STATE OF NORTH CAROLINA

AUDIT OF THE INFORMATION SYSTEMS

GENERAL CONTROLS

NORTH CAROLINA STATE UNIVERSITY

DECEMBER 2008

OFFICE OF THE STATE AUDITOR

LESLIE W. MERRITT, JR., CPA, CFP

STATE AUDITOR

AUDIT OF THE INFORMATION SYSTEMS

GENERAL CONTROLS

NORTH CAROLINA STATE UNIVERSITY

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
Board of Trustees, North Carolina State University
Dr. James L. Oblinger, Chancellor

Ladies and Gentlemen:

We have completed our information systems (IS) general controls audit at North Carolina State University (NCSU). 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 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 specifically reviewed access controls to the Peoplesoft 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 North Carolina State 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 North Carolina State University 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 system (IS) audit of North Carolina State University (NCSU) from August 11, 2008, through October 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. *Our audit identified several significant weaknesses in general security. See Audit Finding 1: General Security Weaknesses.*

The a**ccess 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 other 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).*

Program Maintenance primarily involves enhancements or changes needed to existing systems. *Our audit did not identify any significant weaknesses in program maintenance.*

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 did not identify any significant weaknesses in systems software.*

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.*

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. O*ur audit did not identify any significant weaknesses in physical security.*

The **operations procedures** of the computer center include all of the activities associated with running application systems for users. O*ur audit did not identify any significant weaknesses in operations procedures.*

A complete **disaster recovery** plan that is tested periodically is necessary to enable North Carolina State University to recover from an extended business interruption due to the destruction of the computer center or other University assets. *Our audit identified several significant weaknesses in disaster recovery. See Audit Finding 2: Organizational Resilience Plan Out-of-Date and Business Continuity Plans Not Approved.*

[This Page Left Blank Intentionally]

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 North Carolina State University.

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 North Carolina State University'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

North Carolina State University was founded on March 7, 1887 as a land-grant university in Raleigh. With more than 31,000 students and nearly 8,000 faculty and staff, it is a comprehensive university known for its leadership in education and research, and globally recognized for its science, technology, engineering and mathematics leadership. NC State is committed to playing an active and vital role in improving the quality of life for the citizens of North Carolina, the nation and the world.

NC State operates 13 off-campus regional research and extension centers and nine field laboratories. The University is involved in multiple initiatives, totaling nearly 70 centers, institutes, and laboratories that include every college at NC State as well as industries and national and international corporations. NC State University consists of 12 schools and colleges that collectively offer more than 300 undergraduate and graduate degree programs through 65 departments. The schools and colleges are as follows: College of Agriculture and Life Sciences, College of Design, College of Education, College of Engineering, College of Humanities and Social Sciences, College of Management, College of Natural Resources, College of Physical and Mathematical Sciences, College of Textiles, College of Veterinary Medicine, First Year College and the Graduate School.

On November 1, 2007, the Office of Information Technology (OIT) brought together into one organizational unit, the staff, operations, and responsibilities of Resource Management and Information Systems (RMIS) and the Information Technology Division (ITD).

OIT continues to -

- Provide existing central administrative and academic IT services to campus
- Improve functionality of NC State's IT Infrastructure and services
- Enhance collaboration among OIT units and with campus
- Foster dialog and keep campus informed of OIT news and developments.

The formation of the OIT was a major step in NC State's initiative to reorganize its central IT operations under the leadership of a Chief Information Officer (CIO). A new Vice Chancellor for Information Technology (VCIT) and CIO position was created as part of this initiative. After a national search, Dr. Marc Hoit was named VCIT and CIO. Dr. Hoit took over the helm of OIT effective September 1, 2008.

[This Page Left Blank Intentionally]

The following audit results reflect the areas where North Carolina State 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. *Our audit identified several significant weaknesses in general security.*

AUDIT FINDING 1: GENERAL SECURITY WEAKNESSES

The North Carolina State University's Office of Information Technology (OIT) has performed risk assessment based on incidents that includes tests, exercises, workshops and observation. However, they have not performed an updated, complete, division-wide formal risk assessment to identify potential areas of weaknesses.

Additionally, the North Carolina State University's Office of Information Technology (OIT) does not have in place adequate policies and/or procedures to perform cross-training for critical positions, and to prevent data leakage from university web pages

Without performing a complete, division-wide formal risk assessment on a periodic basis, it will be difficult for the University to adequately plan (in the short-term or long-term) for possible risks (or opportunities) that may face the organization.

Without a division-wide procedure in place to ensure that critical positions are adequately cross-trained, in the event that a key person is unable to work, there would not be a secondary person available to step in as backup. This issue is often realized during times of reorganization and high turnover.

Also, without a policy and procedure to address the control of webpage content, authors of web pages that reside on the organization's servers may "leak" sensitive data that could lead to a compromise of the organization's systems.

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."

COBIT 4.1 PO4.13 Key IT Personnel states that "management should define and identify key IT personnel (e.g., replacements/backup personnel), and minimize reliance on a single individual performing a critical job function."

ISO/IEC 27001:2005(E), A.12.5.4 (Information Leakage) states that "opportunities for information leakage shall be prevented."

