
# STATE OF NORTH CAROLINA

## AUDIT OF THE INFORMATION SYSTEMS

## GENERAL CONTROLS

## UNIVERSITY OF NORTH CAROLINA AT CHARLOTTE

**DECEMBER 2008**

**OFFICE OF THE STATE AUDITOR**

**LESLIE MERRITT, JR., CPA, CFP**

**STATE AUDITOR**

# AUDIT OF THE INFORMATION SYSTEMS

# GENERAL CONTROLS

# UNIVERSITY OF NORTH CAROLINA AT CHARLOTTE

**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.osa.state.nc.us

## AUDITOR'S TRANSMITTAL

The Honorable Michael F. Easley, Governor
Members of the North Carolina General Assembly
Dr. Philip L. Dubois, Chancellor

Ladies and Gentlemen:

We have completed our audit of the University of North Carolina at Charlotte (UNCC). This audit was conducted during the period from March 31, 2008, through September 17, 2008. 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 UNCC. The scope of our IS general controls audit included general security, access controls, program maintenance, systems software, systems development, physical security, and disaster recovery. Other IS general control topics were reviewed as considered necessary.

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

## EXECUTIVE SUMMARY

We conducted an Information Systems (IS) audit at the University of North Carolina at Charlotte (UNCC) from March 31, 2008 through September 17, 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. UNCC has established a reasonable security program that addresses the general security of information resources. *Our audit identified a significant weakness in general security. See Audit Finding 1: UNCC Does Not Have A Current Risk Assessment.*

The **access control** environment consists of access control software and information security policies and procedures. We found 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. *Our audit identified a significant weakness in program maintenance during our audit. See Audit Finding 2: UNCC Does Not Have Current Program Change Control Procedures.*

**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 3: System Software Policy and Procedures Are Incomplete.*

**Systems Development** includes the creation of new application systems or significant changes to existing systems. *We did not identify any significant weaknesses in systems development during our audit.*

**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 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 note any significant weaknesses in operations procedures during our audit.*

A complete **disaster recovery** plan that is tested periodically is necessary to enable UNCC to recover from an extended business interruption due to the destruction of the computer center or other UNCC assets. *We did not identify any significant weaknesses in disaster recovery.*

[ This Page Left Blank Intentionally ]

# AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY

## 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 UNCC.

## 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 UNCC'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 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.

[ This Page Left Blank Intentionally ]

## BACKGROUND INFORMATION

UNC Charlotte is one of a generation of universities founded in metropolitan areas of the United States immediately after World War II in response to rising education demands generated by the war and its technology.

To serve returning veterans, North Carolina opened 14 evening college centers in communities across the state. The Charlotte Center opened Sept. 23, 1946, offering evening classes to 278 freshmen and sophomore students in the facilities of Charlotte's Central High School. After three years, the state closed the centers, declaring that on-campus facilities were sufficient to meet the needs of returning veterans and recent high school graduates.

Charlotte's education and business leaders, long aware of the area's unmet needs for higher education, moved to have the Charlotte Center taken over by the city school district and operated as Charlotte College, offering the first two years of college courses. Later the same leaders asked Charlotte voters to approve a two-cent tax to support that college.

Charlotte College drew students from the city, Mecklenburg County and from a dozen surrounding counties. The two-cent tax was later extended to all of Mecklenburg County. Ultimately financial support for the college became a responsibility of the State of North Carolina.

As soon as Charlotte College was firmly established, efforts were launched to give it a campus of its own. With the backing of Charlotte business leaders and legislators from Mecklenburg and surrounding counties, land was acquired on the northern fringe of the city and bonds were passed to finance new facilities. In 1961, Charlotte College moved its growing student body into two new buildings on what was to become a 1,000-acre campus 10 miles from downtown Charlotte.

Three years later, the North Carolina legislature approved bills making Charlotte College a four-year, state-supported college. The next year, 1965, the legislature approved bills creating the University of North Carolina at Charlotte, the fourth campus of the statewide university system. In 1969, the University began offering programs leading to master's degrees. In 1992, it was authorized to offer programs leading to doctoral degrees.

Now a research intensive university, UNC Charlotte is the fourth largest of the 16 institutions within the University of North Carolina system and the largest institution in the Charlotte region.

The University comprises seven professional colleges and currently offers 17 doctoral programs, 59 master's degree programs and 85 leading to bachelor's degrees. More than 900 full-time faculty comprise the University's academic departments and the 2006 fall enrollment exceeded 21,500 students. UNC Charlotte boasts more than 75,000 living alumni and adds 4,000 to 4,500 new alumni each year.

The central information technology unit at UNC Charlotte is Information and Technology Services (ITS). The mission of the department is as follows:

ITS aims on setting new standards of service and introducing new information systems in support of our clients: faculty, staff, students, alumni and the Charlotte community. Our systems and organization are designed to support the University's goals. A common architecture serves as an enabler for excellent and cost effective services.

Specifically ITS

- Promotes the use of Information Systems for enhancing teaching, learning and research,
- Provides access to secure, quality, and timely information and online services,
- Provides excellent support for campus wide systems and technologies,
- Evaluates and recommends new technologies as to their capability to promote the University's mission and goals, and
- Uses all campus IT resources effectively to provide agreed on services and solutions.

