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. 2001-0201-4C

OFFICE OF THE STATE AUDITOR'S REPORT ON INFORMATION TECHNOLOGY AND FINANCIAL-RELATED CONTROLS AT NORTHERN ESSEX COMMUNITY COLLEGE

MAY 1, 1997 THROUGH JULY 20, 2001

OFFICIAL AUDIT REPORT

AUGUST 12, 2002

TABLE OF CONTENTS/EXECUTIVE SUMMARY

INTRODUCTION	**1**
AUDIT SUMMARY	**12**
AUDIT RESULTS	**17**
1. IT-RELATED CONTRACT MANAGEMENT AND OVERSIGHT	**17**
2. IT-RELATED CONTRACT EXPENSES	**37**
3. HARDWARE INVENTORY CONTROLS	**40**
4. LOGICAL ACCESS SECURITY	**42**
5. DISASTER RECOVERY AND BUSINESS CONTINUITY PLANNING	**47**
6. PHYSICAL SECURITY	**52**
7. ENVIRONMENTAL PROTECTION	**54**
APPENDIX A	**57**
Banner Subsystem and Module Status	
APPENDIX B	**60**
Information Technology (IT)-Related Third-Party Vendor Contracts	
APPENDIX C	**62**
Analysis of NECC Documentation Regarding CWI Contract Addendum 3	
APPENDIX D	**63**
Analysis of NECC Documentation Regarding CWI Contract Addendum 4	
APPENDIX E	**64**
Board of Higher Education Trust Fund Guideline Information	

INTRODUCTION

Background

Northern Essex Community College (NECC) is a Massachusetts institution of higher education offering associate degree and certificate programs. The College, which was established in 1961, is a member of the Massachusetts State College System and is regulated by Chapter 15A, Section 5, of the Massachusetts General Laws (MGL).

The College's primary mission is to provide education for residents of the Commonwealth, focusing on those from the lower Merrimack Valley. The College is located at three campus sites: Haverhill, Lawrence, and the Lawrence Extension. For the 2000-2001 student year, NECC had approximately 3,514 students in day programs and 4,015 in continuing education evening courses, with a total unduplicated student population head count of 6,580.

Northern Essex Community College is governed by a Board of Trustees and is under the direction of the College's President. Additional oversight is provided to the College by the Board of Higher Education which is responsible for monitoring each Massachusetts higher educational institution to ensure that state funds support measurable performance, productivity, and results.

From October 20 through October 23, 2000, the College was subject to a reaccreditation process by the New England Association of Schools and Colleges. All divisions of the College were reviewed with regard to eleven (11) standards and a risk assessment as part of this important process. On December 6, 2000, the College received a ten-year accreditation.

The College's fiscal year 2000 and 2001 expenditures from appropriated funds totaled $15,750,510 and $16,188,181, respectively, which were expended on employee salaries and benefits, supplies, furniture and equipment, and other outlays needed to operate NECC on a daily basis. In addition, expenditures from nonappropriated trust funds administered by the College totaled over $13,029,000 for fiscal year 2000, while as of April 18, 2001, expenditures from nonappropriated trust funds totaled over $11,534,000 for fiscal year 2001. The source of these trust funds included tuitions, fees, fines, grants, and interest income.

Expenditures of appropriated funds are to be made in accordance with various Massachusetts General Laws, as well as policy and procedure documents issued by the Secretary of the Executive Office for Administration and Finance, the Office of the State Comptroller, and the Human Resources Division. Depending upon the type of trust fund, requirements for expenditures are subject to applicable specific regulations, such as the Board of Higher Education's (BHE) "Standards for the Expenditures of Trust Funds" that set forth minimum standards for the management of trust funds. NECC's Board of Trustees is also responsible for establishing policies and procedures regarding the administration and monitoring of trust fund expenditures for the College. Additional requirements may be imposed by external sources of funds such as those from the federal government where the trust funds may be subject to regulations issued by the grantor agency.

Trust funds are used to complement state appropriations in order to help ensure sufficient funding for an institution's total needs. Typically, trust funds are used in connection with a variety of campus activities, such as auxiliary enterprises (e.g., bookstore and food services), student activities, financial aid, medical services, capital improvements, contract employees, consultants, travel, and other general expenses. Funds are received from many sources, including some that are subject to controls established by the funding entities.

The College's administrative mission and overall operations are supported by automated systems and information technology (IT) services provided by the College's Administrative Computing Information Service (ACIS) and the Division of Information Services (DIS). At the time of our audit, the ACIS was composed of six staff members and an Executive Director/Banner Project Manager who reported to the Vice President of Enrollment Management and Student Services Division and the Vice President of Administration. The ACIS provided assistance and guidance to administrative staff and instructors in the use of administrative computer-based systems.

The College's DIS provided a campus-wide network and client infrastructure (NECC network) consisting of eight network file servers, which were configured on a Novell local area network (LAN). The Novell-based LAN supported applications consisting primarily of the Microsoft suite of software products and Internet connectivity for use throughout the College, including

student computer labs. The DIS was composed of two staff members who reported to the Campus Network Director and seven staff members who reported to the Client Computing Director. The two Directors were under the direct control of the Dean of Information Technology and DIS. The Vice President of Enrollment Management and Student Services Division and ACIS and the Dean of Information Technology and DIS both report directly to the President of the College.

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 was the Student Information System (SIS), which is a vendor-supplied software product known as "Banner." Banner consists of a suite of five integrated subsystems: financial operations, alumni development, human resources, student administration, and financial aid applications. Each of these integrated subsystems is composed of modules. For example, the student administration system includes the admissions, registration, and academic history modules, while Banner's financial operations system enables the College to process checks for the College's trust fund activities.

The Banner system uses Oracle's relational-database management system (RDBMS) supporting the integration of the subsystems and reduced data redundancy. At the time of our audit, Banner was operating on a NUMA Data General UNIX (DG/UX) computer that was being supported by the ACIS. The College had a total of over 1,000 workstations, of which over 125 had the Banner software installed that allowed access to the Oracle RDBMS and Banner SIS through the NECC network. Structured Query Language (SQL*PLUS) was available to authorized users to create, store, change, retrieve, and maintain the Banner system information in Oracle. Forms are produced from information in the Oracle database using a tool called SQL*FORMS. In addition, separate from the Banner system, the College uses a nonintegrated, proprietary fixed-asset inventory system that had been purchased by the College in 1993.

The core of the IT infrastructure supporting application systems at the College is electronically connected throughout all campus locations and their associated buildings. All of NECC's eight file servers are dedicated to facilitating computer operations by allowing storage and use of

common programs and data and are connected through a wide area network (WAN). The WAN allows administrative computing access to its three different network operating systems: NUMA DG/UX (used for Oracle and SCT's "Banner" - Student Information System), Novell NetWare (used for the primary network environment, i.e., Plato, an interactive application used to evaluate a student's specific skill set in academia) and Windows NT (Web services and Web CT, a software package permitting instructors to teach on-line). Overall, the NECC network is composed of these three network operating systems. The NECC network is connected throughout the campus by an Ethernet network gateway that uses a fiber optic backbone to allow connectivity to internal and external users. The College had installed Cisco's firewall software product known as "Firewall Featureset" on the NECC network to help secure it from unauthorized access, separating the Internet (public) from the Intranet (private). An independent T1 line with its own proprietary firewall provided full connectivity to the Internet Provider University of Massachusetts (UIS).

The Office of the State Auditor's examination focused on an evaluation of IT-related general controls over NECC's computer operations and a review of certain financial-related activities.

Audit Scope

We performed an information technology (IT) general controls examination of IT activities at the Northern Essex Community College (NECC) for the period May 1, 1997 through July 20, 2001. Our audit scope included an examination of internal controls related to the organization and management of IT activities and operations, logical access security, and physical security and environmental protection over the NUMA DG/UX system, the local area network's (NECC network) file servers, and microcomputer systems connected to the NECC network.

We performed an evaluation of IT strategic planning, IT-related contract management, hardware and software inventory control, business continuity planning and disaster recovery, and on-site and off-site backup media storage. Our audit scope also included an examination of internal controls related to the acquisition of computer assets and IT-related services. In addition, our audit included a review with respect to automated financial transaction processing. The audit was conducted from October 27, 2000 to June 22, 2001.

Audit Objectives

Our primary audit objective was to determine whether adequate controls were in place and in effect to provide reasonable assurance that control objectives would be met for IT-related organization and management, contract management, logical access security, physical security, environmental protection, business continuity planning, on-site and off-site storage of backup media, and hardware and software inventory control. We sought to determine whether NECC's internal control environment, including policies, procedures, practices, and organizational structure, provided reasonable assurance that the College's business objectives would be achieved and that undesired events would be prevented or detected and corrected.

In conjunction with our review of the control environment, we determined whether the College had established a sufficient IT planning framework to generate and implement long-range strategic and short-range tactical plans to help fulfill the College's mission and goals and written and approved policies and procedures regarding the budget process for proper accounting for, authorized access to, and safeguarding of its IT-related assets, and also whether the College had appointed a steering committee to oversee the information technology department function and its activities.

We sought to evaluate whether adequate controls were in place to safeguard information against unauthorized use, disclosure, or modification and damage or loss of the data files and software residing on the College's automated systems, and further whether adequate physical security was in place to restrict access to the NUMA DG/UX system, LAN's file servers, and microcomputer systems to prevent loss of, or damage to, computer equipment or IT-related media. We also sought to determine whether adequate environmental protection controls were in place within the College's computer center and academic labs in order to prevent damage to equipment and data or other IT-related media, and whether adequate preventive and detective control measures had been established regarding computer viruses. We also sought to determine, for each relationship with a third-party IT-related service provider, whether a formal contract with sufficient detail had been defined and agreed upon. In addition, we determined whether contract services had been monitored and evaluated for the provision of adequate services and deliverables.

We sought to determine whether the College had implemented written and approved policies and procedures regarding the proper accounting for, authorized access to, and safeguarding of its IT-related assets, and in conjunction with our review of controls over fixed assets, whether hardware and software were properly accounted for and safeguarded. We assessed whether only authorized copies of software were residing on the file servers and microcomputer systems and whether controls existed to prevent and detect the existence of unauthorized or illegal copies of licensed software.

Regarding systems availability, we sought to determine whether scheduled routine and periodic hardware maintenance was being performed to reduce the frequency and impact of performance failures and whether assessments were being made regularly regarding the need for uninterruptible power supply (UPS) batteries to secure against power failures and fluctuations, and whether adequate business continuity plans were in effect to help ensure that mission-critical and essential systems could be regained within an acceptable period of time should a disaster render processing inoperable. Moreover, we sought to determine whether adequate controls were in place to provide reasonable assurance that appropriate magnetic backup copies of application systems and data files would be available on-site and off-site to support disaster recovery and business continuity planning objectives.

Audit Methodology

To determine the areas to be examined during the audit, we reviewed relevant enabling legislation and the status of issues and concerns brought forth to the College in prior audit work; obtained and recorded an understanding of the College's mission, organization, management, and business objectives; conducted interviews with senior management; and conducted a pre-audit survey and preliminary review of internal controls.

We reviewed the general IT-related internal control environment at the College, which included a review of selected documentation; interviewed senior management and staff; observed IT-related operations and areas housing IT-related assets; reviewed the administrative and academic data processing functions' organizational and management structure; and performed selected tests.

Regarding our examination of organization and management, we interviewed senior management; obtained, reviewed, and analyzed all existing IT-related policies, standards, procedures, and strategic plans to determine their adequacy; and assessed IT-related management practices. We reviewed the IT functional areas for proper span of management, unity of command, reporting lines, oversight mechanisms, and separation of duties. To determine whether NECC'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 that list to the IT Department's organizational chart, each employee's statements concerning his or her day-to-day IT-related responsibilities, and the technology in use at the time. We reviewed the College's policies and procedures for developing an IT-related budget, the IT budget process, budget line items, expenditures, and the variances between the actual and the budgeted expenses. To determine whether an IT-related steering committee was in place and operating for the purpose of providing adequate oversight of IT functions and processes across the College, we interviewed senior management, IT staff, and user department staff and reviewed meeting minutes.

To determine whether system access security controls were in place to provide reasonable assurance that only those authorized to use NECC's network and microcomputer systems were able to gain access to programs and data files, we evaluated procedures for logon user ID and password administration. We interviewed users and observed them obtaining access to the Oracle RDBMS, Banner Student Information System (SIS), Novell network, and Microsoft Outlook messaging system to understand how passwords were being utilized and operating. To determine whether user ID and password security was being properly maintained, we interviewed the security administrator and assessed the level of access security being provided. We reviewed selected user profiles and performed system tests to determine whether a user could deviate from access privileges as specified in user profiles. To determine whether access privileges were provided to only authorized users, we reviewed procedures for granting system access and compared records of the College's employees authorized to use automated systems, including all current employees and any adjunct faculty or others affiliated with NECC, to a list

of authorized NUMA DG/UX, Oracle RDBMS, and Banner system software users. We interviewed NECC IT staff members, reviewed pertinent documentation, and tested the DG/UX and Novell NetWare access procedures to determine who had control over the super-user (i.e., the system administrator) access IDs and passwords. We determined whether procedures were in place to notify NECC's acting security administrator in a timely manner of changes in personnel status (e.g., employment terminations, job transfers, or leaves of absence) that would impact access privileges and possibly require deactivation from the system.

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 standards and procedures. We reviewed potential risk factors regarding physical security through inspection of the computer facility, completion of a risk analysis, 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 sensitive areas, such as the data center, computer and server room, classroom labs, and business offices. We determined whether the College's equipment, including that housed in closets containing network hubs and the operator command console for the NUMA DG/UX, was adequately safeguarded from potential unauthorized use, theft, or damage.

