access to PeopleSoft.

To strengthen access security controls, we recommend that user accounts be reconciled with required and permitted access privileges and that access privileges for users no longer needing access to automated systems, including e-mail accounts, be deactivated in a timely manner. Required periodic changes to passwords should be implemented and the schedule of changes documented in the SSC's internal control plan. Furthermore, password formation and use, including requirements for minimum length of password and strictures on use of familiar words should be documented. The College should increase the frequency of reviews for potential security violations and institute incident reporting. SSC should implement an automatic shutdown of an employee's ability to logon after a specific number of unsuccessful attempts. The "Network Security and Usage Policy" and "IT Security Management" should be reviewed and modified where needed, and the final document should be approved by appropriate senior management and included in the College's internal control plan.

With respect to inventory control, we determined that recordkeeping practices for computer equipment and controls over notebook computers needed to be improved. We believe that the lack of a system of record for all fixed-assets, including IT resources, contributed to the lack of data integrity. To improve controls, we recommend that SSC review appropriate statutory authority, record purchases and delete items in timely manner, and perform an annual physical inventory and reconciliation. Regarding controls over notebook computers, SSC should ensure that all faculty and staff assigned a computer complete sign-out/in forms and that the status of the computers be periodically monitored. We believe that the College's program to provide certain computers to retiring faculty does not comply with statutory requirements regarding the disposition of surplus computer equipment. As a result, the Commonwealth has not received financial benefit from the disposal of the surplus computers. We recommend that SSC comply with appropriate statutes regarding surplus property (see Appendix A, Disposition of Surplus State Property, page 27).

Our audit revealed that controls regarding recovery strategies needed to be strengthened or implemented. We found that although SSC had documented certain service disruptions, a formal

criticality assessment and risk analysis had not been performed. In addition, we determined that, at the time of our audit, the College had not yet finalized the selection of an alternate processing site or performed a formal test of the plan's recovery strategies.

To strengthen business continuity controls, the College should perform a formal risk analysis and criticality assessment. In conjunction with this assessment, the business continuity plan should rank all risks and threats along a continuum indicating the potential occurrence of each risk and document the specific steps needed to address the outcome should an actual risk occur. Furthermore, the plan should document the schedule for restoring automated functions. The College should finalize the selection of an alternate processing site. Once the alternate site has been implemented, the College should perform a test of the recovery strategies.

AUDIT RESULTS

1. Inventory Control over IT Resources

Our audit revealed that although important control practices over IT-related equipment had been implemented, other controls needed to be strengthened to provide reasonable assurance that IT resources would be properly accounted for and, when appropriate, that reliable inventory reports on IT resources could be generated. We determined that physical security and environmental protection over automated systems at the sites reviewed were adequate; staff had been designated to maintain the inventory of IT resources; computer equipment was tagged with state identification numbers; and a software inventory was being maintained. However, we found control weaknesses regarding the receipt of and accounting for SSC's IT-related resources, as of March 8, 2005.

Deficiencies pertaining to asset-related control practices included, but were not limited to, the fact that SSC had not:

- fully developed formal policies and procedures regarding fixed-asset management, including conducting an annual physical inventory and reconciliation, accounting for and monitoring of notebook computers, and accounting for surplus property;
- implemented sufficient controls to properly account for its notebook computers;
- entered sufficient information into the inventory record for computer equipment purchases made during fiscal years 2003 and 2004;
- listed sufficient information, such as cost, date of acquisition, or location on its hardware inventory record to identify and track all computer equipment installed at the College;
- performed an annual physical inventory and reconciliation of IT-related resources, as required by the Office of the State Comptroller for Institutions of Higher Education;
- complied with statutory authority regarding the disposition of surplus property; and
- complied with the Internal Control Act, Chapter 647 of the Acts of 1989 and associated OSC asset-related internal control requirements.

We believe that SSC management had not demonstrated sufficient understanding regarding the management and control of fixed assets.

a. Record-keeping Practices

Our audit indicated that, contrary to Office of the State Comptroller's (OSC) internal control guidelines for fixed-asset management, as promulgated under the authority of the Internal Control Act, Chapter 647, of the Acts of 1989, the College's inventory system of record for computer equipment, as of June 30, 2004, did not include sufficient information to provide reasonable assurance that IT-related equipment purchased during fiscal years 2003 and 2004 was on hand, or that all equipment purchases were properly listed on the record. We initially selected a statistical sample of 73 pieces of IT-related equipment purchased during fiscal years 2003 and 2004 that were listed on the hardware inventory record

as of June 30, 2004 for review. We determined that although a “data field” specifying “location” was listed on the College’s inventory record for the 73 pieces of equipment, four (5.47%) items could not be located at the sites reviewed. As an additional test, we selected a sample of purchase documentation for 48 pieces of equipment purchased during fiscal years 2003 and 2004, with a listed value of $92,798. Based on the sample drawn, we were able to confirm only 27 (56.2%) items to the inventory record. During subsequent fieldwork, with the College’s assistance, we found that an additional 21 of 48 pieces of equipment had been listed on the record. Of the 48 pieces of computer equipment listed on the hardware inventory record, we confirmed 22 items to the actual equipment on hand. Regarding the 26 remaining items, 12 pieces of equipment could not be confirmed from the hardware record to the actual equipment because the cost of each of item was under $500, eight items were installed in multiple locations throughout the three College campuses, and six items purchased in May and June 2004 had not been installed as of March 8, 2005.