Recommendation: NCSU OIT should perform complete, division-wide formal risk assessments on a periodic basis and should develop cross-training procedures to ensure that key staff members have a backup person who can step in to fulfill their critical duties should they be unable to do so. Also, NCSU OIT should establish policies and procedures to address the control of webpage content tied to the University system to provide guidance to staff to prevent sensitive data from being leaked on web pages.

Auditee's Response: A division-wide risk assessment will be conducted on an annual basis starting in 3Q2009, in addition to risks assessments that are currently performed under the OIT resiliency program.

OIT has a comprehensive training plan for staff members covering identified IT and management skills associated with OIT services and projects. In addition to this, OIT currently conducts periodic new staff OIT orientation sessions to assure that staff is aware of division services and responsibilities. OIT will incorporate staff cross-training procedures into the training plan by the end of 3Q2009.

OIT will develop a university regulation to address the control of webpage content and provide guidance to prevent leakage of sensitive university data by end of year 2009.

ACCESS CONTROLS

The most important information security safeguard that NCSU has is its access controls. The access controls environment consists of NCSU'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).*

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. *Our audit did not identify any significant weaknesses in systems software.*

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.*

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. NCSU's physical security controls ensure that the computer service center is reasonably secure from foreseeable and preventable threats to its physical continuity. *Our audit did not identify any significant weaknesses in physical security.*

OPERATIONS PROCEDURES

The operations of the computer center include all of the activities associated with running application systems for users. Procedures should be in place to control the scheduling and running of production jobs, restarting production jobs when problems occur, storing, handling and mounting of tapes, and maintaining computer equipment. *Our audit did not identify any significant weaknesses in the operations procedures.*

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, NCSU'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 identified several significant weaknesses in disaster recovery.*

AUDIT FINDING 2: ORGANIZATIONAL RESILIENCE PLAN OUT-OF-DATE AND BUSINESS CONTINUITY PLANS NOT APPROVED

The North Carolina State University's Office of Information Technology (OIT) has a plan that emphasizes *organizational resilience* rather than the traditional *business continuity/disaster recovery*. All critical business units have business continuity plans (BCP), which are more traditional in their emphasis on *disaster recovery*. We reviewed the OIT Resiliency Plan and a sample of six business units' business continuity plans (Controller's Office, Enrollment Management-Office of Scholarships and Financial Aid, HR-Payroll, University Cashier's Office, University Dining, University Housing) and noted the following deficiencies in the plans:

a) The current resiliency plan for OIT is out-dated and does not reflect the current information technology (IT) operating environment. The current IT operating environment at NCSU for the financial systems is an Enterprise Resource Planning software package running on servers hosting the application and database. OIT is currently developing a new resiliency plan that addresses both the current operating environment and consolidation of the academic and administrative computing departments. As a result, the BCPs of the critical business units will need to be updated when the OIT plan is finalized to ensure the plans include current assumptions of time estimates and prioritization of restoration of services.

b) The business units develop their business continuity plan using a software package called LDRPS. We found the department head's approval for the sampled plans were not documented in LDRPS as required by University policy.

As a result:

a) An out-of-date resiliency and business continuity plan that does not reflect the current computer infrastructure limits the effectiveness of the plan in aiding in the recovery and restoration of services following a disaster. The recovery of critical business services may be affected or delayed without an updated plan.

b) According to University policy: "The respective Department Head/Director, Dean or Vice Chancellor (or designated vice provost or associate vice chancellor), and Cohort Coordinator must review and approve the updated plan on, at least, an annual basis." This approval should be documented in the LDRPS software. Without adequate management review and approval, the plans may not reflect management's expectation for disaster recovery and business continuity.

COBIT 4.1 DS4.4 Maintenance of the IT Continuity Plan states "encourage IT management to define and execute change control procedures to ensure that the IT continuity plan is kept up to date and continually reflects actual business requirements. Communicate changes in procedures and responsibilities clearly and in a timely manner."

According to NC State University regulation: REG04.00.7 - Developing Business Continuity and Disaster Recovery Plans Section 4.4 Plan Maintenance, "Business units are required to review their Business Continuity Plans at least quarterly and update the plans whenever changes occur in their operating procedures, processes, or key personnel. Plans must be updated to maintain accurate lists of key personnel, telephone number, call trees and plan elements that may be affected by changes in unit structure or functions. The respective Department Head/Director, Dean or Vice Chancellor (or designated vice provost or associate vice chancellor), and Cohort Coordinator must review and approve the updated plan on, at least, an annual basis."

Recommendation: OIT should complete the OIT resiliency plan currently being developed as soon as possible. The OIT plan should accurately describe the existing infrastructure with associated risks and organizational responses to those risks. After the OIT resiliency plan is approved, the business units should update their respective business continuity plans to reflect the current assumptions of time estimates and prioritization of restoration of services. The business units should document the designated individual's review and approval of the unit's plan.

Auditee's Response: The OIT Resiliency Plan will be updated to reflect changes in our environment by the end of 2009 and will be updated continuously and reviewed annually. Also, the business continuity plans of the critical business units will be updated in accordance with the approved OIT resiliency plan. A mechanism for documenting the review and approval process of unit plans will be implemented by the end of 3Q2009.

[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