A. JOSEPH DeNUCCI
AUDITOR

The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH
ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108
TEL. (617) 727-6200

No. 2003-0177-4T

OFFICE OF THE STATE AUDITOR'S
REPORT ON THE EXAMINATION OF
INFORMATION TECHNOLOGY-RELATED CONTROLS
AT BRIDGEWATER STATE COLLEGE

July 1, 2002 Through June 3, 2003

OFFICIAL AUDIT REPORT
NOVEMBER 28, 2003

2003-0177-4T

TABLE OF CONTENTS

INTRODUCTION

Bridgewater State College (BSC), which was established in 1840, is a comprehensive public college of liberal arts and professional programs, offering undergraduate, graduate, and continuing education programs on a full-time and part-time basis. BSC is a member of the Massachusetts State College System and is regulated by Chapter 15A, Section 5, of the Massachusetts General Laws (MGL).

Bridgewater State College's primary mission is to educate the residents of southeastern Massachusetts and the Commonwealth and to use its intellectual, scientific and technological resources to support and advance the economic and cultural life of the region and the state. Four Schools administer the College's programs: the School of Arts and Sciences, the School of Education and Allied Studies, the School of Management and Aviation Studies, and the School of Graduate and Continuing Education. The College is located on Summer Street in Bridgewater and consists of 33 academic, residential, and service buildings on 235 acres of land. At the time of our audit, BSC had a total enrollment of 9,561 students: 7,434 undergraduates and 2,127 graduate students. At that time, the College employed 784 full-time and part-time faculty, administrators, and staff members and was supported by a fiscal year 2003 budget of approximately $82 million.

Bridgewater State College's administrative and academic mission and operations are supported by the automated services provided by the College's Information Technology 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 four departments: College Information Systems, Technical Services, Telecommunications, and User Support and Academic Services. At the time of our audit, the IT Division was comprised of 47 staff members, with each of these four departments having an associate director under the direct control of a Chief Information Officer, who reports directly to the College's President. The IT Division, inclusive of these four departments, manages and 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. The IT Division also provides a campus-wide network and client infrastructure (BSC network), consisting of 29 servers that are configured on a Windows NT Local Area Network (LAN) for use throughout the College including the fourteen computer labs and classrooms.

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 applications are the Student Information System (SIS), the Financial Records System (FRS), and the Human Resources System (HRS). At the time of our audit, BSC was involved in a College-wide effort to replace all of its core administrative computer systems (SIS, FRS, and HRS) with a new system, called SCT Banner. The

new system is a vendor-supplied administrative software application consisting of five integrated subsystems: Finance, Student, Financial Aid, Human Resources, and General. Each of these integrated subsystems is comprised of an array of program modules. For example, the student administration system includes the admissions, registration, and academic history modules. At the time of our audit, the College was preparing to initiate Banner's financial aid subsystem that will enable the College to process student information eligibility for tuition assistance for qualified applicants. Initial project activity started on the finance, human resources, and student administration systems in May 2002 with a projected completion date of April 2004. Bridgewater State College has been ranked number 50 on Yahoo! Internet Life magazine's list of "America's Most Wired Colleges 2001". The rankings were determined by individual grades given in six broad categories, which included student resources, web portal, e-learning, tech support, wireless access and infrastructure.

The Office of the State Auditor's examination focused on an evaluation of IT-related general controls over BSC'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 Bridgewater State College (BSC) for the period of July 1, 2002 through June 3, 2003. The audit was conducted from December 3, 2002 through June 3, 2003. Our audit scope included an examination of certain general controls over and within BSC's IT-related environment regarding the extent and adequacy of documented policies and procedures, physical security, environmental protection, inventory control over IT hardware, business continuity planning, and on-site and off-site storage of backup copies of mission-critical and essential computer-related media. Our audit also included a review of the status of a prior audit result brought forward in our prior audit report, No. 96-0177-4F, issued April 30, 1997.

Audit Objectives

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

We sought to determine whether adequate IT-related controls were in place to provide reasonable assurance that IT-related resources would be safeguarded, properly accounted for and available when required. We sought to determine whether adequate physical security and environmental protection controls were in place and in effect to restrict IT access to only authorized personnel and to provide an appropriate processing environment to prevent unauthorized use, damage, or loss of IT resources.

