STATE OF NORTH CAROLINA

AUDIT OF THE INFORMATION SYSTEMS

GENERAL CONTROLS

WESTERN CAROLINA UNIVERSITY

NOVEMBER 2009

OFFICE OF THE STATE AUDITOR

BETH A. WOOD, CPA

STATE AUDITOR

AUDIT OF THE INFORMATION SYSTEMS

GENERAL CONTROLS

WESTERN CAROLINA UNIVERSITY

NOVEMBER 2009

STATE OF NORTH CAROLINA
Office of the State Auditor

Beth A. Wood, CPA
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 Beverly E. Perdue, Governor
Members of the North Carolina General Assembly
Dr. John W. Bardo, Chancellor

Ladies and Gentlemen:

We have completed our Information Systems (IS) audit of the Western Carolina University (WCU). This audit was conducted for the period from November 3, 2008, through January 7, 2009. 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 WCU. 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 WCU 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 WCU 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,

Beth A. Wood

Beth A. Wood, CPA
State Auditor

TABLE OF CONTENTS

PAGE

EXECUTIVE SUMMARY 1

AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY 3

BACKGROUND INFORMATION 5

AUDIT RESULTS AND AUDITEE RESPONSES 7

ORDERING INFORMATION 13

EXECUTIVE SUMMARY

We conducted an Information Systems (IS) audit at the Western Carolina University (WCU) from November 3, 2008 through January 7, 2009. 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: Information Leakage, Audit Finding 2: WCU Does Not Have a Current Risk Assessment and Audit Finding 3: Lack of Policies and Procedures For Updating The Banner Finance User's Manual and Training For Users.*

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. *The results of our audit of program maintenance disclosed no internal control deficiencies or instances of noncompliance or other matters that are considered reportable under Government Auditing Standards.*

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 4*: *Lack of Written Systems Software Change Management Procedures.*

Systems Development includes the creation of new application systems or significant changes to existing systems. *The results of our audit of systems development disclosed no internal control deficiencies or instances of noncompliance or other matters that are considered reportable under Government Auditing Standards.*

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. *The results of our audit of physical security disclosed no internal control deficiencies or instances of noncompliance or other matters that are considered reportable under Government Auditing Standards.*

The **operations procedures** of the computer center include all of the activities associated with running application systems for users. *Our audit identified a significant weakness in operations procedures. See Audit Finding 6: Operations Manual Out-of-Date.*

A complete **disaster recovery** plan that is tested periodically is necessary to enable WCU to recover from an extended business interruption due to the destruction of the computer center or other WCU assets. *Our audit identified a significant weakness in disaster recovery. See Audit Finding 7: Disaster Recovery/Business Continuity Plans Incomplete and Out-of-Date.*

AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY

OBJECTIVES

Under *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 WCU.

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, access controls, program maintenance, systems software, systems development, physical security, and disaster recovery which directly affect WCU's computing operations. Other IS general control topics were reviewed as considered necessary.

METHODOLOGY

To meet our objectives, we reviewed 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.

We conducted this performance audit in accordance with generally accepted government auditing standards and Information Systems Audit Standards issued by the Information Systems Audit and Control Association (ISACA). Information Systems Audit Standards are documented in the Control Objectives for Information and related Technology (COBIT). COBIT is a set of best practices for information technology management created by ISACA and the IT Governance Institute. Generally accepted government auditing standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[This Page Left Blank Intentionally]

BACKGROUND INFORMATION

Western Carolina University, located in Cullowhee, North Carolina, was founded in 1889. Western Carolina University is a coeducational residential public university within the University of North Carolina system. The University has a current enrollment of approximately 9,000 students and offers more than 120 majors and concentrations for undergraduates and over 30 graduate level programs of study.

The Information Technology Division supports all aspects of Western Carolina University's information technology (IT) resources - networks, programming, hardware and software, computer labs and classrooms, training, and business systems.