We determined that the inventory record did not include information regarding cost, date of acquisition, or location for a significant number of pieces of IT equipment listed on the record. In addition, we found that although User Support Services, a work group within MIS, annually reviewed IT resources installed in College departments and developed a list of the equipment, reconciliation to the hardware inventory record had not been performed, contrary to Office of the State Comptroller regulations. It is our understanding that SSC maintained the listing of IT resources to monitor repairs and maintenance of equipment.

Sound management practices and generally accepted industry standards advocate that a perpetual inventory be maintained for all property and equipment, including hardware and software, and that sufficient policies and procedures be in effect to ensure the integrity of the inventory system. Chapter 647 of the Acts of 1989 states, in part, that “The agency head shall be responsible for maintaining accountability for the custody and use of resources and shall assign qualified individuals for that purpose, and periodic comparison should be made between the resources and the recorded accountability of the resources to reduce the risk of unauthorized use or loss and protect against waste and wrongful acts." In addition, Chapter 7, Section 4A of the Massachusetts General Laws states that each agency is required to record and to report on state-owned assets to certain control agencies, such as the Office of the State Comptroller.

The “Massachusetts Management Accounting and Reporting System (MMARS) Fixed Asset Subsystem Policy Manual and User Guide” states, in part, that “Pursuant to Chapter 7A of the Massachusetts General Laws, “the OSC has the responsibility for establishing the state accounting system and has full authority to prescribe the requisite forms and books of account, which includes the classification and accounting of fixed asset activities. The purpose of the Commonwealth Policy Manual is to provide . . . departments with guidance for the appropriate classification and processing of fixed-

asset transactions in compliance with state finance law . . . "Department" includes state agencies, boards, offices, institutions, departments, divisions, constitutional offices, independent agencies, commissions and elected offices of the Commonwealth within the Executive, Legislative and Judicial Branches." Further, the Policy Manual states "all assets entered into the MMARS Fixed Asset Subsystem must be recorded onto the system within seven days of acquisition."

The Office of the State Comptroller requires that a physical inventory and reconciliation of all property and equipment be completed as of June 30th of each fiscal year. Further, OSC's fiscal year 2004 and 2005 Closing and Opening Instructions, section entitled "GAAP, Fixed Assets, and Special Higher Education Reporting" states that "Departments that own fixed assets are responsible for recording all acquisitions, betterments, changes, transfers, and dispositions for GAAP fixed assets and for a physical inventory of non-GAAP fixed assets. . . . Non-GAAP Fixed Assets must be inventoried and controlled." According to OSC internal control documentation, non-GAAP Fixed Assets are buildings and equipment including computer software with a useful life of more than one year and an original cost between $1,000 and $49,999.99, and all electronic and computer components.

The lack of an accurate and complete inventory record for computer equipment hindered the SSC's ability to account for IT resources, detect lost or stolen items, and ensure that IT resources were being used for their intended purpose. In addition, without an accurate, complete, and valid inventory record, the College cannot be assured that all IT resources, including Generally Accepted Accounting Principle (GAAP) Assets have been entered into the College's "Book Asset Detail," as of the end of the fiscal year and, if entered, listed at the proper cost. Because SSC had not performed a physical inventory and reconciliation for IT resources, it could not be determined whether all acquisitions had been entered into the inventory and all items designated as surplus and no longer installed at the College had been removed from the inventory record. Because surplus property records are developed in conjunction with the inventory record, the lack of adequate inventory control procedures regarding IT resources could result in inaccurate records of IT-related surplus property. Assets may be placed at greater risk of loss or theft being detected because equipment was not listed on the inventory record or a list of surplus property. Further, due to the absence of cost information, SSC did not have a readily available accurate total value of computer equipment as of the date of the inventory record, and could not ensure that all GAAP Assets were properly recorded on the record. Further, the absence of information regarding "date of acquisition" and "location" impedes the College's ability to identify, monitor, and track equipment.

Our audit revealed that the procedures used by the College to receive and record IT resources hampered the implementation of appropriate inventory control practices. Upon delivery of computer equipment to the College, the receiving department was required to notify User Support Services of the equipment's receipt and to send the equipment to the designated department for installation. According to the College's documented procedures, USS's responsibilities included installing the equipment,

determining whether it was working properly, and training staff in its use. Once USS was notified of the equipment's receipt and received the supporting invoice from the Fiscal Affairs Section, the item was entered into the hardware inventory record. According to MIS management, the supporting invoices have not been consistently sent to USS. Further, at times, the receiving department has delivered equipment directly to College departments without notifying USS. As a result, the USS lacked sufficient information to enter all pieces of equipment into the inventory record or record their cost to ensure that the College's hardware inventory records are accurate and complete.

