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

Making government work better

Official Audit Report-Issued December 31, 2012

Salem State University

For the period July 1, 2009 through October 31, 2011

TABLE OF CONTENTS/EXECUTIVE SUMMARY

INTRODUCTION 1

Salem State University (SSU) is a member of the Massachusetts Public Higher Education System, which consists of 15 community colleges, nine state universities, and five University of Massachusetts campuses. As of September 30, 2011, SSU had a student population of 9,646; a faculty of 761; and 1,376 professional, administrative, and support staff.

In accordance with Chapter 11, Section 12, of the Massachusetts General Laws, the Office of the State Auditor (OSA) performed an audit of SSU for the period July 1, 2009 through October 31, 2011. Our audit included follow-up testing on issues identified in two previous audits conducted by the OSA. The first audit, No. 2004-0184-4T, reviewed the internal controls SSU established over its Information Technology (IT) resources and activities such as its computer equipment, disaster recovery planning, and business continuity planning. The second audit, No. 2006-0184-12S, was initiated by the OSA based on a notification of a theft of funds at SSU. Specifically, on January 30, 2006, an official from Salem State College (currently Salem State University[1]) notified the OSA, in accordance with Chapter 647 of the Acts of 1989, that a theft of approximately $2,836 had taken place at the central mailing facility located at the college's central campus. Chapter 647 of the Acts of 1989, An Act Relative to Improving Internal Controls at State Agencies, requires the OSA to determine the internal control weaknesses that contributed to or caused an unaccounted-for variance, loss, shortage, or theft of funds or property; make recommendations to correct the condition found; determine the amount of funds involved; identify the internal control policies and procedures that need modification; and report the matter to appropriate management and law enforcement officials. We also conducted follow-up testing on a report issued by a private accounting firm hired by SSU to investigate a theft of cash received for tuition at the SSU Learning Center. SSU filed a Chapter 647 report with the OSA and then engaged this private accounting firm to perform a review of the theft and make recommendations for improvements in controls to reduce the risk of a future theft of this type.

Based on our audit, we have concluded that SSU had implemented appropriate controls to reduce the risk of loss or theft of cash and checks received at the University. However, it still needs to improve its controls over its inventory of computer equipment and enhance its disaster recovery and business continuity plans.

AUDIT RESULTS 4

1. PRIOR AUDIT RESULT RESOLVED: CHAPTER 647-RELATED CONTROLS IMPLEMENTED OVER DIRECT TUITION PAYMENTS AND CHECKS PROCESSED THROUGH THE CENTRAL MAILROOM 4

We conducted follow-up audit work on two prior reports that dealt with a theft of funds reported to the OSA by SSU in accordance with Chapter 647. The first, No. 2006-0184-12S, was issued by the OSA in August 2006 and involved a student employee working in

[1] On July 28, 2010, Chapter 189, Section 12, of the Acts of 2010 elevated Salem State College and eight other public institutions of higher education in the Commonwealth to universities. On October 26, 2010, Salem State College officially became Salem State University.

the SSU mailroom who was able to take three checks totaling $2,836. The second report was issued by a private accounting firm hired by SSU to investigate a theft of cash for tuition received at the SSU Learning Center. Our current audit determined that SSU had implemented appropriate controls to significantly reduce the risk of theft of cash and checks.

2. PRIOR AUDIT RESULTS UNRESOLVED 5

Our follow-up of issues reported in our prior audit of SSU, No. 2004-0184-4T, disclosed that SSU has not taken sufficient corrective action to address the issues the OSA identified regarding a) inventory controls over computer equipment and b) enhancements to the disaster recovery and business continuity plans.

a. Inventory Controls over Computer Equipment Need Improvement 5

Our audit determined that adequate internal controls were not in place to provide reasonable assurance that SSU's computer equipment would be accurately and completely recorded in an up-to-date perpetual inventory system. Specifically, SSU had not recorded all of its computer equipment into its Information Technology Resource Management System (ITRM); there were errors in the amounts SSU recorded as values for equipment items in this system; a complete annual physical inventory and reconciliation of fixed assets for fiscal years 2010 and 2011 had not been performed; and computer equipment items included in SSU's inventory system could not be located. As a result, SSU was unable to maintain a valid and complete perpetual inventory system that could be relied upon to properly account for its computer equipment and support its ITRM. In addition, our audit found that SSU did not keep adequate records of disposed computer equipment and did not obtain the required prior written approval from the Commonwealth’s Operational Services Division before items were disposed.