With respect to the availability of automated processing capabilities and access to electronic information resources, we determined 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 conjunction with our review of the IT environment, we sought to determine whether BSC had implemented IT-related tactical plans that help to fulfill the College's mission and goals and whether the College appointed a Readiness Team responsible for developing and maintaining the disaster recovery plan, managing the disaster recovery activities, and ensuring the continued viability of the plan. Further, we sought to determine whether adequate control procedures were in place regarding on-site and off-site storage of backup copies of computer-related media.

We sought to determine whether adequate controls were in place and in effect to provide reasonable assurance that the College's IT hardware was properly recorded and accounted for in the College's records and safeguarded against unauthorized use, theft, or damage. As part of our review of inventory control, we also sought to determine if BSC had taken corrective action to resolve the audit result related to fixed assets presented in our prior IT audit report No. 96-0177-4F, issued on April 30, 1997.

Audit Methodology

To determine the areas to be examined, we conducted pre-audit work, which included a review of relevant enabling legislation, prior audit results, and existing IT policies and procedures. We obtained and recorded an understanding of the College's IT-related operations including its mission and business objectives. We reviewed and evaluated the general IT-related internal control environment at the College and conducted interviews with senior management regarding BSC's control environment.

In conjunction with our review of the IT internal control environment, we assessed the extent to which BSC had developed, implemented, and documented formal IT-related internal control policies and procedures. We completed an IT-related internal control risk analysis to identify any potential IT environment risks. We interviewed senior management; obtained and reviewed selected IT-related policies, standards, and procedures; assessed the adequacy of IT-related strategic and tactical plans; and assessed IT-related management control practices related to our audit.

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 whether authorized personnel were specifically instructed in physical security operational policies and procedures. We reviewed potential risk factors regarding physical security through inspection of the computer facility, hub networking closets, and student labs. Our review also included a completion of a risk analysis questionnaire, and interviews with the College's management and staff responsible for physical security for IT resources. We assessed the College's physical security program and determined the extent to which physical access was restricted for areas housing IT resources by conducting a walk-through of the computer and server room, hub networking closets, classroom labs, business offices, and the on-site storage area. We obtained and reviewed a list of employees who were authorized to access the College's computer and server room and verified that they were IT personnel by comparing the names to the College's current employee and positional listing. Also, through observation and review, we determined the adequacy of physical security controls by confirming door locks were being used, visitor logs were being maintained, and intrusion alarms were installed and working. We determined whether the College's equipment, including that housed in closets containing network hubs and switches, was adequately safeguarded from unauthorized use, theft, or damage.

To determine the adequacy of environmental protection, we conducted a walk-through of the computer and file server room and assessed the sufficiency of environmental protection-related policies and procedures for the computer and file server room, classroom labs, hub networking closets, and the on-site media storage area. During the audit, we determined and verified the presence of certain environmental protection controls, such as heat, water, smoke detectors; fire-suppression measures; uninterruptible power supply; and shut down procedures regarding the Compaq Alpha servers and workstations. We determined whether individuals identified as being authorized to access areas housing computer equipment were either administrative, faculty, staff, or students of the College.

To determine whether adequate controls were in place and in effect to properly account for BSC's IT-related property and equipment, we reviewed inventory control policies and procedures for hardware. We requested and obtained the College's inventory system of record for hardware items. We reviewed the current system of record to determine whether it contained the appropriate data fields to identify, describe, and indicate the value, location, and condition of the IT-related fixed assets. To determine whether the records regarding hardware for calendar year 2002, valued at $7,362,612, were current, accurate, complete and valid, we used Audit Command Language (ACL) to select a statistical sample of 73 items with an associated value of $175,969 out of a total population of 2,007 items in order to achieve a 95% confidence level. We traced the inventory tags and serial numbers of the hardware items listed on the inventory record to the actual equipment on hand. In addition, to determine the validity of the system of record, we reviewed the physical location and description of the hardware items selected in our test. After our initial tests of the hardware inventory indicated a higher rate of errors than expected, we informed the College of our results. As a result, the College decided to perform a complete reconciliation of the hardware inventory. Following the reconciliation and subsequent adjustments to the inventory record, we compared the IT-related system of record, dated December 2002, against the corrected system of record that was dated May 2003. We also compared the IT-related system of record to BSC's discarded property inventory list, dated June 2002, to determine whether data records of assets surplused were properly removed from the IT fixed-assets system of record and to identify any variances. To further assess the degree of completeness of the system of record, we selected BSC's purchase orders pertaining to IT acquisitions made during the first six months of fiscal year 2003, and determined whether the equipment was properly and completely recorded on the inventory record.

