STATE OF NORTH CAROLINA

AUDIT OF THE INFORMATION SYSTEMS GENERAL CONTROLS

AT

NORTH CAROLINA CENTRAL UNIVERSITY

DURHAM, NORTH CAROLINA

NOVEMBER 2001

OFFICE OF THE STATE AUDITOR

RALPH CAMPBELL, JR.

STATE AUDITOR

AUDIT OF THE INFORMATION SYSTEMS GENERAL CONTROLS

AT

NORTH CAROLINA CENTRAL UNIVERSITY

DURHAM, NORTH CAROLINA

NOVEMBER 2001

STATE OF NORTH CAROLINA
Office of the State Auditor

Ralph Campbell, Jr.
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.osa.state.nc.us

AUDITOR'S TRANSMITTAL

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

Ladies and Gentlemen:

We have completed our information systems (IS) audit of the administrative computer operations at North Carolina Central University (NCCU). 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 the University. The scope of our IS general controls audit included general security issues, access controls, systems development, program maintenance, physical security, operations procedures, system software, telecommunications, and disaster recovery. Other IS general control topics were reviewed as considered necessary.

This report contains an executive summary that highlights the areas where North Carolina Central University has performed satisfactorily and where improvements should be made.

We wish to express our appreciation to the staff at North Carolina Central University for the 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,

Ralph Campbell, Jr.

Ralph Campbell, Jr.
State Auditor

TABLE OF CONTENTS

EXECUTIVE SUMMARY

We conducted an information system (IS) audit at North Carolina Central University from August 9, 2001 through August 31, 2001. 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. We found no final or approved Information Systems Policies and Procedures. See Audit Finding 1, *Information Systems Policies and Procedures* for further information. We also noted that the same individual performs the functions of the Security Administrator and Systems Programmer. See Audit Finding 2, *Segregation of Duties between Security Administration and Systems Programming.*

The **access control** environment consists of access control software and information security policies and procedures. We reviewed the access controls for the NCCU mainframe systems by analyzing the built-in security features of the operating system. We found that operating system access controls are not adequate to protect the critical and sensitive information from unauthorized access. See Audit Finding 3, *Adequacy of Access Controls over the Operating System* for further information.

Systems Development Systems development includes the creation of new application systems or significant changes to existing systems. We found the University did not have a systems development life cycle methodology or a project tracking system. See Audit Finding 4, *System Development Life Cycle and Project Tracking* for further information.

Program maintenance primarily involves enhancements or changes needed to existing systems. We found that application programmers have access to production source libraries. See Audit Finding 5, *Application Programmers Access To Production Source Libraries.*

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 note any significant weaknesses in this area.

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 this area.

System 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. Our audit did not identify any significant weaknesses in this area.

The computer service center's **telecommunications** activities should be operated in a way that protects the security and completeness of data being transmitted. Due to the sensitive nature of the weaknesses found in this area, we have conveyed these findings to management in a separate letter pursuant to the provision of North Carolina G.S. 147-64.6(c)(18).

A complete **disaster recovery** plan that is tested periodically is necessary to enable the University to recover from an extended business interruption due to the destruction of the computer center or other University assets. We found that the University does not have a disaster recovery plan for the computer center and major user departments. See Audit Finding 6, *Disaster Recovery* for further information.

AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY

OBJECTIVES

Under the North Carolina General Statutes Chapter 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. 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, systems development, program maintenance, physical security, operations procedures, systems software, telecommunications, and disaster recovery which directly affect the University's computer operations. Other IS general control topics were reviewed as considered necessary.

METHODOLOGY

This IS audit was performed in accordance with *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. Our methodology included:

- Reviews of policies and procedures.
- Interviews with key administrators and other personnel.
- Examinations of system configurations.
- Tours of the computer facility.
- On-line testing of system controls.
- Reviews of appropriate technical literature.
- Reviews of computer generated reports.
- Use of security evaluation software.

[This Page Left Blank Intentionally]

BACKGROUND INFORMATION

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 four departments: **Academic and Educational Services**, **Special Projects and Training**, **Help Desk, and Administrative Technology and Development.** The Division is under the direct supervision of the Chief Information Officer. The Division administrative offices are the working environment for information systems heads, secretarial and bookkeeping support.

