Commonwealth of Massachusetts
Office of the State Auditor
Suzanne M. Bump

Making government work better

Official Audit Report – Issued January 26, 2012

Northern Essex Community College

For the period July 1, 2009 through May 31, 2011

TABLE OF CONTENTS/EXECUTIVE SUMMARY

Northern Essex Community College (NECC), established in 1961, is a member of the Massachusetts State College System enabled by Chapter 15A, Section 5, of the Massachusetts General Laws. NECC, a member of the Department of Higher Education system, is one of 29 campuses that are divided into three segments: 15 community colleges, nine state universities, and the five University of Massachusetts campuses. At the time of our audit, NECC had a student population of 8,966 (day and evening sessions), faculty of 532, and administration and support staff of 327.

In accordance with Chapter 11, Section 12, of the Massachusetts General Laws, the Office of the State Auditor (OSA) performed an audit of NECC for the period July 1, 2009 through May 31, 2011. Our audit included an examination of general controls pertaining to information technology (IT) organization and management, physical security, environmental protection, system access security, inventory control over computer equipment, business continuity and disaster recovery planning, and IT service contract management. In addition, the audit scope included a review of controls in place to protect the integrity and confidentiality of data contained in the NECC network, including a review of NECC's control practices regarding compliance with Payment Card Industry (PCI) security standards and a review of controls over personally identifiable information (PII).

Based on our audit, we have concluded that, except as reported in the Audit Results section of this report, for the period July 1, 2009 through May 31, 2011, adequate internal controls were in place and in effect to provide reasonable assurance that IT-related control objectives would be met regarding IT organization and management, physical security and environmental protection for areas housing computer equipment, system access security, on-site and off-site storage of backup copies of magnetic media, third-party provider IT service contracts, and compliance with security requirements related to PCI and PII standards.

Our audit disclosed that although NECC had developed an Internal Control Plan (ICP), it did not have a high-level summarization of internal controls containing sufficient cross-referencing to support lower-level detail (e.g., departmental policies and procedures). NECC had not adequately updated the plan as required by the Office of the State Comptroller's (OSC) Internal Control Guide and Chapter 647 of the Acts of 1989, An Act Relative to Improving Internal Controls within State Agencies. As a result, the current ICP does not provide sufficient guidance to ensure that appropriate IT controls are implemented, exercised, monitored, and evaluated to provide reasonable assurance that operational objectives are met and risks are prevented or detected and corrected in a timely manner.

Our audit disclosed that NECC was not recording all purchased computer equipment into Banner, the inventory system of record; that an annual physical inventory and reconciliation of fixed assets for fiscal years 2009 through 2011 had not been performed; and that computer equipment items on the inventory system of record could not be located. As a result, NECC was unable to maintain a valid and complete perpetual inventory system of record that could be relied upon to support IT configuration management and help safeguard NECC's computer equipment. In addition, NECC did not report to the OSA two computer monitors stolen on March 2, 2010. Chapter 647 of the Acts of 1989 requires agencies to file a report on lost or stolen Commonwealth assets with the OSA. Furthermore, NECC's incomplete inventory record hindered its ability to properly account for IT resources, evaluate the allocation of equipment, identify missing equipment, meet IT configuration objectives, and serve as a reliable record of IT equipment. Our audit also disclosed that NECC did not maintain a formal policy to control the assignment and use of notebook computers, which could hinder NECC's ability to properly account for available computers.

Our audit determined that NECC did not have a 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 that, while NECC may have assessed the relative criticality of computing systems and developed various policies, it had not outlined or tested comprehensive recovery strategies to address various disaster scenarios that could result in seriously degraded or lost IT processing capabilities. Additionally, NECC had not documented the necessary tasks and responsibilities for all relevant personnel to carry out NECC's duties and business objectives under various disaster scenarios.

