STATE OF NORTH CAROLINA

AUDIT OF THE INFORMATION SYSTEM GENERAL CONTROLS

AT

SURRY COMMUNITY COLLEGE

DOBSON, NORTH CAROLINA

JUNE 2004

OFFICE OF THE STATE AUDITOR

RALPH CAMPBELL, JR.

STATE AUDITOR

AUDIT OF THE INFORMATION SYSTEM GENERAL CONTROLS

AT

SURRY COMMUNITY COLLEGE

DOBSON, NORTH CAROLINA

JUNE 2004

STATE OF NORTH CAROLINA
Office of the State Auditor

Ralph Campbell, Jr.
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 Surry Community College
Dr. Frank Sells, President

Ladies and Gentlemen:

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

We wish to express our appreciation to the staff at Surry 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.

Ralph Campbell, Jr.
State Auditor

TABLE OF CONTENTS

EXECUTIVE SUMMARY

We conducted an information system (IS) audit at Surry 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 Surry Community College 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 Surry 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. Surry Community College computer center is not secure from foreseeable and preventable security and environmental threats. *See Audit Finding 2, Physical Security of the Computer Processing Facility.*

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. Surry Community College has a disaster recovery plan, however, it is inadequate and incomplete. *See Audit Finding 3, 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 Surry 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 Surry 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

Surry Community College, located in Dobson, North Carolina, was chartered by the NC State Board of Education in January 1964. The College is accredited by the Southern Association of Colleges and Schools (SACS) to award associate degrees, diplomas, and certificates. The College offers Associate of Arts, Associate of Science, Associate of General Education, and Associate of Applied Science degrees. It also awards diplomas and certificates in career technology fields. The mission of Surry Community College is to promote personal growth, and community development through excellence in teaching, learning, and service.

The information technology division at Surry Community College is referred to as the Computer Services division of the College. The Chief Technology Officer for the College is directly responsible for the entire Computer Services division. This position reports to the Vice President for Planning and Information Services.

The mission of the Computer Services division is to provide technical support for the faculty and staff of the College to enable them to achieve the institution's goals. The function of the Computer Services division is to provide the technical support services necessary to enable the College staff and faculty to accomplish their job tasks in an efficient and effective manner. This includes providing hardware and software purchasing, installation, maintenance and training to faculty and staff.

[This Page Left Blank Intentionally]

AUDIT RESULTS AND AUDITEE RESPONSES

The following audit results reflect the areas where Surry 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

North Carolina Community College System (NCCCS) and Surry Community College's (CC) 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:

- Surry CC has no written standards or policies and procedures regarding the monitoring of critical operating systems and servers, and how to respond to security threats. Without adding these critical components to a security program, management has not appropriately communicated to the Surry CC IT staff its overall approach to security and internal control in these aforementioned critical areas.
- NCCCS has not provided Surry CC with a baseline configuration for securing the critical operating system. The critical operating systems will not be secured from common vulnerabilities.
- Surry CC also has not performed a risk assessment of their critical operations. Without a risk assessment, management has not communicated to Surry CC staff, which areas are deemed critical and how to prioritize resources and time to ensure that the critical areas remain effective.

NCCCS and Surry CC'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 Surry CC needs 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 Surry's security policies.

Auditee's Response: Surry Community College recognizes the need to have formal standards in place to ensure that all critical general security issues are addressed in our policies. We also recognize the need to have mechanisms in place to periodically review standards for any new critical areas that should be addressed. In response to this recommendation, the Chief Technology Officer and the System Administrator will maintain communication with the NCCCS to develop a set of formal standards in a timely manner. Communication from the NCCCS has recently begun to be shared as a result of requests for leadership that this office has been receiving following initial IT audits at the state's community colleges. As soon as these standards are developed by the NCCCS and initiated by Surry Community College, a process will be documented by the SCC Technology Committee, and used by that group to periodically review these standards for any new critical areas that should be addressed. This group will also continue to recommend to the College administration policies and procedures regarding these areas.

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 Surry 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 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.

AUDIT FINDING 2: PHYSICAL SECURITY OF THE COMPUTER PROCESSING FACILITY

The computer room is not reasonably secure from foreseeable and preventable threats to its physical continuity. We found the following physical security weaknesses:

- The computer room is not equipped with smoke detectors or an automated fire suppression system.
- The UPS used to protect the critical servers from electrical hazards has not been recently tested. Therefore, Surry CC does not know if it is susceptible to electrical fluctuations or power outages. Electrical fluctuations and power outages can cause data on a computer server to become corrupt non-useable, also it could totally destroy a server's ability to power on. Electrical fluctuations and power outages are another environmental hazard that could cause Surry CC to lose computer processing capabilities.

Management should assure that sufficient measures are put in place and maintained for protection against environmental factors (e.g. fire, dust, power, excessive heat and humidity) and management should assess regularly the need for uninterruptible power supply batteries and generators for critical applications and servers to secure against power failures and fluctuations.

Recommendation: Surry CC should equip the computer room with smoke detectors, and maintain UPS equipment by having this equipment checked on a yearly basis.

Auditee's Response: The College recognizes the need to provide the best fire protection possible for the computer server room. The Chief Technology Officer and the Chief Financial Officer analyzed this issue recently and decided not to purchase an automated fire suppression system for this room at this time due to budget restraints. In response to this audit

recommendation, however, the Chief Technology Officer will purchase and install a smoke detector for this room. This action will be documented through the Division's work order system. The UPS equipment for the computer server room is less than nine months old. Technicians have tested it for proper operation by turning off the circuit breaker, which provides electrical power to the room. On these occasions, the UPS has operated properly. The IT staff will perform similar tests of the UPS on a yearly basis (or more often), as documented by the Division's work order system.

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 3: RESUMPTION OF COMPUTER SYSTEMS

Surry has a disaster recovery plan to ensure the resumption of computer systems during adverse circumstances. However, the disaster recovery plan is incomplete and has not been tested. The plan does not include the following critical components:

- Statement of the assumptions, such as the maximum time without computing, underlying the plan.
- Identification of critical applications in each user department and the priority in which these applications will be restored if resources are limited.
- Identification of key personnel and their assignments during the restoration of processing.
- Alternate user department procedures to manage their workloads until processing resumes.
- A schedule to update the plan when there are major changes to the environment or at least annually

In the event of a disaster, the aforementioned components are necessary to ensure the proper recovery of the computer resources. Also, 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: Surry CC should include all the aforementioned critical components in their plan and should test the plan at least on a yearly basis.

Auditee's Response: Surry Community College maintains a comprehensive disaster recovery plan, which has been approved by the College President. This plan allows for the return to normal operations of all necessary systems within a twenty-four hour period (if required utilities are available). The Chief Technology Officer and the System Administrator will ensure the annual testing of this plan and document its accomplishment through the division's work order system.

[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. Frank Sells	President, Surry Community College

LEGISLATIVE BRANCH

Appointees to the Joint Legislative Commission on Governmental Operations

President Pro Tempore Senator Marc Basnight, Co-Chair	Speaker of the House 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