b. Disaster Recovery and Business Continuity Plans Need to be Enhanced 11

Our audit determined that SSU did not have sufficiently detailed and comprehensive disaster recovery and business continuity plans to provide for the timely restoration of mission-critical and essential business functions should IT systems be rendered inoperable through the loss or inaccessibility of SSU’s data center. We found that while SSU had assessed the relative criticality of computing systems and developed various policies, it had not outlined or tested comprehensive recovery strategies to address various disaster scenarios that could result in seriously degraded or lost IT processing capabilities. The absence of a designated alternate processing site for resuming IT and network operations also places SSU at significant risk of being unable to recover mission-critical systems within an acceptable time period should the data center be lost or become unavailable. Additionally, the absence of on-site storage, the absence of backup media, and the inadequate frequency with which backup copies have been stored off-site could delay recovery efforts and incur data reconstruction costs for SSU. Furthermore, SSU had not documented the necessary tasks and responsibilities for all relevant personnel to carry out SSU’s duties and business objectives under various disaster scenarios.

INTRODUCTION

Background

Salem State University (SSU) is a member of the Massachusetts State College System established by Chapter 15A, Section 5, of the Massachusetts General Laws. SSU is also a member of the Department of Higher Education system, which consists of 15 community colleges, nine state universities, and the University of Massachusetts. With a population, as of September 30, 2011, of 6,241 full-time and 3,405 part-time students, SSU is one of the largest state universities in the Commonwealth. According to the SSU Department of Institutional Research, the University had 761 total faculty and 1,376 professional, administrative, and support staff as of September 30, 2011.

A Board of Trustees, under the direction of SSU's President, governs SSU. Its department operations are supported by automated systems provided by its Information Technology Services Department (ITS). The ITS is comprised of eight divisions: Network Services, Technology Services, Applications Services, Client Services, Instructional Media Services, Faculty Support Services, Training & Change Management, and Technology Integration. The ITS is under the direct supervision of SSU's Chief Information Officer (CIO), who reports to the SSU's Executive Vice President. Oversight of the ITS is provided by an Information Technology (IT) Governance team comprised of the CIO, senior management, and a web steering committee. The Information Technology Resource Management System (ITRM) was developed by ITS in 2007 and is used by SSU to keep a record of all of its IT equipment.

Audit Scope, Objectives, and Methodology

In accordance with Chapter 11, Section 12, of the Massachusetts General Laws, the Office of the State Auditor (OSA) performed an audit of SSU for the period July 1, 2009 through October 31, 2011. Our audit included follow-up testing on issues identified in two previous audits conducted by the OSA. The first audit, No. 2004-0184-4T, reviewed the internal controls SSU established over its IT resources and activities such as its computer equipment, disaster recovery planning, and business continuity planning. The second audit, No. 2006-0184-12S, was initiated by the OSA based on a notification of a theft of funds at SSU. Specifically, on January 30, 2006, an official from Salem State

College (currently Salem State University[2]) notified the OSA, in accordance with Chapter 647 of the Acts of 1989, that a theft of approximately $2,836 had taken place at the central mailing facility located at the college's central campus. We also conducted follow-up testing on a report issued on January 12, 2007 by a private accounting firm hired by SSU to investigate a theft of cash received for tuition at the SSU Learning Center. SSU filed a Chapter 647 report with the OSA and then engaged this private accounting firm to perform a review of the theft and make recommendations for improvements in controls.

The primary objectives of our audit were to:

- Follow up on issues identified in OSA audit report No. 2004-0184-4T by determining whether sufficient corrective measures had been taken by SSU to implement adequate internal controls to provide reasonable assurance that computer equipment would be properly recorded in an inventory system and that IT systems could be recovered within an acceptable period of time should IT systems be rendered inoperable.

- Determine whether appropriate corrective actions had been taken by SSU to reduce the risk of loss or theft of cash and checks processed at SSU.

To achieve our audit objectives, we:

- Reviewed the Chapter 647 incident reports submitted to the OSA by SSU as well as the report submitted to SSU by the private accounting firm it hired to investigate a theft of funds.

- Interviewed SSU senior management and analyzed the organizational structure of the ITS to determine whether an Internal Control Plan and other IT-related policies and procedures were in place, in effect, documented, approved, and communicated to appropriate staff.

