The Commonwealth of Massachusetts
AUDITOR OF THE COMMONWEALTH
ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108

A. JOSEPH DE NUCCI
AUDITOR

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

NO. 2009-0179-7T

OFFICE OF THE STATE AUDITOR'S REPORT ON THE EXAMINATION OF INFORMATION TECHNOLOGY-RELATED CONTROLS AT FRAMINGHAM STATE COLLEGE JULY 1, 2007 THROUGH NOVEMBER 20, 2009

OFFICIAL AUDIT REPORT

MARCH 3, 2010

TABLE OF CONTENTS

INTRODUCTION

Framingham State College (FSC), which was established in 1839, is a comprehensive public college that integrates liberal arts and science programs with a variety of professional programs at the Baccalaureate and Masters levels. FSC also offers continuing education programs on a full-time and part-time basis. Chapter 15A, Section 5, of the Massachusetts General Laws created the Massachusetts State College System, of which FSC is a member.

FSC's primary mission is to educate the residents of MetroWest Boston and the Commonwealth and to use its intellectual, scientific, and technological resources to support and advance the economic and cultural life of the region and the state. FSC is located on State Street in Framingham, and its 17 buildings on 73 acres of land include a campus center, six student residence halls, academic buildings, a planetarium, and an athletic and recreation center. At the time of our audit, FSC had a total enrollment of 6,076 students: 3,952 undergraduates and 2,124 graduate students. At that time, FSC employed 555 full-time and part-time faculty, administrators, and college and contract staff members and was supported by a fiscal year 2009 budget of approximately $61 million.

FSC's administrative and academic mission and operations are supported by technology services provided by FSC's Information Technology Services (ITS), which has planning, delivery, and operating responsibility for all computing, telecommunications, media, and data administration resources for FSC. ITS is comprised of five departments: Systems and Network Services, Applications Support, User Services, Academic Technology and Distance Education, and Training and Support Services. At the time of our audit, ITS was composed of 21 staff members, with each of the five departments having a director/associate director reporting directly to the Chief Information Technology Officer, who reports directly to FSC's Senior Vice President, Office of Administration, Finance, and Technology.

ITS provides assistance and guidance to administrative staff, faculty, librarians, and students regarding the use of IT resources, including the use of administrative computer systems, Internet portal support, personal computer maintenance, web hosting services, print servers, and e-mail. ITS also supports a campus-wide network and client infrastructure (campus network) consisting of 62 servers that are configured on a campus-wide local area network (LAN) for use throughout FSC, including the 18 computer labs and classrooms. Recent upgrades to FSC's network infrastructure now allow users more bandwidth and wireless network connectivity. FSC's IT infrastructure includes 1,072 workstations and 590 notebook computers.

From an administrative perspective, IT systems are used to process FSC's financial management, administrative, and student information activities. FSC's primary application is the Banner system, which is used to process student and administrative financial accounting, student registration, admissions, course schedules, degree credits, and human resources management. FSC's network allows connectivity to the State Human Resources Compensation Management System (HR/CMS) and the Massachusetts Management Accounting and Reporting System (MMARS).

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

In accordance with Chapter 11, Section 12, of the Massachusetts General Laws, we performed a follow-up audit of certain information technology (IT) general controls at Framingham State College (FSC). Our audit, which was conducted from June 24, 2009 through November 20, 2009, covered the period July 1, 2007 through November 20, 2009. The scope of the audit consisted of an evaluation of the status of prior audit results in our prior audit report No. 2005-0179-4T, issued January 13, 2006, regarding system access security, disaster recovery and business continuity planning, and inventory control over computer equipment. We also determined whether FSC had appropriate policies in place regarding the protection of personally identifiable information.

