STATE OF NORTH CAROLINA

AUDIT OF THE INFORMATION SYSTEMS

GENERAL CONTROLS

UNIVERSITY OF NORTH CAROLINA AT ASHEVILLE

DECEMBER 2008

OFFICE OF THE STATE AUDITOR

LESLIE W. MERRITT, JR., CPA, CFP

STATE AUDITOR

AUDIT OF THE INFORMATION SYSTEMS

GENERAL CONTROLS

UNIVERSITY OF NORTH CAROLINA AT ASHEVILLE

DECEMBER 2008

STATE OF NORTH CAROLINA
Office of the State Auditor

Leslie Merritt, Jr.,
CPA, CFP
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.ncauditor.net

AUDITOR'S TRANSMITTAL

The Honorable Michael F. Easley, Governor
Members of the North Carolina General Assembly
Dr. Anne Ponder, Chancellor,
University of North Carolina at Asheville

Ladies and Gentlemen:

We have completed our information systems (IS) general controls audit at the University of North Carolina at Asheville (UNCA). The audit was conducted in accordance with *Government Auditing Standards* and *Information Systems Audit Standards*.

The primary objective of this audit was to evaluate Information Systems (IS) general controls at UNCA. The scope of our IS general controls audit included general security, access controls, systems software, systems development, program maintenance, physical security, operations procedures and disaster recovery. We also specifically reviewed access controls to the Banner application. Other IS general control topics were reviewed as considered necessary.

This report contains an executive summary and audit results which detail the areas where UNCA 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 UNCA 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,

Leslie Merritt

Leslie Merritt, Jr., CPA, CFP
State Auditor

TABLE OF CONTENTS

PAGE

EXECUTIVE SUMMARY

We conducted an information system (IS) audit of the University of North Carolina at Asheville (UNCA) from November 3, 2008, through December 10, 2008. 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. UNCA has established a reasonable security program that addresses the general security of information resources. However, o*ur audit identified four significant weaknesses in general security. See Audit Finding 1: Long-Term And Short-Term Plans Do Not Exist, Audit Finding 2: Anti-Virus Software Installation, Audit Finding 3: Control Over Web Page Content, and Audit Finding 4: Security Statements Are Not Signed.*

The **Access Control** environment consists of access control software and information security policies and procedures. UNCA has established controls to govern access to its critical systems; however some controls are not working as intended. *Our audit identified several significant weaknesses in access controls. Due to the sensitive nature of some 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). Our audit also identified the following significant weaknesses in access controls. See Audit Finding 5: Unsecure Wiring Closets, Audit Finding 6: Annual Recertification and Design of Access Forms*

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. *Our audit identified a significant weakness in systems software. See Audit Finding 7: System Software Upgrades*

Systems Development includes the creation of new application systems by development, acquisition or significant changes to existing systems. O*ur audit did not identify any significant weaknesses in systems development.*

Program Maintenance primarily involves enhancements or changes needed to existing systems. UNCA has established controls to govern maintenance of their critical programs. O*ur audit did not identify any significant weaknesses in program maintenance.*

Physical Security primarily involves the inspection of the agency's computer center for the controls that should reasonably secure the operation of the computer center from foreseeable and preventable threats from fire, water, electrical problems, and vandalism. UNCA has implemented controls to reasonably secure the computer center from fire, electrical, and vandalism. However, o*ur audit did identify a significant weakness in the physical security of the computer center. See Audit Finding 8: Weaknesses In Physical & Environmental Controls.*

Operations Procedures of the computer center include all of the activities associated with running application systems for users. O*ur audit did identify a significant weakness in operations procedures. See Audit Finding 9: Lack of Detailed and Approved Operation Procedures.*

A complete **Disaster Recovery** plan that is tested periodically is necessary to enable UNCA to recover from an extended business interruption due to the destruction of the computer center or other UNCA assets. UNCA has a complete disaster recovery plan, and periodically tests the plan. *Our audit did not identify any significant weakness in disaster recovery.*

OBJECTIVES

Under the *North Carolina General Statutes* 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 UNCA.

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, and disaster recovery, which directly affect UNCA's 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 general 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.

[This Page Left Blank Intentionally]

BACKGROUND INFORMATION

The University of North Carolina at Asheville was founded in 1927 as Buncombe County Junior College for area residents interested in pursuing their educations beyond high school. The school underwent several name changes, merged with local governments and school systems, and moved across Asheville, and in 1957 Asheville-Biltmore College, as it was then called, became the first two-year institution in North Carolina to qualify as a state-supported community college.

The college relocated in 1961 to its present site and two years later it became a state-supported senior college under a new board of trustees. In 1966, the university awarded its first baccalaureate degrees in liberal arts disciplines. 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.

[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 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. UNCA has established a reasonable security program that addresses the general security of information resources. However, o*ur audit identified four significant weaknesses in general security*.