Academic and Educational Services (AES): The Academic and Educational Services department has responsibility for providing user computer support to the faculty, staff, and students. This support includes the installation of NCCU licensed software and specialized software on classroom computer systems and computer labs on the campus. Assistance with instructional programming and academic research is also provided on a limited basis. Electronic mail, network access, multimedia and administrative applications support, and administration for students, faculty and staff not having a departmental server available is provided by AES. A primary goal of this department is to consolidate servers and support for servers that are managed by other departmental units.

Special Projects and Training: The Special Projects and Training department is responsible for supporting North Carolina Central University's teaching and learning mission by providing technology planning and training for faculty, staff and students and procuring resources to upgrade, enhance and facilitate technological support to the campus. The Special Projects and Training department has three goals: 1) create and implement a comprehensive technology training program for the campus, 2) secure fiscal resources and technological equipment for campus users, and 3) provide technological support for special projects.

Help Desk: Help Desk is responsible for providing help desk support for the various University departments faculty, staff and students. The department is also responsible for providing customer service and functions as a single contact center to research, define, identify, and troubleshoot the evolving needs of faculty, staff and students as related to North Carolina Central University's technical environment.

Administrative Technology and Development: The Administrative Technology and Development department has responsibility for computer operations, web development, systems and operations support, and administrative software development including emerging new technologies for NCCU. The department is also responsible for the following applications: financial records system (FRS), student information system (SIS), web for faculty, students and alumni systems, and the human resources system (HRS).

[This Page Left Blank Intentionally]

AUDIT RESULTS AND AUDITEE RESPONSES

The following audit results reflect the areas where North Carolina Central University 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.

AUDIT FINDING 1: INFORMATION SYSTEMS POLICIES AND PROCEDURES

NCCU does not have final or approved Information Systems polices and procedures. The Information Technology Services Division (ITSD) developed a draft policy in 1999, however, this draft requires significant updates to reflect the current unwritten policies and procedures that have been adopted and implemented by the ITSD staff. Lack of approved policies and procedures can lead to control procedures being applied inconsistently by the ITSD staff. Also, management's intentions may not be followed.

According to Control Objectives for Information Technology (COBIT), Management should assume full responsibility for formulating, developing, documenting, promulgating and controlling policies covering general aims and directives. Regular reviews of policies for appropriateness should also be carried out. Additionally, COBIT states that Management should ensure that organizational policies are communicated to and understood by all levels in the organization.

Recommendation: ITSD should update all information technology policies and procedures. The updated polices should then be formally approved by the Chief Information Officer and the University's Chancellor and communicated to all levels in the University.

Auditee's Response: We agree with the audit finding and are in the process of taking corrective action. Corrective action will be completed within ninety days.

AUDIT FINDING 2: SEGREGATION OF DUTIES BETWEEN SECURITY ADMINISTRATION AND SYSTEMS PROGRAMMERS

We found inappropriate segregation of duties between the security administration and systems programming functions. The systems programmer also performs security administration functions. The review of systems programmer logs and the establishment of access standards for the systems programmer is performed by the systems programmer/security administrator. As a result, objectivity is lost and monitoring is unreliable if performed by an individual who serves as both the security administrator and the systems programmer.

Security administration is responsible for the following functions: maintaining access rules to data and other IT resources; maintaining security and confidentiality over the issuance and maintenance of authorized user IDs and passwords; monitoring security violations and taking corrective action to ensure that adequate security is provided; periodically reviewing and evaluating the security policy and suggesting necessary changes to management; preparing and monitoring the security awareness program for all employees; and testing the security architecture to evaluate the security strengths and to detect possible threats.

The systems programmer is responsible for maintaining the systems software including the operating system. This function may require unrestricted access to the entire operating system. This requires that management closely monitor the systems programmer's activities by requiring the systems programmer to keep work logs, and only having access to systems libraries necessary for the systems programmer's job duties.

According to Control Objectives for Information Technology (COBIT), senior management should implement a division of roles and responsibilities, which should exclude the possibility for a single individual to subvert a critical process. Management should also make sure that personnel are performing only those duties stipulated for their respective jobs or positions. In particular, a segregation of duties should be maintained between the system development maintenance function, the processing operations function and the user organization. In addition, the security responsibility should be clearly separated from the processing operations function.

Recommendation: The University should separate the duties of the security administrator and systems programmer.

Auditee's Response: We agree with the audit finding and are in the process of identifying corrective alternatives. Once this research has concluded, we will implement corrective measures.