We determined that, although the College maintained records of GAAP Assets ("Book Value Assets"), SSC had not developed a master inventory record for all property and equipment or recorded equipment into a system of record as it was received at the College. At the close of the fiscal year, USS reviewed and compiled a list of the equipment located in College departments; however, no reconciliation to the hardware inventory record was performed.

b. Accounting for Notebook Computers

Our audit revealed that although SSC had listed 115 notebook computers on its hardware inventory record as of June 30, 2004, the College could not provide reasonable assurance that these computers were properly accounted for, adequately safeguarded from theft, loss, or damage, and used only for their intended purpose. Of the 115 notebook computers, 89 were entered on the record with a listed value of $149, 235. We determined that SSC had not developed formal policies and procedures regarding the distribution to and return of notebook computers from faculty and administrative staff. Further, the College did not maintain a comprehensive record of all staff who had been provided notebook computers or had returned the equipment and the dates of these actions. Further, the College had not implemented a schedule to periodically monitor the status of the computers that had been distributed to personnel. USS management stated that, as part of the annual physical inventory, notebooks located in various College departments were reviewed. According to USS management, as of February 2002, procedures regarding the sign-out/in of notebook computers had been implemented. Subsequent to receipt of a notebook computer, User Support Services required SSC personnel to sign a form indicating that they had been provided with a notebook computer.

During our audit, SSC management provided a list of 21 persons who were assigned notebook computers. However, the list did not include the dates of distribution, description of the computers, identification numbers for all computers, and evidence that any equipment was returned. Further, USS could not provide any sign-out/in forms for the 21 persons recorded on the list, and could not provide any documentation indicating that any notebook computers had been returned to the College. We found that 94 of the 115 notebook computers that were listed on the inventory record along with the name of the person to whom the computer had been assigned, USS could not provide us with sign-out/in documents

for these computers. In addition, USS management stated that various departments also distribute notebooks to faculty and may not require that sign-out/in forms be completed.

Sound management practices advocate that comprehensive control practices regarding the distribution to and return of notebook computers from individuals be implemented. Control procedures should include written instructions regarding distribution and return of equipment, sign-out/in forms, supervisory approvals, and periodic monitoring of the status of computers.

The absence of consistent policies and procedures, a comprehensive set of documented sign-out/in forms, and a schedule for the periodic monitoring of notebook computers hindered designated managers responsible for safeguarding of computers and monitoring their use, specifically ensuring that staff to whom notebooks have been assigned were aware of their responsibilities regarding appropriate use of the equipment. Further, due to the lack of appropriate recordkeeping procedures, notebook computers may be placed at increased risk of loss or theft.

c. Surplus Property

We found that, contrary to statutory authority, as of February 2002, faculty members who were retiring from teaching duties were allowed, upon approval of their respective Deans and the College's Chief Information Officer, to take a "computer" with them. According to the College's Retirement and Computers Retirement Form, "If an employee is retiring, if the computer is more than two years old, and if the supervisor has given permission, Information Technology (Section) approves of the employee taking the computer home. This does not include external peripherals, such as printers, zip drives . . . and other computer-related equipment. This approval is given with the understanding that there is no further support on the computer from the College for software or hardware repairs or upgrades." In addition, the Retirement Policy states "The College removes the machine from the College inventory. It becomes the employee's responsibility to dispose of the computer in an appropriate manner." The Retirement Policy indicated that the retiring faculty member was required to sign a form documenting the retiree's responsibility regarding appropriate care, repair, and disposal of the computer. Further, the Policy recommended that the removal of the computer "be done with the written notification from the employee's supervisor, to the area head, and to Information Technology, including in the memo the tag numbers and serial numbers of the equipment being retired." SSC management could not state the actual number of faculty who, upon retirement, had been allowed to obtain computers. Further, the College could not provide documentation regarding specific computers given to retirees, date of purchase, description, condition, and cost of the equipment. SSC stated that they believed that only four faculty members had been allowed to obtain computers; however, they could only provide evidence that two sign-out forms had been completed by retiring faculty.

Chapter 7, Section 22 of the Massachusetts General Laws states, in part, that "the Commissioner of the Executive Office for Administration and Finance shall, subject to the approval of the Governor and

council, make rules, regulations and orders which shall regulate and govern the manner and method of the purchasing, delivering and handling of, and contracting for, supplies, equipment and other property for the various state departments, offices, and commissions. . . ." All such purchases must be made by or under the direction of the state purchasing agent. In addition, Chapter 7, Section 22 of the General Laws includes two relevant subsections that require approval by the Commissioner: "The use and disposal of the products of state institutions" (subsection 11) and "Disposal of obsolete, excess and unsuitable supplies, salvage and waste material and other property and transfer of same to other departments, offices and commissions . . . "(subsection 12). Only the Legislature and military are exempt from this statute.

