STATE OF NORTH CAROLINA

AUDIT OF THE INFORMATION SYSTEMS

GENERAL CONTROLS

AT

CENTRAL PIEDMONT COMMUNITY COLLEGE

CHARLOTTE, NORTH CAROLINA

SEPTEMBER 2000

OFFICE OF THE STATE AUDITOR

RALPH CAMPBELL, JR.

STATE AUDITOR

AUDIT OF THE INFORMATION SYSTEMS

GENERAL CONTROLS

AT

CENTRAL PIEDMONT COMMUNITY COLLEGE

CHARLOTTE, NORTH CAROLINA

SEPTEMBER 2000

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

Ralph Campbell, Jr.
State Auditor

AUDITOR'S TRANSMITTAL

The Honorable James B. Hunt, Jr., Governor
Members of the North Carolina General Assembly
Board of Trustees, Central Piedmont Community College
Dr. Anthony Zeiss, President

Ladies and Gentlemen:

We have completed our information systems (IS) audit of the administrative computer operations at the Central Piedmont 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 the College. The scope of our IS general controls audit included general security issues, access controls, program maintenance, physical security, operations procedures, system software, telecommunications, 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 College has performed satisfactorily, where improvements should be made, and where further study is necessary.

We wish to express our appreciation to the staff at Central Piedmont 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 systems (IS) audit at Central Piedmont Community College from January 10, 2000 through February 18, 2000. 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 proper segregation of duties is not logically enforced and that the internal auditor was not involved in the review of information systems. See Audit Finding 1, *Segregation of Duties,* and Audit Finding 2, *Internal Auditor Review of Information System Functions,* for further information.

The **access control** environment consists of access control software and information security policies and procedures. The College has several individuals with responsibly for the security administration function and uses the built-in security features of the mainframe operating system and applications to control access. We reviewed the access controls for the mainframe system and the local area networks (LAN). We noted several weaknesses in access controls over the mainframe and LAN servers. See Audit Finding 3, *Security Administration,* Audit Finding 4, *Administration of User IDs,* and Audit Finding 5, *Password Administration,* for further information.

Program maintenance primarily involves enhancements or changes needed to existing systems. We did not note any significant weaknesses in program maintenance during our audit.

The computer service center should be reasonably secure from foreseeable and preventable threats from fire, water, electrical problems, and vandalism. We did not note any significant weaknesses in **physical security** during our review.

The operations of the computer center include all of the activities associated with running application systems for users. We did not note any significant weakness in the **operations procedures** of the computer center during our review.

System 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 detect any significant systems software control weaknesses during our audit.

The computer service center's **telecommunications** activities should be operated in a way that protects the security and completeness of data being transmitted. We noted the College has not implemented a firewall to prevent unauthorized access to the telecommunications network. See Audit Finding 6, *Protection of the Internal Network,* for further information.

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. See Audit Finding 7, *Disaster Recovery Planning*, for further information.

[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 Central Piedmont 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, physical security, operations procedures, systems software, telecommunications, and disaster recovery which directly affect the College's computer operations. Other IS general control topics were reviewed as considered necessary.

METHODOLOGY

This IS audit was performed in accordance with *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. Our methodology included:

- Reviews of policies and procedures.
- Interviews with key administrators and other personnel.
- Examinations of system configurations.
- Tours of the computer facility.
- On-line testing of system controls.
- Reviews of appropriate technical literature.
- Reviews of computer generated reports.
- Use of security evaluation software.

[This Page Left Blank Intentionally]

BACKGROUND INFORMATION

Central Piedmont Community College (CPCC) located in Charlotte, North Carolina is a public two-year college with a mission to advance the life-long educational development of adults consistent with their needs, interests, abilities, and efforts, and to strengthen the economic, social, and cultural life in the Charlotte-Mecklenburg region of North Carolina.

Computing facilities at CPCC consist of an IBM ES-9000 mainframe computer. The mainframe computer supports batch and interactive processing. The mainframe is located on the central campus and serves users at remote campuses over the campus-wide network. The College is currently upgrading its Token ring network to Ethernet. The College currently has over 35 Novell servers providing Email, Internet access and administrative functions for users at all campuses over the network.

Information Technology Services is tasked with providing computing and networking services to the CPCC community - faculty, staff, and students. The organization reports to the Executive Vice-President of Administration and consists of three units, each with its own unique missions:

- Administrative Information Systems - This unit has responsibility for application development, systems, and computer operations. The application development section develops and maintains the mainframe administrative information systems. These systems aid CPCC in information processing of an institutional nature. These central information systems include Student Information, Financial Reporting, and Human Resources. Administrative Information Systems also provides system software support for these information systems and support to faculty, staff and administrators on accessing and using these systems. The systems section supports the mainframe operating system and security. The computer operations section is responsible for maintaining the on-line mainframe systems and running mainframe batch jobs.

- Distributed Technology Services – This unit primary supports CPCC telecommunication infrastructure, the network system, and distributed systems. The telecommunications section provides support for the campus telephone system and voice mail and the network infrastructure. The distributed system section provides support and assistance to the campus community for PC hardware and software. The network system section provides the help desk function and management of the campus-wide network. This section is responsible for administering network security.

- Instructional Technology Services – This unit provides the primary support for members of the faculty who use computing in their curricular applications. In addition, it manages student computer classrooms and labs.

[This Page Left Blank Intentionally]

The following audit results reflect the areas where Central Piedmont Community College has performed satisfactorily, where recommendations have been made for improvement, and where further study is needed.

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, a security organization and resources, policies regarding access to the computer systems and a security education program.

