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. 2005-0179-4T

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

July 1, 2003 through October 14, 2005

OFFICIAL AUDIT REPORT

JANUARY 13, 2006

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 Master's levels. FSC also offers continuing education programs on a full-time and part-time basis. Chapter 15A, Section 5, of the Massachusetts General Laws (MGL) created the Massachusetts State College System of which Framingham State College is a member.

Framingham State College'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. The College is located on State Street in Framingham and its fifteen buildings on 73 acres of land include a Campus Center, six student residence halls, a state-of-the-art Planetarium, and an Athletic and Recreation Center. At the time of our audit, FSC had a total enrollment of 6,156 students: 3,892 undergraduates and 2,264 graduate students. At that time, the College employed 460 full-time and part-time faculty, administrators, and staff members and was supported by a fiscal year 2005 budget of approximately $57 million.

Framingham State College's administrative and academic mission and operations are supported by the automated services provided by the College's Information Technology (IT) Division. The IT Division, which has planning, delivery, and operating responsibility for all computing, telecommunications, media, and data administration resources for the College, 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, the IT Division was comprised of 23 staff members, with each of these five departments having a director/associate director under the direct control of a Chief Information Technology Officer, who reports directly to the College's Vice President for Administration and Finance. The IT Division provided 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. The IT Division also supports a campus-wide network and client infrastructure (FSC network), consisting of 34 servers that are configured on a Windows 2000 local area network (LAN) for use throughout the College, including the eighteen computer labs and classrooms. Recent upgrades to the College's network infrastructure now allow users more bandwidth and wireless network connectivity. The College has more than 2,600 workstations, including 1,386 notebook computers.

From an administrative perspective, IT-related systems are used to process the College's financial management, administrative, and student information activities. In this area, the primary application is the Ingres System. This system functions as FSC's database and application server for all administrative systems, including student and administrative financial accounting, student registration, admissions, course schedules, degree credits, and human resource management. The College also has access to the State Human Resource Compensation Management System (HR/CMS) and the Massachusetts Management Accounting and Reporting System (MMARS).

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

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

In accordance with Chapter 11, Section 12, of the Massachusetts General Laws, we performed an information technology (IT) general controls examination of IT-related activities at the Framingham State College (FSC) for the period of July 1, 2003 through October 14, 2005. The audit was conducted from May 2, 2005 through October 14, 2005. Our audit scope included an examination of IT-related controls pertaining to organization and management, physical security, environmental protection, system access security, inventory control over IT equipment, disaster recovery and business continuity planning, on-site and off-site backup of magnetic media, and IT-related contract management.

Audit Objectives

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

Our audit objective regarding organization and management was to determine whether IT-related roles and responsibilities were clearly defined, points of accountability were established, appropriate organizational controls were in place, and whether IT-related policies and procedures adequately addressed the areas under review. We also sought to determine whether FSC had implemented IT-related strategic and tactical plans that help direct the use of technology to fulfill the College's mission and goals. 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. We determined whether sufficient environmental protection controls were in place to prevent and detect damage or loss of computer equipment and magnetic media residing on the systems.

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

With regard to inventory control over IT equipment, including notebook computers, we evaluated whether an annual physical inventory and reconciliation was conducted and whether IT equipment was accurately reflected, accounted for, and properly maintained in the system of record.

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

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

Audit Methodology

To determine our audit scope and objectives, we obtained an understanding of FSC's mission, organizational structure, and primary business functions. We conducted pre-audit work, which included obtaining and recording an understanding of relevant operations, performing a preliminary review and evaluation of IT-related internal controls, and interviewing senior management to discuss the College's control environment. Subsequently, we documented the significant functions and activities supported by the automated systems and reviewed automated functions related to operations designated as mission-critical or essential. We performed a preliminary walkthrough of the data center and selected administrative offices within the College's main campus. We performed a risk analysis of IT operations and selected applications in order to select areas to be reviewed. Further, we reviewed relevant documents, such as FSC's Administrative Management Systems and Business Process Analysis, and performed selected preliminary audit tests.