To determine the adequacy of environmental protection, we conducted a walk-through of the data center and assessed the sufficiency of environmental protection-related policies and procedures for the data center, computer and file server room, computer laboratories, hub networking closets, and the on-site and off-site facilities for backup media storage. During the audit, we determined and verified the presence of certain environmental protection controls, such as heat, water, smoke detectors, fire-suppression measures, and uninterruptible power supplies for the DG/UX, file servers, and workstations.

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 NECC 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 to be used in the event of a disruption to system availability.

As part of our review of the adequacy of backup 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 backup magnetic media. We interviewed the Director of Campus Networks and the UNIX administrator responsible for the Novell network and NUMA DG/UX, respectively, regarding 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 the IT staff person responsible for the automated live backup of the entire NUMA DG/UX system, and we reviewed the process for adequacy and completeness. This review of the backup operation included the mission-critical SIS application. Further, we interviewed designated personnel to determine whether they were being formally trained in the procedures of performing backups and were aware of the procedures for on-site and off-site storage and the steps required to ensure the protection and safety of the backup media. We further sought to determine whether designated IT Department 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. We reviewed the condition of the fireproof filing cabinet being used to store on-site backup media to determine whether it provided reasonable assurance that no foreseeable disaster would render the stored data irretrievable. We also examined the Lawrence off-site storage facility to determine whether the storage area had adequate physical security and environmental protection. We analyzed the physical access security for the off-site storage facility in order to determine whether the backup files were secured from accidental or purposeful damage and unauthorized examination, removal, or disclosure of confidential information contained therein. In addition, we examined the list of inventoried backup tapes and procedures to determine whether the off-campus backup tapes were being stored in a secure location.

To determine whether adequate controls were in place and in effect to properly account for property and equipment at the College, including procedures to ensure the use of only authorized software residing on its workstations, servers, and DG/UX system, we reviewed NECC's inventory control procedures for hardware and software. We determined whether IT-related equipment was properly tagged with state identification numbers and whether the serial numbers attached to the equipment were properly recorded on the hardware inventory list. We reviewed the current inventory record layout to determine whether it contained the appropriate data fields to identify, describe, value, and indicate location and condition of the fixed assets.

Because the College was only able to provide us with the then current IT-related inventory record, dated February 14, 2001, we compared it to a selected sample of NECC purchase orders for the last four years; the Division of Information Services computer labs inventory record, completed February 22, 2001; and the NECC surplus property inventory list, completed February 14, 2001, in order to determine whether there were any variances among them. We also tested a sample of items on the inventory record to assess the record's accuracy, validity, and completeness.

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 NECC carried out its contractor selection process. The Secretary of the Commonwealth's Office was consulted to determine whether the corporate vendors selected were legally registered with the Commonwealth. Regarding contract documentation, we reviewed original signature pages for proper signatures, including corporation, partnership, trust certification, and NECC signatures, that indicate compliance with all regulations. We assessed the contract monitoring methods and functions in place at the College to determine whether they were sufficient to provide reasonable assurance that contractors consistently provided quality services and deliverables.

We evaluated contract documentation provided to us by NECC to determine whether contract provisions were sufficient to hold the third-party service provider accountable for delivering quality services and whether those services were in fact, being provided. Further, start dates for

work under contract were verified according to dates of contract signature and compliance with contract terms. We also reviewed evidence of deliverables, to the extent it was made available, to determine whether services were furnished and whether such evidence supported quality and effectiveness of services and to assess systems of service delivery. During the course of our audit, we interviewed the following third-party contractors: SCT Corporation, Data General Corporation, and Campus Works, Inc. (CWI).

The audit was conducted in accordance with applicable Generally Accepted Government Auditing Standards (GAGAS) of the United States and related industry auditing practices.

AUDIT SUMMARY

Based on the results of our audit, we found that IT-related controls provided reasonable assurance that control and operational objectives would be met for IT organization, software inventory, and on-site and off-site storage of backup media. While certain internal controls were found to be in place, controls needed to be strengthened for physical security, environmental protection, and business continuity planning to provide reasonable assurance that IT resources are safeguarded and that mission-critical and essential IT systems would be available should business continuity plans need to be activated. Regarding IT-related contract management, we found that adequate contract administration practices were in effect for all IT-related contracts, except for one contractual relationship where adequate control practices had not been exercised. Although good controls were found to be practiced over the UNIX-based system, logon and firewall-related controls needed to be strengthened to ensure an appropriate level of security to the Oracle relational database management system and the SCT Banner system. We determined that, although some controls related to the safeguarding of fixed assets were in place, controls should be strengthened to ensure that all IT assets are properly accounted for and that accurate information regarding value, location, tag number, and status is included in the inventory record for all inventory items.

Based on our audit, we believe that although a certain level of physical security and environmental protection controls were in place over and within the computer room, computer labs, business office area, and the networking hub closets, controls needed to be strengthened in these areas to provide reasonable assurance that all related control objectives are met. At the close of our audit, physical security controls had been strengthened to provide reasonable assurance that only authorized parties could access the data processing facility and other areas housing IT resources during normal working hours. Also, physical security controls in effect over the business offices provided reasonable assurance that only authorized individuals would have access to IT resources. However, we found that a number of physical security controls within the computer room and student labs needed to be strengthened to prevent or detect unauthorized access. Appropriate environmental controls were found to be in place for the

student labs, but similar controls needed to be strengthened for the computer room to adequately protect computer equipment and other IT-related resources.

At the time of our audit, we found that IT management control practices needed to be strengthened over and within the administrative IT function. Tactical planning could also be improved, as could the level of oversight from senior management and the nature and extent of IT-related policies and procedures required to guide IT functions and activities. In some instances, there was an absence of detailed plans, and established policies and procedures were not always adhered to and could be strengthened so that the integrity, security and availability of IT-generated information and systems are not placed at a risk. Regarding IT-related contracts, we found that the College needed to strengthen management oversight and administration practices for service provided by third-party vendors. Enhanced contract procedures would help hold third-party vendors accountable for performance and delivery of services. While the intent to improve IT-related services and bring required expertise into the College by using a third-party vendor was sound, the ability of the College to attain these goals through contracted services was hampered by a less than ideal IT-related working environment, weaknesses in operational planning, and by not exercising sufficient IT management control practices. For example, because the College did not fully measure results against accepted goals for internal and outsourced IT services, it was hindered in fully completing established initiatives.

We found that the College needed to implement a more comprehensive planning process to address the acquisition, deployment, and management of IT resources, including outsourced IT services. Implementation and exercise of sound IT-related project management techniques, combined with IT-related tactical plans that support strategic initiatives, would enhance the College's efforts to manage control and benefit from its IT functions and systems.

We found that the College was aware of the need to develop documented IT-related control practices and had attempted to address these concerns through certain initiatives and contracted services. Although at the time of the audit, some policies and procedures were in place, the nature and extent of documented policies and procedures needed to be strengthened to guide IT activities and to help ensure that IT control objectives would be met.

Our audit disclosed that the College needed to enhance security controls over its administrative IT systems to prevent or detect unauthorized access or changes to critical application programs and data files. At the time of our audit, the College had an assigned system access security administrator. However, we found that software-provided security features available within the NUMA DG/UX computer system (the College's primary computer system) were not being utilized. We recommend that the College review its data architecture to formally establish data classifications, required levels of security with respect to data classifications, and data ownership designations, and determine whether current security requirements and ownership designations are still valid. We also recommend that the College develop, document, and implement procedures to strengthen system access security controls. We further recommend that system security provisions and additional access security software be used to strengthen preventive and detective access security controls. In concert with this effort, the College should document and implement any additional required security policies and procedures that result from the full use of the system-provided security provisions and additional access security software.

Although the College had taken certain measures to begin to address disaster recovery and business continuity planning, our audit disclosed that the disaster recovery and business continuity planning efforts were not comprehensive. As a result, should a disaster occur, the ability to restore automated systems within an acceptable period of time could be jeopardized. We found that although business users had developed business continuity plans to address a loss of automated processing capabilities for a period of 35 to 45 days, a sufficiently comprehensive business continuity and contingency plan for the IT facility had not been developed. We recommend that the College develop, document, and test such a campus-wide disaster recovery and business continuity plan.

Our audit found that, although the College did have formal, approved policies and procedures for inventory control of IT-related hardware, the inventory system of record employed by the College was unable to produce basic inventory reports within an acceptable time frame. The College stated that this was due to a technical problem with its Oracle upgrade.

With respect to IT-related organization and management, internal control practices in place did not appear to represent a consistent framework of control for the overall IT environment. Control practices found to be strong in one area required strengthening in another. We found that controls needed to be strengthened regarding IT management control practices in the areas of tactical planning, data architecture, systems or processes, IT-related policies and procedures, and in the recording of activities, such as for program changes. We found that, although some IT-related policies, procedures, standards, and guidelines were in place, they were sporadic, insufficiently defined, and in need of enhancement (e.g., testing and retention of test results). As a result, there was an increased potential for inconsistent and incomplete implementation of important processes and activities, which could lead to erroneous processing or loss of system and data integrity. Without these written guidelines, there is an increased risk that facility access and protection activities will not be implemented consistently or effectively, thereby placing the College's mission-critical information processing capabilities at risk. In addition, should key personnel terminate employment with the College, the lack of good documentation of the systems and processes could result in the loss of significant portions of the College's knowledge base. Essential documentation requiring improvement included that for:

- Monitoring and evaluation of all IT-related functions,
- Contract administration of third-party vendors,
- Policies and procedures controlling access to the College's computer facility and areas housing IT resources and protecting the facility from hazards,
- Policies regarding access security for NECC's key information systems,
- Disaster recovery and business continuity and contingency plans for NECC's computing applications and activities. The existing disaster recovery plan omitted several components (specifically, sections describing relevant risks, alternative-site agreements, service-level agreements, mainframe access for business resumption, recovery processing procedures, application prioritization, and user training), and
- Documentation of standards and applicable quality review procedures for hardware inventory recordkeeping.

Documentation of key processes and activities for administrative IT functions helps to provide clear guidelines regarding the implementation and execution of appropriate practices and in the measurement and evaluation of results. We found that the College needed to develop and document appropriate monitoring and evaluation techniques to determine whether IT-related internal control procedures are appropriate, in place, understood, and in effect. However, we noted that the College had established a help desk offering quick assistance to the user community and had performed day-to-day tasks essential to keeping the College's network viable.

AUDIT RESULTS

1. IT-RELATED CONTRACT MANAGEMENT AND OVERSIGHT

During the course of our audit, we determined that Northern Essex Community College (NECC) had entered into, or already had in place, 13 third-party vendor contracts for IT-related services for fiscal years 2000 and 2001, with a combined maximum obligation totaling $1,654,986. Our examination indicated that for eleven (11) other IT-related contracts with different vendors appropriate contract administration practices had been followed and contract deliverables had been provided. In particular, we found that for hardware and software maintenance contracts, internal controls were in place to provide reasonable assurance that the College would obtain contracted deliverables and services and that contract expenditures would not exceed contract amounts As of July 25, 2001, the College had expended $1,315,185 for fiscal years 2000 and 2001 for such services. Tables 1 and 2 in Appendix B of this report provide a list of third-party vendors, contract dates, contract amounts, and payments made relating to each contract for fiscal years 2000 and 2001.

Based on documentation and interviews with NECC management, there was adequate justification for obtaining third-party services to assist the College in implementing its student information system and to strengthen project management techniques and skills across the College's IT functions. This included the need to establish a project management framework that required formal project documentation, including written project statements, and the identification of detailed business requirements, staffing and resource requirements, responsibilities and points of accountability, milestones, task breakdowns, time budgets, review and approval points, and checkpoints for each project phase.

Regarding major IT-related contract expenditures, our review of IT-related contracts disclosed that NECC had followed a competitive bidding process, including issuing Requests for Responses (RFRs) except for the contracts with Campus Works, Inc. (CWI). We found that the College, although it felt it had complied with statutory requirements, had not followed generally accepted business practices regarding the CWI consulting contracts, contributing to a contractual relationship that limited the College's ability to realize

contracted deliverables at a fair and equitable price. For major IT contracts, RFRs had been elicited and vendor responses received for the campus-wide telecommunication system (Lucent), the College's mission-critical student information system (SCT's Banner system), and the College's computer-operating system (Data General's NUMA Unix computer). Although the CWI contracts required a more significant outlay of funding than other IT-related contracts over the audit period, RFRs or invitations for bids were not issued for the CWI contracts. The significant financial and administrative impact of the CWI contracts should have prompted the College to solicit additional proposals through an open bidding process from other vendors providing similar services. An open bidding process would have provided the College with the potential to select a more qualified vendor at a more competitive price. In addition, the process would have also provided the opportunity for the College to fine tune its contract requirements and practices related to the desired services. Given the magnitude of the second through fourth CWI contracts, ranging from $200,000 to $694,200, the College may have benefited from putting these contracts out to bid.

Based on our audit, we found that appropriate contract administration controls were in effect for all IT-related contracts except for services contracted from one vendor. Our review also revealed that the management and accountability of the IT-related contract for consultant services from CWI lacked sufficient controls to ensure that the objectives of the contracted services would be realized and that payments would be made for only valid and verifiable amounts billed. With respect to CWI contracted services, it appears that mechanisms to monitor and evaluate critical success factors and key performance indicators were not in effect to help ensure the realization of contracted services.

Adequate control practices were not exercised to provide reasonable assurance that contracted services and deliverables would be attained for contracts with CWI. Our examination indicated that for eleven (11) other IT-related contracts with different vendors appropriate contract administration practices had been followed and contract deliverables had been provided. In particular, we found that for hardware and software maintenance contracts, internal controls were in place to provide reasonable assurance that the College

would obtain contracted deliverables and services and that contract expenditures would not exceed contract amounts.