To assess the adequacy of disaster recovery and business continuity planning, we determined whether formal planning had been performed to provide for the timely resumption of computer operations in the event that the automated systems become inoperable or inaccessible. In addition, we determined whether BSC had assessed the criticality of application systems and whether risks and exposures to computer operations had been evaluated. 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 storage of magnetic media. We interviewed the Senior Systems Administrator responsible for the automated live full backup of the Compaq Alpha servers and Windows NT network, and we reviewed the current back-up procedures in place for their adequacy and completeness. This review of the backup operation included the mission-critical FRS, SIS, and HRS legacy application systems. We 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. In addition, we interviewed designated personnel to determine whether they had been formally trained in the procedures for generating backup copies and were aware of the procedures for on-site and off-site storage and the steps required ensuring the protection and safety of the backup media. We further sought to determine whether designated College 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. Although we did not review the off-site storage facility, we did confirm the College was using an established third-party vendor that has done business with numerous state agencies.

The audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) and industry auditing standards.

AUDIT CONCLUSIONS

Based on our audit, we found that information technology-related controls in place at Bridgewater State College provided reasonable assurance that control objectives regarding generation and on-site storage of backup media, physical security, and environmental protection would be met. In addition, we determined that control practices and procedures for the generation of off-site backup media were adequate. We found, however, that sufficient control practices were not in place to provide reasonable assurance that the IT-related hardware was properly accounted for in College records. Regarding availability of systems, we determined that control practices needed to be strengthened to provide reasonable assurance that normal business operations could be resumed at the College in a timely manner should the LAN, file servers, and microcomputer workstations be unavailable for an extended period.

Our audit revealed that adequate physical security and environmental protection were being provided for BSC's IT-related assets. In this regard, we found that areas housing IT resources were appropriately secured and alarmed, fire detection and suppression controls were in place, processing areas were well maintained, a fire emergency plan was in place and posted, and appropriate air quality was afforded to the computer and file server room.

With respect to recovery strategies and contingency plans, we found that the College, although possessing some elements of a business continuity strategy, did not have a formal, tested business continuity plan for the timely restoration of business functions provided by automated systems to be used in the event that IT resources are rendered inoperable. With regard to the continued availability of computer operations and access to electronic information, we found that the draft version of the business continuity plan needed to be formalized and strengthened. Without sufficient business continuity planning, a possible long-term loss of the College's computer operations could hinder access to processing capabilities and electronic information needed to perform business functions. Although the College generated and stored backup copies of magnetic media at their on-site and off-site locations, the College had not designated an alternate processing site.

Our audit of the IT-related resources revealed that although the College had developed policies and procedures regarding fixed-asset control for IT-related inventory, they were not sufficiently comprehensive as to include a reporting requirement of Chapter 647 the Acts of 1989 stipulating that "All unaccounted for variances, losses, shortages, or theft of funds or property shall be immediately reported to the State Auditor's Office." Also, we determined that the established procedures for fixed-asset control were not consistently monitored and evaluated for compliance. As a result, the College could not provide reasonable assurance that its system of record for IT-related resources, with a listed value of $7.3 million, could be relied upon. Based on our examination, we found that increased effort was needed to ensure that the College's system of record properly accounted for IT hardware. Our audit test, drawn from a

statistical sample of IT-related items from the inventory, dated December 2002, indicated that certain microcomputers were incorrectly tagged and there were instances where the locations of the items on the listing were incorrect. Based upon our sample of 73 items, eight workstations were found at different locations than indicated on the master inventory listing, seven workstations had been surplused and disposed of by the College, and three workstations were leased items and had been returned to the vendor. We found that 180 microcomputer systems that had been leased in October 2002, at a leased cost of $80,166, were not recorded on the College's reconciled inventory record of May 2003. We determined that microcomputer systems previously designated as surplus property had not been either identified as "to be placed in surplus" on the inventory record or removed from the record when the equipment was placed in surplus. The number and cost of these computers could not be determined from BSC records. During the course of the audit, we had recommended that the College perform an annual physical inventory and reconciliation of the inventory record. Toward the end of our audit, the College performed a physical inventory reconciliation of IT hardware and, as a result, acknowledged that 639 items with an historical value of approximately $934,000 should have been removed from the system of record. In addition, upon completion of the physical inventory reconciliation, the College agreed to make all appropriate corrections to the system of record.