Regarding our review of IT organization and management, we interviewed senior management, completed questionnaires, and analyzed and reviewed the organizational structure and reporting lines of the College's IT Department. We obtained, reviewed, and analyzed relevant IT-related policies and procedures and strategic and tactical plans to determine their adequacy. To determine whether FSC's IT-related job descriptions and job specifications were up-to-date and reflected current responsibilities and technological expertise requirements, we obtained a current list of the personnel employed by the IT Department, which included their duties and job descriptions, and compared the list to the IT Department's organizational chart, each employee's statements concerning their day-to-day IT-related responsibilities, and the technology in use at the time.

To evaluate physical security, we determined whether procedures were in place and in effect to help prevent unauthorized persons from gaining access to computer facilities and selected areas housing IT resources, and whether authorized personnel were specifically instructed in physical security policies and procedures. Our review included the completion of a risk analysis questionnaire and interviews with the College's senior management and the FSC Police Department, hereinafter referred to as the Campus Police, responsible for physical security for IT computer equipment. We assessed the College's physical security program and determined the extent to which physical access was restricted for areas housing IT computer equipment by conducting a walkthrough of the data center, classroom labs, business offices, on-site and off-site storage areas, and selected telecommunication closets. We examined the existence of controls, such as the electronic keycard system, motion detectors, and intrusion alarms. To evaluate physical security over the electronic keycard system, we completed a keycard system questionnaire and interviewed College personnel regarding the procedures used in gaining an electronic keycard to access the data center, administrative offices, computer labs, and other areas housing IT computer equipment. We obtained an electronic keycard listing and compared all of the cardholders to an FSC employment listing to verify that all cardholders were current employees of the College.

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

To determine whether system access security controls were in place to provide reasonable assurance that only personnel authorized to use FSC's network and microcomputer systems were able to gain access to programs and data files, we evaluated the College access security policies and procedures. To determine whether system access security was being properly maintained through the management of user IDs, passwords, and user access profiles, we interviewed the security administrator and assessed the level of access security being provided. We determined whether procedures were in place to ensure that the security administrator is promptly and properly notified of changes in personnel status (e.g., employment termination, job transfer, or leave of absence) so that user IDs and passwords could be promptly deactivated from the system or the access privileges be appropriately modified. To determine whether access privileges were provided to only authorized users, we compared records of the College's employees authorized to use automated systems, including all current employees and any adjunct faculty or others affiliated with FSC, to a list of authorized FSC campus network domain and Ingres system users. We also determined whether all persons authorized to access the automated systems were aware of the College's password controls including password composition, required password length, and frequency of change.

To determine whether adequate controls were in place and in effect to properly account for FSC's computer equipment, we reviewed inventory control policies and procedures and requested and obtained the College's inventory system of record for computer equipment. We reviewed the current system of record to determine whether it contained appropriate data fields to identify, describe, and indicate the value, location, and condition of the IT-related fixed assets. We also performed a data analysis on the inventory and made note of any distribution characteristics, duplicate records, unusual data elements, and missing values. To determine whether the system of record for computer equipment dated May 9, 2005, valued at $3,527,750, was current, accurate, complete, and valid, we used Audit Command Language (ACL) to select a statistical sample of 285 items with an associated value of $372,677 out of a total population of 2,265 items in order to achieve a 98% confidence level. We traced the inventory tags and serial numbers of the hardware items listed on the inventory record to the actual equipment on hand. Further, to verify the relevance and completeness of FSC's system of record for IT related equipment, we randomly selected 61 additional computer hardware items in adjacent locations and determined whether they were properly recorded on the College's inventory record.

To determine whether selected computer hardware purchases in fiscal years 2004 and 2005 were accurately listed, we randomly selected 220 items, valued at $188,224, and verified whether the amounts recorded on the College's purchase orders and invoices could be located on the inventory system of record. To determine whether FSC had appropriate control practices in place and in effect to account for and safeguard notebook computers, we interviewed representatives from the IT and facilities department. Further, we reviewed the control form used by each area regarding their computer equipment loan policies for faculty, staff, and students, and requested for review the College's documented policies and procedures to control the assignment and use of notebook computers.