- Obtained the current procedures for cashier closing/balance, transferring interoffice cash, receipting deposits with receipt transmittals, mailroom interactions, accepting and processing student payments, cash payments receipted at teller windows, and online student accounts.

- Interviewed SSU's Director of Financial Services and Quality Assurance, Associate Vice President for Finance and Facilities, Associate Director of Purchasing, and Bursar.

- Reviewed job descriptions for managers and staff responsible for the central mailroom; reviewed documented policies and procedures for processing batches of SSU checks to be mailed.

[2] On July 28, 2010, Chapter 189, Section 12, of the Acts of 2010 elevated Salem State College and eight other public institutions of higher education in the Commonwealth to universities. On October 26, 2010, Salem State College officially became Salem State University.

- Evaluated whether adequate internal controls over inventory were in place and in effect to provide reasonable assurance that IT resources would be safeguarded, properly accounted for, and available when required.
- Examined whether SSU's disaster recovery and business continuity plans would provide reasonable assurance that mission-critical and essential IT capabilities could be regained within an acceptable period of time should IT resources be rendered inoperable or inaccessible.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We interviewed agency officials knowledgeable about the ITRM. Since the ITRM had been designated the system of record for SSU's IT equipment, we assessed the reliability of ITRM data by testing for completeness, consistency, and accuracy. The results of our test showed that data essential to our review was not complete and contained errors. Therefore, we determined that the data was not sufficiently reliable for the purposes of our audit. Also, for the purposes of our audit, we used judgmental sampling during our examination of inventory records to determine the type of equipment to test and random sampling to determine the type of individual equipment items to test. We believe the evidence obtained provides a reasonable basis for our findings and conclusions.

Criteria used in the audit included fixed assets accounting requirements from the Office of the State Comptroller; Chapter 647 of the Acts of 1989, An Act Relative to Improving the Internal Controls within State Agencies; management policies and procedures; and control guidelines outlined in Control Objectives for Information and Related Technology (CobiT version 4.1) issued by the Information Systems Audit and Control Association in July 2007.

Based on our audit, we have concluded that SSU had implemented appropriate controls to reduce the risk of loss or theft of cash and checks received at the University. However, it still needs to improve its controls over its inventory of computer equipment and enhance its disaster recovery and business continuity plans.

AUDIT FINDINGS

1. PRIOR AUDIT RESULT RESOLVED: CHAPTER 647-RELATED CONTROLS IMPLEMENTED OVER DIRECT TUITION PAYMENTS AND CHECKS PROCESSED THROUGH THE CENTRAL MAILROOM

During our current audit, we conducted follow-up audit work on two prior reports that dealt with a theft of funds. The first audit, No. 2004-0184-4T, reviewed the internal controls SSU established over its IT resources and activities such as its computer equipment, disaster recovery planning, and business continuity planning. The second audit, No. 2006-0184-12S, was initiated by the OSA based on a notification of a theft of funds at SSU. On January 30, 2006, an official from Salem State University (SSU)—then known as Salem State College[3]—notified the OSA, in accordance with Chapter 647 of the Acts of 1989, that a theft of approximately $2,836 had taken place at the central mailing facility located at the college's central campus. SSU's Public Safety personnel also notified the Eastern District Attorney's Office of the theft. According to the filed report, a student employee working in the mailroom may have taken three checks during the period August 2005 through January 2006. The student admitted taking a $650 check during August 2005, a second check totaling $1,940 in November 2005, and a third check for $245.95 in November 2005. The student indicated that he had deposited the three checks into his personal bank account. At that time, our audit determined that the theft of these funds occurred because the student, employed at SSU's central mailroom located at the Central Campus, had direct access to all University checks being mailed. We made several recommendations at this time based on our audit work; most significantly that the College should continue to ensure the inclusion of the risk management internal control procedures for the mailroom to address student employees as well as other mailroom employees. Our follow-up audit determined that SSU had implemented appropriate internal controls to reduce the opportunity for theft of checks in the central mailroom. Specific SSU improvements we noted included increased training and supervision of mailroom staff, restriction of student employee access to checks in the mailroom, and timely, direct transport of large amounts of checks to the Salem Post Office.