Chapter 15A, Section 24 of the General Laws is a separate statute applied specifically to community and state colleges. Section 24 provides statutory authority to each board of trustees of public higher education so they may conduct procurements for purchases of two thousand dollars or less for goods of an educational nature: "each board of trustees shall have the authority to make any purchase or purchases in the amount of two thousand dollars or less, and to purchase without limitation of amount library books and periodicals, educational and scientific supplies and equipment . . .and shall, wherever practicable, invite competitive bids." However, Chapter 15A does not provide College trustees with any power regarding the disposal of surplus property. As stated in the Attorney General's Opinion of April 21, 1982, "In exercising authority to sell or otherwise dispose of books of state library, trustees must act in accordance with rules and regulations established by the commissioner of administration, pursuant to statute, concerning disposal of obsolete, excess and unsuitable supplies… and other property." It is our understanding that this regulation should apply to the disposal of obsolete equipment by state institutions, as outlined in Chapter 7, Section 22, Subsections (11) and (12), as noted above. Further, 802 Code of Massachusetts Regulations (CMR) 3.00, authorized by Chapter 7, states that to "insure that the Commonwealth realizes the maximum benefit from surplus personal property by regulating the manner of handling such property, including the disposal of obsolete, excess and unsuitable items." The regulation defines surplus personal property as "All state-owned property, (e.g. furniture, office machines, vehicles) except land and buildings."

The College's procedures for the disposal of surplus state property, specifically computers, are inconsistent with statutory authority and associated regulations, because they fail to maximize the financial benefit from the disposal of surplus personal property. In fact, no benefit is realized. Providing computers to former faculty members does not permit the College's property to be sold or otherwise disposed of in the best interest of the Commonwealth.

Recommendation

We recommend that SSC senior management obtain a sufficient understanding of the Internal Control Act, Chapter 647 of the Acts of 1989, and the management and control policies, standards and procedures required for the safeguarding of, accounting for, and reporting on property and equipment,

including IT-related resources. We recommend that the SSC strengthen current practices to ensure compliance with policies and procedures documented in the OSC's "Internal Control Guide for Departments," "MMARS Fixed Asset Subsystem Policy Manual and User Guide," as of June 30, 2004**,** and its associated internal control policies and procedures, and the Operational Services Division's guidelines regarding the accounting for and disposal of property and equipment. In addition, we recommend that SSC review Chapter 7, Section 22, Subsections (11) and (12) and Chapter 15 A, Section 22 of the Massachusetts General Laws, and their associated regulations regarding the disposition of state property, and comply with statutory authority regarding the disposal of computers.

SSC should strengthen formal policies and procedures regarding the safeguarding of and accounting for IT resources. The formal policies and procedures should include, but not be limited to, the following items: maintaining an inventory record; performing, at a minimum, an annual physical inventory and reconciliation; accounting for and monitoring of property and equipment; and disposal of surplus property. In conjunction with the strengthening of policies and procedures, SSC should include procedures regarding the maintenance of a perpetual inventory, which should be reconciled, at least annually, to the physical assets. The perpetual inventory should indicate the date last updated and reconciled. The policies and procedures, once approved by SSC officials and senior management, should be distributed to the appropriate staff, and the staff should be instructed in their use.

SSC should record new purchases, donations, and transfers of equipment and delete items, as needed, in a timely manner. The College should document its policy regarding the recording of assets into the inventory record, including purchases and leased equipment. To maintain proper internal control, staff members who are not responsible for maintaining the inventory record of property and equipment should perform the periodic reconciliation. Further, the inventory record, once reconciled, should be used as the basis for generating the Commonwealth's required asset-management reports (e.g., GAAP Reports). The inventory record should be amended to reflect inter-office transfers of computer-related equipment. Further, we recommend that the process of transferring equipment and updating the inventory record be monitored. To help ensure the integrity of the inventory record, we recommend that SSC ensure that the location, cost amounts, and dates of acquisition are included on the inventory records.

We recommend that SSC enter all property and equipment, regardless of how acquired, into the fixed-asset inventory record at the date of acquisition. We recommend that the SSC perform an inventory record reconciliation, concurrent with its annual physical inventory, and make any required adjustments to its inventory record. SSC should establish controls, including monitoring and evaluation procedures, to provide reasonable assurance that the inventory records of all property and equipment, including IT-related records, are accurate, complete, valid, and verifiable and are maintained on a current basis.