ACCESS CONTROLS

The access control environment consists of access control software and information security policies and procedures. An individual or 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.

AUDIT FINDING 3: ADEQUACY OF ACCESS CONTROLS OVER THE OPERATING SYSTEM

Access security controls for the NCCU operating system are not adequate to protect the critical and sensitive information from unauthorized access. We found that users of the system have more privileges and access rights than necessary to perform their job functions. Misuse of such privileges could allow these users to access information for which they are not authorized.

According to Control Objectives for Information Technology (COBIT), in an online information technology environment, management should implement procedures in line with the security policy that provides access security control based on the individual's demonstrated need to view, add, change or delete data. Access rights for users should be at the minimum level required for them to perform their job responsibilities. Procedures should be in place to periodically review and confirm access rights.

Recommendation: The University should assess the level of access required to the operating system. Management should ensure that access rights for users are at the minimum level required for them to perform their job responsibilities. Management should establish procedures to periodically review and confirm access rights.

Auditee's Response: We agree with the audit finding and are in the process of identifying corrective alternatives. Once this research has concluded, we will implement corrective measures.

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 agency in significant ways. Consequently, the agency 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.

AUDIT FINDING 4: SYSTEM DEVELOPMENT LIFE CYCLE AND PROJECT TRACKING

The University does not have a formal and approved systems development life cycle methodology (SDLC) and a formal project tracking methodology. Without an approved systems development life cycle, improperly designed or inappropriate purchases of "off the shelf" systems can result. Expensive redesigning or support of these systems may be required, and the University may spend more than originally anticipated because of design flaws, and costly interfaces with existing systems. Also, other departments in the University

may attempt to acquire or develop systems without the approval of ITSD and fail to develop or purchase new systems that are secure or compatible with existing systems.

Without appropriate project tracking, project movement through SDLC phases is uncoordinated, and may remain in the test system until the programmers remind the requesting department to sign off on the project for movement into production.

According to the Control Objectives for Information Technology (COBIT), the organization's senior management should define and implement information systems standards and adopt a system development life cycle methodology governing the process of developing, acquiring, implementing and maintaining computerized information systems and related technology. The chosen system development life cycle methodology should be appropriate for the systems to be developed, acquired, implemented and maintained. In addition to an approved system development life cycle, it is critical to have a method of tracking projects, projected deadlines and completion dates to promote continuous movement of the project through the systems development life cycle.

Recommendation: The University should adopt an approved systems development life cycle, ensure that ITSD is the centralized approving department of all system development and acquisitions, and implement a project tracking methodology.

Auditee's Response: We agree with the audit finding and are in the process of developing a system.

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.

AUDIT FINDING 5: APPLICATION PROGRAMMERS ACCESS TO PRODUCTION SOURCE LIBRARIES

The application programmers are responsible for developing and maintaining application programs. However, these same programmers are also responsible for moving the programs from test into production. As a result, programmers could make unauthorized changes to programs and data and resubmit this changed information into the production environment without leaving an audit trail.

According to Control Objectives for Information Technology (COBIT), Management should define and implement formal procedures to control the handover of the system from

development to testing to operations. The respective environments should be segregated and properly protected.

Recommendation: The University should implement the use of tracking software that logs the activity of the programmers and that the appropriate personnel institute monitoring/oversight procedures.

Auditee's Response: We agree with the audit finding and are in the process of identifying corrective alternatives. Once this research has concluded, we will implement corrective measures.

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. The University's physical security controls ensure that the computer service center is reasonably secure from foreseeable and preventable threats to its physical continuity. During our audit, the University was in the process of moving to a new computer facility that greatly improves the physical security. Therefore, our test work was performed on the new facility. 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.

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. Our audit did not identify any significant weaknesses in systems software.

TELECOMMUNICATIONS

Telecommunications is the electronic transmission of any kind of information by radio, wire, fiber optics, microwave, laser, or any other electromagnetic system. It can be evaluated along several lines including the type of system, the geographical organization and the service environment. The computer service center's telecommunications activities should be operated in a way that protects the security and completeness of data being transmitted.

We noted weaknesses in the controls over telecommunications. Due to the sensitive nature of the conditions found, we have conveyed these findings to management in a separate letter pursuant to the provision of North Carolina G.S. 147-64.6(c)(18).

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 of the 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.