Background

In late 1996, NECC began an initiative to purchase a new integrated student information system (SIS). In January 1997, the College reviewed and evaluated vendor proposals submitted in response to the College's RFRs for a student information system. With the College President's and Board of Trustee's approval, the College selected Systems and Computer Technology Corporation (SCT) and its Banner system to be NECC's replacement student information system.

Following the selection of SCT Banner, an NECC Banner Phase 1 steering committee was established. The steering committee, composed of much of the membership of the initial selection committee, completed a Banner project document by August 1997 that detailed the structure, process, timetables, and designated responsibilities for the installation of the new student information system. From August 1997 through July 1999, the College followed a schedule to bring the Banner system's six subsystems (General, Student, Finance, Financial Aid, Human Resources, and Alumni) into production along with 62 system modules that accompany each of the subsystems. The College had planned to complete the installation work by using in-house IT staff with the assistance of SCT Banner consultants over approximately a two-year period. Appendix A of this report provides a chart of each subsystem and associated modules, as well as stated production dates, if applicable, regarding the NECC Banner Phase I initiative that had been indicated by the College at the end of July 1999 as completed.

By the end of July 1999, the NECC Banner Phase I steering committee, in concert with the NECC IT staff, had been able to bring five of the six subsystems into production, along with thirty-one (31) of the associated modules. Although the technical implementation of the SIS was progressing well, issues had begun to surface regarding general user satisfaction and the overall effectiveness of the steering committee. The College had determined at that time that the intended users of the system were not being given enough consideration. In a

document entitled "Banner - Project Administrative Computing Alternate Resolution Analysis," senior administrators had identified that the problem areas as the functioning of the Banner steering committee and user complaints regarding system access, training, processes, procedures, decisions, and conflict resolution. The problems with respect to the steering committee and the user complaints were caused partly due to the lack of appropriate project management techniques being applied to the overall project. In turn, the steering committee and the user complaint-related problems were key factors in the College's decision to explore available options for obtaining outside assistance to strengthen project management.

At that time, the College considered four alternative solutions to address its concerns: (1) hiring a sole consultant, (2) outsourcing all of the IT functions to a sole provider, such as Colleges, (3) creating a partnership with another community college to share IT-related outsourced vendor services, or (4) hiring a contractor to work with NECC's existing IT staff.

Vendor Selection

According to College officials, the College had explored available options for IT services for an extended period of time. Senior management indicated that they had interviewed and collected relevant information at national conferences, trade shows, and other IT professional meetings. College officials further indicated that it was the primary intent of the College to research and select a vendor that had the expertise and professional experience to provide needed services not possessed by the College's then current staff. They also stated that the College pursued and conducted its analysis based on cost, existing market trends that allowed the College continued control over IT management, personnel administration, and the ability to receive needed services in a flexible manner.

Although the College described the steps taken to select CWI, there was limited documentation regarding the evaluation process undertaken to select CWI or to indicate that a formal selection committee had been used for the initial contracts. Overall, there was a lack of documentation regarding the CWI contracts in terms of vendor selection, contract negotiation, and contract performance. College officials indicated that they had sought and received legal guidance to ensure that the contracts with CWI met all pertinent statutes and

regulations; that there was extensive research and focused interviews with prospective providers of IT-related service; and that, based upon this research and interviews involving senior management and the administration, the College had selected a vendor that could best fulfill its needs. However, there was insufficient documentation related to any of the CWI contracts to indicate that a selection committee was initially used, the extent to which a legal review was conducted or whether a budget analysis or best value analysis had been performed. We also determined that the College had contracted for IT consulting services with CWI without having the benefit of a detailed enterprise-wide IT strategic plan.

There was also a lack of documentation available for review outlining the College's analysis of the implementation and use of contract employees, or for contracting with CWI for employing contract workers in place of state employees. Such analysis would have included determining the manner in which contract personnel would fit into NECC's staffing strategies, taking into consideration business objectives, requirements for existing and future employee skills, compensation costs, workload requirements, and the nature of services to be provided. According to the College, a further issue that had been factored into the option-selection process was that concerns had been raised at that time regarding cost and legal restrictions with respect to the retention of union employees already employed at the College. Although the College provided no documentation regarding this issue, it was cited by the College as a reason for its not outsourcing the entire IT function at NECC.

After contacting and meeting with outside vendors, which included 60 on-site billable hours of consultation time over several days for CWI, the College determined that the best course of action at the time was to engage CWI to work in a "blended" fashion with NECC staff. Although the College indicated that they had had extensive discussions with CWI, there was also little documentation on selection criteria or the steps taken to review CWI's qualifications.

The College had not requested or received a record of the contractor's history of success in the Commonwealth or elsewhere. In addition, although CWI was to provide contract staff, the College did not require the vendor to provide resumés, or statements of experience, of

the proposed contracted staff to evaluate their knowledge and skills for performing the work under contract. Although one of the primary reasons for contracting with the vendor was its Banner system expertise, the consultant's project manger had assigned all-important Banner system-related tasks to a state employee who was also the UNIX administrator. Subsequent to signing the contract with CWI, the College transferred responsibility for Banner project management from the Dean of Information Technology to the Vice President of Enrollment Management and Student Services Division. At the beginning of fiscal year 2000, IT employees from administrative computing who were affiliated the Banner system were reassigned to a newly established division called Administrative Computing Information Services (ACIS).

Contract Agreements

A review of each of the CWI contract agreements indicated that they did not specifically detail contracted deliverables and a description of services, or include the basis upon which contract deliverables and services would be measured and contract costs calculated, which reduced NECC's ability to monitor service deliverables.

With any contract there are at least two parties with whom the responsibilities lie for successful contract performance. Our review of the contracts between NECC and CWI revealed problems in the process on the part of both parties. The absence of key performance indicators and a requirement for regular status reports made evaluating contractor performance more complicated. Our review of the four CWI contract documents indicated that the contracts did not require the submission of any reports to measure performance, however, college officials stated that the contractor did provide a very limited number of reports in a format acceptable to the college. In the absence of a contractual or administrative requirement for progress reports and having contracted staff maintain and submit time records, the College was inhibited from monitoring contract milestones and verifying monthly invoices before making payment.

The CWI contracts also did not clearly specify the basis upon which individual consultant-provided contract services were to be paid. In addition, the CWI contracts did not include language requiring that the contractor submit supporting documentation with their invoices,

such as status reports or copies of receipts for reimbursement of related expenses under contract 3 as a requirement for payment. The third CWI contract, which allowed the vendor to bill the College for "related expenses" did not provide any guidance as to what constituted "related expenses." In addition, the fourth CWI contract, which shifted to a full time equivalent (FTE) basis for vendor billing, did not provide a clear definition of what constituted an FTE in terms of the method by which billable amounts would be calculated.

To ensure that IT initiatives were aligned with the College's overall business strategy and to avoid unnecessary expenditures for readjusting IT strategies in the future, the College should have ensured that IT-related services were procured in accordance with an approved enterprise-wide IT strategic plan and that vendor proposals were solicited for the types of services contracted for in the CWI contacts.

Before entering into contracts for personnel services, contract instruments should be designed to help ensure that desired services are attained and that appropriate terms and conditions are addressed. For example, College management should consider consulting with legal counsel and developing contracts that:

- Specify human resource management responsibilities and the level of authority granted contract personnel to take action (e.g., to transfer, train, evaluate, assign work).
- Identify specific projects to be completed and ensure payments coincide with delivery dates during the project period.
- Consider consultant compensation rates to ensure that they are not significantly greater than the salaries of state employees performing similar tasks.
- Describe how contractor performance will be monitored and assessed.
- Document the scope of services to be provided.
- Describe the skills and experience relevant to contract work.

Without consideration of these issues, entities may not be able to hold contractors accountable for services provided, or the relationship with the contractor may not be clearly

defined, making the contract difficult to manage. In addition, entities may incur increased risk of legal liability when these issues are not considered.

Although we acknowledge that senior managers at NECC were pleased with CWI's efforts, our audit disclosed that the College did not follow generally accepted business practices regarding the CWI IT-related consulting contracts, such as oversight and control, performance monitoring, and verification of contract work and charges, which reduced the opportunity for its obtaining the best value contract on behalf of the Commonwealth.

IT-Related Contract Deliverables

Based on our review and analysis, we found that adequate contract management controls were not exercised with respect to the IT-related contracts with CWI. Overall, four contractual agreements, an initial contract followed by three contract addendums referred to hereafter as contracts 1 through 4, had been entered into between NECC and CWI. While we believe that contracts 1 and 2 could have been strengthened, contract 1 did not represent a significant outlay of funds, and contract 2 was only in effect approximately one month. Our review of work completed under CWI contracts 3 and 4 indicated that much of the services and deliverables that were stated as completed by CWI, or jointly by CWI with NECC, appeared not to have been fully documented.

The first CWI contract, initiated June 7, 1999, was entered into to have an assessment performed of the NECC IT environment with respect to the year 2000 (Y2K) date issue. (See Appendix E.) According to NECC, CWI worked for approximately one to two weeks on the assessment and provided the College with a written report on the status of the IT environment. We confirmed that the College paid the contractor $4,800 for the services rendered. A formal presentation was made by CWI to senior College management.

Our review and analysis of the contractor's report revealed that the two-page document did not provide a detailed assessment of the College's IT infrastructure and IT environment with regard to Y2K. Specifically, it did not identify actual and potential operational concerns, strengths and weaknesses of IT operations, opportunities and problems regarding Y2K, or a

set of recommended courses of action. As a final work product, the CWI document did not provide sufficient explanation or detail to stand on its own. From the perspective of the then pending Y2K problem, the document did not address embedded technology, IT-related inventory, systems issues, and requirements for resources and business continuity and contingency plans. Given that the timing of the vendor's assessment was just six months before the year 2000 deadline, more detailed documentation outlining CWI's assessment regarding the College and its year 2000 readiness should have been provided for presentation to senior management and the Board of Trustees.

Contract 2 with CWI was in the form of an addendum, dated July 28, 1999, to contract 1 in which the vendor was to provide an increased scope of services from August 9, 1999 through August 8, 2000. (See Appendix E.) However, three and a half weeks into this addendum, NECC entered into contract 3 with CWI, which was in the form of another contract addendum signed on September 2, 1999, specifying a total cost of $300,000 for the 10-month period September 6, 1999 to June 30, 2000. (See Appendix E.)

According to contract 3, CWI was to provide assistance to NECC's IT operational information systems environment, which the College had deemed to be operating at a less than acceptable level. The contracted services were to be accomplished by providing NECC with vendor staff to integrate with College staff or to perform specific IT functions. Management and staff-level personnel were to be provided by the contractor to work in a "blended" fashion to enhance and provide Banner-related IT functions for the College in an advisory manner. The arrangement was referenced under the contract as a technology consultant agreement. In that light, CWI was to provide professional staff services to support the NECC IT goals by working as project management consultants. The established short-term goals of the third contract were to focus on SCT Banner training, including that for current and future modules, a business process re-engineering design that was to include a recommended set of business procedures and processes for the SCT banner system, implementation of expanded SCT banner capabilities, and project management assistance. In addition, the deliverables outlined in contracts 2 and 3 were the responsibility of the vendor, including the continued assessment and review of Y2K readiness, business

continuity planning, and network and hardware platform impact of both capacity and operations reliability.

The first stated contract deliverable of contract 3 was a Banner training program to be provided by CWI in order to "facilitate and/or provide the College's Phase II Banner training activities." However, our analysis determined that there was little evidence of formal training being provided by CWI consultants during the period covered by the contract. This was further substantiated by evidence indicating that CWI had only inquired into the price and availability of SCT video tapes regarding the Banner system for NECC staff to review and use as a training tools. NECC staff had only received minimal training from CWI, and it was NECC staff who had independently gathered Banner-related information and distributed the training materials to other NECC employees. Upon request, CWI could not provide specific information to demonstrate that the training required by NECC had actually been provided. We also determined that the College had paid SCT to provide an augmented type of training at a time when CWI was contracted to provide Banner training.

Another contract deliverable from contract 3 focused on the requirement that CWI was to facilitate and prepare in writing a "business process re-engineering design" for the Banner system within 90 to 120 days. The "design" was to include a recommended set of business procedures and processes and a master plan for continued implementation of Banner modules and the revision of completed Banner modules. The contract specified that the master plan was to contain policy and/or organizational changes, timelines for the implementation and sequence (priorities), and identify required support organization changes and staff enhancements. Regarding the use of technology, there was little documentation from the contractor outlining how the College's business processes would be re-engineered and modified, or how workflows and responsibilities would be changed. Our analysis determined that the by-product of the vendor's effort was the completion of a document entitled "Banner Phase II Master Plan, a Road Map Towards Optimum Performance," that had been prepared by CWI, dated November 8-9, 1999.

Our review of the Banner II Master Plan indicated that it was a high-level plan illustrating multiple areas of ongoing support for "work in progress" regarding the Banner modules and subsystems that the College had hoped to implement during the next fiscal year. However, the plan did not include a number of items that are generally accepted as necessary, such as individual task assignments to be performed, milestones, and delivery dates. The absence of specific targeted tasks and milestones may have hindered the College from ensuring the successful completion or items listed in the master plan. With respect to the goals and objectives identified in Banner II Master Plan, according to the NECC Vice President, a number of the items contained in the plan were never completed or fully implemented. Further, when this plan was later categorized by the NECC Vice President as a "wish list" and not an actual project-planning tool, she stated that they had "overestimated" what could be accomplished during this time frame.

