STATE OF NORTH CAROLINA

AUDIT OF THE INFORMATION SYSTEMS

GENERAL CONTROLS

NORTH CAROLINA CENTRAL UNIVERSITY

DURHAM, NORTH CAROLINA

APRIL 2006

OFFICE OF THE STATE AUDITOR

LESLIE W. MERRITT, JR., CPA, CFP

STATE AUDITOR

AUDIT OF THE INFORMATION SYSTEMS

GENERAL CONTROLS

NORTH CAROLINA CENTRAL UNIVERSITY

DURHAM, NORTH CAROLINA

APRIL 2006

STATE OF NORTH CAROLINA

Office of the State Auditor

Leslie W. Merritt, Jr., CPA, CFP
State Auditor

2 S. Salisbury Street
20601 Mail Service Center
Raleigh, NC 27699-0601
Telephone: (919) 807-7500
Fax: (919) 807-7647
Internet
http://www.ncauditor.net

AUDITOR'S TRANSMITTAL

The Honorable Michael F. Easley, Governor
Members of the North Carolina General Assembly
The Board of Directors of North Carolina Central University
Dr. James H. Ammons, Chancellor

Ladies and Gentlemen:

We have completed our information systems (IS) audit of North Carolina Central University (NCCU). This audit was conducted from January 9, 2006 through February 17, 2006. The audit was conducted in accordance with *Government Auditing Standards* and *Information Systems Audit Standards*.

The primary objective of this audit was to evaluate IS general controls at NCCU. The scope of our IS general controls audit included general security, access controls, program maintenance, system development, systems software, physical security, operations procedures, and disaster recovery. Other IS general control topics were reviewed as considered necessary.

This report contains an executive summary and audit results which detail the areas where NCCU has performed satisfactorily relevant to our audit scope, where improvements should be made, and where further study is necessary.

We wish to express our sincere appreciation to the staff of North Carolina Central University for the exceptional courtesy, cooperation, and assistance provided to us during this audit.

North Carolina General Statutes require the State Auditor to make audit reports available to the public. Copies of audit reports issued by the Office of the State Auditor may be obtained through one of the options listed in the back of this report.

Respectfully submitted,

Leslie W. Merritt, Jr.

Leslie W. Merritt, Jr., CPA, CFP
State Auditor

TABLE OF CONTENTS

PAGE

EXECUTIVE SUMMARY

We conducted an Information Systems (IS) audit at North Carolina Central University (NCCU) from January 9, 2006 through February 17, 2006. The primary objective of this audit was to evaluate the IS general controls in place during that period. Based on our objective, we report the following conclusions.

General security involves the establishment of a reasonable security program that addresses the general security of information resources. Our audit did not identify any significant weaknesses in general security.

The **access control** environment consists of access control software and information security policies and procedures. We noted several weaknesses in access controls. Due to the sensitive nature of the conditions found in these weaknesses, we have conveyed these findings to management in a separate letter pursuant to the provision of the North Carolina General Statute 147-64.6(c)(18).

Program maintenance primarily involves enhancements or changes needed to existing systems. Our audit did not identify any significant weaknesses in program maintenance.

Systems software is the collection of programs that drive the computer. The selection of systems software should be properly approved and the software should be maintained by the computer center**.** We found one significant weakness in systems software during our audit. See Audit Finding 1, *Systems Software Standards and Documentation Need Improvement.*

Systems development includes the creation of new application systems or significant changes to existing systems. Systems development projects can be expensive and affect the operations of the university in significant ways. Consequently, the university should have a strategic or master plan for systems development. Each development project should be managed using project management techniques and should adhere to a clearly defined systems development methodology. When a project is completed, the finished product should include a comprehensive set of documentation so that the users, operators and programmers each have the information they need to do their jobs. Our audit did not identify any significant weaknesses in systems development.

Physical security primarily involves the inspection of the university's computer center for the controls that should reasonably secure the operations of the computer center from foreseeable and preventable threats from fire, water, electrical problems, and vandalism. Our audit did not identify any significant weaknesses in physical security.

EXECUTIVE SUMMARY (CONCLUDED)

The **operations procedures** of the computer center include all of the activities associated with running application systems for users. Our audit did not identify any significant weaknesses in operations procedures.

A complete **disaster recovery** plan that is tested periodically is necessary to enable North Carolina Central University to recover from an extended business interruption due to the destruction of the computer center or other university assets. We found one significant weakness in disaster recovery during our audit. See Audit Finding 2, *Back Up Tapes for the Banner Application are not Rotated to an Offsite Facility on a Weekly Basis per NCCU Policy*

AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY

OBJECTIVES

Under the *North Carolina General Statutes* 147-64.6, the State Auditor is responsible for examining and evaluating the adequacy of operating and administrative procedures and practices, systems of accounting, and other elements of State agencies. IS general control audits are examinations of controls which effect the overall organization and operation of the IS function. This IS audit was designed to ascertain the effectiveness of general controls at North Carolina Central University.

