STATE OF NORTH CAROLINA

NORTH CAROLINA A&T STATE UNIVERSITY

INFORMATION TECHNOLOGY GENERAL CONTROLS

JUNE 2010

PERFORMANCE AUDIT

OFFICE OF THE STATE AUDITOR

BETH A. WOOD, CPA

STATE AUDITOR

NORTH CAROLINA A&T STATE UNIVERSITY

INFORMATION TECHNOLOGY GENERAL CONTROLS AUDIT

JUNE 2010

PERFORMANCE AUDIT

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.ncauditor.net

AUDITOR'S TRANSMITTAL

June 14, 2010

The Honorable Beverly Eaves Perdue, Governor
The General Assembly of North Carolina
Dr. Harold L. Martin, Sr., Chancellor

This report presents the results of our performance audit of information technology general controls at the North Carolina Agricultural and Technical State University. Our audit was performed by authority of Article 5A of Chapter 147 of the *North Carolina General Statutes* and was conducted in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States.

The objective of this audit was to review the general controls as they pertain to the University's information technology. The results of our audit disclosed deficiencies that are considered reportable under *Government Auditing Standards.* These items are described in the Audit Findings and Responses section of this report, except those regarding access controls which due to their sensitivity are reported to you by separate letter pursuant to *North Carolina G.S. 147-64.6(c)(18).*

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.

Beth A. Wood, CPA
State Auditor

TABLE OF CONTENTS

BACKGROUND

North Carolina Agricultural and Technical State University is a public, land-grant university committed to fulfilling its fundamental purposes through undergraduate and graduate instruction, scholarly and creative research, and effective public service. The University offers degree programs at the baccalaureate, masters and doctoral levels, with emphasis on engineering, science, technology, literature, and other academic areas.

As one of North Carolina's three engineering colleges, the University offers Ph.D. programs in engineering. Basic and applied research is conducted by faculty in University centers of excellence, in inter-institutional relationships, and through significant involvement with several public agencies. The University also conducts major research through engineering, transportation, and its programs in agriculture.

[This Page Left Blank Intentionally]

OBJECTIVES, SCOPE, AND METHODOLOGY

As authorized by Article 5A of Chapter 147 of the *North Carolina General Statutes*, we have conducted a performance audit at the North Carolina Agricultural and Technical State University (NCA&T). The objective of this audit was to determine the effectiveness of general controls which influence the overall organization and operation of the University's information technology (IT). Our audit was conducted between August 10, 2009 and November 20, 2009.

The scope of our audit included the following IT general controls categories: general security, access controls, program maintenance, systems software, systems development, physical security, operations procedures, and disaster recovery, which directly affect NCA&T's computing operations.

To accomplish our audit objectives, we gained an understanding of University policies and procedures, interviewed key University administrators and other personnel, examined system configurations, tested on-line system controls, reviewed appropriate technical literature, and reviewed computer-generated reports.

As a basis for evaluating general controls, we applied the guidance contained in *Control Objectives for Information and Related Technology* (COBIT), created by the Information Systems Audit and Control Association and the IT Governance Institute. COBIT contains a widely accepted set of best practices in the field of information technology management.

University management, pursuant to North Carolina General Statute §143D-7, bears full responsibility for establishing and maintaining a proper system of internal control which includes IT general controls. A proper system of internal control is designed to provide reasonable assurance, rather than absolute, that relevant objectives are achieved. Because of inherent limitations in internal controls, unauthorized access to data, for example, may nevertheless occur and not be detected. Also, projections of our evaluation in this report of general controls to future periods are subject to the risk that, for example, conditions at the University may change or compliance with University policies and procedures may deteriorate.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those 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.

RESULTS

The results of our audit disclosed general control deficiencies that are considered reportable under *Government Auditing Standards*. Deficiencies noted were as follows:

1. Failure to develop a risk assessment.
2. Failure to develop an effective and approved disaster recovery plan.
3. Failure to develop an evacuation plan that incorporates essential details.
4. Failure of programmers to retain test results of changes made to applications.
5. Failure to maintain segregation of duties within IT positions.
6. Failure to implement access controls in five critical areas.

Details about these deficiencies are described in the Audit Findings and Responses section of this report, except those regarding access controls (number 6 above) which due to their sensitive nature were conveyed to University management in a separate letter pursuant to *North Carolina G.S. 147-64.6(c)(18).*

1. FAILURE TO DEVELOP A RISK ASSESSMENT

North Carolina A&T State University has not created a risk assessment to identify and assess risks to its information technology assets. Without an adequate risk assessment, the University can neither sufficiently anticipate and address threats and vulnerabilities to its assets nor design appropriate controls to mitigate risk.

