STATE OF NORTH CAROLINA

AUDIT OF THE INFORMATION SYSTEM GENERAL CONTROLS

AT

THE UNIVERSITY OF NORTH CAROLINA AT ASHEVILLE

ASHEVILLE, NORTH CAROLINA

MARCH 2003

OFFICE OF THE STATE AUDITOR

RALPH CAMPBELL, JR.

STATE AUDITOR

AUDIT OF THE INFORMATION SYSTEM GENERAL CONTROLS

AT

THE UNIVERSITY OF NORTH CAROLINA AT ASHEVILLE

ASHEVILLE, NORTH CAROLINA

MARCH 2003

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
The Board of Directors of The University of North Carolina at Asheville
Dr. James H. Mullen, Jr., Chancellor

Ladies and Gentlemen:

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

This report contains an executive summary that highlights the areas where The University of North Carolina at Asheville 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 Asheville 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 Asheville from November 13, 2002 through December 13, 2002. 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 that the University does not have written policies and procedures that address key information technology areas. See Audit Finding 1, *Information Technology Policies and Procedures* for further information. We found that the University has not performed a risk assessment of its information technology resources and information. See Audit Finding 2, *Information Technology Risk Assessment* for further information. We also found that a user who is responsible for Quality Assurance and Security Administration also has privileges assigned that grant him the authority equivalent to those of a Systems Programmer. See Audit Finding 3, *Segregation of Duties* for further information.

The **access control** environment consists of access control software and information security policies and procedures. We reviewed the access controls for The University of North Carolina at Asheville's critical operating systems. We found several weaknesses in access controls. 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). We found that policies and procedures for user accounts have not been followed. We considered this weakness to be non-sensitive, but critical. See Audit Finding 4, *Policies and Procedures for Requesting Accounts* for further information.

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

Systems software is the collection of programs that drive the computer. The selection of systems software should be properly approved and the software should be maintained by the computer center. We did not identify any significant weaknesses in systems software 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.

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 did not identify any significant weaknesses in disaster recovery 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 The University of North Carolina at Asheville.

SCOPE

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

METHODOLOGY

We audited policies and procedures, interviewed key administrators and other personnel, examined system configurations, toured the computer facility, tested on-line system controls, reviewed appropriate technical literature, reviewed computer generated reports, and used security evaluation software in our audit of controls. We conducted our audit in accordance with the standards applicable to performance audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States and *Information Systems Audit Standards* issued by the Information Systems Audit and Control Association. [1]

[1] In 1992 the State created the Information Resource Management Commission to provide statewide coordination of information technology resources planning. The IRMC provides state enterprise IT leadership including increased emphasis and oversight for strategic information technology planning and management; policy development; technical architecture; and project certification. Pursuant to North Carolina General Statute 147-33.78 numerous state officials serve on the IRMC

including four members of the Council of State who are appointed by the Governor. The State Auditor has been appointed a member of the IRMC and elected as chair of the IRMC by its members.

[This Page Left Blank Intentionally]

BACKGROUND INFORMATION

The University of North Carolina at Asheville (UNCA) was founded in 1927 as Buncombe County Junior College for area residents interested in pursuing their educations beyond high school. The College relocated in 1961 to its present site, 265 scenic acres one mile north of downtown Asheville.

In 1966, the College awarded its first baccalaureate degrees in liberal arts disciplines and in 1969 it joined The Consolidated University of North Carolina as The University of North Carolina at Asheville, with the distinct mission to offer an undergraduate liberal arts education of superior quality. Today, UNC Asheville is the only designated liberal arts university in The University of North Carolina system and one of only six public universities in the country classified as national liberal arts universities (Liberal Arts I).

The ultimate goal of the University is to provide students with the best possible opportunity to acquire the skills, knowledge, and understanding necessary to pursue their goals, to find meaning in their lives, and to take their places as contributing citizens of a changing society. Its aim is to develop students of broad perspective who think critically and creatively, communicate effectively, and participate actively in their communities.