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

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

As part of our review of the adequacy of generation and storage of backup copies of magnetic media, we assessed relevant policies and procedures, as well as the adequacy of physical security and environmental protection controls for on-site and off-site storage of magnetic media. We interviewed the Senior Systems Administrator responsible for the automated live full backup of the Compaq UNIX boxes and Windows 2000 network, and we reviewed the current backup procedures in place for their adequacy and completeness. This review of the backup operation included the mission-critical Ingres application. We also inspected the on-site daily backup copies of computer media to determine the provisions for storage, the frequency of backup, and the adequacy of controls in place to protect backup media. We interviewed personnel responsible for generating and storing backup copies of electronic media to determine whether they had been formally trained in their duties, including securing and protecting media, and were aware of procedures for on-site and off-site media storage. We further sought to determine whether Technology Center personnel were cognizant of, and trained in, all procedures required to restore systems via backup media that would be required under disaster or emergency circumstances. Also, we examined the off-site storage facility that was located in another building within the campus to determine whether the area had adequate physical security and environmental controls. We reviewed the condition of the fireproof safe being used to store off-site backup media to determine whether it would help ensure that backup media would remain machine-readable for a limited period of time.

The review of IT-related contracts with third-party service providers was accomplished by analyzing policies and procedures used to help ensure that the contractors were fairly and objectively selected when FSC carried out its contractor selection process. The OSS was consulted to determine whether the incorporated vendors selected were properly registered with the Commonwealth. Regarding contract documentation, we reviewed selected contracts to ascertain that the contracts contained the original signature pages with corresponding proper signatures to ensure compliance with applicable state laws and regulations. We evaluated contract documentation provided to us by the College to determine whether contract provisions were sufficient to hold the third-party service providers accountable for delivering quality services and whether payments were made properly. Further, start dates for work under contract were verified according to dates of contract signature and compliance with contract terms.

Our audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) of the United States and generally accepted industry practices. Audit criteria used in the audit included management policies and procedures and control guidelines outlined in Control Objectives for Information and Related Technology (CobiT), as issued by the Information Systems Audit and Control Association, July 2000.

AUDIT CONCLUSION

Based on our audit at Framingham State College (FSC), we found that internal controls in place provided reasonable assurance that IT-related control objectives would be met with respect to IT organization and management, physical security, environmental protection, on-site and off-site storage of backup copies of magnetic media, and third-party provider IT service contracts. However, our audit revealed that controls needed to be implemented or enhanced to provide reasonable assurance that FSC's IT environment would include controls to limit access to only authorized users to its automated systems, properly account for and safeguard computer equipment, and ensure system availability when required. In particular, controls pertaining to hardware inventory, system access security, and disaster recovery and business continuity planning needed to be improved.

The College had a defined IT organizational structure, an established chain of command, clearly delineated reporting responsibilities, and documented job descriptions for information technology staff that reflected current responsibilities. The College had also documented IT strategic and tactical plans. With respect to the use and the safeguarding of information technology, we determined that formal policies and procedures were in existence but needed to be strengthened for physical security, system access security, and business continuity and contingency planning. The absence of sufficiently documented controls increases the risk that desired control practices will not be adequately communicated, administered, or enforced.

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

We found that adequate environmental protection, such as fire prevention and detection controls, smoke and fire detectors and alarms, and fire suppression systems such as sprinklers and fire extinguishers, were in place throughout the FSC campus. In addition, we found that an emergency generator and an uninterruptible power supply were in place for areas housing IT resources to help prevent damage to, or loss of, computer equipment. Our audit disclosed that the data center was neat and clean, general housekeeping procedures were adequate, and temperature levels within the room were appropriate. However, we determined that the data center had a portable air conditioning system that lacked appropriate humidity controls.

