STATE OF NORTH CAROLINA

AUDIT OF THE INFORMATION SYSTEMS

GENERAL CONTROLS

THE UNIVERSITY OF NORTH CAROLINA AT CHAPEL HILL

CHAPEL HILL, NORTH CAROLINA

FEBRUARY 2004

OFFICE OF THE STATE AUDITOR

RALPH CAMPBELL, JR.

STATE AUDITOR

AUDIT OF THE INFORMATION SYSTEMS

GENERAL CONTROLS

THE UNIVERSITY OF NORTH CAROLINA AT CHAPEL HILL

CHAPEL HILL, NORTH CAROLINA

FEBRUARY 2004

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 Chapel Hill
Dr. James Moeser, Chancellor

Ladies and Gentlemen:

We have completed our audit of the University of North Carolina at Chapel Hill (the University). This audit was conducted during the period from May 13, 2003 through August 14, 2003. 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, access controls, program maintenance, systems software, systems development, physical security, operations procedures, and disaster recovery. We also followed up on the resolution of previous audit findings and recommendations and determined the corrective action taken. Other IS general control topics were reviewed as considered necessary.

This report contains an executive summary and audit results which detail the areas where the University has performed satisfactorily relevant to our audit scope, where improvements should be made, and where further study is necessary.

We wish to express our appreciation to the staff of Administrative Information Systems 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 Systems (IS) audit at the University of North Carolina at Chapel Hill (UNC CH) from May 13, 2003 through August 14, 2003. 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. UNC CH has not performed a risk assessment for data and programs. See Audit Finding 1, *Information Technology Risk Assessment,* for additional information.

The **access control** environment consists of access control software and information security policies and procedures. We noted several weaknesses in access controls. Due to the sensitive nature of the conditions found in these 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).

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. UNC CH has not developed systems software maintenance and documentation standards. See Audit Finding 2, *Inadequate Systems Software Maintenance and Documentation Standards,* for additional information.

Systems development includes the creation of new application systems or significant changes to existing systems. Our audit did not identify any significant weaknesses in systems development.

Physical security primarily involves the inspection of the agency'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 note 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 note 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 note any significant weaknesses in disaster recovery procedures during our audit.

[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. IS general control audits are examinations of controls which effect the overall organization and operation of the IS function. This IS audit was designed to ascertain the effectiveness of general controls at the University of North Carolina at Chapel Hill.

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, systems development, physical security, operations procedures, and disaster recovery which directly affect the University's computing operations. Other IS general control topics were reviewed as considered necessary.

Our audit was limited to the general controls for which Administrative Information Services has responsibility.

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 application 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]

The University of North Carolina at Chapel Hill is the country's oldest state university**.** Authorized by the N.C. Constitution in 1776, the University was chartered by the N.C. General Assembly on December 11, 1789.

In fall 2002, the University had an enrollment of approximately 26,000 students, and 3,000 faculty members. The University is a research university and its academic offerings span a broad range of fields that include 69 bachelor's, 111 master's and 75 doctoral degrees as well as professional degrees in dentistry, medicine, pharmacy and law.

Information Technology Services (ITS)

ITS is responsible for all central computing, both academic and administrative; networking; and telecommunications for the campus.

ITS is comprised of five divisions dedicated to providing networking services, application development and technical support for the benefit of departments, faculty, staff, and students across campus. These divisions are Administrative Information Services (AIS), Academic Technology and Networks (ATN), Ibiblio, Knowledge Foundry, and Systems and Procedures.

Administrative Information Services (AIS)

Administrative Information Services (AIS) is responsible for designing, developing, and operating computer based administrative systems. AIS also provides information systems support for the University's administrative operations. Systems installed and supported by AIS include the Payroll System, Student Information System, Grant Management System, Financial Records System, Person ID System (PID), and Alumni Development System.

Administrative Information Services (AIS) is structured into five main organizational units.

- **Administrative Applications**

  Provides analysis, design, programming, project management and maintenance support of the University's administrative applications.

- **Administrative Support**

  Oversees the administrative tasks necessary to the operations at AIS.

- **Data Management**

Maintains the University's administrative databases, provides reports and reporting tools to the University, and researches and evaluates new technologies for departmental use.

- **Computer Operations**

  Directs the operation and maintenance of AIS's central computing resources.

- **Systems**

  Supports the networking, security management, and technical support of the department's server and desktop computers.

Academic Technology and Networks (ATN)

ATN supports University instructional and research programs by providing central services and infrastructure for campus-wide access to information resources and technologies. Services range from technical help and instructional services, to the maintenance of network and telecommunications infrastructures, to providing high performance servers for research, email/web, and other vital services.

Ibiblio

Home to one of the largest "collections of collections" on the Internet, ibiblio.org is a conservancy of freely available information, including software, music, literature, art, history, science, politics, and cultural studies. ibiblio.org is a collaboration of the Center for the Public Domain and the University of North Carolina - Chapel Hill.

KnowledgeFoundry

KnowledgeFoundry is a research initiative which creates media learning resources with innovative faculty for a technological society.

Systems and Procedures

Systems and Procedures' primary mission is to provide management consulting services to the University's departments and organizations.

CURRENT AUDIT RESULTS AND AUDITEE RESPONSES

The following audit results reflect the areas where the 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 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 University. Based on the results of the assessment, management should implement procedures to mitigate the risk identified or document the acceptance of the risk.

Agency's Response: The University agrees that risk assessment, as well as procedures to either mitigate the identified risks or document the acceptance of risk should be performed. Due to the high cost of such an undertaking, the University will begin this process by utilizing such risk assessment as has already been done, and will augment those efforts with risk management projects already in progress.

