STATE OF NORTH CAROLINA

AUDIT OF THE INFORMATION SYSTEM GENERAL CONTROLS

AT

THE UNIVERSITY OF NORTH CAROLINA AT CHARLOTTE

CHARLOTTE, NORTH CAROLINA

FEBRUARY 2002

OFFICE OF THE STATE AUDITOR

RALPH CAMPBELL, JR.

STATE AUDITOR

AUDIT OF THE INFORMATION SYSTEM GENERAL CONTROLS

AT

THE UNIVERSITY OF NORTH CAROLINA AT CHARLOTTE

CHARLOTTE, NORTH CAROLINA

FEBRUARY 2002

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, The University of North Carolina at Charlotte
Dr. James H. Woodward, Chancellor

Ladies and Gentlemen:

We have completed our information systems (IS) audit of the Information Technology Services department at The University of North Carolina at Charlotte (UNC-Charlotte). 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, 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 UNC-Charlotte has performed satisfactorily and where improvements should be made.

We wish to express our appreciation to the staff at UNC-Charlotte 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 UNC-Charlotte from October 24, 2001 through November 30, 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 did not identify any significant weaknesses in general security controls of information resources.

The **access control** environment consists of access control software and information security policies and procedures. We reviewed the access controls for the mainframe system and local area network (LAN). We did not identify any significant weaknesses in access controls over the mainframe and LAN servers during our audit.

Program maintenance primarily involves enhancements or changes needed to existing systems. We did not note any significant weaknesses in program maintenance during our audit.

The operations of the computer center should be reasonably secure from foreseeable and preventable threats from fire, water, electrical problems, and vandalism. We did not identify any significant weaknesses in **physical security** during our audit.

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

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. We did not identify any significant system software control weaknesses during our audit.

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 instances where sensitive information was not adequately protected. Due to the sensitive nature of the conditions found in the control weaknesses, 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** must be developed, approved by management, and tested for the protection of data and the continuity of the entity's operations. This should enable the University to recover from an extended interruption due to the destruction of the computer center or other University assets. The University has a disaster recovery plan for the computer center. However, we identified some deficiencies in the disaster recovery plan during our audit. See Audit Finding 1, *Incomplete Disaster Recovery Plan.*

[This Page Left Blank Intentionally]

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 the University of North Carolina at Charlotte.

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, physical security, operations procedures, systems software, telecommunications, and disaster recovery which directly affect the University's computing 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

The University of North Carolina at Charlotte (UNC-Charlotte) is a public state assisted institution located in Charlotte, North Carolina. UNC-Charlotte is one of a generation of universities founded in metropolitan areas of the United States immediately after World War II in response to rising education demands stimulated by the war and its technology. UNC-Charlotte is a comprehensive University offering a full array of baccalaureate programs, about forty-five programs leading to master's degree and six programs leading to doctoral degrees. Today, the University has approximately 18,000 students, and is the fourth largest of the 16 institutions that make up The University of North Carolina system.

The Computing Services Department reports to the Associate Provost for Information Systems and Chief Information Officer. Its mission is to provide responsive, enterprise-wide information services and technologies to meet the needs of the University.

The department provides information technology planning, project management, and administrative services to the University. It provides systems support for the mainframe operating system and all third party software running on the mainframe and provides additional support to the campus as necessary. The department supports all servers that are under its control and manages the network backbone, including all Ethernet connections and all hubs and router electronics supporting the entire campus network and interfaces to the external Internet.

[This Page Left Blank Intentionally]

AUDIT RESULTS AND AUDITEE RESPONSES

The following audit results reflect the areas where UNC-Charlotte 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, a security organization and resources, policies regarding access to the computer systems and a security education program. The University has established a reasonable security program that addresses the general security of information resources. We did not identify any significant weaknesses in general security during our audit.

ACCESS CONTROLS

The access control 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. The University uses the built-in security features of the mainframe operation system to control access. We did not identify any significant weaknesses in access control during our audit.

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. We did not identify any significant weaknesses in program maintenance during our audit.

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. We did not identify any significant weaknesses in physical security during our audit.

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. We did not identify any significant weaknesses in the operations procedures of the computer center during our audit.