AUDIT FINDING 6: DISASTER RECOVERY

NCCU does not have a final or approved disaster recovery plan. Lack of a disaster recovery plan limits the staffs' effectiveness in restoration of services in the event of a disaster.

According to the Control Objectives for Information Technology (COBIT), a management approved disaster recovery/contingency plan should be created that details the procedures to be followed in the event of a disaster.

Recommendation: The University should finalize and approve a disaster recovery plan.

Auditee's Response: We agree with the audit finding and are in the process of taking corrective action to finalize our disaster recovery plan.

DISTRIBUTION OF AUDIT REPORT

In accordance with G.S. § 147-64.5 and G.S. § 147-64.6(c)(14), copies of this report have been distributed to the public officials listed below. Additional copies are provided to other legislators, state officials, the press, and the general public upon request.

EXECUTIVE BRANCH

The Honorable Michael F. Easley	Governor of North Carolina
The Honorable Beverly M. Perdue	Lieutenant Governor of North Carolina
The Honorable Richard H. Moore	State Treasurer
The Honorable Roy A. Cooper, III	Attorney General
Mr. David T. McCoy	State Budget Officer
Mr. Robert L. Broad	State Controller
Ms. Molly C. Broad	President, The University of North Carolina
Dr. James Ammons	Chancellor The North Carolina Central University

LEGISLATIVE BRANCH

Appointees to the Joint Legislative Commission on Governmental Operations

Senator Marc Basnight, Co-Chairman	Representative James B. Black, Co-Chairman
Senator Charlie Albertson	Representative Martha B. Alexander
Senator Frank W. Ballance, Jr.	Representative Flossie Boyd-McIntyre
Senator Charles Carter	Representative E. Nelson Cole
Senator Daniel G. Clodfelter	Representative James W. Crawford, Jr.
Senator Walter H. Dalton	Representative William T. Culpepper, III
Senator James Forrester	Representative W. Pete Cunningham
Senator Linda Garrou	Representative Beverly M. Earle
Senator Wilbur P. Gulley	Representative Ruth M. Easterling
Senator Kay R. Hagan	Representative Stanley H. Fox
Senator David W. Hoyle	Representative R. Phillip Haire
Senator Luther H. Jordan, Jr.	Representative Dewey L. Hill
Senator Ellie Kinnaird	Representative Mary L. Jarrell
Senator Howard N. Lee	Representative Maggie Jeffus
Senator Jeanne H. Lucas	Representative Larry T. Justus
Senator R. L. Martin	Representative Edd Nye
Senator William N. Martin	Representative Warren C. Oldham
Senator Stephen M. Metcalf	Representative William C. Owens, Jr.
Senator Fountain Odom	Representative E. David Redwine
Senator Aaron W. Plyler	Representative R. Eugene Rogers
Senator Eric M. Reeves	Representative Drew P. Saunders
Senator Dan Robinson	Representative Wilma M. Sherrill
Senator Larry Shaw	Representative Ronald L. Smith
Senator Robert G. Shaw	Representative Gregg Thompson
Senator R. C. Soles, Jr.	Representative Joe P. Tolson
Senator Ed N. Warren	Representative Russell E. Tucker
Senator David F. Weinstein	Representative Thomas E. Wright
Senator Allen H. Wellons	Representative Douglas Y. Yongue

Appointees to the Joint Select Committee on Information Technology

Senator Austin M. Allran
Senator Charles Carter
Senator Daniel G. Clodfelter
Senator Eric Miller Reeves
Mr. Dwight Allen
Mr. Curtis Clark
Ms. Darleen Johns
Representative Joe P. Tolson
Representative Russell Edwin Tucker
Representative William L. Wainwright
Representative Trudi Walend
Mr. Rufus Edmisten
Ms. Robin Render
Ms. Janet Smith

Other Legislative Officials

Representative Phillip A. Baddour, Jr. — Majority Leader of the N.C. House of Representatives
Representative N. Leo Daughtry — Minority Leader of the N.C. House of Representatives
Mr. James D. Johnson — Director, Fiscal Research Division

Other Officials

Chairman and Members of the Information Resource Management Commission

ORDERING INFORMATION

Copies of this report 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

E-Mail: reports@ncauditor.net

A complete listing of other reports issued by the Office of the North Carolina State Auditor is available for viewing and ordering on our Internet Home Page. To access our information simply enter our URL into the appropriate field in your browser: **http://www.osa.state.nc.us**