SSC should document procedures regarding the sign-out/ in 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 should determine the number of notebook computers that have been distributed to personnel and require that individuals assigned notebooks complete a sign-out/in form. Further, the designated fixed-asset manager for IT resources should periodically review the status of notebook computers, especially those that have been signed out. The College should require that, upon termination of employment, the employee be required to account for and return school property, such as card-keys and computers assigned to them. In addition, given that SSC has notebook computers signed out to employees to assist them in their work, we recommend that, on at least a quarterly basis, SSC perform a file comparison of the list of individuals to whom computer equipment has been assigned to the master list of current SSC employees. This would serve as a detective control to identify any instances when IT-related resources had not been returned to SSC upon employee termination, transfer or leave of absence. Further, once the IT resource has been transferred to another party, SSC should require that the transfer be formalized by the completion of a new sign-out form.

The College's disposal practices for surplus property should comply with the Commonwealth's laws and regulations governing the disposal of state property.

SSC should establish monitoring and evaluation procedures and mechanisms to ensure that controls are in place and in effect and provide reasonable assurance that control objectives are addressed. The SSC should take full advantage of the training regarding fixed-asset management provided by the OSC and from other sources.

Auditee's Response:

> *College Management feels it does have a solid understanding of the Internal Control Act as evidenced by a satisfactory citing to this effect for the FY-2003 Single Audit report and further evidenced by annual updates to the Internal Control Plan since that audit. In addition, the College has conformed to the "MMARS Fixed Asset Subsystem policy Manual and User Guide" as evidenced by favorable audit reports concerning Fixed Asset reporting since New MMARS implementation. The College does concur that perhaps a strengthening of understanding could be in order with respect accounting for and disposing of property and equipment especially for technology-related equipment. We have ceased any practices that might give the appearance of improper disposal of equipment. It is anticipated that the College will review training programs offered by the Operational Services Division and send personnel involved with technology property and equipment to such training.*
>
> *It is our opinion that there seemed to be some question as to what was included in the audit sample size for certain pieces of equipment. In discussions with the audit team they cited some pieces of equipment that were missing from their survey however upon further investigation many of these pieces were under the $1,000 floor to record Non-GAAP equipment. It would seem to be an appropriate methodology to include peripheral pieces as part of an equipment purchase bundle and if that bundle conforms to the Non-GAAP definition it be included in Non-GAAP inventory. The College will follow this approach in the future.*

As for other issues brought up, the College will coordinate purchase information from the Purchasing system with the inventory maintained by Information Technology to tie such purchases to appropriate purchase orders. This mechanism is already in place. Further, Information Technology in conjunction with Financial Services will reconcile such activity in a timely manner. Finally, the College will take representatives sample of equipment distributed throughout the campus to reconcile the physical assets to their records.

As indicated in the prior response, the College agrees that the Information Technology department will maintain an asset record and that working with the Financial Services group will enter information for appropriate equipment onto the inventory system upon date of acquisition .The Information Technology department has appropriate sign/in out procedures for all computer equipment and many of these also exist at the departmental level. The Information Technology department will insure that Laptop computers are clearly included in these procedures.

Auditor's Reply:

We are pleased that the College plans to improve control practices regarding the accounting for and disposal of property and equipment, specifically IT resources. We agree with SSC's decision to review the Operational Service Division's training programs and designate appropriate information technology staff to attend the training. We reiterate that SSC should ensure that any revenue received from the sale of equipment is realized by the Commonwealth.

We agree with SSC management's decision to strengthen controls over IT resources by maintaining an inventory record, including important information, such as location and cost for all IT equipment in the inventory record, and by performing an annual physical inventory and reconciliation. Regarding notebook computers, we agree that the College should periodically select a sample of computers distributed to faculty and staff, for review. With respect to the sample of 73 pieces of computer equipment reviewed during our audit, cost amounts were available for 25 items. We found that of the 25 items, 16 pieces of equipment had a listed value over $1,000. We will review inventory control over IT resources at our next scheduled audit.

2. Business Continuity Planning

Our audit revealed that, although SSC had documented important control practices regarding business continuity planning, other controls needed to be strengthened or implemented in order to provide reasonable assurance that normal business operations could be restored in a timely manner should automated systems be unavailable for an extended period. We determined that SSC understood the need for business continuity and disaster recovery planning and that senior management was committed to the process of implementing a formal business continuity plan. We found that SSC had documented key control practices to address recovery strategies regarding mission-critical and essential operations in its draft Disaster Recovery Plan (hereinafter referred to as the business continuity plan or plan), as of June

2004. The plan addressed control procedures, such as a description of various disaster scenarios; instructions to address different types of service disruptions, descriptions of service disruptions ranging from partial interruptions to major system failures and time requirements to address recovery steps; risks to the IT environment and procedures to prevent or mitigate the potential damage; an emergency contact list for employees; a vendor list; and procedures regarding the recovery of backup media. Our audit confirmed that SSC had provided adequate on-site and off-site storage of backup copies of magnetic media residing on its file servers. We found that physical security and environmental protection controls over on-site and off-site storage areas were appropriate.

