STATE OF NORTH CAROLINA

AUDIT OF THE INFORMATION SYSTEM GENERAL CONTROLS

AT

GUILFORD TECHNICAL COMMUNITY COLLEGE

JAMESTOWN, NORTH CAROLINA

JUNE 2004

OFFICE OF THE STATE AUDITOR

RALPH CAMPBELL, JR.

STATE AUDITOR

Audit of the Information System General Controls

At

Guilford Technical Community College

Jamestown, 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 Guilford Technical Community College
Dr. Donald W. Cameron, President

Ladies and Gentlemen:

We have completed our information systems (IS) audit of Guilford Technical Community College. 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 Guilford Technical Community College. 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 Guilford Technical Community College has performed satisfactorily and where improvements should be made.

We wish to express our appreciation to the staff at 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,

Ralph Campbell, Jr.
State Auditor

TABLE OF CONTENTS

We conducted an information system (IS) audit at Guilford Technical Community College (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 Guilford Technical Community College should document user's awareness of security policies and procedures and network imposed restrictions and they should perform a risk assessment of the College's information resources. *See Audit Finding 1, Security Awareness and Risk Assessment.*

The **access control** environment consists of access control software and information security policies and procedures. We reviewed the access controls for Guilford Technical Community College'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. Guilford Technical Community College computer center is secure from foreseeable and preventable security and environmental threats. *We did not detect any 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. Guilford Technical Community College does not have a Disaster Recovery Plan; the plan was in draft form when the audit commenced. *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 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, program maintenance, systems software, physical security, operations procedures, and disaster recovery which directly affect Guilford Technical Community College 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]

BACKGROUND INFORMATION

Guilford Technical Community College (CC) was founded in 1958. The College offers courses at several locations, with the majority of the programs offered on the Jamestown campus in Jamestown, NC. The Southern Association of Colleges and Schools accredits Guilford Technical CC to award degrees, certificates and diplomas. Guilford Technical CC 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 and industry. Guilford Technical CC awards five associate degrees: Associate in Applied Science, Associate in Arts, Associate in Science, Associate in Fine Arts and Associate in General Education. It is the mission of Guilford Technical CC to provide lifelong learning opportunities for personal growth, workforce productivity, and community service by serving all the diverse segments of Guilford County's population and delivering quality educational programs and services through partnerships with business, community groups, and other educational institutions.

The Management Information and Telecommunication Systems (MIS) Unit of Guilford Technical CC is headed by the Director of MIS, who reports directly to the Executive Vice President. The mission of the MIS Unit is to provide timely, accurate data and telecommunication services within the College, as well as to local, state and federal agencies. Additional functions include implementing software, installing equipment, maintaining the Local Area and Wide Area Networks for the College, supporting curriculum labs, and providing hardware and software support for faculty and staff. The function of the MIS Unit is to provide technical expertise in performing application system design, programming, administrative and academic hardware and software support.

[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: SECURITY AWARENESS AND RISK ASSESSMENT

The following critical components were not addressed in Guilford Technical CC's security program:

- Guilford Technical CC users are not required to document that they understand the existing security policies and procedures and the proper use of the network. Consequently, users may be able to avoid penalties associated with violating the existing security policies and improperly using the networks because no document exist to show that users were made aware of these policies and restrictions.

- Guilford Technical CC 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. A risk assessment 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 process should provide for risk assessments at both the global level and system specific levels (for new projects as well as on a recurring basis) and should ensure regular updates of the risk assessment information with results of audits, inspections and identified incidents.

Recommendation: Management at Guilford Technical CC need to establish a document that requires user's signature acknowledging that they read and understood all policies and procedures and also establish a systematic risk assessment framework.

Auditee's Response: The College already had individual security sheets used when an employee requested access to the system. This document has been modified to incorporate a signature acknowledging that the user has read and understood all policies and procedures. The College already has such a policy in the College Management Manual which also outlines the consequences of unauthorized actions. The College will work on a systematic risk assessment document.

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 Guilford Technical Community College'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 Statutes* 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. Guilford Technical Community College computer center is secure from foreseeable and preventable security and environmental threats. *We did not detect any 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 disaster recovery.

AUDIT FINDING 2: RESUMPTION OF COMPUTER SYSTEMS

Guilford Technical CC does not have a final written disaster recovery plan to ensure the resumption of computer systems during adverse circumstances. The plan was in draft form when the audit commenced. In the event of a disaster, there is no final plan in place to determine how the computer systems will be restored. Guilford Technical CC would not be able to process financial transactions or student record information. 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.

Recommendation: Guilford Technical CC should finalize the draft disaster recovery plan and test it on a yearly basis.

Auditee's Response: The College will develop a more complete disaster recovery plan and will test it yearly or more frequently.

[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. Donald W. Cameron	President, Guilford Technical Community College

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