AUDIT FINDING 1: LONG-TERM AND SHORT-TERM PLANS DO NOT EXIST

The University of North Carolina at Asheville does not have sufficient long and short-term plans in place to address information technology issues and opportunities. Without sufficient IT plans in place, technology can become out-dated, investment for IT may exceed budget, and inconsistent technology may be purchased across the University, thus making it hard to support the technology environment.

COBIT PO1.1 (IT Strategic Plan) states that management should "create a strategic plan that defines, in co-operation with relevant stakeholders, how IT goals will contribute to the enterprise's strategic objectives and related costs and risks. It should include how IT will support IT-enabled investment programs, IT services and IT assets. IT should define how the objectives will be met, the measurements to be used and the procedures to obtain sign-off from the stakeholders. The IT strategic plan should cover investment/operation budget, funding sources, sourcing strategy, acquisition strategy, and legal and regulatory requirements."

Recommendation: UNCA's management should develop a written set of long-term and short-term plans to adequately anticipate and address challenges and opportunities as they arise.

Auditee's Response: UNC Asheville concurs with the finding and will consolidate existing planning documents into a single document and make significant progress in refreshing the plan during the next three months.

AUDIT FINDING 2: ANTI-VIRUS SOFTWARE INSTALLATION

The University of North Carolina at Asheville did not install anti-virus software on some of its systems. Failure to install anti-virus software exposes the university to multiple viruses and worms for which the University will not have the ability to detect, quarantine, or eradicate. A virus can cripple systems software, and this would affect UNCA computer processing campus-wide. COBIT DS5.9 (Malicious Software Prevention) states that management should implement preventive, detective and corrective measures (especially up-to-date security patches and virus control) across the organization to protect information systems and technology from malware (e.g. viruses, worms, spyware, spam).

Recommendation: UNCA's management should obtain anti-virus software for all of its computing resources and install it immediately.

Auditee's Response: UNC Asheville concurs with the finding and ITS personnel have installed anti-virus software on the systems which were indicated by the audit. This finding is resolved.

AUDIT FINDING 3: CONTROL OVER WEB PAGE CONTENT

The University of North Carolina at Asheville does not have controls in place to prevent sensitive information from being posted on the internal and external web pages. Currently, web page content is decided by individual University departments. Without such standards in place, too much critical and sensitive information can be posted on the University's website, thus giving unauthorized users too much access to critical or sensitive data.

COBIT PO2.3 (Classification Scheme) states that management should "establish a classification scheme that applies throughout the enterprise, based on the criticality and sensitivity of enterprise data. This scheme should include details about data ownership; definition of appropriate security levels and protections controls; and a brief description of data retention and destruction requirements, criticality, and sensitivity. It should be used as the basis for applying controls such as access controls, archiving, or encryption."

Recommendation: UNCA's management should develop a process that gives the IT department the authority to set standards and guidelines for the types of information that can be posted on the webpage. Management should then communicate these policies and procedures to all faculty, student, and staff. The IT department should periodically scan the university web pages for compliance with the standards.

Auditee's Response: UNC Asheville concurs with the finding and will consolidate existing usage and data management policies into a set of standards and guidelines which web developers must use in publishing information on UNC Asheville web pages.

AUDIT FINDING 4: SECURITY STATEMENTS ARE NOT SIGNED

The University of North Carolina at Asheville does not require employees to sign a "read and understood" security statement. Security statements are used to acknowledge that employees have been informed of IT security issues and to document the employees' agreement that they will adhere to those policies. UNCA recently developed these statements; however, UNCA has not released these statements to all UNCA employees for their signatures. Without these signed statements, employees may not understand their accountability to protect and secure the University computer resources. Also, the University may not have the ability to take appropriate action against employees that do not abide by University policies and procedures.

Security statements should be signed by all employees.

Recommendation: UNCA's management should require all users to sign a "read and understood" security statement to evidence the employee's agreement that they are aware of the IT security policies and will comply with those policies.

Auditee's Response: UNC Asheville concurs with this finding and will develop an electronic approval mechanism whereby employees can certify that they have read and understood existing policy statements regarding legal usage of computing and network resources. Remediation will include recertification of existing employees

ACCESS CONTROLS

The most important information security safeguard that UNCA has is its access controls. The access controls environment consists of UNCA'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. *Our audit identified several significant weaknesses in access controls. Due to the sensitive nature of some 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). However, our audit identified two additional significant weaknesses in access controls.*

AUDIT FINDING 5: UNSECURE WIRING CLOSETS

Various wiring closets throughout UNCA's campus were not secure and/or contained debris, storage of boxes, chemicals, etc. In a defense-in-depth Security model, wiring closets have been identified as one of the most vulnerable and overlooked components in security. Securing wiring closets can be difficult since their locations are often outside of a centralized server room. However, this vulnerability can provide physical access to critical networks, and essentially bypasses all logical access controls implemented to prevent data flow interruption, or corruption of data. Given the high threat level that an improperly secured wiring closet can pose, it is critical that entities take steps to physically secure them in the same manner as the main computing center.

Critical network infrastructure should be physically secure from unauthorized access and free from non-essential network infrastructure items.