AUDIT RESULTS

1. Inventory Control over IT Hardware

Our current audit revealed that although an automated inventory system had been installed and implemented as recommended in our prior report, No. 96-0177-4F, an annual physical inventory and reconciliation was not being performed in a timely manner in order to assist in verifying the accuracy and completeness of the master inventory record. As a result, BSC was unable to adequately ensure the integrity of its inventory system of record as it pertained to IT-related assets or to ensure that inventory records could be effectively used to help safeguard computer hardware. In turn, the absence of a complete hardware inventory may hinder the College's ability to properly account for available hardware systems, undermine its ability to determine whether it is properly allocated to users and weaken configuration management decisions.

Although we determined that the College had documented internal controls regarding the purchasing and receiving of IT-related fixed-asset items, including a comprehensive system to properly record, report, and maintain an inventory system of record, we found the College did not monitor compliance over inventory controls for its IT-related fixed assets as recommended in our prior audit report. Additionally, although documented procedures were in place requiring periodic review, evaluation, and reconciliation of the system of record of IT-related assets, these procedures were not being followed. Although we found appropriate data fields regarding the fixed-asset inventory records, such as date of acquisition, location, description, serial number, and asset value, attributes to support IT configuration management, such as condition, surplus, and obsolescence, were not included.

Bridgewater State College provided us with a master inventory system of record that listed IT hardware as of December 2002 with a total value of $7.3 million. Our inventory tests conducted against the IT-related hardware master inventory record indicated that a number of locations for the items on the listing were incorrect and not all new equipment was being recorded on a timely basis. For example, IT-related fixed assets, received during the first six months of fiscal year 2003 by the College, were not recorded in a timely manner by the BSC’s comptroller’s office for input into the FRS.

We selected four campus locations for inventory testing, representing approximately 70% of the hardware inventory valued at the time of our audit at $5.2 million. Our data analysis using audit software of the College’s system of record or master inventory file indicated that:

- 141 items had no acquisition date;
- 76 items had been incorrectly classified as “misplaced”;
- 10 items had the same serial number;
- 6 items had no serial number; and
- 4 items had the same bar code.

We determined that, contrary to the requirements of the Office of the State Comptroller's (OSC) "MMARS Fixed Asset Subsystem Policy Manual and User Guide," BSC had not consistently maintained and accounted for all fixed-asset transactions, including the proper recording and reconciliation of Non-Generally Accepted Accounting Principles (non-GAAP) Fixed Assets. Non-GAAP Fixed Assets are defined as assets, including computer software and electrical and computer components with a historical cost between $1,000 and $49,999. Our audit tests of 26 IT-related items going from floor to the inventory list disclosed that nine microcomputer systems (35%) could not be traced back from their physical location to the master inventory listing. A test performed on IT-related purchases from October 2002 revealed that these nine items and an additional 171 microcomputer systems with an associated cumulative value totaling $80,166 were leased items that had been received by the College, but had not been posted on the College's reconciled system of record, dated May 2003.

Based on a statistical sample of 73 items with a value of $175,968, we determined that thirteen items (18% error rate) valued at $21,651 could not be located within the College and eight items valued at $14,378 were found in locations other than those stated on the inventory record. Interviews with senior management and staff indicated that these 13 items and at least 14% of the current hardware inventory system of record that was valued in total at the time of our audit at $7.3 million, had either been traded in to vendors for new equipment, state surplused and then discarded to a local recycling company, or donated to other state agencies. Toward the end of our audit, upon our recommendation, the College performed a physical inventory reconciliation of IT hardware and, as a result, acknowledged that 639 items, with an historical value of approximately $934,000 should have been removed from the master file. Based on a review of the purchase orders for the equipment that had been discarded, we determined that all of the items were at least seven years in age and if the College had been depreciating these items annually, those that had not been traded in for new equipment would have had nominal, if any, market value. Although the majority of the items had been purchased with trust fund monies, some had been acquired with state funds and were therefore subject to the policies of Operational Services Division (OSD) State Surplus Property Guidelines. However, we were unable to locate all documentation supporting whether all equipment was properly disposed of as outlined in OSD's SSP policies and procedures.