The ITS department is composed of several service units as follows:

- The Infrastructure unit is responsible for managing the campus voice and data network, server administration, security, desktop support, and the service management center.
- The User Support unit is responsible for managing the Help Center, technical training, student computing, and communications to the campus from ITS.
- The Center for Teaching and Learning (CTL) unit is responsible for managing the online course management systems and providing pedagogical support to the faculty.
- The Information Systems unit is responsible for managing the campus enterprise administrative systems and the web hosting environment for the campus.
- The Enterprise Information Management unit is responsible for managing the DBA services and the reporting infrastructure and support utilizing a central repository of information for campus reporting.
- The Research Computing unit is responsible for managing the shared computing infrastructure supporting faculty research.
- The Project Management and Planning unit is responsible for managing the methodology utilized for project management within ITS, coordinating the strategic and operational planning, and performing project management on large high profile ITS projects.

The following audit results reflect the areas where University of North Carolina at Charlotte (UNCC) 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. UNCC has established a reasonable security program that addresses the general security of information resources. *Our audit identified one significant weakness in general security.*

### AUDIT FINDING 1: UNCC DOES NOT HAVE A CURRENT RISK ASSESSMENT

The University of North Carolina at Charlotte has not performed a current business risk assessment. The University should maintain a current business risk assessment to identify, evaluate, and prioritize business risks which could significantly impact the university. A risk assessment allows the University to place preventive measures in their environment to reduce the risk of loss or irregularities and to ensure that the critical areas remain effective.

COBIT PO9.1 Business Risk Assessment states that management should establish a systematic risk assessment framework. Such a framework 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 policy should mirror the business objectives and focus on the minimization of risks through preventive measures.

*Recommendation:* UNCC's management should adopt a set of formal standards to ensure that critical information security elements are included and kept current in their business risk assessment.

*Auditee's Response:* UNC Charlotte agrees that a formal standard should be adopted to designate and ensure that critical information security elements are included in current business risk assessment as it particularly relates to the Banner environment. UNC Charlotte ITS will work with the Internal Audit department and with the new Associate VC for Risk Management, whose position is currently being filled by the Business Affairs division, to review and determine the set of standards to implement in this matter.

## ACCESS CONTROLS

The most important information security safeguard that UNCC has is its access controls. The access controls environment consists of UNCC'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 a number of 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 identified a significant weakness in program maintenance.*

### AUDIT FINDING 2: UNCC DOES NOT HAVE CURRENT PROGRAM CHANGE CONTROL POLICIES

UNCC program change controls policies and procedures are not current and do not address the existing computer environment. We found the written programmer procedures have not been updated since UNCC migrated the Financial and Student information systems to BANNER. Failure to update policies and procedures reduces the effectiveness of the procedures in conveying management's expectations for managing program changes.

COBIT AI6 states that "Control over all changes, including emergency maintenance and patches relating to infrastructure and applications within the production environment should be formally managed in a controlled manner. Changes (including those to procedures, processes, and system and service parameters) should be logged, assessed and authorized prior to implementation and reviewed against planning outcomes following implementation."

*Recommendation:* Management should update program change control policies and procedures to include the Banner environment.

*Auditee's Response:* UNC Charlotte agrees with this finding and will develop a plan to bring the existing documentation up to date with the Banner environment terminology and practices.

## 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 systems software*.

**AUDIT FINDING 3: SYSTEM SOFTWARE POLICY AND PROCEDURES ARE INCOMPLETE**

UNCC has adopted ITIL's Change Management policy and procedures to address system software changes and upgrades. However, the Change Management policy and procedures are incomplete with respect to system software changes/upgrades and do not contain the following:

- **a)** Test procedures for software implementation and review and approval procedures for test results
- **b)** Performing changes (should be programmers only)
- **c)** Documenting problems and resolutions occurring during system changes
- **d)** System software changes are made when they are least likely to negatively impact production
- **e)** A written procedure is in place for testing changes to system software
- **f)** Problems occurring during testing are resolved and retested
- **g)** Test procedures are adequate to provide reasonable assurance
- **h)** Fallback or restoration procedures are in place in case of unforeseen problem with an upgrade or modification
- **i)** Each change is tested before implementation
- **j)** Proper approval is obtained before implementation
- **k)** Programmers maintain detailed documentation of all changes, testing, results, approvals and move to production

In addition, the ITS Change Management System (Magic) is a work in progress and does not capture the changes until late in the process when the changes are about ready to be put into production. Also, not all of the system software changes (network upgrades, Oracle upgrades, and Banner upgrades) have been captured by Magic.

COBIT DS9.2 Identification and Maintenance of Configuration Items states that management should put procedures in place to identify configuration items and their attributes, record new, modified and deleted configuration items, identify and maintain the relationships among configuration items in the configuration repository, update existing configuration items into the configuration repository, and prevent the inclusion of unauthorized software.

These procedures should provide proper authorization and logging of all actions on the configuration repository and be properly integrated with change management and problem management procedures.

*Recommendation:* The University should ensure all system software changes are documented in Magic, and changes should be entered into Magic at the beginning of the process if possible.

*Auditee's Response:* UNC Charlotte will update the Server Administration written procedures regarding server operating software upgrades and patches to document more clearly the practices being followed and will continue to enter change management tickets in Magic to document these upgrades. The tickets will not contain the details of the patches, but document the dates and times and reason for upgrades and patches. The actual patch details are maintained by Server Administration separately.

## 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. UNCC'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 audit.*

## 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, UNCC'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 weaknesses 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