INTRODUCTION

Background

Northern Essex Community College (NECC) is a public, two-year college that offers academic programs through which students can earn their Associate's Degrees or certificates in specialized programs. NECC, established in 1961, is a member of the Massachusetts State College System enabled by Chapter 15A, Section 5, of the Massachusetts General Laws. NECC is a member of the Department of Higher Education system, one of 29 campuses divided into three segments: 15 community colleges, nine state universities, and the five University of Massachusetts campuses. The Board of Higher Education oversees the system and monitors each Massachusetts higher educational institution to ensure that state funds support measurable performance, productivity, and results.

NECC's main campus is located on Elliott Street in Haverhill, with two additional campuses in Lawrence. According to the NECC Department of Institutional Research and Planning, as of March 2, 2011, NECC had a student population of 8,966 (day and evening sessions), a faculty of 532, and 327 administration and support staff.

A Board of Trustees, under the direction of NECC's President, governs NECC. NECC's administrative mission and department operations are supported by automated systems provided by the Information Technology Service (ITS) Department, which is composed of three divisions under the supervision of a Chief Information Officer (CIO), who reports directly to the President of NECC. The divisions include Management Information Services (MIS), the Network Operations Center (NOC), and Client Services (CS). The NOC and CS divisions report to the Director of NOC, who reports to the CIO.

The Information Technology Committee (ITC) was formed in May of 2009 with the purpose of ensuring that all divisions of NECC's administration have input into information technology (IT) strategic planning. The ITC members consist of the CIO, the Director of NOC, the Dean of Academic Technology, the Director of Online Communications, and one representative of each of the administrative divisions. The Chair is elected on an annual basis, and ITC meets monthly.

NECC's ITS Department provides a campus-wide network and client infrastructure (NECC network) consisting of 50 physical and 25 virtual servers that support over 2,000 workstations and

110 notebook computers. Approximately 600 students use NECC's secure wireless infrastructure. The primary network operating system for NECC's file printing, Domain Name System (DNS), and authentication services is Microsoft Windows 2008, with Windows 7 running on the desktops.

The primary application system is SunGard's Banner Enterprise Resource Planning, using Oracle's relational-database management system to support the integration of the subsystems. SunGard's Banner application is used to process NECC's financial management, administrative, and student information. Banner includes a suite of five integrated subsystems: financial operations, alumni development, human resources, student administration, and financial aid applications

Audit Scope, Objectives, and Methodology

In accordance with Chapter 11, Section 12, of the General Laws, we performed an IT general controls examination at NECC for the period July 1, 2009 through May 31, 2011. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Criteria used in the audit included Chapter 93H of the General Laws; Executive Orders No. 490, No. 491, and No. 504; Chapter 82 of the Acts of 2007; Chapter 647 of the Acts of 1989; management policies and procedures; control guidelines outlined in Control Objectives for Information and Related Technology (CobiT version 4.1) issued by the Information Systems Audit and Control Association in July 2007; and Payment Card Industry (PCI) Data Security Standards.

Our audit scope included an examination of general controls pertaining to IT organization and management, physical security, environmental protection, system access security, inventory control over computer equipment, business continuity and disaster recovery planning, and IT service contract management. In addition, the audit scope included a review of controls in place to protect the integrity and confidentiality of data contained in the NECC network, including a review of NECC's control practices regarding compliance with PCI security standards and a review of controls over Personally Identifiable Information (PII).

The primary audit objective was to determine whether NECC's IT-related internal control environment—including policies, procedures, practices, and organizational structure—provided reasonable assurance that control objectives would be achieved to support NECC's business functions. Our audit also sought to determine whether roles and responsibilities for IT staff were clearly defined, points of accountability were established, appropriate organizational controls were in place and in effect, and whether policies and procedures were appropriate. A further objective was to determine whether NECC had an IT strategic planning process in place from which IT strategic and tactical plans would be developed to help direct the use of technology to fulfill NECC's mission and goals.