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. A lack of monitoring of inventory procedures requiring the timely recording of the receipt and origin (e.g., purchase, donation, surplus,) and disposal of hardware on a perpetual basis, resulted in the master inventory record not being properly maintained and, therefore, reflecting an incorrect total inventory valuation in excess of $860,000. As a result, there was limited assurance that the College's hardware inventory was being properly recorded, reported, and safeguarded, and that sufficient controls were in effect to mitigate the risk of lost

or stolen hardware. Control measures should be in place to ensure that College personnel are aware of and understand the guidelines for hardware inventory and that compliance with College's inventory-related policies and procedures is monitored and evaluated.

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 provide controls of inventories.

Recommendation:

To ensure that the inventory of IT resources is adequately maintained, we recommend that College management strengthen their understanding of the Internal Control Act, Chapter 647 of the Acts of 1989, and that management control practices and procedures required by the Office of the State Comptroller regarding the safeguarding of, accounting for, and reporting on IT-related resources. We recommend that the College strengthen current practices to ensure compliance with policies and procedures documented in the OSC'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 a physical inventory and reconciliation of its IT resources, including computer-related equipment. Based upon OSC guidelines, the College should ensure that they have in place an accurate and complete inventory record of fixed assets, including IT resources. We recommend that a perpetual hardware inventory record be maintained and periodically verified through reconciliation to physical hardware and acquisition and disposal records. Control procedures should be implemented to ensure that all IT procurements that are accepted are included on the inventory record and that inventory data are maintained in an accurate, complete, and timely manner. The record should include IT resources installed in the College's overall IT configuration and any equipment that is available for replacement of installed items, or items to be added to the overall configuration. To maintain proper internal control, staff that are not responsible for maintaining the fixed-asset inventory record should perform the periodic reconciliation. We also recommend that BSC 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. We also recommend that the College consider using a single inventory system, namely the Banner inventory module, to support inventory and configuration management requirements for the Comptroller and IT Division.

Auditee's Response:

> *The audit identifies significant gaps in compliance with stated college policy to accurately record the location of IT assets, to enter data in a timely fashion, to update records in a timely fashion, as assets are moved or surplused, and to conduct periodic audits and reconciliations of the inventory process.*
>
> *As these problems were brought to the attention of the college early in the preliminary audit, the college implemented corrective action to bring our practices in line in these important areas. We assigned two new staff members (A. Patten and A. Andrade) to manage day-to-day data entry of new assets and to keep current all records on equipment moves and asset disposition. Records are now updated on the same day or following day of any change in asset status. A third staff member (M. Guillette) has been assigned to conduct periodic reviews of inventory practice; a fourth staff member (J. Costa) has assumed responsibility for regular audit and reconciliation of IT assets in the field. We have brought all data on assets fully up to date and corrected data entry errors in asset attributes as these have been identified.*
>
> *College management is committed to continuing to strengthen BSC inventory policy and practices to ensure effective management of Commonwealth assets.*

Auditor's Reply:

We commend the actions initiated by College to improve fixed-asset inventory control. We believe a single comprehensive inventory control system for all fixed assets, including IT resources, is an important ingredient for your overall internal control structure. Strengthening inventory control procedures will improve the integrity of the inventory system of record and enhance knowledge of the IT infrastructure. We believe that controls to ensure adequate accounting of fixed assets will be strengthened by 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. Maintenance of a perpetual inventory, coupled with routine reconciliation, should also improve the accounting for any lost, stolen, or surplused equipment. In addition, these efforts should help minimize the risk of lost or stolen equipment and improve the identification of the status of equipment for configuration management purposes.

2. Business Continuity and Contingency Planning

Our audit disclosed that although BSC had a documented disaster recovery and business continuity plan and had on-site and off-site storage of backup copies of computer media, further steps were necessary to provide reasonable assurance that automated systems can be recovered within an acceptable period of time should IT operations be rendered inoperable or inaccessible. We found that the recovery and business continuity plan had not been updated since the draft had been completed in November 2002, nor had it been formally approved or tested.