The University Computing Department

The University Computing (UC) department is tasked with providing computing and networking services to the UNCA community, faculty, staff and students. The Director of UC reports directly to the Vice Chancellor for Academic Affairs. The Academic Computing Services Division handles computing as related to academic issues (faculty and students), while Administrative Computing Services is in charge of the centrally maintained software systems as well as web page support. The Systems and Network division covers system programming, central computing resources and the campus network. Distance Learning Services provides interactive video conferencing and video streaming, as well as web resources. The UC also provides a comprehensive computing support environment for the student body. The key components are the residence hall network, RESNET, and the widely available computer labs.

[This Page Left Blank Intentionally]

AUDIT RESULTS AND AUDITEE RESPONSES

The following audit results reflect the areas where The University of North Carolina at Asheville (UNCA) 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. The University of North Carolina at Asheville has established a reasonable security program that addresses the general security of information resources. However, we identified several significant weaknesses in general security during our audit.

AUDIT FINDING 1: INFORMATION TECHNOLOGY POLICIES AND PROCEDURES

The University's information technology policies and procedures do not address many critical areas. Some areas that were not addressed include: network security, unauthorized use of software; information leakage; the use of security levels and classifications; the use of contracted and non-agency staff etc. Also, the existing policies and procedures are not updated annually to reflect the current unwritten policies and procedures that have been adopted and implemented by UNCA computing staff. Lack of approved policies and procedures can lead to control procedures being applied inconsistently by the UNCA computing staff.

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, Management should ensure that organizational policies are communicated to and understood by all levels in the organization. Management has directed the UNCA internal auditor to coordinate and develop standards for the maintenance and development of campus-wide policy. This effort is currently in progress.

Recommendation: Management should prepare and maintain formally written information technology policies and procedures that should be reviewed and updated on an annual basis. Management should ensure that these polices are developed using the new policy standards.

Auditee's Response: UNCA has organized and updated its existing information technology policies by creating new policies and modifying others. Our new and modified policies cover all areas suggested by the auditors. The new and modified policies are in draft form, and will be submitted to the campus policy approval process. Additionally, we will review all information technology policies annually, and update them as appropriate.

AUDIT FINDING 2: INFORMATION TECHNOLOGY RISK ASSESSMENT

The University has not performed an information technology risk assessment. Without a risk assessment, management has not formally identified the University's risk, has not classified information as critical or sensitive, and has not ensured that sufficient and appropriate procedures are in place to mitigate risk. A risk assessment should incorporate a regular assessment of the relevant information risks to the achievement of the business objectives, forming a basis for determining how the risks should be managed to an acceptable level. The process should provide for risk assessments at both the university level and system specific levels (for new projects as well as on a recurring basis) and should ensure regular updates of the risk assessment information with results of audits, inspections and identified incidents.

Recommendation: Management should perform an assessment to determine the risk and exposures of the computing department. Based on the results of the assessment, management should implement procedures to mitigate the risk identified or document the acceptance of the risk.

Auditee's Response: We have begun a risk assessment for University Computing. We will mitigate identified risks to the degree possible, and document our acceptance of risks that we cannot mitigate completely.

AUDIT FINDING 3: SEGREGATION OF DUTIES

We found inappropriate segregation of duties between the Security Administration and Systems Programming functions. Security Administration is responsible for:

- Maintaining access rules to data and other IT resources
- Maintaining security and confidentiality over the issuance
- 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

- 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, and thus requires that management closely monitor their activities by requiring the systems programmers to keep logs of their work, and only having access to systems libraries necessary for them to perform their job duties.

Because the review of systems programmers logs and the establishment of access standards for the systems programmer is performed generally by the security administrator, objectivity is lost and monitoring is unreliable if performed by an individual who serves as both the security administrator and the systems programmer.

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.

Adequate separation of duties with a small staff is often difficult to maintain. In those instances where separation of duties is not possible because of staff size, other compensating controls and procedures could be established to detect inappropriate events.

Recommendation: Management should investigate removing the Quality Assurance and Security Administrator responsibilities from this individual and give these tasks to another individual who does not have any major responsibilities for maintaining the critical systems.

