STATE OF NORTH CAROLINA

AUDIT OF THE INFORMATION SYSTEM GENERAL CONTROLS

AT

THE UNIVERSITY OF NORTH CAROLINA AT PEMBROKE

PEMBROKE, 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 PEMBROKE

PEMBROKE, 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 Pembroke
Dr. Allen C. Meadors, Chancellor, The University of North Carolina at Pembroke

Ladies and Gentlemen:

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

We wish to express our appreciation to the staff at UNC-Pembroke 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 The University of North Carolina at Pembroke (UNC-Pembroke) from July 25, 2001 through August 27, 2001. The primary objective of this audit was to evaluate the IS general controls in place during that period. We conducted a follow-up review through January 25, 2002, to determine the updated status of IS controls in place as of that date. 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 did not identify any significant telecommunications control weaknesses during our audit.

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 disaster recovery plans for the computer center and major user departments. The current Disaster Recovery Plans are incomplete, have identified weaknesses, and have not been fully tested. See Audit Finding 1, *Incomplete Disaster Recovery Plans.*

[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 Pembroke.

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 Pembroke (UNC-Pembroke) is a public, four-year, constituent institution of The University of North Carolina. UNC-Pembroke was founded in 1887 as a normal school to train Native American public school teachers. Until 1953 it was the only state-supported four-year college for Indians in the nation. In 1969 the General Assembly changed the name to Pembroke State University and made the institution a regional University. Such universities were authorized "to provide undergraduate and graduate instruction in liberal arts, fine arts, and science, and in the learned professions, including teaching" and to "provide other graduate and undergraduate programs of instruction as are deemed necessary to meet the needs of their constituencies and of the state." Three years later, in 1972, the General Assembly established the 16-campus University of North Carolina with Pembroke State University as one of the constituent institutions. On July 1, 1996, Pembroke State University officially became The University of North Carolina at Pembroke.

The Office of University Computing and Information Services (UCIS) reports to the Office of Academic Affairs and provides academic and administrative computing for UNC-Pembroke along with computer-based training to support both the faculty and staff. UCIS provides supervision and technical support for three of the University's microcomputer labs. The mission of UCIS is to provide a technological infrastructure of resources necessary to support the University's mission of teaching, research and service. To fulfill its mission, UCIS provide hardware and systems to facilitate administrative and academic computing across campus, provide networking resources to support computing across campus and provide training for all aspects of computing. UCIS also provide systems analysis, programming and on-going technical support to administrative departments and administrative function of academic departments and provide software, programming and on-going technical support for faculty to support teaching, learning, service and research. In addition, UCIS provide video facilities and support to enable classes to be taught to other public schools, community colleges or universities and to be received from other universities.

[This Page Left Blank Intentionally]

AUDIT RESULTS AND AUDITEE RESPONSES

The following audit results reflect the areas where The University of North Carolina at Pembroke 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. A security administrator 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. The University has adopted adequate program change procedures. 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. The operations procedures at the University are adequate to ensure that computer processing is orderly and well controlled. 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. The systems software at the University is properly approved and maintained by the computer service center. 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 physical access to telecommunications hardware and the transmission of data. We did not identify any significant weaknesses for telecommunications.

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 University has disaster recovery plans for the computer center and major user departments. We have identified some deficiencies in the existing Disaster Recovery Plan for the computer center and user departments.

AUDIT FINDING 1: INCOMPLETE DISASTER RECOVERY PLAN

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

- We found that an alternate processing site has been identified for computer operations in the event a disaster renders the current computer center unusable. However, the existing computer center plan does not include an inventory of additional equipment necessary for the alternate processing site and network connectivity of this site to the campus network has not been fully addressed.

- The current plan defines a timeframe for fully restoring data processing services within thirty days. However, this timeframe may not adequately meet critical user department requirements, which requires computer services to be restored in less than thirty days. Computer center personnel informed us that the actual time period for restoring critical applications systems and certain user departments would actually be less than thirty days. However, the plan does not define these applications and user departments and does not provide guidelines on the priority and timeframes for restoring these critical applications systems and user departments.

- The user department plans do not include alternative processing procedures for operating during the recovery of data processing services. Our review of user departments showed that the departments have developed processing strategies for recovery from three different levels of disasters: minor, moderate, and major, affecting their department. However, the department plans do not include detail procedures for the department's operations during the recovery period. Also the department plans do not have procedures for recovery of data, retaining data during the recovery period, and entering data for a disaster affecting the computer center and the lost of data processing services.

- The current disaster recovery plan for the computer center and the department plans have not been tested to ensure that the plans provide sufficient details to allow the University to recovery from a disaster.

Recommendation: The University should continue its efforts to develop and implement a comprehensive business continuity plan for the University for data processing services and the user departments. The computer center plan should include an inventory of additional equipment necessary for the alternate processing site and should define plans to connect the site to the campus network. The time period for restoring data processing services should be redefined to reflect actual time for restoring critical applications systems and data processing services to key user departments. The plan should provide guidelines on the priority and timeframes for restoring these critical applications systems and user departments. The user department plans should include alternative processing procedures for operating during the recovery of data processing services based on the priority and timeframes defined in the computer center's plan. These procedures should include recovery of data, retaining data during the recovery period, and entering data once data processing services is restored. The user departments should expand their plans to include procedures to implement the strategies for recovery from the three different levels of disasters that may affect their department. Once the plans are complete and updated, they should be tested and updated at least annually or when major changes in the data processing environment are made.

Auditee's Response: The University of North Carolina at Pembroke concurs with the auditors' finding and recommendation regarding Disaster Recovery Planning. The University is developing a strategy to address the issues raised during the audit.

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. Allen C. Meadors	Chancellor The University of North Carolina at Pembroke

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