With respect to system access security, our audit disclosed that control practices need to be strengthened to provide reasonable assurance that only authorized users have access to the campus network domain. Certain system access security controls were in place, such as a documented responsible use policy, a detailed control process for authorizing access, and a single point of accountability for access security through a Security Administrator. Our test revealed that all Ingres system users were current employees. We also determined that FSC had implemented certain procedures regarding deactivation of logon ID's, passwords, and user access profiles. However, campus network domain user accounts were found to be active for 246 individuals no longer employed by the College. We noted that a number of these individuals with active campus network domain user accounts had been separated from the College for over three years. In addition, documentation of stated control practices with respect to policies and procedures for monitoring user privileges and password administration and configuration needed to be enhanced.

Our audit revealed that FSC could not provide reasonable assurance that the inventory system of record for computer equipment, with a listed value of $3,527,750, 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. We found IT purchases made during fiscal years 2004 and 2005 were included in the inventory system of record and our data analysis of the entire population of 2,265 IT hardware items indicated that there were no missing fields of information with respect to asset number, location, model and serial number, and value. Our test of 61 hardware items, traced from multiple physical locations back to the inventory listing, indicated that all of the selected items were on the inventory list. However, our inventory test of 131 items, totaling $151,010, indicated that 37 pieces of computer equipment, totaling $30,946, could not be located. Furthermore, an inventory test of 154 notebook computers, totaling $221,667, indicated that 23 notebook computers, totaling $43,097, could not be found. We found that FSC did not adequately maintain its records for computer equipment loaned to administrators and faculty. Our test disclosed that FSC did not have supporting documentation regarding the annual renewal of assigned computer equipment for 200 items.

Regarding surplus property and equipment, our audit revealed that although FSC was aware of the Operational Services Division's (OSD) policy and procedures, the College was not in full compliance. During the course of our audit, we determined that items designated for surplus, for over 16 months by the College, had not been submitted to OSD for approval, and that several designated surplus items were still on the inventory listing. We found that, although FSC's Internal Control policies included control and reporting requirements set forth in Chapter 647 of the Acts of 1989, our audit revealed that the College did not comply with the requirements of Chapter 647 of the Acts of 1989 when FSC had failed to notify the Office of the State Auditor of approximately $11,800 of stolen computer equipment.

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

Regarding IT-related contracts with third-party vendors, we found that the College exercised adequate management oversight to hold contracted parties sufficiently accountable for their performance and delivery of services. Regarding contract documentation for our selected test sample, we found all original signature pages contained only authorized signatures as well as compliance with all applicable state laws and regulations. However, the College needed to have vendors better document their deliverables in order to adequately measure results against the accepted stated goals of the contract and to complete established initiatives within scheduled timelines. In addition, our audit disclosed that three of the 22 vendors that we tested for corporate registration were not registered with the Office of the Secretary of State to conduct business within the Commonwealth, as required by Massachusetts General Laws (MGL), Chapter 181, Section 4, which requires the registration of foreign corporations within ten days of commencing business within the Commonwealth.

AUDIT RESULTS

1. System Access Security

Our audit disclosed that although certain system access security controls were in place, other control practices needed to be enhanced to provide reasonable assurance that only authorized users have access to Framingham State College's (FSC) local area network (FSC network) for administrative systems. The Campus Network allows users to access automated systems, such as the mission-critical Ingres application system, that are used by the College to support its mission. We found that control practices needed to be implemented or strengthened regarding the deactivation/deletion of logon IDs and passwords, frequency of required password changes, and the degree of documented access security policies and procedures.

Regarding authorization, we determined that control procedures granting users access to the Ingres application system were generally adequate. We found that FSC had an established process for authorizing new employees to access the Campus Network and Ingres application. The documented procedures indicated that the IT Division would be notified of new employee hiring by the Human Resources Department together with information regarding the individual's position and assigned department. Based on this input, which is deemed as authorization for system access, the IT Division establishes e-mail and login accounts for the new users. If the new employee were an Ingres application user, the IT Division would assess the user's system needs, assign a security class, and configure an appropriate level of access to the Ingres application system. Regarding password administration, the College had written procedures in place for the requesting, approval, and assignment of new passwords for all automated systems and had required users to complete an "Application for Access to Information Systems and Services Form" in order to be assigned a user ID and password. However, we determined that FSC management did not require a mandatory timeframe for changing passwords, limit the number of invalid access attempts, and identify, log, or investigate terminal access violations.