Audit Objectives

The primary objective of our audit was to determine whether corrective action had been taken with respect to our prior audit results and to review selected IT general controls. Our objective regarding system access security for user account management was to determine whether adequate controls were in place for the activation, maintenance, and deactivation of access privileges to ensure that only authorized personnel had access to the campus network and the Banner application system. Furthermore, we sought to determine whether IT security staff were actively monitoring the management of user accounts. We also sought to determine whether adequate disaster recovery and business continuity plans were in place to provide reasonable assurance that computer operations would be regained within an acceptable period should a disaster render FSC's computerized functions inoperable. In addition, we sought to determine whether adequate controls were in place and in effect to provide reasonable assurance that IT resources were properly accounted for in an inventory system of record and safeguarded against unauthorized use, theft, or damage. A further objective was to determine whether FSC's policies and procedures were in place to protect personally identifiable information.

Audit Methodology

To evaluate whether corrective action had been taken on our recommendations presented in our prior audit report, we first performed pre-audit work that included a review of prior audit work papers and gaining an understanding of FSC's current IT environment, including audit work on the prior topic areas. We reviewed our prior recommendations and examined the extent to which FSC had implemented corrective action regarding system access security, disaster recovery and business continuity planning, and inventory control over computer equipment.

During our current examination of system access security controls, we reviewed policies and procedures to authorize, activate, and deactivate access privileges to the campus network and Banner application system. The Banner system, which resides on FSC's file servers, is accessed through microcomputer workstations located at FSC's administrative offices and individual campus locations. We reviewed control policies and procedures regarding logon ID and password administration and password composition for access to the network domain and to the mission-critical Banner application by evaluating the appropriateness of documented policies and guidance provided to FSC personnel, reviewing documentation, and interviewing FSC's security officer and IT management. In addition, we reviewed control practices used to assign FSC and contract employee 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. We determined whether all individuals authorized to access system applications were required to change their passwords periodically and, if so, the frequency of the changes. In addition, we reviewed selected access user privileges, access logs, and evidence that passwords were required to be changed on a pre-determined basis. To verify that all users of the Banner application system and the campus network domain were current FSC employees or contract employees, we obtained system-generated user account lists containing all active user accounts as of August 31, 2009 and compared them to a FSC full-time employee payroll list and lists of contract employees and other FSC contractors. We developed an exception list of those individuals no longer requiring access privileges to the Banner application and the campus network. Our audit did not include an examination of controls over network security.

To assess the adequacy of business continuity planning, we determined whether any formal planning had been performed by FSC to resume IT operations should the network application systems be inoperable or inaccessible. In addition, we determined whether the criticality of application systems had been assessed, and whether risks and exposures to computer operations had been evaluated. We conducted interviews with department heads to evaluate the potential impact on the business processes should the critical applications become unavailable for various periods of time. Furthermore, to evaluate the adequacy of controls to ensure that backup copies of application systems and data files would be available for recovering automated systems and network services, we interviewed FSC staff regarding the generation and storage of backup copies of magnetic media. We reviewed policies and procedures for the generation

and on-site and off-site storage of backup copies of magnetic media backup tapes, and inspected the on-site and off-site storage locations.

To evaluate inventory control over computer equipment, we obtained and reviewed the inventory record for computer equipment, as of August 8, 2009, and reviewed inventory control policies and procedures. We reviewed the current inventory system of record to determine whether it contained appropriate data fields to identify, describe, and indicate the value, location, and condition of computer equipment. We reviewed the content of selected data fields, such as state identification number, serial number, cost, and equipment location, in order to assess the level of accuracy and completeness of the system of record and to determine whether sufficient information was available to perform audit tests, including a reconciliation of items listed on the record to the actual equipment.

