STATE OF NORTH CAROLINA

AUDIT OF THE INFORMATION SYSTEMS GENERAL CONTROLS

AT

UNIVERSITY OF NORTH CAROLINA AT WILMINGTON

WILMINGTON, NORTH CAROLINA

NOVEMBER 2001

OFFICE OF THE STATE AUDITOR

RALPH CAMPBELL, JR.

STATE AUDITOR

AUDIT OF THE INFORMATION SYSTEMS GENERAL CONTROLS

AT

UNIVERSITY OF NORTH CAROLINA AT WILMINGTON

WILMINGTON, 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, University of North Carolina at Wilmington
Dr. James R. Leutze, Chancellor

Ladies and Gentlemen:

We have completed our information systems (IS) audit of the administrative computer operations at The University of North Carolina at Wilmington (UNCW). 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 The University of North Carolina at Wilmington has performed satisfactorily and where improvements should be made.

We wish to express our appreciation to the staff at The University of North Carolina at Wilmington 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 Wilmington from July 9, 2001 through July 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 during our audit.

The **access control** environment consists of access control software and information security policies and procedures. We reviewed the access controls for the UNCW mainframe systems by analyzing the built-in security features of the operating system. We also reviewed the access controls over the Human Resources System (HRS) payroll application. We found that operating system access controls are not adequate to protect the critical and sensitive information from unauthorized access. See Audit Finding 1, *Adequacy of Access Controls Over Mainframe Operating System* for further information. We did not identify any significant weaknesses in access controls over the HRS payroll application.

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

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

The **operations procedures** of the computer center include all of the activities associated with running application systems for users. We did not identify any significant weaknesses in operations procedures 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 noted that the systems software change management policies and procedures are inadequate. See Audit Finding 2, *Systems Software Changes, Standards, Policies and Procedures* for further information.

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 physical access to telecommunications hardware is inadequate. See Audit Finding 3, *Security of Telecommunication Closets* for further information. Due to the sensitive nature of the conditions found in the other 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 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. The University has disaster recovery plans for the computer center and major user departments. We did not identify any significant disaster recovery control weaknesses during our audit.

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 University of North Carolina at Wilmington.

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 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

The University of North Carolina at Wilmington (UNCW) is a public state assisted institution located in Wilmington, North Carolina. Founded as Wilmington College in 1947, the University offers a wide range of undergraduate and master's degree programs, as well as a cooperative doctoral program in marine science. The University's continuing focus is on teaching, expanding basic and applied research activities, and meeting the public service needs of southeastern North Carolina.

The **Information Technology Systems Division** at The University of North Carolina at Wilmington is committed to ensuring that students, faculty and staff have full access to the power of information technologies. The University has taken the unique step of aligning its primary IT resources under the coordination of this newly created division. This division was formulated in July of 1999 and is made up of the following departments.

Department of Application Services

The mission of Application Services is to provide the information infrastructure that supports the University's missions of instruction, research, and public service. Application Services enables the University's teachers, researchers, managers, and staff to carry out their responsibilities, and to do so effectively and efficiently. The Department provides a full range of development and maintenance services including systems analysis, programming, and on-going technical support and liaison to the administrative departments and the administrative functions of the academic departments of the University.

Department of AV/Media Services

The Department of Audiovisual/Media Services provides audiovisual equipment and technical support for services that are too expensive or technical for departments to provide.

Department of Client Services

The Department of Client Services is responsible for the planning and delivery of personal computer technology and support services to the campus community. These services include Help Desk/User Support for initial problem reporting and resolution, desktop software training and support, personal computer maintenance and support, management of the student computing labs, and instructional and research support. Technology and services provided by this group enables faculty, staff and students to utilize efficiently and effectively UNCW's information technology resources for teaching, research, public service, and information management. This unit works integrally with allied units such as the Center for Teaching Excellence, and maintains close working relationships with IT support staff in other departments.

Department of 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 UNCW's information technology resources for teaching, research, public service, and information management. The staff also provides specialty ordering and networking capabilities, technical assistance with computer lab wiring, and network equipment configurations.

