STATE OF NORTH CAROLINA

AUDIT OF THE INFORMATION SYSTEM GENERAL CONTROLS

AT

NC CENTER FOR APPLIED TEXTILE TECHNOLOGY

BELMONT, NORTH CAROLINA

JUNE 2004

OFFICE OF THE STATE AUDITOR

RALPH CAMPBELL, JR.

STATE AUDITOR

AUDIT OF THE INFORMATION SYSTEM GENERAL CONTROLS

AT

NC CENTER FOR APPLIED TEXTILE TECHNOLOGY

BELMONT, NORTH CAROLINA

JUNE 2004

AUDITOR'S TRANSMITTAL

The Honorable Michael F. Easley, Governor
Members of the North Carolina General Assembly
The Board of Directors of NC Center for Applied Textile Technology
Dr. James Lemons, President

Ladies and Gentlemen:

We have completed our information systems (IS) audit of the NC Center for Applied Textile Technology. 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 the NC Center for Applied Textile Technology. The scope of our IS general controls audit included general security, access controls, program maintenance, systems software, physical security, and disaster recovery. Other IS general control topics were reviewed as considered necessary.

This report contains an executive summary that highlights the areas where the NC Center for Applied Textile Technology has performed satisfactorily and where improvements should be made.

We wish to express our appreciation to the staff at the NC Center for Applied Textile Technology 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,

Ralph Campbell, Jr.
State Auditor

TABLE OF CONTENTS

EXECUTIVE SUMMARY

We conducted an information system (IS) audit at the NC Center for Applied Textile Technology (CC) from April 4, 2003 - April 30, 2004. 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. We found that the NC Center for Applied Textile Technology should adopt formal standards for information technology (IT) to improve the IT Security Policies and Procedures. *See Audit Finding 1, IT Security Policies and Procedures.*

The **access control** environment consists of access control software and information security policies and procedures. We reviewed the access controls for the NC Center for Applied Textile Technology's critical operating systems. We found several weaknesses in access controls. Due to the sensitive nature of the conditions found, we have conveyed these findings to management in a separate letter pursuant to the provision of *North Carolina General Statute* 147-64.6(c)(18).

Program maintenance primarily involves enhancements or changes needed to existing systems. Because the same procedures are used to patch and upgrade the critical application and the operating system, we indirectly tested program changes to the critical application in our test of system software 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. We found a significant weakness in systems software maintenance. Due to the sensitive nature of the condition found, we have conveyed this finding to management in a separate letter pursuant to the provision of *North Carolina General Statute* 147-64.6(c)(18).

Physical security primarily involves the inspection of the College'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 NC Center for Applied Textile Technology computer center is secure from foreseeable and preventable security and environmental threats. *We found no significant weaknesses in physical security.*

A complete **disaster recovery** plan that is tested periodically is necessary to enable the College to recover from an extended business interruption due to the destruction of the computer center or other college assets. The NC Center for Applied Textile Technology has a Disaster Recovery Plan, however, the plan has not been tested. *See Audit Finding 2, Resumption of Computer Systems.*

[This Page Left Blank Intentionally]

AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY

OBJECTIVES

Under the *North Carolina General Statutes* Chapter 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. This IS audit was designed to ascertain the effectiveness of general controls at the NC Center for Applied Textile Technology.

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, physical security, operations procedures, and disaster recovery which directly affect the NC Center for Applied Textile Technology computing operations. Other IS general control topics were reviewed as considered necessary.

METHODOLOGY

We audited policies and procedures, used questionnaires to interview key administrators and other personnel, developed a program to generate information from the critical operating systems to examine 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 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. [1]

---

1 In 1992 the State created the Information Resource Management Commission to provide statewide coordination of information technology resources planning. The IRMC provides state enterprise IT leadership including increased emphasis and oversight for strategic information technology planning and management; policy development; technical architecture; and project certification. Pursuant to *North Carolina General Statute* 147-33.78 numerous state officials serve on the IRMC including four members of the Council of State who are appointed by the Governor. The State Auditor has been appointed a member of the IRMC and elected as chair of the IRMC by its members.