[This Page Left Blank Intentionally]

GENERAL SECURITY

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 three significant weaknesses in general security.*

AUDIT FINDING 1: INFORMATION LEAKAGE

Western Carolina University (WCU) has their internal information technology policies and procedures on the public website. WCU has established standards for information that is appropriate to reside on the University's internal and external web pages, but the internal policies and procedures were posted on the external web page in error. As a result, individuals outside the University environment can view these documents.

Management should ensure that security documentation is not disclosed unnecessarily.

Recommendation: WCU's management should remove the internal policies and procedures from the public website. WCU should periodically review their public web site for inappropriate material.

Auditee's Response: WCU's informational technology internal policies and procedures will be removed from the public website. Any additional information technology policies and procedures located on the externally facing web pages will be reviewed and those with sensitive information will also be removed.

AUDIT FINDING 2: WCU DOES NOT HAVE A CURRENT RISK ASSESSMENT

WCU has recently installed a new financial system. The University has not performed a risk assessment to identify the risks for the new financial system. These risks would include security risks, financial system availability risks, and financial system integrity risks. The risks associated with these areas should be identified along with measures that can be put in place to reduce or control these risks. Whenever the university environment changes, the risk assessment should be updated to reflect the risks associated with the changes in the environment.

Computer industry standards recommend an organization maintain a current business risk assessment to identify, evaluate, and prioritize risks which could significantly impact the organization's computer operations. These standards recommend the risk assessment be reviewed regularly and updated for changes in computer operations. The risk assessment for computer operations should be a part of the overall business risk assessment for the entire organization.

Recommendation: WCU should develop policies and procedures for performing a risk assessment that includes the new application system. These policies and procedures should require that this risk assessment be reviewed and updated regularly. The assessment should be updated whenever there are major changes in the university environment. The risk assessment should be reviewed at least annually to ensure it is current and covers any new risks for changes in the environment.

Auditee's Response: Risk assessment policies and procedures will be developed. These policies will require all enterprise level applications undergo a risk assessment prior to moving to production and will require an annual review of each risk assessment.

AUDIT FINDING 3: LACK OF POLICIES AND PROCEDURES FOR UPDATING THE BANNER FINANCE USER'S MANUAL AND TRAINING FOR USERS

Western Carolina University has no written policies and procedures for periodically reviewing, updating, and approving the Banner finance user's manual. Also, the University does not have formal training for new users and needs better documentation for training status and schedules for intermediate and advanced users. As a result, the Banner finance user's manual may become out-of-date and may not reflect the current operating environment. Also, new Banner users may not be adequately trained according to management's intentions and existing user's Banner skills may not be current.

Management should transfer knowledge and skills to enable operations and technical support staff to effectively and efficiently deliver, support and maintain the system and associated infrastructure.

Recommendation: Management should adopt a set of policies and procedures for updating the Banner finance user's manual on a periodic basis. Also, WCU should provide formal training for new users and adequately document the training status and scheduling for intermediate and advanced users.

Auditee's Response: WCU will develop written policies and procedures to define regular maintenance and updates to the Banner finance user's manual.

User training will be scheduled, provided and documented to the fullest extent possible within available resources.

ACCESS CONTROLS

The most important information security safeguard that WCU has is its access controls. The access controls environment consists of WCU'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. *The results of our audit of program maintenance disclosed no internal control deficiencies or instances of noncompliance or other matters that are considered reportable under Government Auditing Standards.*

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 4: LACK OF WRITTEN SYSTEMS SOFTWARE CHANGE MANAGEMENT PROCEDURES

Western Carolina University's draft policies and procedures for system software changes have not been approved by management. Draft policies and procedures may lead to inconsistent application of systems software changes. Also, management's intentions may not be followed.

Management should develop and maintain a set of policies to support IT strategy. These policies should include policy intent; roles and responsibilities; exception process; compliance approach; and references to procedures, standards and guidelines. Their relevance should be confirmed and approved regularly.

Recommendation: The University should adopt adequate systems software change management policies and procedures and these policies and procedures should be approved by management and communicated to the appropriate employees.