Our audit disclosed that BSC provided adequate on-site storage and provisions for the generation of off-site backup copies of mission-critical and essential software and data files. However, as of our audit completion date, the College had not formally designated an alternate processing site for IT operations should a disaster render the computer systems inoperable or inaccessible. To the College's credit, at the time of our audit, management had assessed the relative importance of their systems classifying them as either mission-critical or essential. In addition, the tasks and responsibilities necessary to address the College's mission and business objectives under various disaster scenarios for all BSC IT-related and vendor personnel, including user area plans, were documented.

Without a comprehensive disaster recovery and contingency plan, including required user area plans and communication components, information modules (e.g. general ledger, purchasing, accounts payable, billing, accounts receivable, student grades, and financial-aid related to BSC's Colleague SIS), and adequate testing, the College is at risk of not being able to recover mission-critical and essential data processing within an acceptable time should automated capabilities be severely disrupted or lost. A loss of processing capabilities could adversely affect administrative and academic functions supported by the College's IT Division. Depending on when a disaster occurred during the academic year, the impact could hamper the College's ability to function. Also, the lack of a comprehensive and tested disaster recovery plan could result in unnecessary costs and significant processing delays, including the timely issuance of student billings, and loss of good will by students as well as faculty.

Disaster recovery and business continuity plans should be tested to assess the viability of recovery strategies to enhance timely recovery, provide adequate security and content, and reduce the risk of errors and omissions when restoring computer operations. BSC's disaster recovery plan provides specific instructions for various courses of action to address different types of disaster scenarios; identifies the ways in which essential services would be provided without full use of the data processing facility and, accordingly, the manner and order in which processing resources would be restored or replaced; and identifies the policies and procedures to be followed, detailing the logical order for restoring critical data processing functions i.e., accounting programs, registration, or student transcripts would be brought on line first, either at the original site or at an alternate-processing site. In addition, the plan describes 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; but does not designate an alternate processing site.

Sound management practices, as well as industry and government standards, emphasize the need for a comprehensive business continuity strategy. Contingency planning should be incorporated with the functions of the organization, upon successful implementation of an approved plan. Due to the fact that the criticality of systems may change, a process should be in place that would identify a change in criticality and amend the contingency plans accordingly. System modifications, changes to equipment configurations, and user requirements should be assessed in terms of their impact on existing disaster recovery and contingency plans.

Recommendation:

We recommend that the disaster recovery and contingency plan be reviewed and tested to the extent possible to assess its overall viability and to determine whether the plan contains sufficient, relevant, reliable, and current information to support recovery strategies. The results of all tests should be documented and maintained to provide a sufficient management audit trail for reference. The approved disaster recovery and contingency plan should be subject to periodic review and subsequent testing along with user area plans, to help ensure continued viability. We recommend that copies of the recovery and business continuity plan, including user area plans, should be stored in the off-site location for emergency access. The plans should be communicated to all responsible parties and those individuals who are assigned disaster recovery and business continuity responsibilities and having sufficient knowledge, skills and authority to carry out their responsibilities.

To ensure that sufficient recovery plans and procedures are in place for the continued availability of mission-critical and essential IT-supported services, we recommend that a policy statement be documented and distributed outlining management's commitment regarding disaster recovery and business continuity planning. In addition, the College should provide the necessary resources to ensure that business continuity plans are developed, implemented, and maintained. The disaster recovery and contingency plan and user area plans should be periodically assessed and amended if necessary to address changes in technology, business requirements, and risks to the operational and technical environment.

The College should identify potential alternate processing sites to be utilized should a disaster disrupt its current data processing or business operations. BSC should update the disaster recovery business continuity plan to include an alternate processing site when designated and seek appropriate approval of the updated plan and, once approved, implement periodic testing of the plan and evaluate it on a continuing basis to ensure its viability.

Auditee's Response:

As this audit period commenced, BSC was in the process of drafting a new disaster recovery and business continuity plan (DR/BCP) to replace a plan from 1995 that was becoming outdated. This process was about mid-way to completion at the beginning of the audit. A full plan had been drafted and staff response teams had been identified and assigned to respond in the event of a disaster or business disruption. In addition, a full inventory of mission critical systems had been developed and acceptable recovery times were defined for each system, which the audit commends.