Contract 3 also included a requirement that the CWI consultants provide IT-related project management assistance to the College, such as a review of project management tasks, including project status, technical and user-area review, and assistance to NECC's designated general management during the duration of the third contract. This particular area of the contract deliverables was important to the College, as it had already identified the need to strengthen project management techniques. Documentation supplied to us by NECC management evidenced the College's need to significantly strengthen its IT-related project management methodology and skills, including the establishment of a project management framework that would require clearly written project statements defining the nature and scope of every project before work on the project begins. The project statement should identify the extent of project planning, resource requirements, staffing, allocation of responsibilities and authorities, task breakdowns, budgeting of time and resources, milestones, checkpoints, and approvals for each phase of the project by designated managers before the next phase would begin. A summary of the documentation we received from the College representing work performed by CWI regarding contract 3 deliverables is located in Appendix C of this report.

Based upon our review, sufficient evidence could not be provided by the College or the vendor to support the receipt of an acceptable level of contracted services and/or deliverables. Documentation provided to us did not support completion of contract deliverables or demonstrated that services had not been fully provided. Although the College's decision to contract with a third-party vendor to provide project management input and technical skills and to develop project management guidelines was sound, the vendor did not assign personnel who demonstrated adequate knowledge and skill in project management techniques.

We found that the College's inadequate monitoring and evaluation of contract payments for the third CWI contract resulted in a cost of $6,248 above its $300,000 maximum as of April 30, 2000. NECC's permanent file for the CWI contracts did not include documentation in the form of letters of understanding or memoranda from senior NECC staff to indicate the reasons for this cost overrun.

Contract 4, which was signed May 15, 2000 with Campus Works, Inc., covered the period May 15, 2000 through June 30, 2001 at a maximum obligation of $694,200. (See Appendix E.) Although contract 4 refers to the term full time equivalent (FTE) under the "Modified Scope of Services," the contract did not provide a specific explanation as to what criteria and guidelines were to be used in determining the FTEs. However, College officials indicated that an FTE was equivalent to one full-time employee. The invoices submitted for our review illustrate that 21 out of 21 days worked was equal to one FTE, or 168 hours worked, on a monthly basis. Because individual months fluctuate regarding the amount of actual working days, the average of all months was equal to 160 hours per FTE. Using the contract and contractor time sheets provided to our audit team, we determined that one FTE, or 160 hours, was equal to $24,948 on a monthly basis and was inclusive of reimbursable expenses for this particular contract.

The absence of a specific definition of FTE in terms of how the vendor calculated its monthly invoices may have also contributed to a lack of clear understanding on the part of the College as to the exact basis of payments to CWI. For example, one senior

administrator from the College indicated that the consultant was to be on site to accrue billable hours, while another administrator stated that work could be completed away from the College. With this in mind, consultants' invoices for billable hours should have been monitored by the contract managers through the use of project status reports and job cost allocations. However, the College did not require that a formal mechanism be used in conjunction with the consultants to justify and verify work completed for the College during the contract period. In fact, our review of the weekly timesheets regarding CWI consultants performing services for the College revealed that the stated hours on the timesheets sometimes did not reflect the hours that had been billed by the consultant. Based upon the formulas above and documentation presented for our review, including the CWI time sheets and FTE reports, we determined that the College should review and reconcile CWI invoices and payments to ensure that all payments were appropriate.

Although the vendor did not consistently provide weekly status reports to the College, status reports were required from the NECC IT staff to the consultant. Our audit team received two reports that had been completed by the vendor for the College's overview of work completed. In fact, during an interview with the CWI on-site staff member designated as the Banner Project Manager by the College, we were informed that all documentation regarding completed or successful projects was not retained as required. Subsequent to the end of our audit fieldwork and upon being informed of our concerns in this regard, the CWI Executive Director indicated that work team minutes, project implementation plans, and final work team reports were now on file. We requested from both the College and the vendor documentation to provide evidence of work performed under the CWI contracts. With respect to the substance of those status reports completed and presented to us during the audit, all items listed on the status reports were exclusive of reference to time allocation or business process owner. We found little detail on the contractor's status reports then submitted monthly to the College based upon the "Consulting Services."

Essentially, a very low level of documentation was subsequently provided to demonstrate work performed by CWI. A graphical representation of the documentation we received from the College, representing work performed by CWI regarding contract 4 deliverables, is

located in Appendix D of this report. Our review indicated, moreover, that much of the services and deliverables stated as completed, either jointly by NECC with CWI or solely by CWI, appeared not to have been fully delivered as documented. Our effort to review IT project documentation within ACIS was hindered by an overall lack of detailed documentation. A review of this documentation would have provided evidence as to how the contractor was implementing project management techniques as well as how well the IT projects were being managed.

A number of key issues were revealed regarding contract administration during the audit, including the fact that the College had not established adequate guidelines for the project management of new Banner module implementations and upgrades. One example resulting from inadequate implementation of a system module was the College's inability to submit necessary data to the federal Student Loan Data System from information residing within the Banner financial aid module. This project was assigned to a CWI, according to College officials, as a stopgap measure, due to the College's impending need. Because of inadequate oversight and the consultant's subsequent departure from the College, the project was never completed.

Another example of inadequate implementation concerning a Banner system module occurred in the Alumni module conversion project, which had a start date of September 9, 1999, whereby alumni constituent information residing on a legacy system was to be migrated to the Banner system. With respect to this conversion project, we noted that no one affiliated with the CWI vendor had prior experience with the legacy system software code, and, therefore, they were unable to adequately address this issue, which as of the end of our fieldwork had remained unresolved for almost two years. Without a documented migration and data verification process to confirm that there was no loss of information or degradation of data integrity, the College cannot ensure the reliability of the data post-migration.

Our audit determined that the College had disbanded the previously established Banner Phase I IT Steering Committee that had provided management oversight. According to

NECC management, the steering committee had not performed adequately regarding the Banner Phase I objectives. However, our analysis determined that since the steering committee had been disbanded and a consultant was appointed as the Banner project manager, only one new Banner subsystem had been deployed as of the end of our audit fieldwork. The lack of an active IT steering committee to provide direction and review and approve IT initiatives contributed to inadequate oversight and a failure to address internal control issues regarding IT-related activities, such as having documented policies and procedures, and disaster recovery and business continuity plans. With respect to internal control, it is management's responsibility to ensure that internal controls are in place to provide reasonable assurance that organizational control objectives will be met and that undesired events will be prevented or detected and corrected in a timely manner. The primary functions of a steering committee are to oversee the allocation and control of scarce IT resources, advise in setting IT priorities, serve as a conduit for user department input, review and help in improving IT activities, and approve tactical and strategic plans.

The absence of appropriate controls over contract expenditures resulted in a number of issues ranging from potentially inappropriate contract payments to apparent over-billing by the contractor. The following issues regarding payments were disclosed during our audit:

- The contract had outlined an agreement to provide contracted services through June 30, 2000 with a maximum estimated obligation of $300,000. As of the end of April 2000, the College had paid the contractor $306,249, or $6,249 over the contract's maximum obligation.

- Procedures were not in place to ensure that payments made for "related expenses" under the third CWI contract were for only valid expenses. Essentially, the College accepted all billed amounts for related expenses as valid and paid them accordingly. Moreover, our examination of receipts provided by the vendor during our audit as supporting documentation of related expenses indicated that the College had reimbursed the vendor for several questionable expenses. (See Audit Result No. 2.)

- CWI contracts represented hourly billable rates in the range of $180 to $200 per hour, which is significantly higher than the rates that would have been paid for full time state positions and were unusually high for the contracted positions.

Use of Contracted Staff

Our review indicated that CWI contracted staff often performed the work of existing College staff because an adequate framework had not been established regarding the use of contracted staff under the CWI contracts. Although NECC administrators indicated that the management of IT was a College responsibility, there was some evidence that management responsibility had been shifted to the outside vendor. At the time of our audit, we found that the outsourced Executive Director was performing routine administrative activities that could have been or previously had been performed by state employees at the College. Based upon the job description submitted to our audit team, the consultant was to "supervise the day-to-day operation of the Department, in conjunction with non unit staff" and to "secure appropriate hardware and software for ACIS staff." In addition to performing day-to-day functions, such as establishing user accounts for access to automated systems and activating user IDs and passwords, which had been formerly the duty of a designated NECC IT staff member, the contractor also directed NECC IT staff in the assignment of certain tasks and activities.

Moreover, from a management perspective, having one party direct the efforts of staff and not be responsible either for their actions under the contract, or by any other means, tends to undermine accountability.

Our review of the duties performed by the outsourced Executive Director also raised some concern with respect to the level of human resource management exercised by that individual over state employees. Decisions as to how positions are to be filled in state entities should be made by state administrators. The CWI consultant apparently recommended that the Oracle database administrator position be outsourced. Moreover, the consultant provided advice in making employment decisions concerning the individual to be hired as the part-time Oracle database administrator, with little involvement by state administrators in the process. College officials indicated that the outsourced Executive Director had been assigned the duty of selecting the outsourced database administrator for the College. State administrators should have been more directly involved in the process to ensure that it was an open recruitment and that the consultant did not unduly influence the

final decision in the selection process. Under this situation, the CWI consultant selected a fellow CWI employee to fill the position of database administrator. To help provide for a long-term, sustainable knowledge base at a competitive rate, the College should have first advertised for a database administrator at an acceptable salary level.

IT-Related Contract Management Polices and Procedures

Our review of NECC contract-related policies and procedures indicated that guidelines and procedures were in place, including the designation of either the President or Vice President of Administration as being the only authorized employees to enter into contracts with outside vendors, to cover the majority of the types of contracts entered into by the College. However, we found that the policies and procedures needed to be strengthened to address the types of service contracts entered into by the College with CWI. The College's contract-related policies and procedures would be strengthened by including guidelines for:

- Use of contract employees instead of state employees.
- Types of work performed by state employees and contract workers.
- A method for analyzing costs and benefits.
- Performing risk analysis and productivity analysis.
- Contract worker selection.
- Contract workforce management.
- Requirements for legal review.
- Monitoring and evaluating the performance of contracted workers and contracted companies.

The use of contract workers requires state entities to understand and manage the complexities of contracted worker relationships. Although College officials stated that best business practices do not apply to the College, we believe that it is important to have documented guidelines that outline generally accepted management practices to assist the organization in managing contract workers. Although according to procedure 5 in NECC's

Contract Management Policy ("Contract managers are then responsible to manage [the] contract on behalf of the College"), little additional documented guidance was available.

We found that, with respect to the CWI contracts, certain tenets regarding good practices for managing employee relationships needed to be addressed, as evidenced by guidelines not being documented for using contract workers, time limits for project assignments not being defined, and required skill sets not being specified for positions now filled for contract employees.

While ultimate responsibility for contract management rests with the College, the vendor did not adequately address certain of its responsibilities with respect to standard contractual terms and conditions. However, had the College exercised stronger contract administration practices, it is likely that either all of the Commonwealth's "Terms and Conditions" would have been addressed or that appropriate action would have been taken.

Recommendation

NECC should strengthen its methods for monitoring and evaluating IT-related contracted services and establish methods to provide adequate assurance that it has received all contractual services and deliverables. Included in the scope of monitoring and evaluation would be compliance with contract terms and conditions and financial evaluation (budget tracking and review and approval of contract expenditures).

In addition, the College should strengthen its IT-related contract policies and procedures to include guidelines for the selection and management of contract employees. To help ensure that the College receives acceptable IT-related services and deliverables at the best value from qualified vendors, IT-related contracts should provide:

- A clear statement of work to be performed and the deliverables to be provided by the contractor and contracted personnel. In contracting for services related to specific projects, the contract documents should specify project time frames and milestones.

- A clear statement restricting the use of contracted personnel to supervise agency or state employees. For example, contracted personnel should be restricted from making decisions related to the employment of state workers.

- Definition and delineation of the contractor's role in supervisory and payment-authorization tasks.

- Identification of required knowledge and competency levels of contracted personnel.

- Requirements for contractor reporting of the status of work completed and to be performed and deliverables to be provided.

- College approval authority for high-level contractual employees and subcontractors.

Written contracts and contract administration practices should require an overall up-to-date, detailed contractor master plan covering contracted services and detailed planning documents for individual projects under the contract. Documentation requirements should be delineated to ensure that contractors provide sufficient system as well as project-related documentation. Documentation guidelines should include requirements for project documentation, system narratives, detailed and functional specifications, audit and management trails, operations manuals, user manuals, training materials, flowcharts, data flow diagrams, feasibility studies, test scripts, test results and evaluations, and reviews and approvals. Moreover, contracted personnel should be fully acquainted, when appropriate, with the College's record retention policy to ensure that appropriate records are retained and reduce the risk of public documents being discarded.

With respect to oversight and review and approval of contracted work, an IT steering committee should be used for enterprise-based and mission-critical systems or IT infrastructure changes to strengthen the evaluation of work performed. The College should strengthen its monitoring and evaluation methods for assessing contractor performance and to ensure that contracted services are being provided. Such procedures would include a requirement that the contractor submit detailed status reports on a daily, weekly, or monthly basis that clearly delineate work performed and outstanding tasks or activities remaining to be addressed. In addition, a monitoring process should be

established to provide project-specific feedback that can be used to update and maintain strategic and tactical plans.

The College should also perform an assessment of current IT-related knowledge and skills of personnel performing IT-related functions. For those skill sets requiring contracted staff, reasonable efforts should be made to achieve knowledge sharing and skill set training where possible and practical. As a part of the knowledge transfer from outsourced service providers, the College should capture, develop, and document best practices for IT-related planning and incorporate those practices into the College's guidelines and policies. The contract documents should include specifics on the nature and extent of the knowledge transfer, specific associated costs, and the methods and means of this knowledge transfer.

To strengthen the overall management of contracts for IT-related personnel or services, performance measures should be established, contractors should employ appropriate quality assurance standards, and a framework should be established to classify service problems based on importance and requirements for response. Any outstanding issues should be logged, and guidelines should be followed regarding time lags for resolving such issues.