We reviewed control procedures regarding the tagging of computer equipment purchased by FSC. By observation, we determined whether the computer equipment was properly tagged with state identification numbers and that the tag numbers were accurately recorded on the inventory system of record. In addition, we determined whether computer equipment serial numbers were accurately recorded on the hardware inventory record. To determine whether the inventory system of record for computer equipment for FSC was current, accurate, and complete, we reconciled the inventory list provided by FSC to the actual computer equipment on hand and supporting documentation. We used ACL software to select a random sample of 63 pieces of IT equipment from FSC's listing of computer equipment consisting of 4,196 items. We traced our random sample of equipment items from the inventory list to their physical locations. We also selected the top 10 valued IT assets to include in our test. We determined whether numbered identification tags were affixed to computer equipment and whether the tag numbers were properly recorded on the inventory record. We selected and traced 28 additional IT hardware items from their physical locations back to the inventory list to verify whether the tag numbers were accurately recorded. Regarding new purchases of IT equipment, we obtained purchase orders for all 107 purchases of IT equipment for the audit period and traced the items to the inventory, then randomly selected 37 items on the inventory to determine whether the equipment was on hand in the location recorded on the inventory record. We also reviewed the sign-out policies and receipt logs for 15 of the 590 items listed as notebook computers. Furthermore, we reviewed FSC property disposal practices to determine whether procedures required by state law and regulations were being followed when FSC disposed of surplus assets. In addition, we reviewed any reports of stolen or lost IT equipment and determined whether FSC complied with the requirements of Chapter 647 of the Acts of 1989.

To assess the adequacy of FSC's effort to protect personally identifiable information, we interviewed senior management to determine the controls in place related to FSC's policies and procedures implemented in order to protect personally identifiable information.

Our audit was conducted in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States through the U.S. Government Accountability Office and generally accepted industry practices. Audit criteria used in the audit included management policies and procedures and control guidelines outlined in Control Objectives for Information and Related Technology, as issued by the Information Systems Audit and Control Association in July 2007, and the Office of the State Comptroller's guidelines. Our audit criteria consisted of relevant FSC policies and procedures and generally accepted control practices.

AUDIT CONCLUSION

Our examination of the status of audit results from our prior audit report No. 2005-0179-4T, issued January 13, 2006, indicated that Framingham State College (FSC) had taken corrective action to address control objectives regarding disaster recovery and business continuity planning. However, although controls had been strengthened for system access security and inventory control over computer equipment, additional effort is needed to provide reasonable assurance that related control objectives would be met. Regarding system availability, our audit indicated that FSC had a formal business continuity and disaster recovery plan to help ensure the resumption of mission-critical and essential processing should IT systems be rendered inoperable or inaccessible.

Our review found that system access security controls needed to be strengthened for the campus network and the Banner application system that supports mission-critical processing for student and administrative financial accounting, student registration, admissions, course scheduling, degree credits administration, and human resources management. With respect to system access security, we found that appropriate control policies were in place regarding the authorization of personnel to be granted access to network resources and the activation and deactivation of access privileges. Although we found that policies were in place to help ensure that access privileges would be deactivated, or appropriately modified, should FSC employees terminate employment or incur a change in job requirements, user accounts were not always deactivated in a timely manner.

We determined that control practices regarding logon ID and password administration were not adequately in effect to provide reasonable assurance that only authorized parties could access FSC's IT resources. We found that 73 user accounts for former FSC employees and contractors had not had the access privileges deactivated to the campus network or the Banner system. We found that, contrary to FSC policy regarding system access security controls, the security administrator was not being consistently informed by department heads, superintendents, or contractors of changes in user status (e.g., resignations, terminations, name changes) that would require modification or deactivation of access privileges. Our audit disclosed that a user account remained active until brought to FSC's attention for an FSC employee whose employment had been terminated on June 23, 2006. Although our review of the 73 user accounts indicated that the majority had limited access privileges, tighter control over timely deactivation of user accounts would reduce the risk of unauthorized access to mission-critical systems and IT capabilities. We recommend that FSC enforce its current policy requiring that department heads,

supervisors, and the FSC Human Resources Department notify the security administrator of changes in user status that could warrant modification or deactivation of user accounts.

Regarding password administration, we found that employees were required to change passwords on a predefined basis and that appropriate policies and procedures were documented, security administration had been assigned, appropriate rules for user access activation and password length and composition were in place, and security requirements had been established. However, we found that the Banner application does not prompt users to change their passwords in a predetermined number of days and that therefore some employees have not been changing their passwords on a regular basis.