Under the auspices of the Office of the President, in 2002, the University engaged Kroll, Inc, a risk consulting company, to assess UNC Chapel Hill's crisis management plans, emergency procedures, and crisis communication plans, business continuity plans and disaster recovery plans. While the scope of this study is much broader than information technology, disaster recovery is included within the report. The report identifies a number of IT strengths, but recommends addressing a number of areas. Because these areas require a substantial additional budget, we will only address these as resources become available.

In addition to the University wide effort, a risk management processes is being developed for those areas of the University subject to HIPAA. The first risk assessment of these areas will be completed before July 1, 2004. We anticipate that the risk management process developed for HIPAA will be applicable to other areas as well.

Additionally each summer the Security Office offers a service which involves in depth vulnerability assessments, training, and recommendations for remediation. Last summer more than two dozen departments took part in this endeavor. Assessments are prioritized, with priority given to departments with health information or other confidential data and to departments with State or Federal regulatory requirements concerning electronic information.

Lastly, the ATN Control Center monitors network health 7X24. With intrusion detection systems, intrusion prevention systems, and other tools, the network environment is continually assessed for new and emerging threats. Security Office computer incident response procedures include immediate isolation of systems when necessary and other protective measures.

ACCESS CONTROLS

The most important information security safeguard that the University has is its access controls. The access controls environment consists of the University's 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 noted several weaknesses in access controls. Due to the sensitive nature of the conditions found in the 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).

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.

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. Systems software changes should be properly documented and approved.

AUDIT FINDING 2: INADEQUATE SYSTEMS SOFTWARE MAINTENANCE AND DOCUMENTATION STANDARDS

The AIS systems software maintenance and documentation standards are inadequate. We reviewed the standards in order to evaluate their adequacy and we noted that the standards lacked:

1. Procedures for logging of system software upgrades and patches received by UNC-CH from vendors.
2. Written procedures requiring the following controls over system software installation:
    - Establishing a written plan for testing.
    - Completing all planned testing.
    - Resolving problems encountered and re-testing.
    - Testing is adequate to provide reasonable assurance that problems with changes are identified and corrected.
    - Backing up the current version of the systems software in case problems occur during or after implementation.
3. Written procedures for maintaining an inventory of installed and uninstalled software.
4. Written procedures requiring users to maintain application systems that are compatible with new versions of systems software.Written procedures requiring system software changes to be performed at a time with the least impact on IS processing.
5. Written procedures addressing system software selection that meets both IS long range and business plans, including IS processing and control requirements, an overview of capabilities of software and control options, and meet the IS business requirements.
6. Written procedures requiring a feasibility study and selection process to determine that proposed system objectives and purposes are consistent with the request/proposal and the same selection criteria is applied to all proposals.
7. A written procedure requiring that the current version of system software be maintained by its vendor.
8. Procedures to review the cost/benefit of software changes, including direct financial costs, cost of maintenance, hardware requirements and capacity, training and technical support requirements, impact on processing reliability, impact on data security, and financial stability of vendor's operations.

As a result of inadequate software maintenance and documentation standards we noted:

1. There was no documentation of the testing of system software changes before they are moved into production.
2. There was no documentation of management's approval of system software changes before they are moved into production.

3. There was no documentation that the existing version of systems software was backed up before the new version was moved into production.
4. There was no documentation of the testing of system software changes, the problems encountered, if any, and the steps taken to resolve the problems encountered.
5. The inventory listing of systems software is incomplete. It does not include other types of systems software that AIS is using such as database management software, tape and disk management systems, utility programs and job scheduling software.

In addition, inadequate systems software maintenance and documentation standards may cause the system software changes to be mismanaged. Therefore, inappropriate system changes may result which could cause excessive amounts of downtime and may have an adverse effect on the users' applications.

Recommendation: UNC-CH AIS should develop and implement adequate systems software maintenance and documentation standards.

Agency's Response: AIS recognizes that our systems software maintenance and documentation standards are inadequate. The Systems Department has undertaken a project to ensure that this is corrected and that the AIS Standards Manual is updated to correct the inadequacy.

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

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. We did not note any significant weakness in the operations procedures of the computer center during our review.

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. We did not note any significant weakness in disaster recovery planning during our review.

[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 Moeser	Chancellor, The University of North Carolina at Chapel Hill

LEGISLATIVE BRANCH

Appointees to the Joint Legislative Commission on Governmental Operations

President Pro Tempore Senator Marc Basnight, Co-Chair	Speaker of the House Representative James B. Black, Co-Chair
Senator Charles W. Albertson	Representative Richard T. Morgan, Co-Chair
Senator Patrick J. Ballantine	Representative Martha B. Alexander
Senator Daniel G. Clodfelter	Representative Rex L. Baker
Senator Walter H. Dalton	Representative Bobby H. Barbee, Sr.
Senator Charlie S. Dannelly	Representative Harold J. Brubaker
Senator James Forrester	Representative Debbie A. Clary
Senator Linda Garrou	Representative E. Nelson Cole
Senator Wilbur P. Gulley	Representative James W. Crawford, Jr.
Senator Fletcher L. Hartsell, Jr.	Representative William T. Culpepper, III
Senator David W. Hoyle	Representative W. Pete Cunningham
Senator Ellie Kinnaird	Representative W. Robert Grady
Senator Jeanne H. Lucas	Representative Joe Hackney
Senator Stephen M. Metcalf	Representative Julia C. Howard
Senator Anthony E. Rand	Representative Joe L. Kiser
Senator Eric M. Reeves	Representative Edd Nye
Senator Robert A. Rucho	Representative William C. Owens, Jr.
Senator R. C. Soles, Jr.	Representative Wilma M. Sherrill
Senator Scott Thomas	Representative Thomas E. Wright

Other Legislative Officials

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