Department of Telecommunications

The Telecommunications Department has the general responsibility for managing and supporting the campus telephone system and the communications infrastructure wiring plant, both building and underground. Additionally, it has supporting responsibilities for the planning, and in some cases installation, of communications networks in new and existing buildings; working with architects to develop drawings of communications needs; and to produce auto cad drawings when requested for offices within buildings. Other services include alarm system wiring, campus-wide facility access readers, and HVAC and fire systems wiring. Services are provided through a combination of staff resources and contractual arrangements for both outside vendors and the UNCW Physical Plant. The Telecommunications Department is staffed by a wide variety of technical, administrative and customer support personnel, including skilled telecommunications analysts and technicians, cabling designers, telecommunications center systems administrators and operators, and related supervisory and administrative personnel.

AUDIT RESULTS AND AUDITEE RESPONSES

The following audit results reflect the areas where The University of North Carolina at Wilmington 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. Our audit did not identify any significant weaknesses in general security issues.

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. We reviewed the access controls for the UNCW mainframe systems by analyzing the built-in security features of the operating system. We also reviewed the access controls over the Human Resources System (HRS) payroll application. We did not identify any significant weaknesses in access controls over the HRS payroll application

AUDIT FINDING 1: ADEQUACY OF ACCESS CONTROLS OVER MAINFRAME OPERATING SYSTEM

Access security controls for the UNCW mainframe operating system are not adequate to protect the critical and sensitive information from unauthorized access. In an online information technology environment, management should implement procedures that provide 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. We found that users of the system have more privileges than necessary to perform their job functions. Misuse of such privileges could allow these users to access information for which they are not authorized.

Recommendation: The University should assess the level of access required to the mainframe. Management should ensure that access rights and privileges 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 and privileges.

Auditee's Response: The University will continually review the access rights of users to ensure that they are at the minimum level required to perform their job responsibilities. By December 1, 2001, the University will implement a procedure to semiannually (in January and July) review all accounts on the VMS mainframe system. All accounts that have not been logged into within the last six months will be restricted from having access to the command line prompt.

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 weaknesses in program maintenance.

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. 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.

AUDIT FINDING 2: SYSTEMS SOFTWARE CHANGES, STANDARDS, POLICIES AND PROCEDURES

The Department of Computing Services system software change standards, policies, and procedures are deficient in the following areas.

- There are no procedures that require all changes to be approved via a change control process and a change control form.
- The department has not designed procedures to require a list of systems software upgrades or changes to be kept.
- Procedures are lacking that require documentation to be maintained for the testing, approval, and implementation of all systems software upgrades or changes.
- There are no procedures that require problems detected and resolved during testing or operations to be documented.
- There is no requirement that documentation of systems software versions are kept for the Windows NT, Unix, and Linux platforms.

If the systems software changes are not managed properly, inappropriate system changes may result which could cause excessive amounts of downtime and may have an adverse effect on the users' applications.

Recommendation: UNC-W should develop and implement policies and procedures to ensure that:

- Changes to be approved via a change control process and a change control form is used.
- An inventory of systems software upgrades or changes should be maintained.
- Documentation should be maintained for the testing, approval, and implementation of all systems software upgrades or changes. Problems detected and resolved during testing or operations should also be documented.
- An inventory of all systems software versions should be maintained.

Auditee's Response: The University has inventoried all current systems software and modified its procedures to require the approval, adequate testing, and complete documentation of all future systems software changes.

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.

AUDIT FINDING 3: SECURITY OF TELECOMMUNICATION CLOSETS

We found that the University has not implemented controls over the physical access to telecommunications hardware and the transmission of data for one of their wiring closets. This room also served to store break room supplies, office supplies, and other items. Appropriate physical security and access control measures should be established for telecommunications hardware that conforms to the general security policy. Access should be restricted to only individuals that need access to perform their job. Unauthorized individuals may gain access and compromise the data residing on the critical telecommunications hardware or transmitting on the networks. Furthermore, these individuals could adversely affect the operations of the University if the individual were to maliciously damage the telecommunication hardware or network.

Recommendation: The University should remove all break room supplies, storage, and office supplies from the telecommunications closets. We also recommend that the university assesses the overall security of telecommunication equipment and closets to ensure only authorized individuals are allowed in these areas.

We also noted other 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).

Auditee's Response: The Department of Telecommunications is completing a campus-wide effort to ensure that all wiring closets are secured by lock and key, and that access is limited to authorized individuals. This work will be completed by December 1, 2001. A policy assigning full responsibility to wiring closets has been submitted to the Chancellor's Cabinet.

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. Our audit did not identify any significant weaknesses in disaster recovery.

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 R. Leutze	Chancellor The University of North Carolina at Wilmington

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. Diana Oblinger
Ms. Janet Smith

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

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**