The College should continue to involve the legal division in the review and approval of new contracts and any amendments to existing contracts. The College should also ensure that the proper personnel manage the contracts and oversee the contractor's adherence to contract provisions.

The College should also continue its efforts to establish a viable project management framework for IT-related projects. In that light, we recommend that the College enhance its project management practices requiring documentation defining the nature and scope of every project before work on the project begins. The documentation should include a requirement for defined project planning, staffing levels, allocation of responsibilities and authorities, task breakdowns, budgeting of time and resources, milestones, checkpoints, and approvals for each phase of the project by designated managers before the next phase begins.

The ACIS and DIS should establish and document standard procedures for IT operations where needed. With respect to IT-related policies and procedures, the College should establish an enterprise-based framework that requires all IT functions and processes, regardless of their business process unit or department, to be subject to the College's IT-related policies and procedures. In addition, College management should periodically review polices and procedures to assess their continued appropriateness and to help ensure effectiveness and adherence. For example, management controls should provide adequate documentation of IT activities, including computer operations and accesses to systems. Automated activity logs should exist to provide an audit trail that would enable management to review for inappropriate or unauthorized system-related activities and take corrective actions as required. For remote operations, specific policies and procedures should ensure that the connection and disconnection of links to the remote sites are defined, implemented, and monitored in accordance with the instructions of the College management.

2. IT-RELATED CONTRACT EXPENSES

NECC authorized and paid CWI IT-related reimbursable "related expenses" without requiring adequate supporting documentation. Initially, CWI sent NECC a monthly invoice indicating "Reimbursable Expenses for Month," with no indication as to the general nature of the expenses or detailed explanation and no supporting documentation to demonstrate that these costs were valid and related to NECC business. As a series of contract addenda were generated to extend the contract over several years, CWI was later allowed to submit invoices that did not delineate between what was consulting services and reimbursable expenses, making it extremely difficult for the College to be aware of what, if any, reimbursable expenses were incurred by the consultants.

Regarding fiscal year 2000, we found that as monthly payments were made to CWI, the College did not have adequate documentation relative to the $30,865 that CWI presented as reimbursable for "related expenses" under the third CWI contract. Although the consultant total expense cost breakdown report provided by CWI totaled $30,865, as reported on May 10, 2001, and subsequently amended by CWI to $29,219 on May 24, 2001, supporting documentation provided to us with regard to reimbursable expenses totaled only $27,701, a

$3,164 and $1,518 variance, respectively. Further, individual expense reports furnished by CWI for each of its consultants totaled $19,274, whereas the supporting documentation for these expenses totaled only $16,773, a $2,501 variance. Because NECC had not requested supporting documentation for the IT consultant expenses that were billed by CWI, neither NECC nor the Commonwealth could be assured that all of the "related expenses" were reasonable and proper. According to NECC's Comptroller, all invoices from CWI that had been approved by senior management were to be paid, and it was assumed that the contract manager had the necessary documentation to support the expenditure.

It is our understanding that the mechanism for payment of the CWI contracts and contract-related expenses was through the use of student fee-based trust fund monies. The College's student fee-account trust, which is funded by billing $25 per enrolled course from each student's semester payments, is used for all types of administrative purposes, including IT-related consultant contracts. Although this fund is under the control of the College President, who authorizes all expenditures, the responsibility for regulating and controlling the expenditure of campus trust funds rests with each college's Board of Trustees.

During our audit, we determined that certain CWI reimbursement items appeared to be questionable. Specifically, the submitted receipts raised concerns with respect to the validity and appropriateness of the expenses in that they did not appear to directly benefit NECC's operations, or were outside of the guidelines used within the Commonwealth to support authorization of payment.

Our review of CWI receipts submitted to NECC disclosed several receipts that apparently were also submitted to another Massachusetts State College. Our analysis of these receipts disclosed $7,000 for lodging and $1,245 for other expenses with inadequate documentation as to purpose.

CWI also expensed over $2,486 for meals and groceries from September 1999 to April 2000. While prudent business practices advocate that business meals must be reasonable, appropriate and documented to support the business nature of the expenditure, with few

exceptions, meal invoices did not include reference to a purpose or provide evidence of a business-related agenda.

We also found other CWI expenses, which were not supported by any evidence that the expenditures were related to the CWI contract. These included expenses for unsubstantiated airline travel ($2,000), computer and electronic equipment ($1,089), communication costs ($1,256) and other miscellaneous expenses ($172).

Regarding reimbursable expense documentation for fiscal year 2001, College officials explained that they had agreed to pay a "flat fee" to the vendor and that they no longer required CWI to furnish separate line items in the invoice delineating expenses incurred by the consultants. However, nowhere within the contract was there a formula outlining what part of this "flat fee" pertained to expenses.

Sound business practices advocate that it is the contracting entity's (NECC's) responsibility to ensure, and be able to demonstrate, that reimbursed expenditures are valid and verifiable and are made in accordance with contractual specifications and state guidelines. Because NECC did not obtain and subsequently maintain appropriate supporting documentation, it was unable to demonstrate that reimbursable expenses that had been paid to the vendor were appropriate and accurate.

NECC department heads and senior administrators did not establish an adequate plan to account for, monitor, and control expenditures at the various levels within NECC, and the Board of Trustees did not issue more specific guidelines for reimbursable expenses for IT-related consultants expensed by trust fund accounts. As a result, the Trustees and the Board of Higher Education do not have adequate assurance that all reimbursable expense vouchers from vendors provided a legitimate benefit to NECC and conformed to all applicable guidelines, laws, rules, and regulations. Further, there is inadequate assurance that all expenditures were being properly monitored and controlled and that all necessary documents were timely and properly received, recorded, reported, and disbursed. Due to the inadequate documentation provided by CWI and NECC, the extent to which these costs were associated with NECC services could not be determined. Further, NECC did not

have sufficient documentation detailing the need for these items, nor was it possible to determine who had possession of all of reimbursable equipment. Moreover, we question why these costs were being borne by NECC and not by the consulting company.

Recommendation

To improve controls over reimbursable expenses for IT-related vendors, the College should establish adequate controls, policies, and procedures over the approval, review, and payment of IT-related non-payroll expenses. At a minimum, these policies and procedures should establish an adequate segregation of duties and require that adequate supporting documentation be provided and an independent review be performed of all such expenses before payment is authorized. NECC officials should properly review all IT-related expenses and request additional information regarding any expenditure documentation that is questionable or inadequate.

In addition, NECC administrators should develop written internal control policies and procedures that require contract managers to more closely monitor expenditures. NECC administrators need to ensure that, at a minimum, future contracts contain explicit language and reference the requirements for reimbursable expenditures in accordance with relevant guidelines and generally accepted business practices.

3. HARDWARE INVENTORY CONTROLS

We determined that, although some controls related to the safeguarding of fixed assets were in place, controls to properly account for NECC's fixed assets needed to be strengthened to ensure that all assets are properly accounted for and that accurate information regarding value, location, tag number, and status is included for all inventory items. Our audit disclosed that, although the College had documented policies and procedures related to inventory and had developed an inventory record of hardware and equipment, administrators could not provide reasonable assurance that the policies and procedures were followed and that perpetual inventory records were maintained. Although we found some appropriate information on the fixed-asset inventory records, such as date of acquisition,

location, description, serial number, and asset value, information regarding condition, surplus, and obsolescence were not included.

We determined that although there were three hardware computer inventory records maintained at NECC, including the student computer labs and surplus inventory listings maintained by the Division of Information Services (DIS) Client Computing Department and the hardware computer inventory listing controlled by the Comptroller, it was the Comptroller's version that was considered the official system of record for the College. Our audit revealed that the three computer hardware inventory records were not in agreement with the Comptroller's Hardware Computer Inventory Listing and needed to be reconciled. Although we found no items missing, our audit disclosed that seven items from the DIS student computer labs inventory, with a value of $9,679, could not be located on the master inventory record and that 28 items, with a value of $25,589, had not been properly retired to the approved surplus inventory listing. Also, our random test of the selected inventory items, valued at $244,843, indicated that 69 items valued at $47,336 could not be located on the inventory system of record.

Our audit tests included a reconciliation of IT procurement documentation to IT hardware located using the NECC's inventory record. Our tests disclosed discrepancies in the IT hardware records. Specifically, we determined that some new equipment was not being tagged with the NECC identification numbers and was not being recorded on a timely basis.

Because adequate controls were not in place over IT-related hardware, there was an increased risk that property would not be used as intended and that IT-related hardware would be exposed to possible misuse, loss, or theft. We found that managers had not placed sufficient emphasis on ensuring the sufficiency of controls in this regard. Generally accepted industry standards and sound management practices advocate that adequate controls be implemented to account for and safeguard property and equipment. As is the case with software-related assets, Chapter 647 of the Acts of l989, states, in part: "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 OSC's "Internal Control Guide for Departments," promulgated under Chapter 647 of the Acts of 1989, states that fixed assets should be accounted for in accordance with existing regulations and safeguarded to ensure that they are being used as intended, and a property officer should be designated to provide control of inventories. Inadequate record keeping may also have resulted in overstatement of non-GAAP-related inventory.

Recommendation

The College should review policies and procedures regarding asset management, including procedures regarding the maintenance of a perpetual inventory record. Furthermore, the College should comply with all state reporting requirements for fixed assets.

The College should, in a timely manner, record new purchases, donations, transfers, and deleted items that have been sold, donated, or transferred to surplus property. In addition, inter-campus transfers of computer equipment should be monitored and recorded on the inventory record. Further, we recommend that the College list all College-specific inventory control numbers, dates of purchase, and cost amounts on its inventory record.

In addition, the College should periodically perform a physical inventory and reconcile items within the current perpetual inventory record. To maintain proper internal control, a staff person who is not responsible for maintaining the fixed-asset inventory record should perform the periodic reconciliation. Further, the inventory record should be used as a source and as a means of documenting the Commonwealth's required asset management reports, so that the reports reconcile with the inventory record. The College should also ensure that the non-GAAP related inventory is accurate and complete.

4. LOGICAL ACCESS SECURITY

Our audit disclosed that the College had not established adequate security controls over the mission-critical Banner Student Information System (SIS) and the Oracle Relational

Database Management System (RDBMS) within which it operates. Adequate security controls are necessary to prevent or detect unauthorized access and changes to critical application programs and data files. At the time of our audit, the College had contracted for an Oracle database administrator (DBA) who was to maintain the integrity of the Oracle RDBMS and administer database security, including monitoring of the Banner List servers in order to ensure that users who no longer should have access to the College's systems have had their associated user access disabled. However, based on our audit, we determined that the DBA was not adequately monitoring the security software and password control tables that were then in place as provided by the Oracle RDBMS and the Banner SIS. We noted that, although a generic data security policy existed, including reference to data ownership, confidentiality of information, and the use of passwords, the policy did not have documented procedures in place for security over access to automated systems and a lack of written procedures for the maintenance and control over passwords.

The College had written procedures in place for requesting, approving, and assigning new passwords for all automated systems and required users to complete a "User Access Request Form" in order to be assigned a user ID and password. However, access security controls needed to be strengthened to include procedures requiring that passwords be changed regularly, users be advised not to write down their passwords, that passwords be changed when an employee changes job responsibilities, employee exit procedures be used that include notification of the IT Department for deactivating the employee's access privileges, limiting the number of invalid access attempts, and identifying, logging, or investigating system access violations.

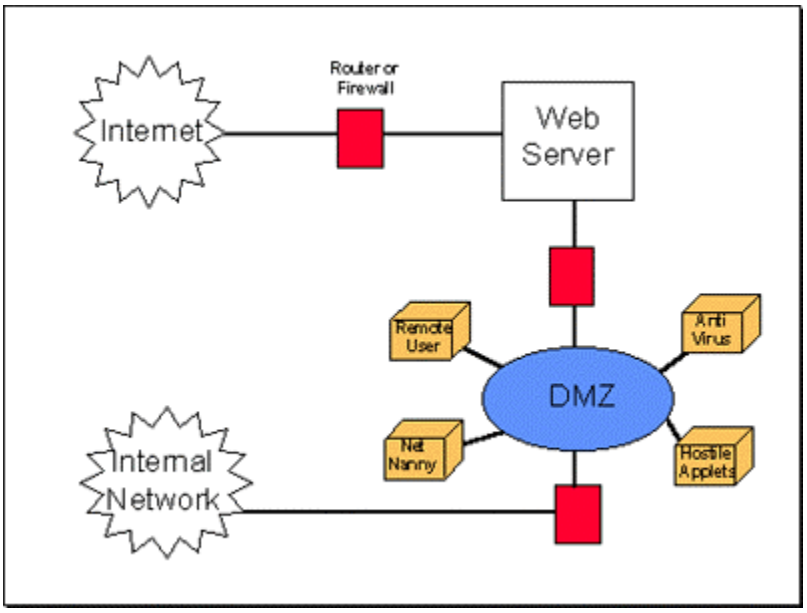
Computer industry standards advocate that policies and procedures for system access security be documented and approved to provide a basis for proper protection of information assets. The policies and procedures should address authorization for system users, development of user IDs and passwords, authentication of users, activation of access privileges, establishment of audit trails, notification of changes in user status, frequency of password changes, deactivation of access privileges, and procedures to be followed in the event of an unauthorized access attempt or unauthorized access. The absence of written

system access security policies and procedures and adequate controls places mission-critical and essential software and data at risk of unauthorized access, modification, or loss.

