The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH

ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108

A. JOSEPH DE NUCCI
AUDITOR

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

No. 2009-0192-4T

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

July 1, 2007 through August 14, 2009

OFFICIAL AUDIT REPORT

JANUARY 4, 2010

TABLE OF CONTENTS

INTRODUCTION

Bunker Hill Community College (BHCC) is a two-year Massachusetts institution of higher education offering associate degrees and certificate programs. BHCC, which was established in 1973, is a member of the Massachusetts State College System and is regulated by Chapter 15A, Section 5, of the Massachusetts General Laws. BHCC's primary mission is to provide academic preparation for transfer to four-year institutions, career preparation for entry into occupational fields, developmental courses to prepare students for college-level work, and job retraining.

BHCC is governed by a Board of Trustees and is under the direction of BHCC's President. The Department of Higher Education provides additional oversight to BHCC and monitors each Massachusetts higher educational institution to help ensure that state funds support measurable performance, productivity, and results. For the spring semester of 2009, BHCC had a student enrollment of 9,866 day and evening students. BHCC's Charlestown campus is located on New Rutherford Avenue in Boston and its Chelsea campus is located on Hawthorne Street. Satellite operations are located in Cambridge, Boston, Somerville, and Malden. BHCC maintains information technology (IT) facilities and computer labs at both Charlestown and Chelsea campuses.

The Information Technology Services Department supports BHCC's mission by providing IT services to administrative staff, instructors, and the student population. BHCC's information systems are used for administrative and academic computing and provide financial, college management, and student service functions. The primary administrative system is a vendor-supplied, integrated application known as "Colleague" that has a Unidata database system operated on a Sun Solaris v890 server. The Colleague application is composed of integrated modules (or subsystems) that provide automated processing for purchasing and accounts payable, accounts receivable and cash receipts, general ledger, financial aid, fixed assets, admissions, registration, curriculum management, and academic records. A secondary Sun Solaris server facilitates a backup role for disaster recovery and business continuity, while a third Solaris server supports testing and stores archived files for legacy usage.

BHCC uses the Microsoft Windows server platform for file and print services. The servers utilize a Windows Server 2003 operating system and are patched at a consistent level using Microsoft's Windows Software Update Services (WSUS). Patch levels for both Windows servers and workstations are reviewed on a regular basis through the reporting features of WSUS.

BHCC's present network consists of Windows 2003 Active Directory servers, and Windows XP Professional as the standard desktop operating system. BHCC also uses Solaris, Linux, and Mac servers, but the "core" can be considered Microsoft-based for authentication, file and print, and administration. A high-bandwidth Ethernet Virtual Private Local Area Network was added in early 2009 to support Internet connectivity between the Chelsea and Charlestown campus. Also, BHCC implemented a Cisco firewall device at Chelsea that complements the Cisco firewall devices at the Charlestown campus.

The fall 2005 semester marked the first time in BHCC's history that students were provided email accounts. During the summer of 2008, BHCC "in-sourced" student email, improving student email access and reducing costs by $70,000. At the time of the audit, faculty, staff, and student email accounts resided on Microsoft Exchange Servers. The BHCC community presently uses Microsoft Outlook and Web-Based Access.

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

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

In accordance with Chapter 11, Section 12, of the Massachusetts General Laws, we performed an information technology (IT) general controls examination of IT-related activities at the Bunker Hill Community College (BHCC) for the period July 1, 2007 through August 14, 2009. The audit was conducted from February 23, 2009 through August 14, 2009. Our audit included a review of corrective action taken in response to prior audit results brought forward in our prior audit report, No. 2002-0192-4T, issued July 11, 2002, pertaining to IT-related contract management and business continuity planning. Our audit scope also included an examination of internal controls relating to administrative and academic computing regarding IT-related organization and management, system access security, and on-site and off-site storage of backup media. Our audit also included a review of BHCC's policies and procedures to protect and maintain confidential personal information as required by Executive Order No. 504 and Chapter 93H of the Massachusetts General Laws.

Audit Objectives

Our primary audit objective was to determine whether adequate IT-related controls were in place and in effect for selected functions of BHCC's IT processing environment. In this regard, we sought to determine whether BHCC's IT-related internal control environment, including policies, procedures, practices, and organizational structure, provided reasonable assurance that IT-related control objectives would be achieved to support BHCC's business functions. Our audit objective regarding organization and management was to determine whether IT-related roles and responsibilities were clearly defined, points of accountability were established, appropriate organizational controls were in place, and IT-related policies and procedures adequately addressed the areas under review. In conjunction with our review of the IT operations, we sought to determine whether BHCC had implemented IT-related strategic and tactical plans that help to fulfill BHCC's mission and goals. We sought to determine whether BHCC had implemented written and approved policies and procedures regarding the proper accounting for, authorized access to, and safeguarding of its IT-related assets. We further sought to determine whether adequate controls were in place to prevent and detect unauthorized system access to the data files and software residing on the Unidata database system.