We also followed up on an audit report that was issued by a private accounting firm concerning a theft of cash for tuition received at the SSU Learning Center. SSU filed a Chapter 647 report

[3] On July 28, 2010, Chapter 189, Section 12 of the Acts of 2010 elevated Salem State College and eight other public institutions of higher education in the Commonwealth to universities. On October 26, 2010, Salem State College officially became Salem State University.

with the OSA but engaged a private accounting firm to perform a review of the theft and make recommendations for improvements in controls. The accounting firm issued a letter report on January 12, 2007 with suggestions for SSU to make certain improvements, including enhancing internal controls related to tuition receipts, cash handling, and the timely reporting of received cash. The accounting firm also recommended that SSU receive all direct payments of tuition centrally at the Bursar's Office.

During our current audit, we interviewed SSU senior management, reviewed job descriptions for Financial Services and Bursar's Office managers and staff, and reviewed documented policies and procedures for receiving, accounting, and safeguarding direct tuition payments. We determined that SSU had implemented appropriate internal controls over tuition payments. Specific SSU improvements include only allowing cash to be received at the Learning Center on orientation day; providing trained Bursar's Office staff at the Learning Center to receive, account for, and safeguard the cash; and having SSU Police transport the cash to the bank.

2. PRIOR AUDIT RESULTS UNRESOLVED

Our follow-up audit disclosed that SSU has not taken sufficient corrective measures to address the issues raised in a prior OSA report (No. 2004-0184-4T) regarding (a) inventory controls over computer equipment and (b) enhancements to the disaster recovery and business continuity plans, as discussed below.

a. Inventory Controls over Computer Equipment Still Need Improvement

Our prior audit revealed that although important control practices over Information Technology (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. At that time 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 SSU's IT-related resources. Specifically, we noted that SSU had not:

- Developed formal policies and procedures regarding fixed-asset management, including conducting an annual physical inventory and reconciliation, accounting for and monitoring 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.

- Performed an annual physical inventory and reconciliation of IT-related resources.

- Properly disposed surplus property.

- Complied with Chapter 647 of the Acts of 1989 and associated Office of the State Comptroller (OSC) asset-related internal control requirements.

Our current audit disclosed that SSU's inventory control procedures and practices regarding computer equipment still needed to be strengthened to ensure that ITresources are properly accounted for. In addition, our audit determined that SSU was not recording all purchased computer equipment into the Information Technology Resource Management System (ITRM) and had not performed a complete annual physical inventory and reconciliation of computer equipment for fiscal years 2010 and 2011. Furthermore, we found that the Information Technology Service Department (ITS) lacked adequate segregation of duties for essential inventory control practices, including ordering of computer equipment, verifying the receipt of purchased equipment, recording items into the ITRM, and overseeing the annual physical inventory and reconciliation of computer equipment. Overall, we found that although the ITRM had been designated as the system of record for SSU's IT equipment, it was not subject to oversight by SSU's Chief Financial Officer or other senior managers of the Finance and Facilities Department.

Our audit also determined that SSU's formal fixed-asset policies and procedures and Internal Control Plan (ICP) did not have detailed procedures for recording all computer equipment and performing a complete annual physical inventory and reconciliation. Further, SSU did not adequately monitor the ITS for compliance with the OSC's fixed-asset regulations, SSU asset-management policies, and the Commonwealth's Operational Services Division's policies and procedures for disposing Commonwealth assets. In addition, SSU lacked adequate internal control procedures and practices to ensure that a current, accurate, and complete perpetual inventory record of computer equipment is maintained.

Fixed-asset guidelines promulgated by the OSC require that assets be recorded within seven days of acquisition and that a complete annual physical inventory and reconciliation be performed. Additionally, although Chapter 647 requires that all transactions and other significant events to be promptly recorded, clearly documented and properly classified, our audit tests disclosed the following:

- The ITRM was not updated to reflect disposed equipment items. Specifically, the ITRM inventory as of August 4, 2011 contained 9,309 items with a cost of $8,963,489. However, we found that 2,277 of these items totaling $2,274,062 on the ITRM had been disposed of and were no longer at SSU.

- There were over 290 items with invalid recorded costs, ranging from $2,500 to $60,000 per unit. The total amount of the 290 items with invalid costs (inflated unit costs) is $1,492,501. We determined that incorrect unit costs resulted from invoice totals being recorded rather than the individual asset costs.