SCOPE

General controls govern the operation and management of computer processing activities. The scope of our IS general controls audit was to review general security issues, access controls, program maintenance, systems software, system development, physical security, operations procedures, and disaster recovery which directly affect NCCU's computing operations. Other IS general control topics were reviewed as considered necessary.

METHODOLOGY

We audited policies and procedures, interviewed key administrators and other personnel, examined system configurations, toured the computer facility, tested on-line system controls, reviewed appropriate technical literature, reviewed computer generated reports, and used security evaluation software in our audit of information systems. We conducted our audit in accordance with the standards applicable to performance audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States and *Information Systems Audit Standards* issued by the Information Systems Audit and Control Association.

[This Page Left Blank Intentionally]

North Carolina Central University (NCCU) is a public state assisted institution located in Durham, North Carolina. The university's continuing focus is on teaching, expanding basic and applied research activities, and meeting the public service needs of Central North Carolina.

The Information Technology Services Division (the Division) consists of nine departments: Business Management, ITS Campus Relations & Communications, Campus Support Services (Client & ResNet Support Services), Enterprise Systems Development & Support, Information Technology Security, IT Planning & Programs, IT Computing Services, Telecom Operations & Engineering, Web Management. The Division is under the direct supervision of the Chief Information Officer.

Business Management (BM)

ITS Business Management was created to provide centralized management of the Office of Information Technology's budgetary, purchasing and human resource functions. This office provides both internal and external support to the Information Technology departments. BM is also responsible for providing assistance to administrative and academic units here at North Carolina Central University in coordinating hardware and software purchases and networking services in addition to IT contract management. The staff assists the Chief Information Officer with coordination of Information Technology resources as they relate to the long-range strategic plan. This office also provides assistance with reporting requirements for internal, external, federal and state audits.

ITS Campus Relations & Communications

ITS Campus Relations & Communications assist the ITS organization with communicating IT related information to faculty, staff and students at North Carolina Central University. The Office of Campus Relations & Communications also assist ITS with any technology related press or media activities.

Campus Support Services (Client & ResNet Support Services)

Client & ResNet Support Services provides hardware and software support for computers and related equipment used in labs, kiosk, and offices throughout North Carolina Central University's campus. These services consist of providing student technical support services (ResNet), managing calls at our help desk, supporting Information Technology computer labs, providing documentation, and assisting with the operation of the campus network.

Enterprise Systems Development & Support

Enterprise Systems (ES) designs, implements, and supports North Carolina Central University Enterprise, Resource, and Planning (ERP) systems (administrative systems); provides professional assistance in the area of decision support; researches and evaluates new software and reporting tools; and provides infrastructure support to all administrative system customers including training and user support of information systems.

Information Technology Security

IT Security manages the university's Information Technology Security Program. This program addresses university compliance with federal and state IT regulations and standards, internal and state IT audits, disaster recovery planning, IT policy development, user awareness and education, incident response and recovery, and user account security on administrative systems. The mission of IT Security is to establish a secure digital environment that safeguards the university's electronic information and information technology.

IT Planning & Programs

IT Planning & Programs is responsible for the planning, creation, and deployment of North Carolina Central University evolving enterprise IT technologies. The office of planning & programs is responsible for developing common systems and procedures for security, data reporting, and general data management for the University administrative systems working with the appropriate business units on campus. This office is also responsible for ITS Disaster Preparedness/Recovery, and IT Policy Formation/Maintenance.

IT Computing Services

The Department of Computing Services is responsible for the planning, installation, management and support of the campus-wide computing and data network infrastructure. This infrastructure enables faculty, staff and students to utilize efficiently and effectively NCCU's information technology resources for teaching, research, public service, administration and information management. This unit is responsible for the delivery of core network and intranet services to the campus, and for access to the Internet.

Telecom Operations & Engineering

The Office of Telecommunications is responsible for all functions related to North Carolina Central University’s telephone system and telecommunication services. In addition, the Telecom Operations & Engineering office is responsible for engineering issues associated with the university’s networking infrastructure.

Web Management

The Office of Web Management is responsible for the overall quality, utility and ease of access and navigation of the NCCU Web presence. The office is charged with establishing and maintaining general guidelines intended to ensure a common look and feel and consistent navigation systems within web sites under the university umbrella. The office is authorized to review official university sites for quality of design and general continuity and compliance with the university web policy. In cooperation with the Special Assistant to the Chancellor for public relations, the Webmaster shall assist organizational units or persons with their efforts to create web sites in compliance with university standards. The Office of Web Management is also responsible for the planning, purchasing and maintenance associated with web servers used to provide the campus wide presence on the Web. The office also assists with services including delivery of the NCCU home page, database connectivity, content management tools, live streaming video and other content resources.

CURRENT AUDIT RESULTS AND AUDITEE RESPONSES

The following audit results reflect the areas where NCCU has performed satisfactorily and where recommendations have been made for improvement.