The college shares the perspective of the auditors of the importance of the DR/BCP process. We have made substantial progress on our planning during the time that the audit was conducted. Since the audit commenced, our initial draft plan has undergone three revisions and is now in final form, adopted as IT policy. The IT disaster response teams have met to review staff assignments in the event of an emergency and have held briefings and training sessions. We have conducted full backup and restores using off-site data, as outlined in the plan, as recovery protocol in response to disk hardware failures. We have also scheduled structured tests of the plan, to occur over the next two months during off-peak times that will be minimally disruptive to the campus community. We will continue to work aggressively with the Commonwealth Information Technology Division and other state agencies to identify appropriate and affordable contingency sites to serve as our data center in the event of a major catastrophe.

Auditor's Reply:

We are pleased that the College has developed a viable business continuity and disaster recovery plan but even after completed, the plan should be reviewed and updated annually or whenever there are significant changes to processing requirements, risks, or changes made to the College's IT infrastructure. Designation of an alternate processing site and procedures for the generation and storage of backup copies of magnetic media are an integral part of any recovery strategy and should be maintained and appropriately monitored.

Appendix A

PRIOR AUDIT RESULT

Prior Audit Result Unresolved

1. Inadequate Inventory Control of IT-related Assets

Our prior report, No. 96-0177-4F, indicated that Bridgewater State College's inventory control over IT-related assets needed to be strengthened in order to ensure proper recording and accounting of these assets. Specifically, we had found that there was no formal mechanism in place to ensure that the asset manager was notified when BSC's personnel changed the location of IT-related equipment so that inventory records could be updated accordingly.

Our current audit disclosed that by March 1998, BSC had upgraded its physical inventory system using the Universal Asset Technology System and had converted to a bar-coding system. This new system put in place a formal mechanism that would help ensure that the asset manager would be notified when BSC's personnel changed the location of IT-related equipment and by updating its perpetual inventory records to properly reflect all additions and deletions of fixed assets. However, we determined an annual physical inventory was not being performed in a timely manner in order to assist in verifying the master inventory record. As a result, BSC was unable to ensure the integrity of its perpetual inventory system of record as it pertained to IT-related assets or to ensure that inventory records could be effectively used to help safeguard computer hardware.

Auditee's Response:

> *In response to the "Prior Audit Result Unresolved" noted in Appendix A, we have implemented a new web system to ensure that all moves of IT assets are recorded in real time as equipment is installed or moved to new locations. The web interface prompts for all necessary data and routes that data to inventory control staff for confirmation and entry into the online inventory system.*

Auditor's Reply:

We commend the actions of the College in improving their inventory control and maintenance of their system of record for IT assets. The College should note that continuous monitoring and evaluations is a necessary ingredient for the success of any inventory control system.

Appendix B

GLOSSARY

FRS	Financial Records System is a legacy system that is operated by and under the direct control of Bridgewater State College.
SIS	Student Information System is a legacy system.
HRS	Human Resources System is a legacy system.
GAGAS	Generally Accepted Government Auditing Standards.
HRMIS	Human Resources Management Information Systems is a legacy system that is operated by and under the direct control of Computing and Information Technology Services (CITS), located in Hadley, Massachusetts, near the Amherst Campus.
Internet portal	A Web site that provides a variety of services including Web searching, news services, white and yellow pages directories, e-mail, discussion groups, and links to other sites.
LAN	(Local Area Network) A communications network that serves users within a confined geographical area. It is made up of one or more file servers, a network operating system, a communications link, and workstations.
Legacy application	An application system that has existed in production for some time. It often refers to mainframe and ERP applications; however, it may refer to a system that is supported by a previous generation of technology.
Network file servers	Servers are high-speed computers that hold programs and data shared by network users.
Operating system	The operating system is a set of programs required for the computer to operate and manage programs and devices, such as printers, terminals and other peripherals. Operating systems perform basic tasks, such as recognizing input from the keyboard, sending output to the display screen, keeping track of files and directories on the disk.
Workstations	The workstations are the users' personal computers, which perform stand-alone processing and access the network servers as required.
Web hosting services	Placing a customer's Web page or Web site on a Web server. Many Internet Service Providers host a personal Web page at no additional cost above the monthly service fee, but the address is subordinate to the ISP. Multi-page, commercial Web sites are hosted at a very wide range of prices, and the customer's registered domain name is often used. A single computer can hold dozens to hundreds of small Web sites, while larger Web sites use a dedicated computer or even multiple computers.
WAN	(Wide Area Network) A computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local-area

networks (LANs). Computers connected to a wide-area network are often connected through public networks, such as the telephone system. They can also be connected through leased lines or satellites. The largest WAN in existence is the Internet.