Auditee's Response: WCU will develop and disseminate to appropriate employees a policy to mandate that the addition, modification or removal of approved, supported or baseline hardware, network devices, software, applications, support environment, systems or desktop

builds must be documented, reviewed and approved by management in the form of a Change Approval Board.

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. *The results of our audit of systems development disclosed no internal control deficiencies or instances of noncompliance or other matters that are considered reportable under Government Auditing Standards.*

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. WCU's physical security controls ensure that the computer service center is reasonably secure from foreseeable and preventable threats to its physical continuity. *The results of our audit of physical security disclosed no internal control deficiencies or instances of noncompliance or other matters that are considered reportable under Government Auditing Standards.*

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 ensure adequate and authorized scheduling and running of production jobs, restarting production jobs when problems occur, storing, handling and mounting of tapes, and maintaining computer equipment. *Our audit identified a significant weakness in operations procedures.*

AUDIT FINDING 5: OPERATIONS MANUAL OUT-OF-DATE

The operations manual for the Western Carolina University IT department is out-of-date with the cover page of the document indicating it was last updated in 2006. Supporting documentation in appendices and attachments has not been updated since 2002 in some cases. The operations manual does not include the Banner environment.

Without an up-to-date operations manual, staff in the data center responsible for daily operations may not have the necessary direction and may neglect to perform certain procedures. All policies and procedures should be updated on a regular basis.

Recommendation: WCU management should update the operations manual and should implement procedures to update the manual on a periodic basis. The manual should be updated sooner if a major upgrade in the computer system causes the manual to become obsolete.

Auditee's Response: WCU will update its operations manual to reflect the current environment and will develop procedures requiring updates to the manual on a periodic basis.

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, Western Carolina University'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 two significant weaknesses in disaster recovery*.

AUDIT FINDING 6: DISASTER RECOVERY/BUSINESS CONTINUITY PLANS INCOMPLETE AND OUT-OF-DATE

The WCU IT department disaster recovery plan is out-of-date and there is no documented formal process in place to maintain an up-to-date disaster recovery plan. Also, some user department plans insufficiently detail alternate processing procedures and are also out-of-date.

Without a formal process for periodic review and approval of changes, it will be impossible to properly maintain the disaster recovery/organizational resilience plan to ensure continued service to dependant business units in the event of a disaster.

Without alternate processing procedures, the user departments will not know what procedures they need to perform in the event of a disaster to keep their business operations functioning until the computer system can be restored.

A business unit must establish alternate processing procedures to enable it to continue its function within the larger organization, basing its plan on reasonable assumptions that have been provided by the service provider department.

Recommendation: Both the WCU IT department and the critical business units should update their disaster recovery/business continuity plans to provide alternate processing procedures in the event of a disaster. WCU should establish a formal review and approval process to ensure the disaster recovery/business continuity plans are kept up-to-date.

Auditee's Response: WCU will update the IT and critical business units' disaster recovery/business continuity plan to provide alternate processing procedures in the event of a disaster. WCU will establish a policy that requires a formal review and approval process to keep these plans up to date.

AUDIT FINDING 7: DAILY BACKUP TAPES NOT STORED OFFSITE

While full weekly backup tapes are taken offsite to a third party provider, the daily incremental tapes are stored in the data center. This could result in up to one full week's worth of backups being lost (up to last full weekly offsite tape) in the event of a disaster affecting the data center.

Management should store offsite all critical backup media, documentation and other IT resources necessary for IT recovery and business continuity plans. IT management should ensure that offsite arrangements are assessed, at least annually, for content, environmental protection and security. Management should ensure compatibility of hardware and software to restore archived data, and periodically test and refresh archived data.

Recommendation: Management should rotate the daily backups to a location other than the building the computer center is located in.

Auditee's Response: WCU's Backup and Retention Policy has been edited to reflect changes in tape storage procedures. Tapes are moved from the datacenter to a secure location on campus daily (M-F), and are sent to a secure offsite location once a week.

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