GENERAL SECURITY ISSUES

General security issues involve the maintenance of a sound security management structure. A sound security management structure should include a method of classifying and establishing ownership of resources, proper segregation of duties, a security organization and resources, policies regarding access to the computer systems and a security education program. North Carolina Central University has established a reasonable security program that addresses the general security of information resources.

ACCESS CONTROLS

The most important information security safeguard that NCCU has is its access controls. The access controls environment consists of access control software and information security policies and procedures. An individual or a group with responsibility for security administration should develop information security policies, perform account administration functions and establish procedures to monitor and report any security violations. During our audit, we noted network architecture controls that strengthen the control environment at the university. However, we also found several weaknesses in access controls. Due to the sensitive nature of the conditions found in the weaknesses, we have conveyed these findings to management in a separate letter pursuant to the provision of North Carolina General Statute 147-64.6(c)(18).

PROGRAM MAINTENANCE

Program maintenance consists of making changes to existing application systems. Programmers should follow program change procedures to ensure that changes are authorized, made according to specifications, properly tested, and thoroughly documented. Application programmers should be restricted to a test environment to ensure that all changes to production resources are tested and approved before moving the changes into production. Changes to application system production programs should be logged and monitored by management. Our audit did not identify any significant weakness in program maintenance.

SYSTEMS SOFTWARE

Systems software is the collection of programs that the computer center uses to run the computer and support the application systems. This software includes the operating system, utility programs, compilers, database management systems and other programs. The systems programmers have responsibility for the installation and testing of upgrades to the system software when received. Systems software changes should be properly documented and approved. We found one significant weakness in systems software during our audit.

AUDIT FINDING 1: SYSTEMS SOFTWARE STANDARDS AND DOCUMENTATION NEED IMPROVEMENT

The NCCU's systems software standards did not address the following:

- System software changes are scheduled when they least impact IS processing.
- Problems encountered during testing or operations were resolved and the changes were re-tested. These problems should be documented.
- Fallback or restoration procedures are in place in case of production failure.

Also, NCCU did not maintain any supporting documentation for their Banner system software upgrades.

Recommendation: NCCU should make modifications to address the missing components to their existing systems software standards.

Auditee's Response: The University will revise the Systems software standards.

SYSTEMS DEVELOPMENT

Systems development includes the creation of new application systems or significant changes to existing systems. Systems development projects can be expensive and affect the operations of the university in significant ways. Consequently, the university should have a strategic or master plan for systems development. Each development project should be managed using project management techniques and should adhere to a clearly defined systems development methodology. When a project is completed, the finished product should include a comprehensive set of documentation so that the users, operators and programmers each have the information they need to do their jobs. Our audit did not identify any significant weaknesses in systems development.

PHYSICAL SECURITY

Controls over physical security are designed to protect a computer center from service interruptions resulting from fire, water, electrical problems, vandalism, and other causes. Physical security controls ensure that the computer service center is reasonably secure from foreseeable and preventable threats to its physical continuity. Our audit did not identify any significant weaknesses in physical security.

OPERATIONS PROCEDURES

The operations of the computer center include all of the activities associated with running application systems for users. Procedures should be in place to control the scheduling and running of production jobs, restarting production jobs when problems occur, storing, handling and mounting of tapes, and maintaining computer equipment. Our audit did not identify any significant weaknesses in operations procedures.

DISASTER RECOVERY

Disasters such as fire and flood can destroy a computer service center and leave its users without computer processing support. Without computer processing, many university services would grind to a halt. To reduce this risk, computer service centers develop disaster recovery plans. Disaster recovery procedures should be tested periodically to ensure the recoverability of the data center. We found one significant weakness in disaster recovery during our audit.

AUDIT FINDING 2: BACK UP TAPES FOR THE BANNER APPLICATION ARE NOT ROTATED TO AN OFFSITE FACILITY ON A WEEKLY BASIS PER NCCU POLICY

Back-up tapes for the Banner application are not rotated to an offsite facility on a weekly basis as documented in the NCCU Disaster Recovery Plan.

In the event of a disaster, or loss of data regarding the Banner application, the user departments affected by such a loss may not have sufficient resources, or the ability to re-enter, or recompile lost data that has not been backed up over an extended period of time.

Recommendation: NCCU should rotate backup data tapes for the Banner application to an offsite facility on a weekly basis, as documented in the NCCU Disaster Recovery Plan

Auditee’s Response: The University will rotate the Banner backup data tapes to its offsite facility, on a weekly basis, as documented in the NCCU Disaster Recovery Plan.

[This Page Left Blank Intentionally]

ORDERING INFORMATION

Audit reports issued by the Office of the State Auditor can be obtained from the web site at www.ncauditor.net. Also, parties may register on the web site to receive automatic email notification whenever reports of interest are issued. Otherwise, copies of audit reports may be obtained by contacting the:

Office of the State Auditor
State of North Carolina
2 South Salisbury Street
20601 Mail Service Center
Raleigh, North Carolina 27699-0601

Telephone: 919/807-7500

Facsimile: 919/807-7647