[This Page Left Blank Intentionally]

The North Carolina Center for Applied Textile Technology (NC Textile Center), located in Belmont, NC, was founded in 1943 and is a member of the NC Community College System. It is considered an institution because it does not receive accreditation from the Southern Association of Colleges and Schools. The mission of the NC Textile Center is to provide educational and training programs for occupational preparation and skills upgrading for the textile industry and others. The Center will provide these programs statewide or in cooperative arrangements with other institutions and agencies in North Carolina. The NC Textile Center offers continuing education courses in Textiles, Management, Computers, Safety, and other areas and are authorized to offer an associates degree in Textile Management, but do not actively pursue students for this degree. Instead, students mainly take continuing education courses. Some of these continuing education courses count towards a certificate from NC Textile Center.

The information technology services at the NC Center for Applied Textile Technology is provided by two individuals that also have various other duties. The two positions performing these functions are the Dean of Academic Affairs and Information Technology and the Systems Administrator. The Dean of Academic Affairs and Information Technology reports directly to the President. The Information Technology staff act as a service facility to the students, faculty and staff of NC Textile Center and strictly adheres to the policies and procedures thereof. The objective of the IT staff is to provide accurate, timely and professional computer technology and telecommunication services to the overall organization.

[This Page Left Blank Intentionally]

The following audit results reflect the areas where the NC Center for Applied Textile Technology has performed satisfactorily and where recommendations have been made for improvement.

<div align="center">**GENERAL SECURITY ISSUES**</div>

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.

AUDIT FINDING 1: IT SECURITY POLICIES AND PROCEDURES

North Carolina Community College System (NCCCS) and the NC Center for Applied Textile Technology's (NC Textile Center) management has not adopted formal information technology (IT) standards to help them address all critical areas of their IT security environment. The following critical policies and procedures were not addressed in their security program:

- NC Textile Center has no written standards or policies and procedures regarding user access, new account procedures, group assignment and reassignment, procedures for super users, the monitoring of critical operating systems and servers, how to respond to security threats, and how users should securely use the networks. Without adding these critical components to a security program, management has not appropriately communicated to the NC Textile Center staff its overall approach to security and internal control in these aforementioned critical areas.

- NCCCS has not provided NC Textile Center with a baseline configuration for securing the critical operating system. The critical operating systems may not be secure from commonly known vulnerabilities.

- NC Textile Center has not performed a risk assessment of their critical operations. Without a risk assessment, management has not determined which areas are deemed critical and how to prioritize resources and time to ensure that the critical areas remain effective.

NCCCS and NC Textile Center's management should assume full responsibility for developing a framework policy, which establishes the organization's overall approach to security and internal control. The policy should comply with overall business objectives and be aimed at decreasing risks through preventive measures, timely identification of irregularities, limitation of losses and timely restoration. In addition, management should ensure that this policy specifies the purpose and objectives, the management structure, the scope within the organization, the assignment of responsibilities for implementation and the definition of penalties and disciplinary actions associated with failing to comply with security and internal control policies.

Recommendation: Management at NC Textile Center need to work with NCCCS to develop and adopt a set of formal standards to ensure that all critical general security issues are addressed in their policies and procedures. Also, they should have a mechanism in place to periodically review standards for any new critical areas that should be addressed and include policies and procedures regarding these areas in NC Textile Center's security policies.

Auditee's Response: NCATT management agrees with finding. We will work with NCCCS to address these issues.