With respect to procedures to deactivate access privileges, our audit revealed that FSC had no written policies and procedures in place to provide reasonable assurance that access privileges would be deactivated for users no longer authorized or needing access to the Campus Network and Ingres application system.

We obtained the computer system access lists for the Campus Network and the Ingres application and reviewed and compared these lists against the most current FSC personnel listing, dated July 2005. Our audit tests concerning the Campus Network indicated that of the 742 authorized users, 246 (33%) were individuals no longer associated with the College, some for over 35 months. We notified the Campus Network system administrator who subsequently disabled all 246 users from the system. It should be noted that for the entire

246 Campus Network user accounts that were still active past their respective separation date, there was no evidence that any of these accounts had been used after the individual's departure from the College. However, the failure to deactivate user accounts in a timely manner places the College at risk of unauthorized use of established privileges, such as using another individual's user account having higher access privileges, or to unauthorized access. Our audit test concerning the Ingres system indicated that of the 203 users, one individual could not be associated with active personnel within the College. Subsequent to our review, the Ingres system administrator disabled the user account for the individual no longer employed by FSC. Because this individual still had this active Ingres system access for over one year after separating from the College, unauthorized additions, modifications, or deletions from critical data files (e.g., student billing balances) could have occurred.

Access to computer systems, program applications, and data files should be authorized on a need-to-know and need-to-perform, as well as a need-to-protect, basis. To ensure that only authorized access privileges are maintained, timely notification should be made to the security administrator of any changes in user status by human resource and business department heads, which could impact the individual's level of authorization and access privileges. For example, Human Resources should notify the security administrator of changes in employment status to help ensure immediate deactivation of access privileges for an employee no longer needing or authorized to have access. Our review indicated that there was evidence of initial authorization, but that procedures were not in place to inform the security administrator of changes in employment status. As a result, critical information on the College's systems may have been vulnerable to unauthorized access, alterations, or deletions.

Generally accepted computer industry standards dictate that IT resources be made available to only authorized users and that the resources be used for only authorized purposes. To help ensure that only authorized users have access to IT resources, appropriate controls also need to be implemented to prevent and detect unauthorized access by individuals, or other systems, not granted access to the resources. Sufficient security controls should be exercised to protect the confidentiality and integrity of important and sensitive data and to limit access to data and system functions to only authorized parties. Control practices should include formal procedures to ensure that users granted access privileges to automated systems are properly authorized, assigned logon IDs and passwords, and that access privileges are modified or deactivated when employee status changes. Controls should be in place to monitor user access accounts and to detect unauthorized access to IT resources. Appropriate corrective controls should be in effect to mitigate risks of unauthorized access. Overall, monitoring and evaluation mechanisms should be in place to provide assurance that control practices are in effect to address control objectives. Access security controls are also necessary to meet risks associated with the technological environment, including the Internet.

Recommendation:

We recommend that FSC evaluate the required frequency of password changes and implement a required schedule for users to change passwords periodically. We recommend that for administrative users, the College should consider requiring password changes not to exceed 60 days and that at least ten prior passwords not be available for use for each employee. In addition, to reinforce user responsibilities regarding access privileges, we recommend that the FSC require all users to sign a formal statement acknowledging the confidentiality of their passwords and commitment to protect the password from unauthorized use and/or disclosure. With respect to authorization of users to access automated systems, we recommend that FSC review all persons currently granted access to the network and Ingres application system and ensure that all users have been properly authorized. In addition, we recommend that FSC monitor users with active access privileges to the Ingres application and the Campus Network.