- To verify the integrity of the ITRM, we selected all 72 vendor invoices in fiscal years 2010 and 2011 over $2,500, which contained 751 equipment items with a total cost of $797,327. We verified whether the asset information, including serial numbers contained on the purchase orders and related invoices, were properly recorded in SSU's inventory system. Our testing determined that SSU had not recorded 99 items totaling $105,106 (13.2%) and had inaccurately recorded 38 other items totaling $40,344 (5%) in its ITRM.

- To verify the existence of computer equipment on hand, we selected a random sample of 91 desktop computers with a total cost of $121,614 out of 2,001 desktops with a total cost of $2,571,836 contained on the September 6, 2011 ITRM. In addition, we randomly selected 81 notebook computers with a total cost of $117,212 out of 1,384 notebook computers with a total cost of $1,903,284 listed in this system. We also performed a 100 percent test of the 82 items contained on the ITSD list of computer equipment items located in SSU's new data center. To evaluate whether the system of record accurately and completely reflected the items of computer equipment, we verified the location, description, inventory tags, and serial numbers of the hardware items listed on the inventory system of record and compared the inventory record to the actual equipment on hand. Our audit testing determined that not all computer equipment was located in the areas listed in the inventory system. Based on our review, there were six notebooks and five desktop computers that were located in a different area than what was listed on the inventory record. Moreover, we determined that 17 of the tested items, consisting of nine (10%) of the 91 selected desktops and eight (10%) of the 81 selected notebooks, could not be located. The total cost of the 17 missing computers was $18,300. Furthermore, SSU was unaware that the 17 computers had been missing because it had not conducted physical inventories of these items.

- Regarding the segregation of duties, the ITS's purchasing administrator was ordering, receiving, and recording computer equipment as well as maintaining the ITRM of record. The basic goal of segregation of duties is that no individual should have excessive control over more than one critical process. Managing operations of an activity and performing recordkeeping of the same activity are incompatible duties when performed by the same person. Without adequate segregation of duties, there is a heightened risk that errors could be concealed or not be detected in a timely manner or that assets could be misappropriated.

- SSU did not maintain a written policy and procedure to control the assignment and use of notebook computers. Faculty and staff with assigned notebook computers were not required to sign a control sheet acknowledging responsibility for the equipment's security and authorized use. The lack of written policies and procedures to control notebook computers could hinder SSU's ability to properly account for available computer equipment.

- Regarding disposals of computer equipment, we found that SSU did not maintain adequate records of disposed assets. Through our discussion with responsible officials and our review of available records, we determined that SSU had disposed of over 3,000 computer equipment items since 2007 but did not maintain lists of the disposed items. Since SSU did not maintain an accurate and complete listing of items disposed of, the exact dollar value of disposed items is unknown. In addition, we found that SSU did not obtain the required prior written approval for surplus status from the Commonwealth's Operational Services Division (OSD) before disposing equipment items. Reporting procedures to OSD are specified in 802 Code of Massachusetts Regulations (CMR) 3.00: Disposition of Surplus State Property, which lists agencies' responsibilities and policies governing distribution of surplus property.

- No policies and procedures were in place that could be used by SSU to train all staff responsible for monitoring and safeguarding computer equipment to ensure that SSU complies with Chapter 647 of the Acts of 1989. In fact, we found that SSU had underreported stolen computer equipment items to the OSA. Specifically, 25 computer equipment items, including 20 notebooks and three desktop computers with a cost of $36,777, were listed as stolen in the September 6, 2011 ITRM records. However, our review determined that SSU had filed Chapter 647 incident reports to the OSA for only 14 stolen computer equipment items.

Chapter 647 states, in part:

> *All transactions and other significant events are to be promptly recorded, clearly documented and properly classified. Documentation of a transaction or event should include the entire process or life cycle of the transaction or event, including (1) the initiation or authorization of the transaction or event, (2) all aspects of the transaction while in process and (3), the final classification in summary records.*
>
> *All unaccounted for variances, losses, shortages or thefts of funds or property shall be immediately reported to the state auditor's office, who shall review the matter to*

> *determine the amount involved which shall be reported to appropriate management and law enforcement officials.*

As a result of the unrecorded purchased equipment, not conducting complete annual physical inventories and reconciliations, and lack of timely updates to the ITRM record, SSU was unable to maintain a valid, accurate, and complete perpetual inventory system of record that could be relied upon to support IT configuration management and help safeguard SSU's computer equipment.