To determine whether adequate controls existed over third-party IT-related service provider contracts, we reviewed whether a formal contract was in place to cover IT-related services in sufficient detail, the contract was properly signed and dated, and incorporated vendors were properly registered with the Office of the Secretary of State. In addition, we also verified whether contract services had been monitored and evaluated for the provision of adequate services and deliverables through the establishment and enforcement of IT-related contract administration policies and procedures recommended in our prior audit report.

Regarding systems availability, we sought to determine whether adequate disaster recovery and 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 IT 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. We further sought to determine that a sufficiently comprehensive business continuity and contingency plan had been completed as recommended in our prior audit.

We also sought to evaluate whether adequate controls were in place to protect personal information and to determine whether BHCC's control policies and procedures were adequate to comply with the Commonwealth's data breach notification requirements. Personally identifiable information consists of information that can potentially be used to uniquely identify individuals.

Audit Methodology

To determine the areas to be examined during the audit, we conducted pre-audit work, which included a review of relevant enabling legislation and the status of issues and concerns brought forth to BHCC in prior audit work. We also obtained and recorded an understanding of BHCC's mission, organization, management, and business objectives. We reviewed and evaluated the general IT-related internal control environment at BHCC and conducted interviews with senior management to discuss BHCC's control environment. In conjunction with our review of the internal control environment, we determined whether BHCC had developed and implemented formal internal control documentation and IT-related policies and procedures and sufficient controls for physical security and environmental protection for BHCC data centers. In order to obtain a preliminary understanding of BHCC's activities regarding IT-related contract administration and the safeguarding, accounting for, and reporting of property and equipment, we interviewed College management and staff, reviewed relevant Commonwealth statutes and regulations regarding fixed-asset management, and reviewed BHCC's related policies and procedures, selected contracts, and records.

Regarding our examination of IT organization and management, we interviewed senior management; reviewed, analyzed, and assessed the adequacy of existing IT-related policies, standards, procedures, and IT-related strategic and tactical plans; and assessed IT-related management practices. To determine whether an IT-related users group was in place and operating for the purpose of providing adequate oversight of IT functions and processes across BHCC, we interviewed senior management and IT staff. To determine whether BHCC's IT-related job descriptions and job specifications were up-to-date and reflected current responsibilities, we obtained a current list of the personnel employed by the Information Technology Services Department, as well as copies of their duties and job descriptions. We compared the job descriptions to the employee listing and the Information Technology Services Department's organizational chart, and interviewed employees concerning their IT-related duties and responsibilities.

To determine whether system access security controls were in place to provide reasonable assurance that only those personnel authorized to use BHCC'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. Regarding password administration, we reviewed controls to activate and deactivate user IDs and passwords, require appropriate length and composition of passwords, and ensure that passwords are periodically changed. We determined the frequency with which all staff authorized to access the automated systems were required to change their passwords. To determine whether user IDs and password security were being properly maintained, we interviewed the security administrator and assessed the level of access security being provided. To determine whether access privileges were provided to only authorized users, we reviewed procedures for granting system access and compared the list of staff authorized to access the information systems with the current BHCC employee list, which included all current employees, adjunct faculty, and other persons affiliated with BHCC. We determined whether procedures were in place to provide reasonable assurance that BHCC's security administrator was notified, 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 of access privileges.

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 using BHCC's contractor selection process. The Commonwealth's Secretary of State's Office was consulted to determine whether the incorporated 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 BHCC signatures indicating proper authorization and approval to meet compliance with applicable regulations. We assessed the contract monitoring methods and functions in place at BHCC to determine whether they were sufficient to provide reasonable assurance that contractors consistently provided quality services and deliverables outlined in the contract document.

Regarding the safeguarding of personal information, we reviewed BHCC's attempt to comply with Chapter 93H of the General Laws, Executive Order No. 504, and policy and guidance issued by the Commonwealth's Information Technology Division. In addition, we reviewed BHCC's policies and procedures, interviewed key BHCC management regarding the protection of sensitive College information, and reviewed a report issued by an outside vendor hired to perform a risk assessment as required by Executive Order No. 504.