To achieve our audit objectives, we:

- Interviewed senior management and analyzed and reviewed the organizational structure of the ITS department to determine whether an Internal Control Plan (ICP) and other IT-related policies and procedures were in place and in effect, and whether they were documented, approved, and communicated to appropriate staff.
- Evaluated whether adequate controls were in place to provide reasonable assurance that IT resources would be safeguarded, properly accounted for, and available when required.
- Determined whether adequate physical security, environmental, system access security, and inventory controls were in place to prevent loss, damage, or unauthorized access to IT resources.
- Examined whether NECC's disaster recovery and business continuity plans would provide reasonable assurance that mission-critical IT capabilities could be regained within an acceptable period of time should IT resources be rendered inoperable or inaccessible
- Determined whether adequate monitoring and evaluation controls were in place over third-party IT service contracts.
- Determined whether NECC was in compliance with PCI and Personally Identifiable Information (PII) data security standards.

Based on our audit, we have concluded that, except as reported in the Audit Results section of this report, for the period July 1, 2009 through May 31, 2011, adequate internal controls were in place and in effect to provide reasonable assurance that IT-related control objectives would be met regarding IT organization and management, physical security and environmental protection for areas housing computer equipment, system access security, on-site and off-site storage of backup copies of magnetic media, third-party provider IT service contracts, and compliance with security requirements related to PCI and PII standards.

AUDIT RESULTS

1. INTERNAL CONTROL PLAN NEEDS IMPROVEMENT

Our audit disclosed that although Northern Essex Community College (NECC) had developed an Internal Control Plan (ICP), it did not have a high-level summarization of internal controls containing sufficient cross-referencing to support lower-level detail (e.g., departmental policies and procedures). NECC had not adequately updated the plan as required by the Office of the State Comptroller's (OSC) Internal Control Guide and Chapter 647 of the Acts of 1989, An Act Relative to Improving Internal Controls within State Agencies. As a result, the current ICP does not provide adequate guidance to ensure that appropriate information technology (IT) controls are implemented and exercised so that operational objectives are met; risks are prevented or detected and corrected in a timely manner; and the integrity, security, and availability of its systems and records and effectively protected.

Chapter 647 of the Acts of 1989 establishes the minimum level of quality acceptable for an internal control system in operation throughout the Commonwealth's departments, agencies, and colleges. Chapter 647 states that "internal control systems for the various state agencies and departments of the Commonwealth shall be developed in accordance with internal control guidelines established by the Comptroller." Subsequent to the passage of Chapter 647, the OSC issued the Internal Control Guide for Managers and the Internal Control Guide for Departments. In these guides, the OSC stressed the importance of an internal control plan and the need for state entities to develop internal control policies and procedures.

NECC management indicated that they recognized the need to complete a comprehensive ICP to strengthen NECC's framework of control and address the control requirements set forth by the OSC.

Recommendation

NECC's Internal Control Officer should work with NECC's various departments to identify and document operational and control objectives and risks and identify existing control policies, procedures, and management control practices. The process of completing the ICP should include identifying any gaps in required controls and developing a framework to design, implement, and exercise any additional controls required. Finally, the ICP should address the components of the

Committee of Sponsoring Organizations of the Treadway Commission (COSO) control model and ensure compliance with the OSC's internal control guidelines.

Auditee's Response

> *The contents of the report are accurate, and we offer the following in response to the audit results. In May of this past year NECC hired a new Vice President of Finance / Chief Financial Officer (CFO). As part of his organization review the CFO has recommended and then received Presidential Cabinet approval to create a new Policy Committee. The Policy Committee will be co-chaired by the CFO and Chief Information Officer (CIO). The Committee will begin work in early September and one of the first items they will focus on will be updating the Internal Control Plan (ICP). This will ensure that controls are coordinated with proper policies and procedures in each critical division across the College. In addition, the Committee will provide the vehicle to develop new policies for Cabinet approval. The updated ICP is scheduled to be completed by January 2012.*

2. INVENTORY CONTROLS OVER COMPUTER EQUIPMENT NEED IMPROVEMENT

Our audit disclosed that NECC's documented inventory control procedures and practices regarding computer equipment need to be strengthened and formalized to ensure that IT resources are properly accounted for in a complete and current system of record. Further, NECC was not recording all purchased computer equipment into Banner, NECC's system of record for fixed assets, and had not performed an annual physical inventory and reconciliation of fixed assets for fiscal years 2009 through 2011.