ACCESS CONTROLS

The access control environment consists of 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 reviewed the access controls for the NC Center for Applied Textile Technology's critical operating systems. We found several significant weaknesses in access controls. Due to the sensitive nature of the conditions found, we have conveyed these findings to management in a separate letter pursuant to the provision of *North Carolina General Statute* 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. Because the same procedures are used to patch and upgrade the critical application and the operating system, we indirectly tested program changes to the critical application in our test of system software 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. We found a significant weakness in systems software maintenance. Due to the sensitive nature of the condition found, we have conveyed this finding to management in a separate letter pursuant to the provision of *North Carolina General Statute* 147-64.6(c)(18).

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. The NC Center for Applied Textile Technology computer center is secure from foreseeable and preventable security and environmental threats. *We found no significant weaknesses in physical security.*

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, many college services would grind to a halt. To reduce this risk, computer service centers develop disaster recovery plans. Disaster recovery procedures should be tested periodically to ensure the recoverability of the data center. Our audit identified one significant weakness in the disaster recovery planning.

AUDIT FINDING 2: RESUMPTION OF COMPUTER SYSTEMS

The NC Center for Applied Textile Technology has an adequate disaster recovery plan to ensure the resumption of computer systems during adverse circumstances. However, the disaster recovery plan has not been tested. A disaster recovery plan should be tested to ensure that the plan is effective.

Recommendation: NC Textile Center should test the plan at least on a yearly basis.

Auditee's Response: NCATT will test the disaster recovery plan annually to make sure it is effective.

[This Page Left Blank Intentionally]

DISTRIBUTION OF AUDIT REPORT

In accordance with General Statutes 147-64.5 and 147-64.6(c)(14), copies of this report have been distributed to the public officials listed below. Additional copies are provided to other legislators, state officials, the press, and the general public upon request.

EXECUTIVE BRANCH

The Honorable Michael F. Easley	Governor of North Carolina
The Honorable Beverly M. Perdue	Lieutenant Governor of North Carolina
The Honorable Richard H. Moore	State Treasurer
The Honorable Roy A. Cooper, III	Attorney General
Mr. David T. McCoy	State Budget Officer
Mr. Robert L. Powell	State Controller
Mr. Martin Lancaster	President
	The North Carolina Community College System
Dr. James Lemons	President, NC Center for Applied Textile Technology

LEGISLATIVE BRANCH

Appointees to the Joint Legislative Commission on Governmental Operations

President Pro Tempore	Speaker of the House
Senator Marc Basnight, Co-Chair	Representative James B. Black, Co-Chair
Senator Charles W. Albertson	Representative Richard T. Morgan, Co-Chair
Senator Patrick J. Ballantine	Representative Martha B. Alexander
Senator Daniel G. Clodfelter	Representative Rex L. Baker
Senator Walter H. Dalton	Representative Bobby H. Barbee, Sr.
Senator Charlie S. Dannelly	Representative Harold J. Brubaker
Senator James Forrester	Representative Debbie A. Clary
Senator Linda Garrou	Representative E. Nelson Cole
Senator Wilbur P. Gulley	Representative James W. Crawford, Jr.
Senator Fletcher L. Hartsell, Jr.	Representative William T. Culpepper, III
Senator David W. Hoyle	Representative W. Pete Cunningham
Senator Ellie Kinnaird	Representative W. Robert Grady
Senator Jeanne H. Lucas	Representative Joe Hackney
Senator Stephen M. Metcalf	Representative Julia C. Howard
Senator Anthony E. Rand	Representative Joe L. Kiser
Senator Eric M. Reeves	Representative Edd Nye
Senator Robert A. Rucho	Representative William C. Owens, Jr.
Senator R. C. Soles, Jr.	Representative Wilma M. Sherrill
Senator Scott Thomas	Representative Thomas E. Wright

Other Legislative Officials

Mr. James D. Johnson	Director, Fiscal Research Division

Other Officials

Chairman and Members of the Information Resource Management Commission

ORDERING INFORMATION

Copies of this report 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
>
> Internet: http://www.ncauditor.net
>
> Telephone: 919/807-7500
>
> Facsimile: 919/807-7647