With respect to disaster recovery and business continuity planning, we found that FSC had a formal business continuity plan to help ensure the resumption of mission-critical and essential processing should IT systems be rendered inoperable or inaccessible. According to departments within FSC, the level of business impact would vary depending on processing requirements and the time of the operational year. We determined that FSC had adequate provisions for generating backup copies of magnetic media and adequate on-site and off-site storage for backup media to support recovery efforts. We found that backup copies were maintained in secure on-site and off-site storage locations.

Regarding inventory control, although FSC had policies and procedures for inventory control, FSC should increase efforts to strengthen current policies and procedures. The controls should be strengthened to provide a higher level of assurance that the inventory can be relied upon. We found that 167 computer equipment inventory items on FSC's computer equipment inventory list were understated by $15,266. In addition, our review revealed that FSC staff responsible for the inventory were unaware of the reporting requirements for missing or stolen Commonwealth assets under Chapter 647 of the Acts of 1989 and that FSC had not reported occurrences of missing or stolen computer equipment to the Office of the State Auditor during the audit period. We recommend that FSC document the process for performing an annual physical inventory that reconciles the inventory system of record to the physical inventory and documents equipment acquisition and disposal. We also recommend that FSC enhance the inventory system of record to include complete information with respect to cost, condition of equipment, and date of purchase.

Our review found that FSC's policies and procedures to protect information appeared to be detailed and comprehensive from a process perspective. Regarding FSC's efforts to protect personally identifiable information, we found that FSC had appropriate policies and procedures to protect personally identifiable information.

AUDIT RESULTS

1. Prior IT Audit Results Unresolved

a. System Access Security and Password Administration

Our prior audit report (No. 2005-0179-4T) on Framingham State College (FSC) revealed that procedures needed to be strengthened to ensure that access privileges to the automated systems would be deactivated in a timely manner for those individuals no longer requiring access and that users change their passwords on a regular basis. During our follow-up review, we found that control weaknesses still existed in user account management for the applications we reviewed, as discussed below.

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

Our tests of system access security for the campus network and the Banner application system indicated that, contrary to sound access security practices, there were active user IDs and passwords for individuals who were no longer employed by FSC. Our tests indicated that 73 users having active user accounts could not be identified on FSC's September 2, 2009 payroll and contractor registers. Although the majority of the user accounts that had not been deactivated were for individuals who had left employment with FSC within the previous six months, there were six user accounts for which the termination dates were before January 1, 2009, with one account going back to June 23, 2006.

Access to network IT resources, application systems, and data files should be authorized on a need-to-know, need-to-perform, and need-to-protect basis. To ensure that only authorized users have access privileges, timely notification should be made to the security administrator of any changes in user status that would impact the user's level of authorized access. For example, the Human Resources Department or other departments where employees were assigned should notify the security administrator of changes in employment status so that access privileges may be deactivated in a timely manner for individuals no longer requiring authorized access. Although procedures were in place to inform the security

administrator of changes in employment status, the procedures were not always followed. As a result, user accounts for which access was no longer needed or authorized were not always deactivated in a timely manner. Further, unauthorized users could have accessed, altered, or deleted critical information on the IT network or the Banner application.

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

Our review of password administration of the Banner application revealed that although FSC had policies for password length and composition, passwords had not been changed on a regular basis. The failure to change passwords for user accounts on a regular basis places FSC at risk of unauthorized use of established privileges or unauthorized access.

Recommendation

FSC's system access security policies and procedures should be followed to ensure the prompt disabling of access privileges when an employee's or a contractor's active service ends or when there is a required alteration in their level of access due to a change in job functions. FSC should designate an appropriate official to be responsible for ensuring compliance with this requirement and for monitoring the results on a regular basis so that the user list is promptly updated and contains only active, legitimately enabled user accounts.