Recommendation

SSU should strengthen its documented inventory control policies, procedures, and practices to ensure compliance with the OSC's fixed-asset guidelines and its Internal Control Plan. We recommend that SSU:

- Ensure that all purchased computer equipment is properly recorded in the ITRM.
- Complete an annual inventory and reconciliation of the inventory system of record for computer equipment.
- Develop formal policies and procedures to ensure adequate segregation of duties for inventory control of computer equipment.
- Provide Finance and Facilities Department oversight and review SSU's ITS inventory system and related internal control practices to ensure that all received computer equipment items are promptly and accurately recorded into the ITRM and that updates are processed in a timely manner to reflect all received, relocated, or disposed equipment items.
- Develop written detailed procedures and assurance mechanisms for the performance of a complete annual physical inventory and reconciliation of computer equipment, maintain and document the inventory system on a perpetual basis, and periodically verify computer equipment items through reconciliation to physical inventory, acquisition, and disposal records.
- Develop written policies and procedures requiring that all users assigned notebook computers sign a control sheet for their equipment. Procedures to support the policy should be documented and implemented to help ensure that the equipment is used for approved purposes and that appropriate security measures are taken to reduce the risk of loss or misuse of the equipment.
- Comply with OSD fixed-asset regulations that require prior written approval before disposing Commonwealth assets and maintain adequate records for all disposed computer equipment.

- Strengthen internal controls to provide prompt notification and update the inventory record when equipment is purchased, relocated, or disposed of.

- Develop written policies and procedures and train all staff responsible for monitoring and safeguarding computer equipment to ensure that SSU complies with Chapter 647 of the Acts of 1989 reporting requirements for lost or stolen assets.

Auditee's Response

100% Annual Inventory

A 100% physical inventory of SSU computers was initiated in November 2011 and is still continuing. During the inventory each computer is physically examined, the serial number and tag number are verified as correct in ITRM and any missing or incorrect ITRM data fields are corrected. At the same time, the person responsible for the computer is confirmed and that employee is asked to sign a Computer Responsibility (CR) form. The employee is also given a copy of the Acceptable Use Policy.

The CR forms are scanned into OnBase and a check box in ITRM indicates that a CRF is on file. Two employees have worked a total of about 15 hours per week since February 2012 and we expect to complete the inventory by June 30, 2013. When the inventory is complete, should any computers be considered lost the appropriate Chapter 647 report will be filed.

Going forward, a complete physical inventory will be conducted by ITS staff each year. Subsequent physical inventories will require less effort because the database will be clean and there will not be a need to get signatures on CR forms.

When new computers are deployed, acquisition of signature on the CR form is a routine prerequisite to deployment of the asset.

A Loaner Laptop form has also been developed. When an employee borrows an ITS laptop a return date is agreed upon and the form is signed. If the laptop is not returned on the agreed upon date the employee is contacted to return the laptop or to visit ITS to sign an extension.

Segregation of Duties and Financial Services Oversight

A plan has been developed to segregate the duties for inventory control of computer equipment. This plan calls for staff from ITS, Purchasing, Material Management and Director of Quality Assurance and audit to participate in the asset purchasing and inventory verification process. Internal control steps will be developed to ensure that no one person has control and oversight over multiple areas of this process.

Disposal of Surplus Computers

Since the auditor's visit, a new procedure has been established with regard to the disposal of surplus (retired) assets. The ITS Purchasing Budget administrator through the university's Property Manager will submit an appropriate request to the Comptroller's office for disposal of the asset(s). Upon approval, hard drives will be drilled by ITS technicians and the retired equipment will be loaded on pallets for secure destruction.

ITRM is updated to remove the equipment from the active asset inventory and place it in the surplused equipment records.

Written Policies and Procedures

Written policies and procedures have been created for:

- *100% annual inventory and reconciliation*
- *Requiring all employees to sign Computer Responsibility forms*
- *Disposal of Commonwealth assets consistent with Commonwealth property guidelines.*
- *Train all staff responsible for monitoring and safeguarding computer equipment.*

b. Disaster Recovery and Business Continuity Plans Need to Be Enhanced

Our prior audit found that although SSU 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 of time. In terms of disaster recovery, we found that although SSU 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.