We found that, at the time of our audit, certain control practices needed to be implemented. Our audit indicated that although the College had made progress toward the designation of an alternate processing site to be used in the event that the data center was damaged or destroyed, a site had not yet been selected or approved. As a result, recovery operations at an alternate site could not be tested. According to instructions documented in the business continuity plan, "the Chief Information Officer will periodically appoint a review team . . . to review and update the plan." In conjunction with the review and update of the plan, "the Emergency Coordinator will design, schedule, and notify team members of the annual review . . . The test must address all major procedures involving all teams and must test the ability to process at the contingency site." Failure to adequately test a comprehensive business continuity plan does not allow SSC to attain reasonable assurance that the recovery plan will effectively address various disaster scenarios. Moreover, the lack of tests of recovery strategies may impede the periodic review and modification of the plan. If the plan is not modified when needed, SSC may not be able to rely upon the plan's current viability due to factors, such as changes in the risks and threats to the IT environment, IT infrastructure vulnerabilities, IT application systems, network and communication changes, security requirements, electronic interfaces, personnel, logistics, and organizational changes.

We determined that the loss of the SSC's data center, specifically during critical periods, such as scheduled class registration, would severely impact the College's normal administrative functions and financial-related activities. According to senior management, administrative operations were wholly dependent upon PeopleSoft, SSC's mission-critical application. PeopleSoft's suites, such as Student Administration tools, were used by the Registrar's, Bursar's, and Financial Aid offices. Further, PeopleSoft included a suite of financial tools comprising the general ledger, accounts payable, accounts receivable, purchasing, and billing. Without access to the file servers, on which PeopleSoft resides, the College could not perform these critical functions. According to IT management, SSC was negotiating a mutually acceptable agreement with another entity that would enable the College to designate an alternate processing site and conduct tests of recovery steps to ensure that processing could be resumed.

We found that certain control procedures documented in the business continuity plan needed to be improved. Although the plan documented a series of potential disruptions, such as fire, power outages,

flooding, and network failures, and procedures to detect, prevent, or mitigate the disruptions, a formal criticality assessment and risk analysis had not been performed. A risk analysis should identify the relevant threats that could damage the systems, the likelihood of the threat and frequency of occurrence, the impact of the occurrence on the automated systems, and the cost of recovering the systems. In addition, we found that certain portions of the recovery plan needed to be completed or stated control procedures enhanced, such as restoration of communication components for network operations, a schedule for the restoration of automated functions, written "user area" contingency plans for resuming critical and essential applications, and detailed training plans for appropriate staff.

The objective of business continuity planning is to provide reasonable assurance of the continuation of mission-critical functions should a disaster cause significant disruption to computer operations. Business continuity planning for information services is part of business continuity planning for the entire organization. Generally accepted practices and industry standards for IT operations support the need for each entity to have an ongoing business continuity planning process that assesses the relative criticality of information systems and develops appropriate contingency and recovery plans. Business continuity plans need to be developed to effectively address short, medium, and long-term recovery requirements. In the short term, mission-critical systems and services should be restored. Medium-term plans address recovery of systems and services on a temporary basis, including leased equipment; long-term plans involve the total recovery of the IT processing environment.

The business continuity plan should also incorporate user area plans describing the procedures for user departments and their staffs to follow when changing to alternate-processing activities should a disaster render the automated systems inoperable. Further, the recovery plan should identify contingency procedures that could be used during an interim recovery period. The recovery plan should address procedures for the restoration of critical IT functions and should indicate the logical order of system implementation and integration. The plan should be distributed to appropriate staff, such as SSC officials, senior management, and IT administrators and staff. A copy of the plan should be stored in a secure off-site location and should be available in electronic and hardcopy form. The SSC should consider whether additional copies of the business continuity plan should be stored in other secure locations.

Recommendation

We recommend that to strengthen business continuity planning, the College should:

- Review the business continuity-planning framework outlining business continuity, recovery and contingency objectives for mission-critical and essential business operations. The framework should include a criticality assessment and risk analysis, policies; procedures; defined responsibilities; documented management control practices; organizational controls, such as steering committee, recovery teams, and oversight functions; and assurance mechanisms.

Assurance mechanisms would include internal reviews, testing, and independent examination and verification. The framework should also include senior management assignment of enterprise responsibility for additional recovery strategies.