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

Auditee's Response

Framingham State College will strengthen system access security and password administration practices in order to ensure that management and de-provisioning of access to protected information systems in the following specific manner:

1. *The Office of Human Resources and other Administrative Offices or Academic Departments will provide Information Technology Services with more consistent formal notification of changes in employment status which would impact the individual's continued authorization to access information systems or privileges granted to perform specific functions.*

2. *The Office of Human Resources will also run reports every two months to determine which contractors have not been paid in a while and then will follow-up with the appropriate Administrative Office or Academic Department to determine employment status.*

3. *Users of the College's administrative and student information system (a.k.a. Banner), campus network, and e-mail system will be required to change their passwords periodically in accordance with updated policies and procedures that specify the intervals according to best practices within higher education.*

Auditor's Reply

We commend FSC for initiating steps to address the security concerns related to user account management. We believe that FSC's efforts to improve communication regarding changes in network security status or access privileges as well as the periodic change of passwords will enhance controls over user account management. We suggest that the more formal notification process include having ITS acknowledge to the Office of Human Resources and other administrative offices or academic departments that the requested change (modification or deactivation of access privileges) has been made. By using the concept of a turnaround document, the acknowledgment from ITS helps ensure that required changes in user access privileges do not go unattended. In addition, the acknowledgment is important in that the department requesting the change is more likely to be the owner of data and has primary responsibility for its security.

b. Inventory Control over Computer Equipment

Our prior audit disclosed that FSC could not provide reasonable assurance that the inventory system of record for computer equipment could be relied upon, since an annual physical inventory and reconciliation was not being performed to assist in verifying the accuracy and completeness of the inventory record. Our prior audit also revealed that FSC did not comply with Chapter 647 of the Acts of 1989 when it failed to notify the Office of the State Auditor of approximately $11,800 of stolen computer equipment. Our follow-up review disclosed that inventory control practices over computer equipment still need strengthening to ensure that IT resources are properly accounted for in FSC's inventory system of record for property and equipment, as discussed below.

Our follow-up review found that FSC was maintaining an inventory of IT resources and had performed an annual physical inventory in compliance with Office of the State Comptroller requirements. We also determined that FSC had taken steps to improve inventory control by establishing a centralized inventory system of record and conducting annual inventories of equipment on hand. However, we found that the inventory system of record did not contain appropriate data fields, including historical cost and condition, and that inventory reconciliations were not being performed. Regarding compliance with Chapter 647 of

the Acts of 1989, reporting requirements for missing or stolen Commonwealth assets, our review revealed that FSC staff responsible for the inventory were unaware of the reporting requirements and that FSC had not reported occurrences of missing or stolen computer equipment to the Office of the State Auditor during the audit period.

Our audit disclosed that inventory control practices over computer equipment needed to be strengthened to ensure that IT resources would be properly accounted for in FSC's inventory system of record for property and equipment. We found that controls needed to be strengthened to provide prompt notification and update of the inventory record when equipment is relocated, disposed of, lost, or stolen. In addition, inventory records did not appear to be adequately reviewed for accuracy and completeness, and an appropriate level of reconciliation was not in place. The absence of a sufficiently reliable inventory of computer equipment hinders FSC's ability to properly account for IT resources, evaluate the allocation of equipment, identify missing equipment, and meet IT configuration objectives.

Although we determined that FSC had documented internal controls regarding the purchasing, receiving, and recording of IT resources, we found that documented policies and procedures needed to be enhanced regarding the maintenance, compliance monitoring, and reconciliation of the inventory system of record for IT resources. For example, although documented procedures were in place requiring an annual campus-wide inventory to be conducted at the end of each fiscal year, documentation was unavailable to support an annual physical inventory. Our tests of the inventory system of record, as of August 8, 2009, indicated that the total value of computer equipment of $3,482,690 might not be sufficiently reliable due to discrepancies in cost figures for some of the computer equipment items on the list. The integrity of the system of record for computer equipment could not be determined because of missing data fields as well an inventory system of record that could not be reconciled.