Although as of the end of our fieldwork, the Division of Information Services (DIS) was strengthening controls over the College's LAN, the lack of effective centralized control over the College's LAN and an inadequate firewall together created a heightened risk of unauthorized system access. The decentralized nature of LAN security and the ability of an antiquated firewall required IT management to set its firewall access at the "all access" level. For a firewall to be effective, it must inspect all traffic to and from the Internet, including the area known as the demilitarized zone (DMZ). Other devices that may need to be installed on the DMZ are:

- A virus scanner to scan all incoming mail, attachments, data and files for viruses and other malicious code.
- A hostile applet scanner to check incoming files written in Java or ActiveX that may contain harmful or malicious code.
- Net nanny software to restrict the sites that users may visit in order to limit their ability to see, browse, or download obscene or other undesirable material.
- A remote authentication server to vet all applications for access to the organization's systems that come from outside of the organization.

Below is a graphical representation of a firewall topography:



The DMZ includes the majority of servers within NECC because of their need to be open to the public to acquire data, such as the College's e-mail. If the DMZ were not properly controlled, it can allow unauthorized traffic to pass, making the firewall penetrable to possible computer hackers. An effective firewall decreases the risk that unauthorized individuals could gain access to College systems through the Internet. Unauthorized use could also result in damage to the Banner SIS and its associated data or disclosure of sensitive information.

As of the end of our audit, senior management had begun to concentrate its resources on the purchase of an effective firewall as part of its improvement of LAN security. Administration of the College's LAN had been divided between a DIS centralized function, and an Administrative Computing Information Service (ACIS) department-level function. Given this organization, strong, uniform policies and procedures are essential for critical areas, such as access to office computer rooms, authorization of access to the LAN, and remote dial-in access to the LAN. Our audit disclosed that such policies and procedures

were not in place. As a result, the two groups enforced uncoordinated, varying levels of security.

We obtained the computer system access lists for the NUMA DG/UX, Oracle RDBMS, and the Banner SIS and reviewed and compared these lists against the most current NECC personnel listing. Although an audit test indicated that access privileges for the NUMA DG/UX included only current authorized College personnel, our audit tests concerning the Banner SIS and Oracle RDBMS indicated 83 and 84 user IDs and passwords, respectively, remained active for individuals who were no longer employed by the College. Because one needs an active combination of a Banner SIS and Oracle RDBMS to permit unauthorized additions to, modifications of, or deletions from critical data files (e.g., student billing balances), a further audit test was completed having the 83 Banner SIS users compared against the 84 Oracle RDBMS users. The comparison of the two lists revealed that 72 users had matching user IDs and passwords, thereby in some cases enabling an unauthorized user total read/write access for the mission-critical Banner SIS. Under these circumstances, the risk of unauthorized access and changes to data is greatly heightened. When controls over program file security are weak, the possibility for undetected manipulation of both data and processing routines increases significantly. Access security is an important control mechanism for the College because the College processes sensitive data, including general ledger, purchasing, accounts payable, billing, accounts receivable, student grades, and financial aid data related to NECC's Banner SIS.

Access to computer systems, program applications, and data files should be authorized on a need-to-know and need-to-perform 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 that would impact the individual level of authorization. For example, Human Resources should notify the security administrator of changes in employment status so that access privileges may be deactivated in a timely manner for individuals no longer needing access. Our review indicated that there was evidence of initial authorization, but that procedures were not in place to inform the security administration of changes in employment status. As a result, mission-critical and essential information on the College's

systems may have been vulnerable to unauthorized access, alterations, deletions, and disclosure.

Recommendation

NECC should establish written policies and procedures for Banner SIS and Oracle RDBMS security to ensure that only authorized users have access to its systems. The access policies and procedures should also address password administration, including the length and composition of passwords, frequency of password changes, guidelines for access security, access privilege activation, authentication of users, access privileges deactivation, establishment of audit trails, and procedures to be followed in the event of unauthorized access attempts or unauthorized access. Further, policies and procedures should address emergency access guidelines for critical applications to ensure that, under emergency or disaster recovery situations, only authorized access is granted. The College should establish procedures requiring written notification to the security administrator from the College's Human Resources Department of changes in personnel status to help ensure timely deactivation of, or changes to, access privileges.

The College needs to have in place an up-to-date and properly configured firewall that can provide the additional protection needed. By its nature, a firewall is a bit of a hybrid. Ideally, it should prevent all incoming information or data from penetrating the web server and ensure maximum protection by using the "deny all" concept. Clearly, this provides absolute security, but does not allow the organization to communicate with the outside world. The firewall therefore must be relaxed to allow some traffic. In order to provide security on this material, other controls must be in place to restrict any potential damage. For this reason, the firewall should be located on its own network (DMZ) located outside of the main College network.

5. DISASTER RECOVERY AND BUSINESS CONTINUITY PLANNING

Although NECC had developed a disaster recovery and business continuity and contingency plan for its IT-related systems regarding anticipated potential disasters, such as Y2K, our audit disclosed that current, comprehensive College-wide written plans had not been

completed, which could jeopardize the restoration of automated systems in the event of a disaster. Business continuity and contingency plans need to be developed to satisfy short-, medium-, and long-term recovery requirements. In the short term, it is important that mission-critical systems and services are restored. Medium-term plans address recovery of systems and services on a temporary basis, sometimes involving borrowed or leased equipment, while long-term plans involve the total recovery of the IT processing environment.

The plan should cover all levels of disaster, from partial to total destruction of facilities, and ought to contain guidelines to help determine the level of recovery necessary. The plan should also detail the additional controls to be affected during recovery and the priorities for the recovery of each business function, and should outline the procedures for keeping the plan current. A copy of the plan should be securely stored off-site. Contingency plans should also be prepared for remote distributed system sites. Disaster recovery and business continuity and contingency plans outline steps to secure or recover information when a catastrophe prevents normal operations. The College's plans did not include detailed steps, and the College did not require periodic tests to verify that plans will work. A business continuity plan should document the College's recovery strategies with respect to various disaster scenarios. This includes planning for total disaster, bomb threats, fires, partial disasters, and the like. Without a comprehensive, formal, and tested 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 NECC's Banner Student Information System) may be unavailable should the automated systems be rendered inoperable. Detailed restart procedures must be documented. When a disaster occurs, procedures should be in place to ensure that applications can readily be restarted.

Our audit disclosed that, in fact, the College's disaster recovery plan had not been tested off site and did not detail the priority with which programs would be brought on line. That is, the plan did not detail what Banner SIS modules, (i.e., accounting programs, payroll programs, or student transcripts) would be brought on line first. Documentation, such as

the disaster recovery plan itself, was not available at the back-up site, and vendors had not been contacted regarding the level of service each can provide in the event of a disaster. As of the end of our audit, the plan was out-of-date with regard to the College's then current IT staff, and IT personnel were not adequately informed of the specifics of the plan.

Although a College-wide risk analysis had been completed, it did not provide detailed response procedures for threats such as fire. The College also had not tested a formal business continuity contingency plan for a timely post-disaster restoration of mission-critical and important business functions processed through the NUMA DG/UX, the LAN file servers, or applications residing on the workstations. Our audit revealed that, although NECC provided adequate on- and off-site backup storage for critical and important administrative applications and data files, the College had not designated or tested alternate processing sites for operations should a disaster renders mission-critical or essential computer systems unusable or inaccessible.

The absence of a documented plan and testing of recovery strategies may inhibit the College's ability to safeguard data files and regain mission-critical and essential information technology processing functions after a disaster. The disaster recovery plan should outline the recovery strategy and detail the steps to regain mission-critical and essential information technology within an acceptable time period. The plan should also incorporate user area plans, describing the steps for user departments and their staff to follow when shifting to alternate-operating modes in the event that a disaster render the user's current automated processing capabilities inoperable.

The overall objective of disaster recovery and business continuity planning is to ensure that mission-critical and essential computer operations can be regained within an acceptable time period should significant disruptions or loss of processing capabilities occur. The absence of adequately detailed disaster recovery and contingency plans could delay recovery efforts and adversely impact administrative and academic functions. Moreover, depending upon the time of the academic year, a loss of automated processing for administrative functions could impede the College's ability to operate.

An effective disaster recovery plan should identify contingency procedures for restoring information technology, including alternate processing procedures used during the interim recovery period. Understandably, the structure, content, and format of detailed recovery and business continuity plans depend on the recovery strategies, communications requirements, complexity of systems, the processing load under various time-of-year scenarios, and targeted recovery times.

The recovery plan should include procedures detailing the restoration of critical information system functions and should be used to determine the logical order of system implementation and integration. Further, the plan should address tasks and responsibilities necessary to move and/or safeguard backup software, data, and program and system documentation from the off-site storage area.

At minimum, a business continuity and disaster recovery plan should include:

- A description of the College's computer systems operating environment (identification of IT platforms, networks, interfaces, information systems, and other IT-related resources);
- A description of operational and user requirements;
- Identification of mission-critical, essential, and less essential application systems and processing requirements and a statement of recovery objectives and strategies for each system;
- Classification of types of delays and disruptions in information technology/systems services;
- Identification of essential data files and software for each critical application according to impact (i.e., catastrophic, severe, serious, or limited);
- Documentation of responsibilities and activities of functional areas supported by critical and essential information technology operations;
- Names, addresses, and phone numbers of key emergency recovery personnel, important vendors, campus security, and user management, and identification of any known limitations on the availability or travel restrictions of key staff under various time scenarios with regard to alternate processing;

- Procedures for notifying management, users, and other parties who oversee or are dependent upon the computer operations should processing capabilities be disrupted or lost;

- Documented user-area contingency plans for departments supported by critical and important systems, with completion and/or latest revision dates, and provisions to ensure that the user-area plans are kept current;

- Emergency supplies inventory, including the quantity and location of each item;

- Copies of agreements for service and hardware replacement (access to the agreements could become critical during an emergency);

- Procedures for the purchase and/or lease of hardware and other specialized equipment; and

- Emergency drill procedures and test criteria.

The disaster recovery and business continuity plan should identify all responsible parties and their respective duties and responsibilities. Regardless of the size and complexity of information technology operations, organizations should not rely upon a single individual to develop and be responsible for executing a contingency plan. The plan should identify the parties who have prepared and are responsible for each section of the disaster recovery and user-area plans and indicate the latest version dates for each section.

It is important that disaster recovery and contingency planning be considered as an ongoing process. To ensure that the recovery and contingency plans are viable, they must be subject to appropriate testing, be properly maintained, and be communicated to all responsible parties. The plans should be periodically reviewed and updated as necessary, and copies of the recovery and business continuity plans should be kept in more than one secure location.

Recommendation

College officials should document their disaster recovery strategy and prepare a written disaster recovery and business continuity plan that incorporates user-area plans. The disaster recovery plan should focus first on those automated systems that are mission-critical to the business objectives and operations of the College.

Management should establish an ongoing contingency planning process that periodically reassesses the relative criticality of automated systems and the IT infrastructure, and updates recovery and business continuity plans accordingly. We recommend that a risk analysis be performed on the College's information technology environment on an annual basis, or upon major changes to systems or the IT environment. An impact analysis of the denial of processing functions should be performed in conjunction with the risk analysis.

The College should develop appropriate policies and procedures to support disaster recovery and business continuity planning, which address recovery and operational objectives, procedures, assignments of responsibilities, controls, monitoring and evaluation, and security measures.

We further recommend that the disaster recovery and contingency plan be periodically reviewed and tested to ensure that it is current, accurate, and complete. The results of all tests should be documented and maintained and copies of the recovery and business continuity plan, including user area plans, should be stored in the off-site location. The plans should be communicated to all responsible parties and that individuals who are assigned disaster recovery and business continuity responsibilities have sufficient skills and knowledge to carry out their responsibilities.

Lastly, to ensure that sufficient recovery plans and procedures are in place to ensure 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.

6. PHYSICAL SECURITY

Our audit disclosed that, although certain physical security controls were in place over areas housing IT resources, a significant number of controls within the computer room and student labs needed to be strengthened to prevent or detect unauthorized access. The computer center, inclusive of the computer and file server room, was located in one of the campus buildings, while the computer labs were located throughout the campus.

At the time of our audit, the following observations were recorded with regard to physical security of the IT-related facilities.

- Although there were limited tacit policies regarding physical security, there were no written standards or procedures to ensure that adequate physical security controls would be in effect.
- There was no list of employees who had authorized access to the computer center.
- No one had been formally assigned the responsibility for the physical security of the computer and file server room and off-site storage areas.
- The doors to the student computer laboratories were frequently found to be open when the labs were neither staffed nor proctored.
- Certain items of the computer equipment contained in some of the student labs were not physically secured through the use of cables or other locking devices.

At the close of our audit, physical security controls in place provided reasonable assurance that only authorized parties could access the computer center during normal working hours. Physical security controls in effect over the business offices provided reasonable assurance that only authorized individuals would have access to IT resources. Security for non-business hours should be strengthened by having adequate detection devices to identify any unauthorized access to the computer facility. Controls needed to be strengthened for non-business hours such as the installation of adequate detection devices to identify any unauthorized access, in order to provide an adequate level of security over the computer labs.

Generally accepted security practices require that adequate preventive and detective physical access security controls be in effect to ensure that only authorized access can be obtained. Failure to effectively manage facilities that accommodate the technology used to deliver mission-critical services to support the College's business objectives could result in the theft or destruction of IT resources, and disruptions or loss of IT services.

Recommendation

The College should perform a physical security risk assessment of the entire campus and identify any and all potential threats and exposures to IT-related resources, including equipment, communication infrastructure, software, media, and proprietary documentation. The College should also perform a complete inventory of all IT resources, including the network infrastructure and its hubs and routers throughout the College.

The College should define and ensure that there is an adequate understanding by all staff of the control objectives regarding physical security. We recommend that IT-related policies be enhanced regarding physical security of IT resources throughout the College. Policies, procedures, and responsibilities for physical security should be written, reviewed, and approved, and distributed to all appropriate staff members. The College needs to establish a single point of accountability for physical security. We also recommend that the College formally assign responsibility regarding physical security for the computer center, computer labs, and off-site storage areas. The assigned responsibilities should be comprehensive, understandable, and properly communicated. The College should also establish adequate mechanisms to monitor and evaluate the effectiveness of physical security controls. Monitoring mechanisms should include formal reporting of lapses in security, adherence to established procedures, and identification of security problems and their resolutions.