Auditee's Response: We investigated removing Quality Assurance and Security Administrator responsibilities from the individual in question, but found that to be impractical for our small organization. Instead, we are in the process of developing a compensating control involving periodic, unscheduled review of appropriate system logs by a third party who has no privileges in either of these areas.

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. We reviewed the access controls for The University of North Carolina at Asheville's critical operating systems. We found several significant weaknesses in access controls. 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). We also found one other weakness in access controls that we considered non-sensitive, but critical.

AUDIT FINDING 4: POLICIES AND PROCEDURES FOR REQUESTING ACCOUNTS

The University has developed polices and procedures for the usage of these account request forms. These policies have not been updated to reflect current practices, are incomplete, and unclear. Account request forms are used to document and control who is authorized to access a critical system. Supervisors are to provide the computing center with account request forms, which will document who should access the system and what level of access should be granted to individuals. The staff of the computer center is responsible for adding new users to the system as requested by the account request forms. The lack of clear policies has led to:

- Documentation not being retained
- Supervisors not properly approving or signing the account request forms as stated in the policy
- Users requesting user ID's for themselves
- Inconsistent use of the account request form
- Lack of documentation for revoked user IDs for terminated or separated employees.

These practices increase the risk of an unauthorized user gaining access to the critical systems, or granting users more privileges to the systems than required.

Recommendation: Management should ensure that polices and procedures are complete, clear and updated to reflect current practices. Management should also establish monitoring procedures to ensure those tasks are performed in accordance with the policy.

Auditee's Response: Our policies have already been revised to reflect our current sound practices. The policies are in draft mode, pending submission to the campus approval process. We will institute periodic, unscheduled monitoring of our account creation procedures to make sure they conform to our policies. Additionally, we will perform an annual assessment of the adequacy of the policies, and make adjustments as necessary.

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 significant weaknesses in program maintenance.

SYSTEMS SOFTWARE

Systems software is the collection of programs that the computer center uses to run the computer and support the application systems. This software includes the operating system, utility programs, compilers, database management systems and other programs. The systems programmers have responsibility for the installation and testing of upgrades to the system software when received. Our audit did not identify significant weaknesses in system software.

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. Our audit did not identify 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 significant weaknesses in the operations procedures of the computer center.

DISASTER RECOVERY

Disasters such as fire and flood can destroy a computer service center and leave its users without computer processing support. Without computer processing, many university services would grind to a halt. To reduce this risk, computer service centers develop disaster recovery plans. Disaster recovery procedures should be tested periodically to ensure the recoverability of the data center. Our audit did not identify any significant weakness in the disaster recovery planning.

[This Page Left Blank Intentionally]

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. Mullen, Jr.	Chancellor The University of North Carolina at Asheville

LEGISLATIVE BRANCH

Appointees to the Joint Legislative Commission on Governmental Operations

Senator Marc Basnight, Co-Chairman
Senator Charlie Albertson
Senator Kever M. Clark
Senator Daniel G. Clodfelter
Senator Walter H. Dalton
Senator James Forrester
Senator Linda Garrou
Senator Wilbur P. Gulley
Senator Kay R. Hagan
Senator David W. Hoyle
Senator Ellie Kinnaird
Senator Jeanne H. Lucas
Senator William N. Martin
Senator Stephen M. Metcalf
Senator Eric M. Reeves
Senator Larry Shaw
Senator R. C. Soles, Jr.
Senator David F. Weinstein

Representative James B. Black, Co-Chairman
Representative Richard T. Morgan, Co-Chairman
Representative Martha B. Alexander
Representative E. Nelson Cole
Representative James W. Crawford, Jr.
Representative William T. Culpepper, II
Representative W. Pete Cunningham
Representative Beverly M. Earle
Representative Stanley H. Fox
Representative R. Phillip Haire
Representative Dewey L. Hill
Representative Maggie Jeffus
Representative Edd Nye
Representative William C. Owens, Jr.
Representative Drew P. Saunders
Representative Wilma M. Sherrill
Representative Joe P. Tolson
Representative Thomas E. Wright
Representative Douglas Y. Yongue

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

Internet: http://www.ncauditor.net

Telephone: 919/807-7500

Facsimile: 919/807-7647