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 BHCC 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 an alternate processing site to be used in case of a disruption or loss of 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 copies of magnetic media. We interviewed the Senior Systems Administrator responsible for the automated live full backup of the system and reviewed the current backup procedures in place for their adequacy and completeness. We analyzed the physical access security for the off-site storage facility in order to determine whether the backup copies of data files were secured from accidental or purposeful damage and unauthorized examination, removal, or disclosure of confidential information contained therein.

Our audit was conducted in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States through the U.S. Government Accountability Office and generally accepted industry practices. Audit criteria used in the audit included management policies and procedures and control guidelines outlined in Control Objectives for Information and Related Technology (CobiT version 4.1), as issued by the Information Systems Audit and Control Association, July 2007.

AUDIT CONCLUSION

Based on our audit, we found that Bunker Hill Community College's (BHCC) internal controls provided reasonable assurance that IT-related control objectives pertaining to organization and management, IT strategic and tactical planning, system access security, on-site and off-site storage of backup copies of magnetic media, and business continuity and disaster recovery would be met. We also found that controls in place provided reasonable assurance that personally identifiable information would be protected from unauthorized access or disclosure.

Our review of IT management and organizational controls indicated that BHCC had an appropriate and defined organizational structure and chain of command for the IT Department with assigned reporting responsibilities and documented job descriptions. In addition, BHCC had documented IT strategic and tactical plans that identified business goals and addressed risks to the IT environment and mission-critical applications. The IT strategic plan supported business requirements by helping to ensure that control practices, such as system access security and hardware inventory controls, would be adequately communicated and administered.

Regarding system access security, our audit revealed that adequate controls were in place and in effect to provide reasonable assurance that only authorized users would be able to access BHCC's automated systems. We determined that BHCC had documented procedures in place for the activation of user IDs and passwords that allow network access privileges by faculty, staff, and students. We also determined through our test of user accounts that controls were in place to provide reasonable assurance that network access privileges would be disabled in a timely manner for faculty and staff who would be no longer employed by BHCC. The College had all system users sign a "Technology Use Policy" form to help ensure that users understood their responsibilities regarding acceptable use, data confidentiality, copyright protection, virus protection, security, and email usage. We determined that each office is responsible for overseeing access rights within their respective areas.

Our review of controls over personal information determined that BHCC had adopted controls to address Executive Order No. 504 and policy and guidance issued by the Commonwealth's Information Technology Division to protect electronic and hardcopy information that can potentially be used to uniquely identify an employee or student of BHCC. We also determined that user access to the system to add, update, and electronically view sensitive information is monitored and approved by the appropriate office managers.

Regarding IT-related contracts with third-party vendors, we found that BHCC exercised adequate management oversight to hold contracted parties sufficiently accountable for their performance and delivery of service through the establishment and enforcement of IT-related contract administration policies and procedures, and that the incorporated vendors selected were legally registered with the Commonwealth.

We also determined that BHCC had completed a sufficiently comprehensive disaster recovery plan and business continuity plan to provide for the timely restoration of mission-critical and essential business functions should IT systems be rendered inoperable or inaccessible. We found controls over the information technology systems ensuring the continuance of essential business functions to be in place and in effect in the event of a disaster. Our audit also confirmed that comprehensive BHCC user area plans for the "Colleague" academic and financial functions had been developed and were incorporated into the disaster recovery and business continuity plan. The BHCC disaster recovery and business continuity plan provides up-to-date specific instructions for various courses of action to address different types of disaster scenarios at the Charlestown data center.

Regarding the availability of mission-critical and essential systems at BHCC, we found that BHCC's disaster recovery plan included policies and procedures to support recovery of mission-critical systems and included background information for each system, system dependencies, support information, back-up procedures, recovery steps, and data-loss risk assessments. Our audit indicated that BHCC would be able to access backup magnetic media for its system/applications should a disaster render BHCC's computer system unavailable or inaccessible. BHCC's management indicated that, based on their current tests of the disaster recovery and business continuity plan, they are confident that BHCC would be able to conduct business, regardless of the location of BHCC's IT systems, within 48 hours of a disaster that had caused a total shut down of IT operations.

BHCC should continue to assess the extent to which it is dependent upon the continued availability of information systems for all required processing or operational needs and should continue to develop its recovery plans based on the critical aspects of its information systems. BHCC should continue its effort to implement procedures to provide reasonable assurance that the criticality of systems is evaluated, business continuity requirements are assessed on an annual basis or upon major changes to user requirements or the automated systems, and that appropriate business continuity plans and user area plans are reviewed and updated for all mission-critical and essential applications.

Auditee's Response

> *We agree with the audit results and your recommendations and appreciate the professionalism displayed by the audit staff throughout the entire audit process.*