Moreover, although FSC had policies and procedures for tagging IT assets, we determined that FSC was not tagging all IT assets. The Office of the State Comptroller's Accounting and Management Policy requires that "All assets, regardless if they are fixed or not, must be accounted for, managed, and reported in accordance with all applicable laws and regulations of the Commonwealth." Furthermore, although FSC has policies and procedures for the return of laptops when an employee ends employment, laptops were not being turned in to the Property Control Office by retiring faculty. Although FSC had adequate policies and procedures for the disposal of surplus property and Chapter 647 requirements, FSC was not fully complying because of its failure to submit reports to the Office of the State Auditor.

We found that although FSC's inventory record had certain fields of information, the system of record lacked data fields to properly account for IT-related computer equipment and support asset or IT configuration management. For example, there was no data field for "condition of item" to support IT

configuration management by noting the asset's status, such as being repaired, obsolete, or designated for surplus, or a data field for "date of purchase" to identify when FSC purchased the computer item and to support decision-making regarding equipment replacement or upgrade.

Our inventory tests were conducted on the total population of 4,196 items of computer equipment. We used ACL software to select a sample of 63 computer equipment items to be traced from the listing to their location. Although all 63 computer hardware items in the sample were located, only 57 of the 63 items had proper asset tags attached. To further test the integrity and completeness of the inventory system for computer equipment, we randomly selected 28 additional items in various locations to be traced to the inventory list. Our audit test revealed that asset tag numbers could be verified for 25 of 28 IT-related items. However, three computer equipment inventory items totaling $1,127 were not on the August 8, 2009 computer equipment inventory list. The absence of a complete inventory listing may hinder FSC's ability to properly account for available hardware systems and may undermine its ability to detect missing or stolen equipment.

We obtained purchase orders for the 107 acquisitions of computer equipment made during fiscal year 2009 and traced the items to the inventory listing. In addition, we randomly selected 37 of the items purchased in fiscal year 2009 and physically located 36 of the sampled items to the equipment on hand. According to FSC, the missing item was a notebook computer that had been available to be loaned out and would not have contained personal information. Subsequent to our audit field work, FSC attempted to locate the equipment and has reported the loss to Campus Police.

We found that the computer equipment loan program that is administered by the FSC library appeared to be well managed, with an appropriate sign-out form for students to request equipment for a short duration. FSC had policies and procedures for faculty and staff members interested in using a notebook computer. Based on a judgmental sample of 15 notebook computers valued at $20,219, out of a total of 177 loaned to faculty and staff, all 15 of the computers selected were locatable. There were property loan report forms on hand for 13 of the 15 notebooks that the audit team reviewed as part of the test. However, we found that although FSC had policies for the return of notebook computers when an employee ends employment, retired faculty were not returning FSC's notebooks in a timely manner, often taking months to submit the notebooks to the Property Control Office.

Our audit disclosed that FSC had thefts of five laptop computers, valued at $6,856, during the audit period. Chapter 647 of the Acts of 1989, An Act Relative to Improving the Internal Controls within State Agencies, requires agencies to immediately report unaccounted-for variances, losses, shortages, or thefts of funds or property to the Office of the State Auditor. We determined that incident reports for the stolen laptops had been filed with the Campus Police. However, no reports regarding these incidents had been

forwarded to Office of the State Auditor. Generally accepted industry standards and good management practices require that adequate controls be implemented to account for and safeguard fixed assets against loss, theft, or misuse.

Our examination of computer equipment that had been designated as surplus property indicated that FSC had policies and procedures for the disposal of surplus state property and the state surplus forms were being submitted in a timely manner to the Operational Service Division's State Surplus Property Officer. There are policies and procedures for expediting the process of surplus capital equipment (e.g., computer equipment). We found that FSC was following its documented policies and procedures regarding the steps to be followed in designating computer equipment as surplus and in disposing of it.