- Perform an enterprise-based risk analysis and criticality assessment to ensure that all functional areas and business processes are evaluated and update, if necessary, the risk analysis results for the IT Section. The risk analysis and criticality assessment should include all external partners and outsourced services.
- Review the list of disaster scenarios already documented by SSC to determine whether all potential scenarios have been identified, and update the list accordingly with respect to likelihood and impact. Develop and update recovery and business continuity strategies for each of the disaster scenarios identified.
- Reconfirm SSC's understanding of the relative importance of business functions and the potential impact of a loss IT processing support. SSC should formally rank mission-critical, essential, and less essential business process functions and IT processes for development and update of disaster recovery, business continuity and contingency plans.
- Obtain an understanding and adequate level of assurance of disaster recovery and business continuity plans for required services and support from all mission-critical and essential business partners and third-party providers.
- Update existing recovery and business continuity plans to ensure adequate coverage of SSC as a whole.
- Establish a single organizational framework to which business process area plans and IT plans can be linked to an overall business continuity plan. In conjunction with the development of the business continuity plan, SSC should establish targets for acceptable time periods by which mission-critical IT operations need to be recovered.
- Aggressively pursue the selection and approval of an alternate processing site and ensure that appropriate resources are available, such as suitable hardware and communication equipment; supplies; adequate space in which to resume operations; backup copies of all required application programs, data files and system utilities; documented policies and procedures; and sufficient personnel.
- Develop and perform appropriate levels of testing to provide SSC with sufficient assurance as to the viability of recovery and business continuity plans. Tests should be performed on control practices that can be reviewed and evaluated independently of the test of recovery strategies in conjunction with the implementation of the alternate processing site. Once tests are completed,

test results should be reviewed against expected test plan results and reviewed and approved by business process operations and IT management.

- Review business continuity requirements periodically or upon major changes to user requirements regarding the automated systems. We recommend that subsequent to testing the business continuity plan, the plan should be updated when needed to provide reasonable assurance that it is current, accurate, and complete. The completed plan should be distributed to all appropriate staff members, including SSC officials, senior management, and IT administrators and staff.
- Train the SSC staff in the execution of the business continuity plan under emergency conditions. Ensure that all key business process and IT management and staff have adequate skill and knowledge to carry out all tasks and activities outlined in recovery and business continuity plans.
- Coordinate the IT components of the plan with the business continuity planning for the Department's operational functions.

Auditee's Response:

This plan is reviewed on an annual basis, and the improvements noted above will be incorporated on the next review.

The current risk analysis will be reviewed and updated in the next review cycle. This review will be included and an update prepared in the next review cycle.

The current application recovery priorities will be reviewed for accuracy and completeness in the next review cycle.

After each review cycle, a copy of the IT Disaster Recovery Plan will be forwarded to executive management for incorporation into the College-wide preparedness planning.

The recovery timeframes will be reviewed and updated appropriately, in conjunction with the application priority review noted above.

Work has already been initiated in the development of secondary and tertiary sites, and will be pursued aggressively until such sites have been established.

Once the alternate recovery site has been established, and suitable equipment installed, a periodic testing cycle will be established to insure the viability of business application recovery for the College's key business applications. All test results will be documented appropriately.

All new requirements for recovery planning will be added to the College's Disaster Recovery Plan as a component of the initial installation process. The subsequent, periodic review will verify that suitable updates were included.

All periodic tests of the College's Disaster Recovery preparedness will be executed with the key IT and business personnel that would be impacted should an actual disaster occur.

Auditor's Reply:

We are pleased with SSC management's commitment to strengthen its business continuity planning through the implementation of control practices, such as an alternate processing site and the development of a program for the periodic testing of the plan. We will review business continuity planning at our next scheduled audit.

Appendix A
Salem State College
Summary of 801 CMR 3.00
Disposition of Surplus State Property

Purpose of the Regulation

. . . To insure that the Commonwealth realizes the maximum benefit from surplus personal property by regulating the manner of handling such property, including the disposal of obsolete, excess and unsuitable items, waste materials, and other property and the transfer of same to other departments, offices or commissions or storage in state warehouses. . .

Responsibilities of State Agencies

All agencies must examine their inventories of equipment, supplies and materials and periodically report property that is no longer need to the State Surplus Property Officer. The disposal of all surplus, salvage, scrap, and worthless property must be coordinated through the State Surplus Property Officer. State agencies may not transfer, donate, destroy or otherwise dispose of property without following these procedures.

Items declared as surplus, salvage, or scrap under appropriate condition code will remain the responsibility of the declaring agency until disposal, as authorized by the State Surplus Property Officer, has been completed. Items may not be reclaimed by the agency without proper notification and approval of the State Surplus Property Officer. State Surplus Property Officer must be notified immediately.

Agencies must advise the State Surplus Property Officer of all items which are of no further use to them except worthless property.

. . . Form OSD 25 (previously called PAD 25) describing the surplus property should be sent to the State Surplus Property Officer. . . . Agencies must assign condition codes . . . . to all items listed on the OSD 25.

Transfer to Another State Agency

Upon receipt of Form OSD 25, the State Surplus Property Officer will determine if the equipment meets the needs of any state agency, contact those agencies who express a need and inform them that if they are interested in the available items, they should contact the donor agency and arrange for an inspection. If no request for the item, the State Surplus Property Officer lists the item in the "Memorandum of Surplus and salvage Property" sent to all State agencies. Items are transferred on a "first come, first served basis."