To determine whether the inventory system of record for computer equipment was current, accurate, complete, and valid, we selected a statistical sample of 95 items out of a total population of 1,697 items contained on the March 14, 2011 system of record. To evaluate whether the system of record accurately and completely reflected the items of computer equipment, we verified the location, description, inventory tags, and serial numbers of the hardware items listed on the inventory system of record and compared the inventory record to the actual equipment on-hand.

To verify the reliability and completeness of the NECC system of record, we randomly selected 62 additional computer hardware items in adjacent locations to our original inventory sample and determined whether they were properly recorded. To determine whether selected computer hardware purchases in fiscal years 2010 and 2011 were accurately and completely listed, we judgmentally selected 47 vendor invoices containing 214 equipment items valued at $271,000 and verified whether the asset information, including serial numbers contained on the purchase orders and related invoices, were properly recorded on the inventory system of record. Our sample testing of the 214 computer equipment items determined that NECC had not recorded 121 (56.5%) of the items with an approximate cost of $95,000 on the inventory system of record, and eight items—four of which were notebook computers—valued at $8,078 could not be located. Twenty-four items were found in different locations than those recorded on the inventory system of record. Eight items did not contain NECC asset tags, as required by OSC fixed asset guidelines. We also found that NECC did not maintain a formal policy to control the assignment and use of notebook computers. Employees assigned notebook computers were not required to sign a control sheet acknowledging responsibility for security and authorized use. The lack of formal policies and procedures to control notebook computers could hinder NECC's ability to properly account for available computer equipment. In addition, NECC did not report to the Office of the State Auditor (OSA) two computer monitors stolen on March 2, 2010. Chapter 647 of the Acts of 1989 requires agencies to file a report on lost or stolen Commonwealth assets with the OSA. Furthermore, NECC had not performed an annual physical inventory and reconciliation of computer equipment in fiscal years 2009 through 2011, as required by fixed asset guidelines promulgated by the OSC.

NECC's formalized fixed asset policies—specifically the NECC ICP, last updated March, 2010—lack detailed procedures regarding timely recording of all received assets and the performance of an annual physical inventory, and NECC did not adequately monitor compliance with the ICP. In addition, NECC lacked adequate control procedures and practices to ensure the maintenance of a current, accurate, and complete perpetual inventory record of computer equipment. Regulations promulgated by the OSC require that assets be recorded in a timely manner and that an annual physical inventory and reconciliation be performed annually. As a result of the unrecorded purchased equipment and the failure to conduct annual physical inventories and reconciliations of fixed assets, NECC was unable to maintain a valid and complete perpetual inventory system of record that could be relied upon to support IT configuration management and help safeguard NECC's computer equipment. Controls need to be strengthened to provide prompt notification and update of the inventory record when equipment is purchased, relocated, or disposed.

Recommendation

NECC should strengthen documented inventory control policies, procedures, and practices to ensure compliance with policies and procedures promulgated in the OSC's fixed asset guidelines and its associated internal control documentation. Specifically, NECC should:

- Record all received computer equipment items within seven days and perform a complete annual physical inventory and reconciliation of computer equipment. Maintain and document the inventory system of record on a perpetual basis and periodically verify computer equipment items through reconciliation to physical inventory, acquisition, and disposal records.

- Develop formal policies and procedures requiring that users assigned notebook computers must sign a responsibility and acceptable usage form. Procedures to support the policy should be documented and implemented to help ensure that the equipment is used for approved purposes and that appropriate security measures are taken to reduce the risk of loss or misuse of the equipment.

- Develop formal policies and procedures and train all staff responsible for monitoring and safeguarding computer equipment to ensure that NECC complies with Chapter 647 of the Acts of 1989 reporting requirements.