COBIT standards state that an organization should 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: North Carolina A&T State University management should develop a risk assessment that will assist the University in anticipating and mitigating threats and vulnerabilities to its assets, especially information technology assets. University management should design controls appropriately in order to mitigate risk.

Agency Response: The University concurs with the finding. The University will establish a process for conducting a risk assessment on an annual basis. An information technology risk assessment is currently in progress.

2. FAILURE TO DEVELOP AN EFFECTIVE AND APPROVED DISASTER RECOVERY PLAN

North Carolina A&T State University's disaster recovery plan lacks critical elements, including a statement of assumptions and alternate user department procedures. Additionally, the current disaster recovery plan is in draft form, and has not been approved by executive management. As a result, it may not enable the University to restore all of its critical functions if a disaster were to occur. Also, management's intentions may not be carried out in the event of a disaster.

COBIT standards state that without a formal process for periodic review and approval of changes, it will be difficult to properly maintain the disaster recovery plan to ensure continued service in the event of a disaster.

Recommendation: NCA&T's management should develop a comprehensive disaster recovery plan that anticipates potential service interruptions and devise contingencies to either minimize or address those potential interruptions. Additionally, the disaster recovery plan should be reviewed and approved by executive management to ensure it has campus-wide support.

Agency Response: The University concurs with the finding. Since business continuity encompasses disaster recovery and alternate user departmental procedures, the University will form a campus-wide Business Continuity Committee. The Business Continuity Committee's broad oversight will include developing implementing and maintaining a comprehensive business continuity and disaster recovery plan that address both academic and administrative needs.

3. FAILURE TO DEVELOP AN EVACUATION PLAN THAT INCORPORATES ESSENTIAL DETAILS

North Carolina A&T State University's evacuation plan for the computer center does not designate an assembly area. Also, the plan neither specifies positions to serve as evacuation personnel, nor includes procedures for rapidly securing the agency's facilities, assets, and records. Failure to include these details in the evacuation plan may result in confusion at the time of an emergency which may lead to jeopardizing university personnel and assets.

COBIT states that continuity plans should be complete and include all elements of an evacuation plan.

Recommendation: The University should revise their evacuation plan for the computer center to include the designation of an assembly area, the specification of positions to serve as evacuation personnel, and procedures for rapidly securing the agency's facilities, assets and records.

Agency Response: The University concurs with the finding. The evacuation plan for the computer center was revised and now includes designated assembly areas, positions to serve as the evacuation chain of command, and procedures for rapidly securing the University's facility. The plan will be reviewed annually.

4. FAILURE OF PROGRAMMERS TO RETAIN TEST RESULTS OF CHANGES MADE TO APPLICATIONS

North Carolina A&T State University does not retain test results of changes made to applications. By not retaining the results of changes including the results of user acceptance tests, the risk of unauthorized changes being entered into the system, as well as the risk that changes made were not accepted by the users who requested the changes, is increased.

COBIT states that documentation of changes made to applicatons and the results of the tests of the changes should be retained.

Recommendation: NCA&T's management should require programmers to retain the test results of changes made to applications. NCA&T should establish a tracking and reporting system to document rejected changes, and to communicate the status of approved, in-process, and completed changes.

Agency Response: The University concurs with the finding. The User Acceptance Sign-off process was amended to include test results.

5. FAILURE TO MAINTAIN SEGREGATION OF DUTIES WITHIN IT POSITIONS

North Carolina A&T State University has failed to maintain segregation of duties within some IT positions due to the overlap of incompatible responsibilities.

- The application programmers have the ability to serve as database administrators. This is a segregation of duties conflict because the programmers have access to application programs as well as to production data.
- Systems administrators have the ability to serve as application programmers and database administrators. This is a segregation of duties risk because systems administrators have access to systems software, application programs as well as production data.

These conditions allow users to modify critical data for their use and benefit with little to no detection by management.

COBIT states that management should implement a division of roles and responsibilities that reduces the possibility that a single individual could compromise a critical process.

Recommendation: University management should consider removing incompatible roles and/or responsibilities from IT personnel to reduce the risk of unauthorized acts. The reports produced by tracking software should be sent to a security or internal audit group for review.

Agency Response: The University concurs with the finding. University management is currently performing a thorough assessment of the roles and responsibilities within the Information Technology department. Any responsibilities that create segregation of duty issues will be remedied.

[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