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 system 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.

The University has implemented controls over the access to telecommunications hardware and the transmission of data. We noted instances where sensitive information was not adequately protected. Due to the sensitive nature of the conditions found in the control weaknesses, 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. The Computing Services department has developed a disaster recovery plan for the computer center. We have identified some deficiencies in the existing Disaster Recovery Plan for the computer center.

AUDIT FINDING 1: INCOMPLETE DISASTER RECOVERY PLAN

The current Disaster Recovery Plan for the computer center is incomplete, has identified weaknesses, and has not been fully tested.

- We found that an alternate processing site has not been identified for computer operations in the event a disaster renders the current computer center unusable. The recovery of computer operations will be delayed until another facility that will accommodate the computing equipment is identified.

- The current timeframes for restoring data processing services are not based on any contingency site location and specifications. There is no contingency site location on which to base the timeframes therefore, the current timeframes may not be realistic or attainable.

- The existing computer center plan does not include a complete and detailed inventory of equipment required for full recovery. The absence of this inventory will delay the recovery process until the mainframe, server, data and telecommunications, peripheral equipment, system and application software required for recovery is identified.

- A copy of the disaster recovery plan is not stored at an off-site storage facility. In the event of a disaster in which the computer center is destroyed, the disaster recovery plan will also be destroyed. This will leave the center without a plan from which a timely recovery can be started.

- Alternate processing procedures for the user departments to follow during the recovery period have not been documented. In the event of a disaster, the lack of alternate processing procedures will delay the recovery of data because the users in the departments may not know the process for capturing data until processing is restored.

- The current disaster recovery plan does not include recovery plans for the key user departments of the University. The lack of a comprehensive disaster recovery plan that includes the user departments may cause the current plan to be ineffective if a user department is affected by a disaster and Computing Services is not.

It should be noted that a committee is presently working on the development of a comprehensive disaster recovery plan for the University that would incorporate the user departments.

Recommendation: The University should continue its efforts to develop and implement a comprehensive business continuity plan for data processing services and the user departments. An alternate processing site should be identified and timeframes for restoring data processing services should be developed to reflect this contingency site location and specifications. A complete and detailed inventory of equipment required to restore full data processing services should be included in the plan. A copy of the disaster recovery plan should be stored at an off-site storage facility. Once the plan is complete, it should be tested and updated at least annually or when major changes in the data processing environment are made.

Auditee's Response: The University has two major efforts underway that address all of the points identified in this finding. First, a steering committee and a management committee are in place and actively working on the development of a University Business Continuity Plan (BCP). The details of this effort were shared with the audit staff when they were on site and progress is underway to fully address this scope. Secondly, a Request For Proposal (RFP) has been developed and forwarded to Purchasing to pursue a contract to provide alternate processing capabilities for the central computer room of the University. This scope includes all equipment currently located in that room. The vendor responses to this RFP are due February 15, 2002 and will be evaluated during the latter part of February. The plan is to have the contract awarded as soon after that as possible considering the funding issues that have to be addressed. The plan to expand the scope to include other equipment around campus critical to departmental processes will be incorporated in the final BCP as approved by the steering committee.

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. Powell	State Controller
Ms. Molly Corbett Broad	President, The University of North Carolina
Dr. James H. Woodward	Chancellor The University of North Carolina at Charlotte

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. Hogan	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 Miller 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

DISTRIBUTION OF AUDIT REPORT (CONCLUDED)

Other Legislative Officials

Representative Philip A. Baddour, Jr.	Majority Leader of the N.C. House of Representatives
Senator Anthony E. Rand	Majority Leader of the N.C. Senate
Senator Patrick J. Ballantine	Minority Leader of the N.C. Senate
Representative N. Leo Daughtry	Minority Leader of the N.C. House of Representatives
Representative Joe Hackney	N.C. House Speaker Pro-Tem
Mr. James D. Johnson	Director, Fiscal Research Division

Other Officials

Chairman and Members of the Information Resource Management Commission

February 27, 2002

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

Internet: http://www.ncauditor.net

Telephone: 919/807-7500

Facsimile: 919/807-7647