To strengthen deactivation procedures of logon IDs and passwords, we recommend that FSC coordinate notification by department managers and the Human Resources Department to the IT Division personnel responsible for access security administration of changes in employee status, such as terminations, extended leaves of absence, or employee transfers. Documented control practices should also help ensure that the IT Division staff is notified in a timely manner. Once notified of the change in employment status, IT Division staff should deactivate and/or delete the logon ID and password in a timely manner. Appropriate staff should be instructed regarding compliance with these policies and procedures.

We recommend that documented control practices regarding logon ID and password administration, including authorization and activation of access privileges, be included in the College's internal control plan. Policies and procedures should also include procedures for deactivation and deletion of logon IDs and passwords. We also recommend that the internal control plan address security violations, monitoring and reporting of access attempts, and follow-up procedures to address attempted and actual violations.

Auditee's Response:

> *In response to the "System Access Security" audit result, the Information Technology Services division of the College has developed policies for password frequency change and the ability to use prior passwords. Information Technology Services is also working with the Office of Human Resources and other departments to formally document policies and procedures for deactivating user account access to information systems and services for reasons of termination, extended leave, and transfer. There will be an internal security class audit conducted twice a year for all administrative users. These policies and procedures are being documented for Presidential approval, and will be implemented in conjunction with the pending conversion to a new administrative management system.*

Auditor’s Reply:

We are pleased that the College will take steps to improve controls for system access security, including the enhancement of related policies and procedures. With respect to deactivation policies and procedures, we suggest that requirements be included for notification from user departments when changes in job responsibilities necessitate modification of user access privileges. The latter would pertain to those situations where there is no transfer involved, but rather a change in assigned duties where a different level or composition of access is needed. We suggest that the College review and strengthen mechanisms for monitoring and evaluating active user accounts and password administration to ensure that access security objectives are being addressed. Furthermore, once the College has formally documented access security policies and procedures, we suggest that FSC periodically review them, to continually meet the needs of changing IT environments and risk management objectives.

2. Disaster Recovery and Business Continuity Planning

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

Without a comprehensive, formal, and tested recovery and contingency plan, the College’s ability to regain critical processing capabilities and access information related to its various application systems would be impeded. Given the absence of recovery plans, a significant disaster impacting the College’s automated systems would seriously affect the College’s ability to regain critical and important data processing operations. Business continuity and contingency planning has assumed added importance given the potential processing disruptions that could be caused by man-made events. Further, the

College had not implemented or tested a formal business continuity plan for a timely post-disaster restoration of mission-critical important business functions processed through the local area network servers, or the applications residing on the workstations.

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

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

Recommendation:

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

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

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

Auditee’s Response:

> *In response to the “Disaster Recovery and Business Continuity ” audit result, the disaster recovery plan of the College for information technology has been formally documented and expanded upon. The plan will be added to, and updated twice a year. Currently, the plan provides for the complete recovery for an event that requires the College’s primary administrative system (a.k.a. Ingres) to be relocated to another on-campus location and fully restored. The procedures documented for restoring the Ingres system have also been tested and proven to work. Other systems and services will be added to this plan according to relative priority, as determined by additional risk assessment and potential operational impact.*
>
> *An off-campus alternative site will be pursued with another state or community college, and/or a third party service provider. The College's pending decision on a new administrative management system will also shape off-campus alternate site prospects.*

Auditor’s Reply:

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

3. Inventory Control over Computer Equipment

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 Framingham State College's (FSC) inventory system of record for property and equipment. We determined that adequate controls were not in effect to ensure that a current, accurate, and complete perpetual inventory record of computer equipment was being maintained. We found that controls needed to be strengthened to provide prompt notification and update of the inventory record when equipment is 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. As a result, the integrity of the inventory system of record for computer equipment could not be adequately assured. The absence of a sufficiently reliable inventory of computer equipment hinders the College's ability to properly account for IT resources, evaluate the allocation of equipment, identify missing equipment, and meet IT configuration objectives.

Although we determined that the College 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 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, we could not find documentation to support an annual physical inventory. Also, although the College had an adequate policy and procedure for the disposal of surplus property and Chapter 647 requirements, it was not being followed by the failure to submit reports to the Operational Services Division's (OSD) State Surplus Property Officer and the Office of the State Auditor respectively.