Auditee's Response

The CFO and Director of facilities have begun to analyze the inventory process for IT equipment at the College and will develop a procedure to ensure equipment received over a certain dollar amount is entered into the accounting fixed asset management system of record (Banner) within fourteen days of receipt. The new procedure will include an annual inventory reconciliation of computer equipment and will ensure the financial records in Banner will be linked to the physical IT inventory in the Dell KACE system by an asset tag number. The CIO will also ensure the current laptop receipt form signed by employees for temporary use is also signed by employees with permanent laptop assignments. These new procedures will be in place by December 2011.

3. DISASTER RECOVERY AND BUSINESS CONTINUITY PLANS NEED TO BE DEVELOPED

Our audit determined that NECC did not have a comprehensive disaster recovery plan (DRP) and business continuity plan (BCP) to provide for the timely restoration of mission-critical and essential business functions should IT systems be rendered inoperable or inaccessible. IT contingency planning is a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of IT systems, operations, and data. This strategy represents a broad scope of activities designed to sustain and recover critical IT services following an emergency. IT contingency planning fits into a much broader emergency preparedness environment that includes organizational and business process continuity and recovery planning.

We found that, while management may have assessed the relative criticality of NECC's computing systems and developed various policies, NECC had not outlined or tested comprehensive recovery strategies to address various disaster scenarios that could result in seriously degraded or lost IT processing capabilities. In addition, every department should develop specific contingency plans to address their critical functions. As part of the ICP, risk is discussed in a number of paragraphs; however, it lacks the necessary level of specificity to determine the extent of potential risks and exposures to IT operations and scenarios. Although NECC understands the importance of recovering data processing systems, the risk analysis should identify the relevant threats that could significantly degrade or render IT systems inoperable or inaccessible, the likelihood of the threat, and expected frequency of occurrence for each disaster scenario. Additionally, NECC had not documented the necessary tasks and responsibilities for all relevant NECC personnel to carry out NECC's duties and business objectives under various disaster scenarios.

Business continuity planning helps ensure the timely recovery and continuation of mission-critical functions should a disaster cause significant disruption to computer operations. Business continuity planning for information services is part of business continuity planning for the entire organization. Generally accepted practices and industry standards for computer operations support the need for each entity to have an ongoing business continuity planning process that assesses the relative criticality of information systems and develops appropriate contingency and recovery plans. To that end, the entity should assess the extent to which it depends upon the continued availability of information systems for all required processing or operational needs and should develop its recovery plans based on the critical aspects of its information systems.

An up-to-date, effective BCP should identify the manner in which essential services would be restored or replaced without the full use of the data center facility or loss of network communications. The BCP should identify the policies and procedures to be followed, detailing the logical order for restoring critical data processing functions either at the original site or at an alternate processing site. In addition, the BCP should describe the tasks and responsibilities necessary to transfer and safeguard backup copies of data files, program software, and system documentation from off-site storage to the site being used for restoration efforts.

Recommendation

NECC should complete a DRP and BCP that incorporate criticality and impact assessments; business continuity planning development; risk management; and recovery plan testing, maintenance, training, and communication. NECC should document recovery strategies to address various disaster scenarios that could adversely impact IT operations and test its DRP and BCP to determine their viability. The plans should assign roles and responsibilities to specific staff members; present detailed steps for them to follow in recovering mission-critical and essential IT systems and operations; and address the telecommunications and security issues that would arise if NECC had to conduct off-site computer operations. In addition, the BCP should document vendor protocol for the emergency use of computers suitable for operating the NECC's mission-critical application and conduct periodic training for the staff and ensure that complete hard copies and electronic copies of the plans are stored in a secure off-site location.

Auditee's Response

> *The Policy Committee will also develop new Disaster Recovery (DR) and Business Continuity (BC) plans that encompass all divisions across the College. The Information Technology and Enrollment Management DR plans will be used as guides to build on and ensure all divisions have performed adequate risk assessments and that plans are properly reviewed by Information Technology for prioritization and feasibility. These plans will be properly vetted and receive Cabinet approval by June 2012.*