Sale of State Property by the State Surplus Property Officer to Non-State Purchasers

When the State Surplus Property Officer determines that there is no further use for surplus, salvage, or scrap property, the State Surplus Property Officer will decide whether to sell (1) through an auction, (2) through a sealed bid, or (3) through a telephone bid.

Property Disposed of Directly by the Owning Department

The State Surplus Property Officer can authorize an agency to dispose of property that has insufficient value. Formal authorization is given by return of the OSD 25 approved by the State Surplus Property Officer. If usable property, the agency sells the property at the best price obtainable by departmental bid procedures. All checks are sent to the State Surplus Property Officer. If unusable property, the agency sells the property at the best obtainable price. Price can be based on weight of scrap material. The agency must be paid by certified check payable to Commonwealth of Massachusetts before relinquishing control of property. All checks must be sent to State Surplus Property Officer.

Appendix A
Salem State College
Summary of 801 CMR 3.00
Disposition of Surplus State Property

Disposal of Worthless Property

Agencies are authorized to destroy items considered to be worthless.

The administrative officer of the agency must appoint, when practicable, a three member property disposal team comprised of the Agency Head, Fiscal Officer, and a third party. Team members are required to personally inspect and determine value of the property. If property is determined to be worthless, each member must sign a certification to that effect. Certifications are sent to the State Surplus Property Officer.

Prior to destruction, the agency should remove any part of an assembly that can be used or stocked for repair of other items.

Property can be temporarily stored at a location approved by the State Surplus Property Officer for up to 30 days. Stored items automatically become surplus after 30 days and made available for transfer or sale.

Appendix B
Salem State College
Summary of Internal Control Practices
as of March 8, 2005

Pg.ref	Control Area	Control Objective	Control Activities	Status of Control	Documented Controls	Adequacy of Documentation
9,10	Physical Security	Provide reasonable assurance that only authorized staff can access business offices, file server room, microcomputer workstations, and client records in hardcopy form to prevent unauthorized use, loss or damage	Control over access to offices, computer rooms, file servers, and microcomputer workstations; designated facilities manager; intrusion detection devices; locked doors, foot patrols	In Effect	Yes	Inadequate
10	Environmental Protection	Provide reasonable assurance that IT-related resources operate in an appropriate environment and are adequately protected from loss or damage	Proper ventilation, temperature control, fire alarms, fire suppression mechanisms, water sprinklers, posted emergency procedures	In Effect	Yes	Inadequate

Status of Control-Key:

In Effect = Control in place sufficient to meet control objective.

None = No internal control in place.
Insufficient = Partial control in place but inadequate to meet control objective.

Adequacy of Documentation-Key:
Adequate = Standard or guideline sufficient to describe, review, and follow significant controls.
Inadequate = Standard or guideline insufficient to describe, review, and follow significant controls.
N /A = Not Applicable

Appendix B
Salem State College
Summary of Internal Control Practices
as of March 8, 2005

Pg. ref	Control Area	Control Objective	Control Activities	Status of Control	Documented Controls	Adequacy of Documentation.
10,11	System Access Security	Provide reasonable assurance that only authorized users are granted access to the automated systems and that logon IDs and passwords are deactivated for users no longer needing access	Passwords required to access automated systems, changes of passwords required at least every 60 days; formal rules for password formation and use; formal procedures for deactivation of logon IDs and passwords	In Effect, except for schedule for password changes	Yes	Adequate, except for password use and formation
11,13	Inventory Control over IT-related Resources	Provide reasonable assurance that IT-related resources are properly safeguarded, accounted for in the inventory record.	Maintenance of an up-to-date inventory record; hardware tagged with state ID tags; annual physical inventory and reconciliation performed	Insufficient, due to lack of data integrity	Yes	Inadequate
12,21	Business Continuity Planning	Provide reasonable assurance that mission-critical and essential functions can be restored in a timely manner should file servers and microcomputer workstations be rendered inoperable or be inaccessible.	Current, formal, tested business continuity plan; alternate processing site; periodic review and modification of plan; plan implemented and distributed; and staff trained in its use	In Effect, except for designated alternate processing site and test of recovery strategies	Yes	Adequate, except for control practices, such as ranking of risks, schedule for restoring automated functions

Appendix B
Salem State College
Summary of Internal Control Practices
as of March 8, 2005

Pg.ref	Control Area	Control Objective	Control Activities	Status of Control	Documented Controls	Adequacy of Documentation
9,21	On-site storage	Provide reasonable assurance that backup copies of magnetic media are available should computer systems be rendered inoperable or inaccessible	Magnetic media backed up nightly; appropriate records maintained of backup; physical access security and environmental protection of storage are adequate; storage area is a separate on-site location	In Effect	Yes	Adequate
9,21	Off-site storage	Provide reasonable assurance that critical and important backup copies of magnetic media are available should computer systems be rendered inoperable or inaccessible	Same as above. Storage area in a separate off-premises location	In Effect	Yes	Adequate