



STATE OF NORTH CAROLINA

AUDIT OF THE INFORMATION SYSTEMS

GENERAL CONTROLS

GUILFORD TECHNICAL COMMUNITY COLLEGE

SEPTEMBER 2007

OFFICE OF THE STATE AUDITOR

LESLIE MERRITT, JR., CPA, CFP

STATE AUDITOR

AUDIT OF THE INFORMATION SYSTEMS

GENERAL CONTROLS

GUILFORD TECHNICAL COMMUNITY COLLEGE

SEPTEMBER 2007



Leslie Merritt, Jr.,
CPA, CFP
State Auditor

STATE OF NORTH CAROLINA
Office of the 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
The Board of Directors of Guilford Technical Community College
Dr. Donald W. Cameron, President

Ladies and Gentlemen:

We have completed our audit of Guilford Technical Community College. This audit was conducted during the period from June 5, 2007, through June 19, 2007. 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 Guilford Technical Community College. The scope of our IS general controls audit included general security, access controls, systems software, 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 Guilford Technical Community College 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 Guilford Technical Community College 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 W. Merritt, Jr.

Leslie Merritt, Jr., CPA, CFP
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	11

EXECUTIVE SUMMARY

We conducted an Information Systems (IS) audit at the Guilford Technical Community College from June 5, 2007, through June 19, 2007. 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. Guilford Technical Community College has established a reasonable security program that addresses the general security of information resources. We did identify a significant weakness in general security during our audit. *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 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).

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 did not find any significant weakness in systems software 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.*

A complete **disaster recovery** plan that is tested periodically is necessary to enable Guilford Technical Community College to recover from an extended business interruption due to the destruction of the computer center or other Guilford Technical Community College assets. Our audit did note a weakness in disaster recovery. *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* 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 Guilford Technical Community College.

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, systems software, physical security, and disaster recovery which directly affect Guilford Technical Community College'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 general 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

Guilford Technical Community College is a two-year accredited community college. It opened in 1958 with 50 students and two classes as the Guilford Industrial Education Center on the site of the Guilford County Tuberculosis Sanatorium, which had operated from 1924 to 1955. In 1965, the school became Guilford Technical Institute (GTI) and was given authority to grant associate degrees. In 1981, the State Board of Community Colleges began administration of the Department of Community Colleges. That board approved the GTI's request to add a college transfer program in 1983, and GTI changed its name to Guilford Technical Community College. The College offers certificates, one-year and two-year career-related programs, a two-year college transfer program, personal enrichment courses, a variety of adult literacy opportunities and training for business industry. Guilford Technical Community College's goal is to meet the needs of each and every citizen by offering the education tools necessary to broaden and enhance their personal and professional lives.

The IT division at Guilford Technical Community College is referred to as the Management Information Systems division of the College. The Chief Information Officer, who is responsible for the entire computing of Guilford Technical Community College, heads the Management Information Systems division. This position reports to the Executive Vice President. The mission of the Management Information Systems division is to insure the integrity of the administrative systems and infrastructure. The function of the Management Information Systems division is to provide installation, upgrade and support services for the administrative systems of the College and to develop, maintain, and upgrade the College information infrastructure in support of expanding technology goals.

[This Page Left Blank Intentionally]

AUDIT RESULTS AND AUDITEE RESPONSES

The following audit results reflect the areas where Guilford Technical Community College 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.

AUDIT FINDING 1: IT SECURITY POLICIES AND PROCEDURES

Guilford Technical Community College 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:

- Guilford Technical Community College does not monitor its current system configuration against an approved baseline for system security that will assist the college in identifying unauthorized changes to the system. Without a baseline configuration for securing the critical operating system, the operating system may not be secure from commonly known vulnerabilities.

Guilford Technical Community College 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.

Recommendation: Guilford Technical Community College should develop an approved baseline for system security. North Carolina Community College System (NCCCS) is in the process of developing a baseline configuration that is scheduled for completion in July 2007. Guilford Technical Community College should use the completed NCCCS baseline as a guideline for minimum security configurations, and document any differences between the college's baseline and the NCCCS baseline. Guilford Technical Community College should develop procedures to monitor their system configuration against the college's developed baseline settings to detect any unauthorized changes to the system.

Auditee's Response: The NCCCS baseline was not approved prior to the college's audit. Now that it is approved, Guilford Technical Community College will have executive management approve and will be in compliance by the deadline of December 31, 2007. In addition, a new policy will be written to address compliance with the baseline and the procedures for monitoring compliance.

AUDIT RESULTS AND AUDITEE RESPONSES (CONTINUED)

ACCESS CONTROLS

The most important information security safeguard that Guilford Technical Community College has is its access controls. The access controls environment consists of Guilford Technical Community College'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).

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 a weakness in system software.

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. Guilford Technical Community College'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 a significant weakness 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

Guilford Technical Community College has a disaster recovery plan to ensure the resumption of computer systems during adverse circumstances. However, the disaster recovery plan is incomplete and is not being tested. Guilford Technical Community College also does not store the plan offsite. The plan is missing the following components:

AUDIT RESULTS AND AUDITEE RESPONSES (CONCLUDED)

- Executive management's signature of approval of the plan.
- Statement of the assumptions, such as the maximum time without computing, is underlying the plan
- An inventory of equipment, special stock and arrangements to acquire replacement equipment.
- Alternate user department procedures to manage their workloads until processing resumes.

In the event of a disaster, the aforementioned components are necessary to ensure the proper recovery of the computer resources. In addition, a disaster recovery plan should be tested to ensure that the plan is effective. Management should ensure that a written plan is developed and maintained in accordance with the overall framework for restoring critical information services in the event of a major failure. The disaster recovery plan should minimize the effect of disruptions. Procedures should require that the plan be reviewed and revised annually or when significant changes to the college's operations occur.

Recommendation: Guilford Technical Community College should include all the aforementioned critical components in their plan and should test the plan at least on a yearly basis. Guilford Technical Community College should also store the plan offsite.

Auditee's Response: Guilford Technical Community College has just completed its first plan, which is in the process of being approved by executive management. The plan will be reviewed and added to as necessary in the following year, and the aforementioned items will be included. In addition to the Business Continuity Plan, the college has brought together a task force headed by the Executive Vice President that is working on more catastrophic scenarios and how the college would respond to those.

[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