We found that although the College'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. The College should include a 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. The inclusion of this information will help ensure that the College's IT-related computer equipment will be properly accounted for during the College's annual physical inventory. However, our audit tests performed on 220 computer hardware items, valued at $188,224 selected from invoices for fiscal years 2004 and 2005 revealed that all of these items were included in the College's inventory system of record.

The College provided an inventory system of record that listed IT-related assets as of May 9, 2005 with a total value of $3,527,750. Our inventory tests were conducted against the 2,265 IT-related assets on the inventory record. Based on a statistical sample of 131 items of computer equipment, valued at $151,010, selected from the inventory record, we verified by inspection the existence and the recorded location of the computer equipment as listed on the College's inventory record. We found that 37, or 28%, of the 131 items, valued at $30,946 that were selected from the system of record, were not at the locations as indicated on the inventory record and could not be found by the College. However, we were able to determine that three of the sample items drawn from the system of record had been designated by the College as surplus. With respect to these items, there was no documentation available to support whether the equipment was properly disposed of, in accordance with the OSD's Surplus Property policies and procedures. We also determined whether the items were properly tagged, in good condition, and whether the serial numbers affixed to the equipment were accurately recorded on the inventory system of record. Of the 94 items of computer equipment that were recorded on the inventory from the actual equipment selected, all were properly tagged, and the correct serial numbers and manufacturer were listed on the inventory. We further note that all item descriptions for the 94 items were reasonably correct. Furthermore, to verify the integrity and completeness of the inventory system for computer equipment, we randomly selected 61 additional items of computer equipment as found in actual floor locations and determined that all items were on the College's system of record. FSC's lack of a complete hardware inventory listing hinders the College's ability to properly account for available hardware systems and undermines its ability to detect missing or stolen equipment.

We found that FSC lacked adequate policies and procedures for the allocation and assignment of IT resources, including notebook computers. We found that the computer equipment loan program that is administered by the College library appeared to be well-managed with an appropriate sign-out form for students to request equipment for a short duration. However, the process and forms used to sign-out computer equipment for faculty and staff should be strengthened. Our audit disclosed that although the College had a policy in place regarding the assignment of equipment to faculty and staff, the College failed to renew and complete an annual agreement form, signed by the user, regarding the responsibilities and acceptable usage for personally-assigned IT computer equipment. Our review of selected annual loan agreement forms indicated that over 200 IT items used for faculty and staff had not been completed and signed by the person assigned the equipment. As a result of not monitoring the responsibility for computer equipment, both the security for ensuring proper use of the equipment and recovering the item from its user could be hindered.

FSC's lack of a centralized policy to control IT resources also hindered the College's ability to properly account for available hardware systems, undermined its ability to determine whether IT resources were properly allocated to users, and decreased the opportunity for recovery from an assigned user in the event of loss or theft of these assets. In addition, our audit test of notebook computers indicated that of the 154 notebook computers tested totaling $221,667, a total of 23 notebook computers totaling $43,097 could not be found.

Our audit further indicated that FSC's monitoring of IT equipment inventory needed to be strengthened. Specifically, FSC's senior management has not performed an annual physical inventory during our audit period and could not provide verification records supporting any annual physical inventory nor a reconciliation of IT-related equipment to the College's inventory system of record. The absence of documented policies and procedures regarding inventory verification hindered the College's ability to ensure the integrity of its inventory system of record as it pertained to IT-related assets.

Our examination of computer equipment that had been designated as surplus property indicated that the College had not complied with the Commonwealth of Massachusetts regulations for the disposal of surplus equipment. Although adequate documentation was in place to support the initial request to obtain approval from the State Surplus Property Officer, the College had failed to submit the documentation to OSD for approval, as outlined in the Surplus Property policies and procedures. An audit test of 30 surplus IT items disclosed that four items tested were still on the inventory listing. We found that the College needed to enhance its documented policies and procedures regarding the steps to be followed in designating computer equipment as surplus and in disposing of it.