Our current audit determined that SSU did not have a sufficiently comprehensive and up-to-date disaster recovery plan (DRP) and business continuity plan (BCP) to provide for the timely restoration of mission-critical business functions should its data center and IT systems be rendered inoperable or inaccessible. We found that SSU's DRP did not include an alternate processing site to recover operations should the data center be unavailable for use. Disaster recovery planning is a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of IT systems, operations, and data. This strategy represents a broad scope of activities designed to sustain and recover critical IT services following an emergency that results in a loss of IT capabilities. IT contingency planning fits into a much broader emergency preparedness environment that includes organizational and business process continuity and recovery planning.

We found that, although management may have assessed the relative criticality of SSU's computing systems and developed various policies, SSU had not outlined or tested comprehensive recovery strategies to address various disaster scenarios that could result in seriously degraded or lost IT processing capabilities. In addition, every department should develop specific contingency plans to address their critical functions. As part of the SSU Internal Control Plan, risk is discussed in a number of paragraphs; however, it lacks the necessary level of specificity to determine the extent of potential risks and exposures to IT operations and scenarios. SSU's risk analysis should identify the relevant threats that could significantly degrade or render IT systems inoperable or inaccessible, the likelihood of the threat, and the expected frequency of occurrence for each disaster scenario. Additionally, SSU had not documented the necessary tasks and responsibilities for relevant personnel to carry out under various disaster scenarios.

Business continuity planning helps ensure the timely recovery and continuation of mission-critical functions, including information services, should a disaster cause significant disruption to computer operations. Generally accepted practices and industry standards for computer 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. To that end, SSU should assess the extent to which it depends upon the continued availability of information systems for all required processing or operational needs and should develop its recovery plans based on the critical aspects of its information systems.

An up-to-date, effective BCP should identify the manner in which essential services would be restored or replaced without the full use of the data center facility or loss of network communications. The BCP 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 BCP 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

SSU should complete a DRP and a BCP that incorporate criticality and impact assessments; business continuity planning development; risk management; and recovery plan testing, maintenance, training, and communication. SSU should document recovery strategies to address various disaster scenarios that could adversely impact IT operations and periodically test its DRP and BCP to determine their viability. The plans should assign roles and responsibilities to specific staff members, present detailed steps for them to follow in recovering mission-critical and essential IT systems and operations, and address the telecommunications and security issues that would arise if SSU had to conduct off-site computer operations. In addition, the BCP should document vendor protocols for the emergency use of computers suitable for operating the SSU's mission-critical application and conduct periodic training for staff and ensure that complete hard copies and electronic copies of the plans are stored in a secure off-site location. Moreover, SSU should identify an alternate site from which IT systems could be recovered should the SSU's data center become inaccessible for an extended period of time. We further recommend that SSU reassess the provisions for on-site and off-site storage of backup media and increase the frequency by which backup media is stored off site.

Auditee's Response

With the construction of a new data center at Salem State University during the summer of 2011, the primary data center is now much more secure and survivable. Mitigating risk at the primary site was the top priority during that year. In 2012 Salem State will turn its attention to strengthening disaster recovery and business continuity planning in regard to the potential loss of the data center. A search for an alternative site has begun and the most likely partner appears to be UMass Medical which plays this role for other higher education institutions.

Salem State has moved many critical applications such as the learning management system, room allocation system, tuitions payment system, course catalog, job posting, and student application system to hosted cloud services. These hosted services provide a level of redundancy and survivability that it would be impossible for any State institution to replicate. MMARS and HRCMS are critical applications that run in ITD data center(s) and are secured by ITD disaster recovery and business continuity plans. The Salem State website is replicated in the Google cloud nightly and in the event of a disaster this site can be activated within minutes. This scenario has been successfully tested several times.

It should also be noted that the university has extensive information and procedures readily available for staff to respond to any number of critical situations. As a result of a campus–wide initiative proposed by the President, the university undertook a thorough evaluation of response procedures in anticipation of the looming H1N1 pandemic. As a result all critical operations were assessed for their business continuity should that or other critical situations arise. It is anticipated within the next year, the university will revisit these procedures in conjunction with other disaster recovery and business continuity planning.

Finally, the President has authorized the creation of a new Risk Management Office which will serve as the enterprise level disaster recovery and business continuity planning entity. The Risk Management Office will work to enhance existing emergency response plans including disaster recovery and business continuity.