Recommendation

We recommend that FSC perform a reconciliation of the inventory system of record as part of the annual physical inventory of its IT resources to ensure that an accurate, complete, and valid inventory record of IT resources is in place. We recommend that the inventory system of record be maintained on a perpetual basis and that it be periodically verified through reconciliation to physical hardware and to records of acquisition, theft/loss, and disposal. We also recommend that FSC refer to the policies and procedures outlined in the Office of the State Comptroller's Internal Control Guide to help achieve the goal of ensuring the integrity of the inventory record and enhancing knowledge of the IT infrastructure. In addition, policies and procedures for the return of notebook computers when an employee ends employment should be strengthened to require the Human Resources Department to inform both the retiring employee and the Property Control Office that the notebook needs to be returned.

We recommend that the responsibilities for recording, maintenance, disposition, and reconciliation of the inventory and configuration information be defined to provide appropriate segregation of duties and management review and oversight. We further recommend that FSC management use Chapter 647 of the Acts of 1989, An Act Relative to Improving Internal Controls within State Agencies, as a guide for establishing inventory controls regarding the safeguarding of, accounting for, and reporting of IT-related resources. FSC should formalize a process for notifying the appropriate individual responsible for maintaining the IT system of record of any lost, stolen, or missing items. FSC should maintain policies and procedures that will comply with Chapter 647 of the Acts of 1989 and immediately report all instances of unaccounted-for variances, losses, and thefts of funds or property to the Office of the State Auditor. FSC should communicate requirements for all internal and external notifications of thefts to a designated staff member. Furthermore, FSC should continue to investigate how these thefts occurred and try to establish controls to minimize the risk of reoccurrence.

With respect to IT configuration management, we recommend that the data fields in the IT inventory be expanded to include the condition and status of the IT resource. The recommended control procedures should provide increased assurance that all IT-related equipment is recorded on the inventory record in a complete, accurate, and timely manner to enable FSC to produce a complete record of all IT-related equipment on a perpetual basis. To help ensure the integrity and enhance the usefulness of the inventory record, we recommend that FSC ensure that the dates of acquisition and accurate cost figures are included on the inventory record. FSC's inventory records should reflect any changes to computer hardware items, including location or status, for both deployed equipment and items held in storage. The inventory record should be amended to reflect inter-office transfers of computer-related equipment. Furthermore, we recommend that the process of transferring equipment and updating the inventory record be monitored.

Sound management practices advocate that comprehensive control practices regarding the distribution and return of notebook computers 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.

FSC should record new purchases, donations, and transfers of equipment and delete items, as needed, in a timely manner. 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. Furthermore, the inventory record, once reconciled, can then be used as the basis for generating the Commonwealth's required asset-management reports (e.g., GAAP Reports).

Auditee's Response

Framingham State College will strengthen inventory control practices in order to ensure that IT resources are properly accounted for in the college's inventory system of property and equipment recording in the following specific manner:

1. *Documentation will be maintained to support the annual physical inventory procedure for any IT item with a value of $100 or more.*

2. *Data fields that include, but are not limited to, condition of IT equipment items, date of purchase, location of equipment, and value of each IT item will be established and maintained.*

3. *A procedure will be established, in Accordance with the Internal Control Act, Chpt. 647 of the Acts of 1989 that will account for the proper reporting to the OSA regarding any lost, stolen, or missing IT items. This procedure will include notification the OSA if the item is recovered.*

4. *All IT items received at the college will be properly inventoried and tagged, including items that are a gift to the college and items that are free to the college.*

5. *A reconciliation of the annual physical inventory will be performed. In addition, periodic reconciliations of the inventory record including accounting for inter-office transfers of computer equipment will be performed.*

6. *A procedure will be established to account for, manage, and report on assets that are required to be returned to the college by employees who end their employment, prior to their leaving the college.*

2. Prior IT Audit Results Resolved – Disaster Recovery and Business Continuity Planning

Our prior audit indicated that FSC did not have a comprehensive disaster recovery and business continuity plan to provide reasonable assurance that mission-critical and essential data processing operations for administrative and academic functions could be regained effectively and in a timely manner should a disaster render automated systems inoperable.

Our follow-up review indicated that FSC had adequately resolved this prior issue. Specifically, FSC had a formal business continuity plan to help ensure the resumption of mission-critical and essential processing should IT systems be rendered inoperable or inaccessible.