7. ENVIRONMENTAL PROTECTION

Our audit revealed that, although the College had certain environmental protection controls in place within the computer center, student labs, and classrooms, the environmental protection controls in the computer room at the Haverhill Campus needed to be strengthened to adequately protect critical IT equipment. Specifically, although adequate air conditioning, temperature, and humidity controls were in place, we found that controls to prevent, detect, and correct water and fire damage needed to be addressed. We found that the College had neither developed nor documented policies and procedures regarding environmental protection. Policies and procedures relating to environmental protection controls should be in place to provide an adequately controlled environment within which

computer equipment can operate under appropriate conditions and to safeguard hardware and software from environmental damage due to extreme heat, fire, excess humidity, power outages, water problems, dust and dirt, and/or other environmental hazards. The College had not implemented and posted emergency procedures in the computer room to help ensure staff safety and the safe and orderly shutdown of computer equipment in the case of an emergency. Although the College had experienced brownouts and other environmental problems, no records were maintained of environmental problems and their resolution.

The College did not have adequate controls to prevent and detect water damage regarding the computer room. In addition, the College had not purchased or installed water detection devices within the computer room to help ensure the safeguarding and protection of the equipment, even though the College had suffered water damage due to a crack in the wall in the basement computer facility years before and early in 2001. The College should also consider the purchase of plastic covers for critical IT equipment to help provide some level of protection against the risk of water damage.

The overall housekeeping of the computer area was very good, as storage items were in cabinets or on shelves, and the area was very clean even though renovations were taking place in the office space next to the computer room. However, during our review of the computer room, we noted that three of the smoke detectors were not functioning as intended. A closer inspection revealed that each smoke detector unit did not contain the necessary batteries. Senior management indicated that these batteries had been removed due to the dust problem created as a result of the renovations in the outer office space. We informed senior management of our concerns and, subsequently, the batteries were replaced in each smoke detector when the renovations were completed. However, the smoke alarms were not hard wired into a security console, making it difficult to ensure proper notification to a central security station of problems detected during non-business hours. A hand-held fire extinguisher was located at the entrance to the office area of the computer room; however, none were located within the computer center. Also, no automatic fire-suppression system was present within the computer center.

Generally accepted standards indicate the need for sufficient environmental protection to safeguard data processing facility staff, computer equipment, application software, and critical and important data residing on the automated systems from accidental loss, damage, or destruction.

Recommendation

The College should review the current status of the controls regarding environmental protection in and around the computer room on the Haverhill campus. The College should develop written policies and procedures to address environmental protection for its computer room, data processing facility staff, computer equipment, application software, and critical and important data.

We recommend that IT staff receive training, which should include specifics on what steps to take when an alarm sounds, evacuation from the building, and the notification of the appropriate authorities (i.e., security officers, police, and fire departments) of the emergency. Procedures for the emergency shutdown of the computer should be documented and readily available. In addition, steps for the protection of equipment and records, and use of fire extinguishers should be documented. Also, there should be periodic evacuation drills of the documented emergency evacuation plan. The College should establish adequate mechanisms to monitor and evaluate the effectiveness of environmental protection controls. Monitoring mechanisms should include periodic examinations regarding the adherence to established procedures and the identification of environmental problems and their resolutions. We also recommend that the College install water detectors in the computer room and that sufficient equipment covers be available in the case of emergency. The College should also consider moving the computer room to another area with better environmental controls; to reduce the risk of flooding, the computer room should not be located in the basement. We also recommend that, in the absence of an automatic fire-suppression system, hand-held fire extinguishers be installed in the computer room.

APPENDIX A

Banner Subsystem and Module Status

Subsystem / Module	In Production	Date of Production
A. General (6 Modules)	Yes	July 1998
1. Job Submission	Yes	July 1998
2. Population Selection	Yes	November 1998
3. Letter Generation	Yes	November 1998
4. Graphing	No	N/A
5. System Functions / Administration	Yes	July 1998
6. Event Management	No	N/A
B. Student (14 Modules)	Yes	November 1998
1. Course Catalog	Yes	March 1998
2. Class Schedule	Yes	November 1998
3. General Person	Yes	July 1998
4. Faculty Load	No	N/A
5. Location Management and Housing	Yes	July 1998
6. Recruiting	No	N/A
7. Admissions	Yes	November 1998
8. General Student	Yes	July 1998
9. Registration	Yes	November 1998
10. Accounts Receivable	Yes	November 1998
11. Academic History	Yes	January 1999
12. Curriculum, Advising, and Program Planning (CAPP)	No	N/A
13. Student System Management	No	N/A
14. Information Access	No	N/A
C. Finance (11 Modules)	Yes	July 1998
1. General Ledger	Yes	July 1998
2. Finance Operations	Yes	July 1998
3. Purchasing and Procurement	Yes	July 1998
4. Accounts Payable	Yes	July 1998
5. Stores Inventory	No	N/A
6. Budget and Position Control	No	N/A

APPENDIX A

NECC BANNER PHASE I INITIATIVE SUBSYSTEMS AND ASSOCIATED MODULES
WITH STATED PRODUCTION DATES AS INDICATED AS COMPLETED BY THE COLLEGE
AS OF JULY 1999.

Subsystem / Module	In Production	Date of Production
7. Fixed Asset	No	N/A
8. Cost Accounting	No	N/A
9. Accounts Receivable	Yes	November 1998
10. Investment Management	No	N/A
11. Research Accounting	No	N/A
D. Financial Aid (13 Modules)	Yes	June 1999
1. Applicant Record Creation	Yes	June 1999
2. Need Analysis / Verification	Yes	June 1999
3. Requirements Tracking	Yes	June 1999
4. Student System Shared Data	Yes	June 1999
5. Pell Electronic Data Exchange	No	N/A (June 1999)
6. Packaging Disbursements	Yes	June 1999
7. Budgeting	Yes	June 1999
8. Award History / Transcripts	No	N/A
9. Funds Management	Yes	June 1999
10. Common Functions	Yes	June 1999
11. Short-Term Credit	No	N/A
12. Student Employment	No	N/A (April 2000)
13. Reporting	Yes	June 1999
E. Human Resources (9 Modules)	Yes	July 1999
1. Position Control	Yes	July 1999
2. Position Budgeting	No	N/A
3. Applicant Tracking	No	N/A
4. Employment and Compensation Administration	No	N/A
5. Benefits Administration	No	N/A
6. Time Entry	Yes	July 1999
7. Payroll Calculation	Yes	July 1999
8. Payroll Adjustments and History	Yes	July 1999
9. Electronic Approvals	No	N/A

APPENDIX A

NECC BANNER PHASE I INITIATIVE SUBSYSTEMS AND ASSOCIATED MODULES
WITH STATED PRODUCTION DATES AS INDICATED AS COMPLETED BY THE COLLEGE
AS OF JULY 1999.

Subsystem / Module	In Production	Date of Production
F. Alumni (9 Modules)	No	N/A
1. Constituent System	No	N/A
2. Organizational Processing	No	N/A
3. Membership Processing	No	N/A
4. Project Management Processing	No	N/A
5. Designation Processing	No	N/A
6. Solicitor Organizational Processing	No	N/A
7. Campaign Processing	No	N/A
8. Pledge Processing	No	N/A
9. Gift and Pledge Payment Processing	No	N/A

APPENDIX B

Information Technology (IT)-Related Third-Party Vendor Contracts

Fiscal Year 2000

Contract Number	Vendor Name	Contract Period	Contract Amount	Percentage of IT-Related Contract Amount	Total of Actual Expenditures	Payment Type: State Funds	Payment Type: College Trust Funds	Payment Amount Over / Under	Percentage of Total Actual Contract Expenditures
1	Campus Works, Inc. + (Contract Addendum)	9/6/1999 – 6/30/2000	$300,000	44.87%	$355,150	-	$355,150	($55,150)	53.79%
2	SCT Corporation (Banner and Oracle System License, Implementation, Training, and Maintenance Contract)	5 Year Lease 5/1/1997 – 4/30/2002	Five Year Contract Total = $616,510 One Year Average = $123,302	18.44%	$143,474	$19,920	$123,554	($19,920)	21.73%
3 & 4	Data General Corporation (Maintenance Agreement) & (Lease Agreement)	7/1/1999 – 6/30/200/ 4 Year Lease Thru 11/15/2001	One Year Lease Average = $113,695	17.01%	$63,453	$51,814	$11,639	$50,242	9.61%
5	Lucent Technologies	Master Service Agreement	$100,000	14.96%	$60,821	$51,039	$9,782	$39,179	9.21%
6	University of Massachusetts. (UIS)	7/1/1999 – 6/30/2000	$ 24,000	3.59%	$28,371	$12,739	$15,632	($4,371)	4.30%
7	CBE Technologies	7/01/1999- 6/30/2000	$ 5,273	0.79%	$6,704	$5,667	$1037	($1.431)	1.02%
8	Recall Corporation	Minimum Service Agreement	$100 per Month with an Additional $10 Admin. Fee.	0.18%	$1,230	$300	$930	$0	0.18%
9	Scantron Service Group	7/1/1999 – 6/6/200	$ 615	0.09%	$615	-	$615	$0	0.09%
10	Nortel Networks	1/5/1999 – 1/2/2000	$ 460	0.07%	$460	-	$460	$0	0.07%
			---	---	---	---	---	---	
	Totals:		$668,575	100.00%	$660,278	$141,479	$518,799	$9,979	100.00%

Information Technology (IT)-Related Third-Party Vendor Contracts

Fiscal Year 2001
As of July 25, 2001

Contract Number	Vendor Name	Contract Period	Contract Amount	Percentage of IT-Related Contract Amount	Total of Actual Expenditures	Payment Type: State Funds	Payment Type: College Trust Funds	Percentage of Total Contract Expenditures as of 7/25/2001
1	Campus Works, Inc. (Contract Addendum)	5/15/2000 – 6/30/2001	$594,200	60.24%	$483,651	-	$483,651	73.00%
2	SCT Corporation (Banner and Oracle System License and Maintenance Contract)	5 Year Lease 5/1/1997 – 4/30/2002	Five Year Contract Total = $616,510 One Year Average = $123,302	12.50%	$58,534	$55,699	$2,835	8.83%
3 & 4	Data General Corporation (Maintenance Agreement) & (Lease Agreement)	7/1/1999 – 6/30/200/4 Year Lease Thru 11/15/2001	One Year Lease Average = $113,695	11.53%	$33,355	$33,336	$19	5.20%
5	Avaya Inc. (Formally Lucent Technologies)	Master Service Agreement	$100,000	10.14%	$23,221	$21,098	$2,123	3.50%
6	University of Massachusetts. (UIS)	7/1/2000 – 6/30/2001	$ 24,000	2.43%	$23,699	$23,661	$38	3.60%
7	Net Casters	10/16/2000 – Unspecified End Date	$ 12,750	1.29%	$13,250	$8,500	$4,750	1.85%
8	3 Comm	6/26/2000 – 9/21/2001	$ 10,226	1.04%	$10,226	$10,226	-	1.54%
9	CBE Technologies	7/01/2000-6/30/2001	$ 5,273	0.53%	$6,006	$5,270	$736	0.90%
10	Recall Corporation	Minimum Service Agreement	$100 per Month with an Additional $10 Admin. Fee.	0.19%	$1,890	$630	$1260	0.28%
11	Scantron Service Group	6/6/2000 – 6/5/2001	$ 615	0.06%	$8587	-	$8587	1.23%
12	Nortel Networks	1/2/200 – 1/5/2001	$ 460	0.05%	$460	-	$460	0.07%
			---	---	---	---	---	
	Totals:		$986,411	100.00%	$662,879	$158,420	$504,459	100.00%