Recommendation: UNCA should ensure all wiring closets are properly secured, and free from non-essential network infrastructure items.

Auditee's Response: UNC Asheville concurs with this finding and will comply with the recommendation.

AUDIT FINDING 6: ANNUAL RECERTIFICATION AND DESIGN OF ACCESS FORMS

The University of North Carolina at Asheville failed to develop a formal process to annually recertify user's access to one of its critical applications. Also, the volunteer access rights form was not sufficiently designed to capture who authorized the volunteer's access to the system and the volunteer's level of access required to the system. Without annual recertification and a properly designed access form, UNCA may inadvertently grant more access to resources than necessary.

Control Objectives for IT (COBIT) DS5 (Ensure Systems Security) section 5.5 (Management Review of User Accounts) states that management should have a control process in place to review and confirm access rights periodically. Periodic comparison of resources with recorded accountability should be made to help reduce the risks of errors, fraud, misuse, or unauthorized alteration.

Recommendations: UNCA should annually recertify user's access to its critical systems by surveying data owners to determine if users still require the same level of access. UNCA should also redesign the volunteer access rights form to include the level of access to the system required by the volunteer and who authorized this level of access.

Auditee's Response: UNC Asheville concurs with this finding and will develop an electronic web document which will require annual recertification for user access.

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. *Our audit identified a significant weakness in system software.*

AUDIT FINDING 7: SYSTEM SOFTWARE UPGRADES

The University of North Carolina at Asheville failed to upgrade its system software on a frequent basis. This increases the risk that information contained on the computer system could be compromised via a vulnerability that should have been patched.

Computer systems' software should be upgraded in a timely manner, after appropriate testing has taken place, when new versions become available.

Recommendation: UNCA's management should ensure that upgrades to system software are performed according to an agreed upon schedule to ensure continuous maintenance and the security of systems software.

Auditee's Response: UNC Asheville concurs with this finding. IT management will ensure that upgrades to system software are performed according to a schedule currently under development.

SYSTEMS DEVELOPMENT

Systems development includes the creation of new application systems by development or acquisition 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.*

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.

UNCA' physical security controls ensure that the computer service center is reasonably secure from foreseeable and preventable threats to its physical continuity. *Our audit did identify a significant weakness in physical security.*

AUDIT FINDING 8: WEAKNESSES IN PHYSICAL & ENVIRONMENTAL CONTROLS

The University of North Carolina at Asheville's computer room uses an electronic access control device to access the computer room. During our walk-through, we learned that this device was not updated on a regular basis. Because of the sensitive nature of information contained on the servers within this room, UNCA should update this device more regularly.

We also found that water detectors in the computer room were not operational. Ceiling tiles revealed that leaks have occurred within the computer room. These leaks could have dripped onto expensive equipment below. Without operational water detectors, UNCA staff does not have a notification system to alert them of water leaks. This introduces an unnecessary security and environmental risk to the computer room.

Management should have controls in place to ensure that the organization has established adequate security over the physical access and environment that houses its critical servers and infrastructure.

Recommendation: UNCA's management should regularly change the electronic access control device and an operator from the computer room should be made responsible for obtaining updates from other departments, such as the university's human resource department to update this device on a regular basis. Also, the university should replace water detectors if the existing detectors are not operational.

Auditee's Response: UNC Asheville concurs with this finding. The computer room access device has been updated and will be on a regular, continuing basis. Repair of water detectors in the computer room is under review and will be addressed.

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 identify a significant weakness in the operations procedures.*

AUDIT FINDING 9: LACK OF DETAILED AND APPROVED OPERATION PROCEDURES

The University of North Carolina at Asheville's operation procedures are not approved by UNCA management. Although UNCA provided operation procedures to explain how critical application jobs are run, these procedures were not apart of UNCA's published policies and procedure manual. Since UNCA operations are manually performed, operations procedures should be approved and formalized to ensure critical computer processing for critical applications are performed as intended. Without these controls in place, operation procedures may be inadequate, not properly defined, and improperly communicated to operators.

Management should have operations procedures in place that are adequate to ensure that computer processing is orderly and well-controlled.

Recommendation: UNCA management should incorporate the existing operations procedures into its IT policies and procedures manual. Also, UNCA management should implement a mechanism to periodically review and approve these procedures to ensure that procedures are current with UNCA's changing environment.

Auditee's Response: UNC Asheville concurs with this finding and will formalize operations procedures. Periodic reviews of the procedures will be approved by data managers.

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, UNCA's operations would be interrupted. To reduce this risk, computer service centers develop business continuity plans. Business continuity procedures should be tested periodically to ensure the recoverability of the data center. *Our audit did not identify any significant weakness in disaster recovery.*

[This Page Left Blank Intentionally]

ORDERING INFORMATION

Audit reports issued by the Office of the State Auditor can be obtained from the web site at www.ncauditor.net. Also, parties may register on the web site to receive automatic email notification whenever reports of interest are issued. Otherwise, copies of audit reports 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