Our audit revealed that the College had not complied with Chapter 647 of the Acts of 1989 by failing to submit reports to the Office of the State Auditor of lost or stolen equipment. We determined that six incident reports over the audit period for missing or stolen IT equipment, valued at $11,809, had been filed with the Campus Police. However, no reports regarding these incidents had been forwarded to the 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. Chapter 647 of the Acts of 1989, states, in part, that "… the agency shall be responsible for maintaining accountability for the custody and use of resources and [shall] assign qualified individuals for that purpose, and [that] 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." Moreover, the Office of the State Comptroller's (OSC) "Internal Control Guide for Departments," promulgated under Chapter 647 of the Acts of 1989, notes that fixed assets should be accounted for per existing regulations, that they be safeguarded to ensure that they are being used as intended, and that a property officer be designated to manage the College's inventory system of record. During the course of our audit, we determined that the College did not report to our Office any computer equipment that had been lost or stolen as required by Chapter 647.

Recommendation:

To ensure that the inventory of IT resources is adequately maintained, we recommend that the College strengthen current practices to ensure compliance with policies and procedures documented in the Office of the State Comptroller's "MMARS Fixed Asset Subsystem Policy Manual and User Guide," and its associated internal control documentation, and the Operational Services Division's guidelines regarding the accounting for and disposal of property and equipment.

We recommend that the College perform an annual physical inventory and reconciliation 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, acquisition, and disposal records. To maintain proper internal control, the periodic reconciliation should be performed by staff who are not responsible for maintaining the inventory system of record. 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.

We recommend items that have been transferred to surplus property, traded in for new equipment, or donated should be deemed obsolete and deleted from the master inventory listing in a timely manner. The College should consider the use of the inventory/asset management module in the integrated accounting information system that is currently installed. In addition, we recommend that the inventory 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 believe that it would benefit the College to use a single inventory system to support inventory and IT configuration management requirements. We recommend that the College management use the Internal Control Act, Chapter 647 of the Acts of 1989, as a guide for establishing inventory controls regarding the safeguarding of, accounting for, and reporting on IT-related resources. The College should formalize a process for notifying the appropriate individual responsible for maintaining the IT system of record of any lost, stolen, or missing items.

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. In addition, the College should consider including data fields that record information related to hardware or software maintenance and whether the IT resource is a core requirement for disaster recovery and business continuity planning. We also recommend that all IT resources be included on the inventory to support IT configuration management objectives. 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 the College to produce a complete record of all IT-related equipment on a perpetual basis. The College's inventory records should reflect any changes to computer hardware items, including location or status, for both deployed equipment and items held in storage.

With respect to notebook computers, we recommend that FSC monitor and enforce current policies requiring users who are assigned notebook computers or other IT resources to sign an annual appropriate and acceptable usage form. The responsible parties' information should be recorded and updated on the inventory system of record. The College should maintain a register of all equipment that is signed out. Procedures to support College policies should be documented, implemented, and monitored to help ensure that equipment is used for approved purposes and that appropriate security measures are taken to reduce the risk of loss, theft, or misuse of equipment.

Auditee's Response:

> *Framingham State College has initiated a change in policy and procedures to better comply with the recommendations set forth in the audit document. Authorization to proceed with modifications to the current procedures has been given and more stringent controls have been developed for oversight of fixed asset/inventory management. It is expected/intended that the Administrative Management System soon to be purchased by the College will include Fixed Asset/Property Management Software that will be utilized to better control and document all College property.*

Auditor's Reply:

We commend the actions initiated by FSC to improve fixed-asset inventory controls. We believe a single comprehensive inventory control system for all fixed assets located throughout the College is an important ingredient for the College's overall internal control structure. Strengthening inventory control procedures will improve the integrity of the system of record regarding fixed assets and assist the College in making IT infrastructure and configuration management decisions. We believe that controls to ensure adequate accounting of fixed assets will be strengthened by perpetually updating the inventory record when changes in status or location occur and then routinely, or on a cyclical basis, reconciling the physical inventory to the system of record.