APPENDIX C

Analysis of NECC Documentation Regarding CWI Contract Addendum 3

Chart 1

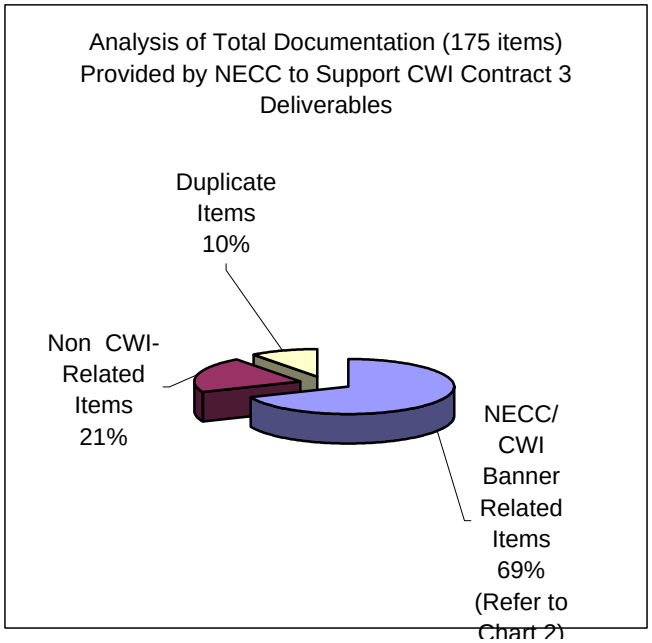


Chart 2

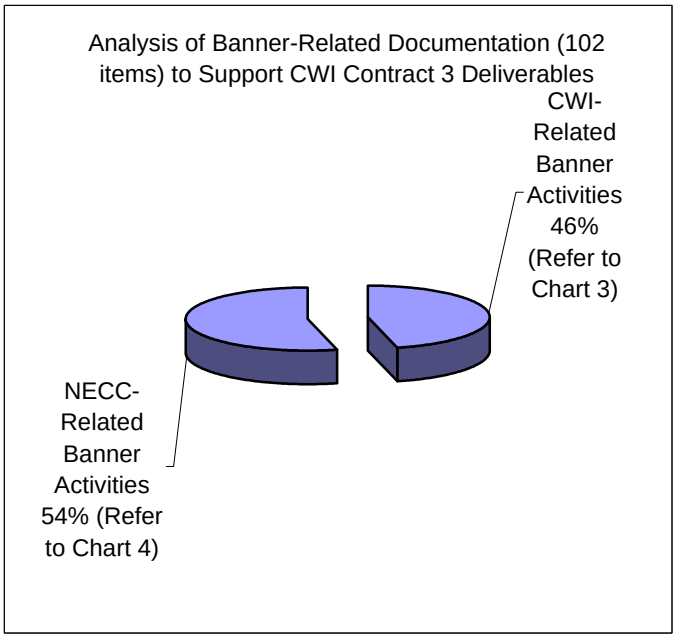


Chart 3

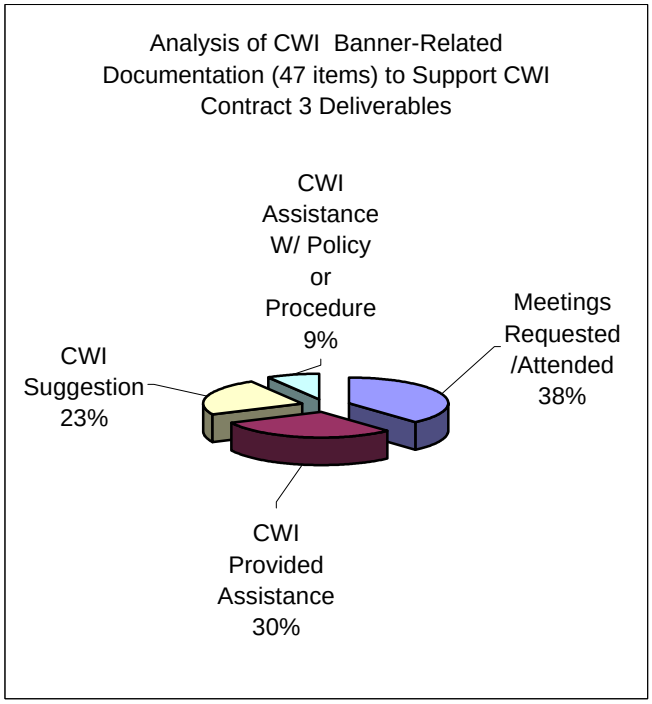


Chart 4

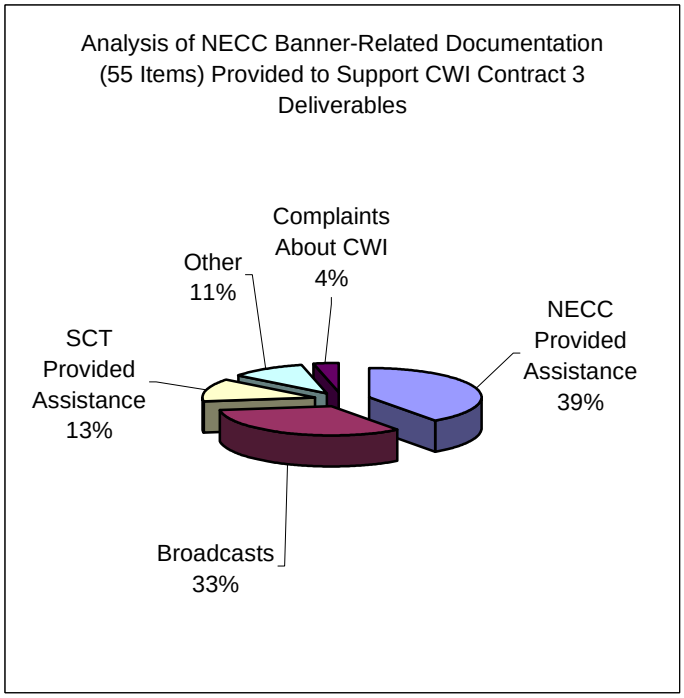


Chart Number 3 illustrates CWI scope of work performed.

APPENDIX D

Analysis of NECC Documentation Regarding CWI Contract Addendum 4

Chart 1

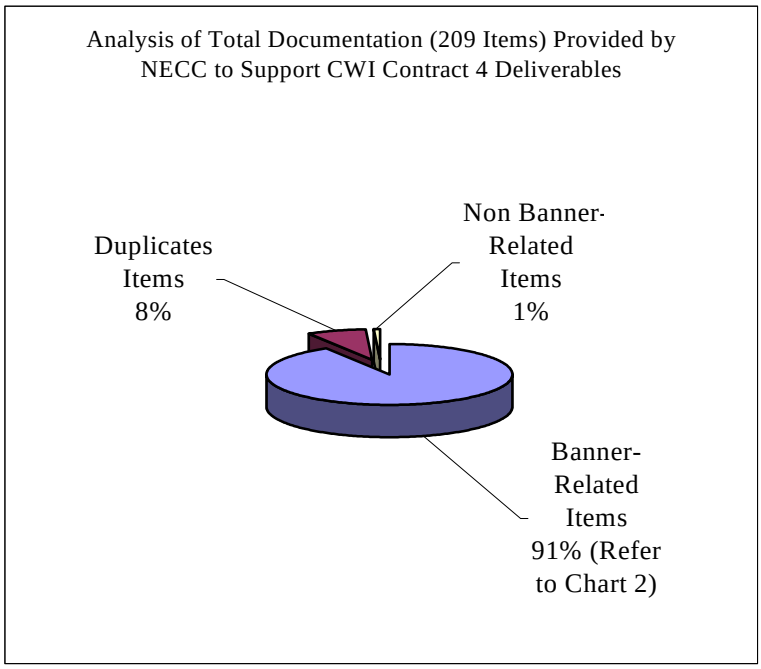


Chart 2

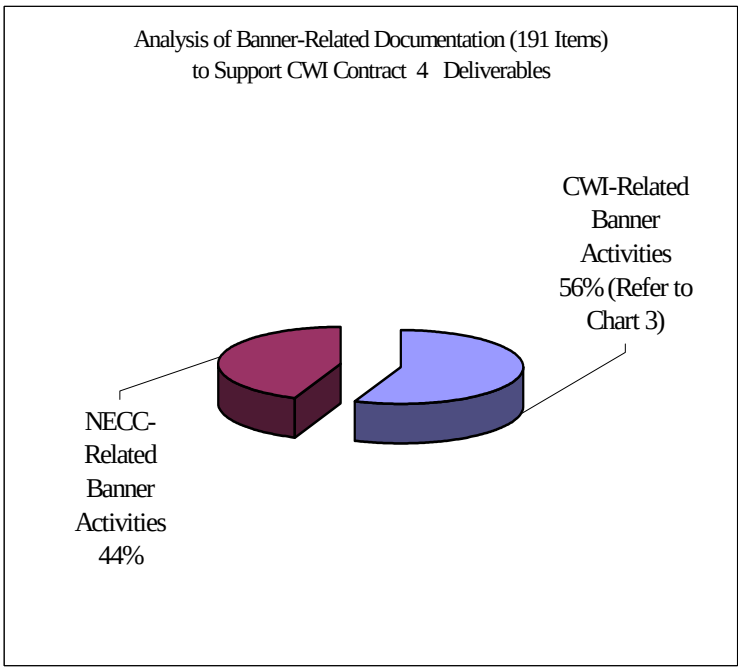


Chart 3

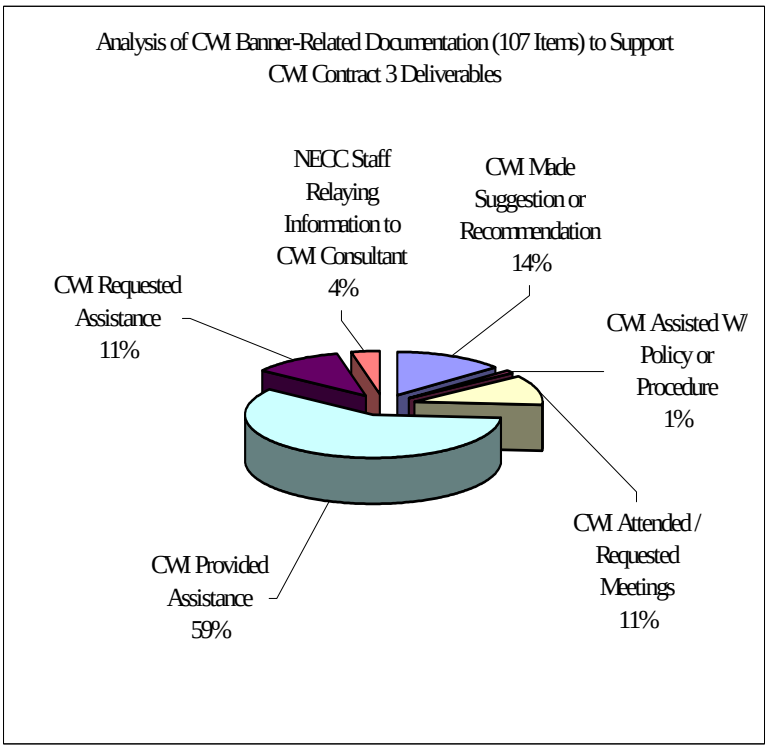


Chart Number 3 illustrates CWI scope of work performed.

APPENDIX E

Board of Higher Education Trust Fund Guideline Information

Contract 1 Signed:	June 7, 1999
Contract Period:	Work completed on July 30, 1999
Type of Contract:	Information Technology Retainer Agreement
Compensation:	24 hours of service at a $200 per hour rate, not to exceed $4,800. Reasonable travel and per diem expenses were also reimbursable. Both consulting fees and expenses were to be payable upon receipt of CWI's invoice.
Invoice Dated:	August 2, 1999 for $4,800
Invoice Paid:	August 11, 1999 for $4,800
Contract 2 Signed:	July 28, 1999
Contract Period:	August 9, 1999 through August 8, 2000
Actual Contract Period:	August 9, 1999 through September 4, 1999
Type of Contract:	Addendum to Information Technology Consulting Retainer Dated May 26, 1999
Compensation:	The estimated cost for CWI time and expenses for the period August 9, 1999 to September 4, 1999 was $ 18,000 to $22,000. The cost was based on a Principal Consultant Rate of $1,600 - $2,000 per person day ($200 to $250 per hour) and estimated expenses
Invoice Dated:	September 8, 1999 for $22,000
Invoice Paid:	September 15, 1999 for $22,000
Contract 3 Signed:	August 30, 1999
Contract Period:	September 6, 1999 through June 30, 2000
Actual Contract Period:	September 6, 1999 through April 30, 2000
Type of Contract:	Addendum to July 28, 1999 Information Technology Consulting Retainer.
Compensation 1:	For the period September 6, 1999 through January 5, 2000, the estimated cost for professional staff time and related expenses was $200,000. For the same period, the estimated monthly cost for professional staff time and related expenses (assuming a range of sixteen to twenty-two person days per month) was $45,000 to $55,000. This "range" equals a cost per day of $2,812 to $2,500.
Formula 1:	The consultant rate for senior level CWI professional staff time was not to be greater than $2,000 per day as established by documentation provided to the audit team in the form of vendor reports and invoices. Thus, the service time expenses range from $32,000 (16 days times $2,000 per day) to $44,000 (22 days times $2,000 per day). The remainder of $13,000 to $11,000 would be attributed to expenses.

Compensation 2:	For the period January 6, 2000 through June 30, 2000, the estimated cost for professional staff time and related expenses was $100,000. For the same period, the estimated monthly cost for professional staff time and related expenses (assuming a range of seven to eight person days per month) was $16,000 to $17,000. The consultant rate for senior level CWI professional staff was $1,600 to $2,000 per person per day, plus expenses.
Formula 2:	The consultant rate for senior level CWI professional staff is $1,600 to $2,000 per person per day as outlined in contract 2. Thus, the service time expense ranges are from $11,200 to $14,000 (seven days times $1,600 to $2,000 per day) to $12,800 to $16,000 (eight days times $1,600 to $2,000 per day).
Contract 4 Signed:	May 15, 2000
Contract Period:	May 15, 2000 through June 30, 2001
Actual Contract Period:	May 1, 2000 through June 30, 2001. This was a fourteen-month contract
Type of Contract:	Addendum to August 30, 1999 Information Technology Consulting Retainer.
Compensation 1:	For the period May 1, 2000 through June 30, 2000, the total cost for CWI professional services shall be $44,200, or a monthly cost of $22,100.
Formula 1:	Flat rate of $22,100 per month with no reference to expenses.
Compensation 2:	For the period July 1, 2000 through June 30, 2001, CWI shall provide approximately 1.45 to 2.2 FTE (including approximately .2 FTE for general management oversight) at a total cost between $434,100 and $650,000 or a monthly cost between $36,175 and $54,167. Of this amount, one-half of the one-half to one FTE for the Oracle DBA cost amounts to between $69,000 and $138,000.
Formula 2:	<u>CWI Senior Staff:</u> 1 FTE equals 160 hours per month, full-time employee, as stated by the College and CWI invoices presented to our audit team with an associated cost of $28,948. 1.45 FTE @ $36,175 per month equals $24,948 per monthly FTE rate. FTE @ $54,167 per month equals $24,621 per monthly FTE rate. <u>Oracle DBA:</u> One-half FTE of one-half equals one-quarter (.25) FTE, therefore, .25 FTE @ 40 hours equals $6,237. One-half of one FTE equals one-half (.50) FTE, therefore, .50 FTE @ 80 hours equals $12,474.