AUDIT FINDING 1: SEGREGATION OF DUTIES

Proper segregation of duties is not logically enforced for the staff of the Information Technology Services at the College. Application programmers have the same level of access to operation system resources as system programmers. The application programmers administer security for the on-line application systems and have update access to the production systems resources. Computer operators and other information system personnel have access to the production system libraries. Improper segregation of duties, whether organizational or logical, may provide individuals the opportunity to circumvent internal control procedures allowing them to perform unauthorized acts and to hinder the detection of the unauthorized activity.

Recommendation: Management should implement a division of roles and responsibilities that exclude the possibility for a single individual to subvert a critical process. Management should also make sure that personnel are only performing those duties required by their respective jobs and positions. Where feasible, a segregation of duties should be maintained between system administration, computer operations, security administration, systems development and maintenance, and change management. The small staff size for Information Technology Services may not allow management to fully segregate duties. However, in the absence of proper segregation of duties, management should ensure that compensating controls have been implemented and that the individual's system activities are closely monitored.

Auditee Response: The College does not completely concur with the finding. The auditors have accurately pointed out the root cause of this situation: "The small staff size for Information Technology Services may not allow management to fully segregate duties." Our size forces us to do a lot of cross training and backing up of each position by another employee with in the department. For example: the systems programmer is backed up by an application programmer analyst, application programmer analysts are backed up by other application programmer analysts, and computer operators are backed up by the systems programmer and application programmer analysts. Each of these positions have their own areas of responsibility: systems programmer maintains the operating system, application programmer analysts design, write and modify software code, and the computer operators keep the system up and run batch jobs that are scheduled and requested.

Complying fully with the recommendation for complete segregation of duties would require hiring additional employees; we do not have the budgets or positions available at this time.

We do have controls in place to protect critical process. The controls are:

- Daily run logs are stored and reviewed.
- When programs are modified the system automatically logs who changed the code and date it was changed.
- Financial reports are balanced by the business office.
- Payroll reports are balanced by the payroll office.
- All system modifications are scheduled by the manager and reviewed.
- We have regular staff meetings and discuss programming being done by each employee.

Additional controls will be added to:

- Limit system level access for programmer/analysts to as needed basis and its use will be monitored.
- A separate ID will be created for backup.
- Programmer update access to production files will be removed.

The new MIS system selected by the Department of Community College will have a big effect on security and software development since most of these responsibilities will be transferred to the North Carolina Community College System office.

AUDIT FINDING 2: INTERNAL AUDITOR REVIEW OF INFORMATION SYSTEM FUNCTIONS

Management at the College has not directed the internal auditor to review information system security and controls. As a result, the internal auditor has not been involved in monitoring or reviewing the information system functions for the College. The current internal auditor has not received the necessary training to review and report on information system controls.

Recommendation: Management should have the internal audit staff review the security and controls for information system processing, assess their effectiveness, and report on them on a regular basis. Management should ensure that the internal audit staff receives sufficient training to perform this function.

Auditee Response: The College concurs with the finding. We have met with the internal auditor; the staff size and their current responsibilities will not leave much time for this task. The auditor will include a limited review of ITS security and controls in its annual review.

The new MIS system selected by the Department of Community Colleges will have a big effect on security and software development as most of these responsibilities will be transferred to the North Carolina Community College System office.

ACCESS CONTROLS

The access control environment consists of access control software and information security policies and procedures. An individual or 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.

AUDIT FINDING 3: SECURITY ADMINISTRATION

There are no formal security policies and procedures to provide guidance to the individuals performing security administration. Several individuals at the College perform security administration functions. These individuals perform their security duties without a centralized security administration function to oversee and monitor their activities. Without formal security standards and an oversight function for security administration, actual security may not meet management's expectation for security over system resources and data.

Recommendation: Management should develop an information security policy and establish a security administration function (officer) to oversee its implementation. The security administration function should have organization-wide responsibility for formulating internal control and security (both logical and physical) policies and procedures. The information security officer should ensure that security is administered consistent with the organization's information security policies and procedures.

Auditee Response: The College concurs with the finding. We will be developing a security policy for the College; this should be in place by March 2001. The policy will cover logical and physical procedures.

We do not have the funds or a position at this time for an information security officer. The Manager of Computing Services and Manager of Distributed Services will share the duties of monitoring security administration.

AUDIT FINDING 4: ADMINISTRATION OF USER IDS

We found default user ids for some of the operating systems still active. Default user accounts shipped with operating systems should be revoked or removed from the system. These accounts and default passwords are well known to hackers and outside users. Leaving these default user ids on the system provide unauthorized users a means to attempt to gain access to the College's information systems.

We also found user ids shared by several individuals that have update access to system resources. User ids with update access should be assigned to specific individuals to provide accountability. If an error or irregularity occurs while someone is using a shared user id it is not possible to identify the responsible individual.

Recommendation: Default user ids for systems should be disabled, removed, or the default passwords changed immediately when these ids are loaded on the system. Shared user ids should be removed and individual user ids assigned to the staff using these ids. The College should develop a policy that individual user ids should be assigned to all users requiring update access. Shared users ids should be limited to inquiry access to information not considered confidential or sensitive.

Auditee Response: We agree with you on default passwords. We will eliminate all default passwords and assign our own passwords once the operating system is installed. All default passwords will be eliminated within 90 days.

We agree with you on the use of shared user ids for update access. We are in the process of going through the security system, contacting the users who use shared user ids and informing them that they can only use their personal ID. We will severely limit shared user ids to display only per your recommendation. Security policy will cover user ids.

If an employee's employment is terminated their user id is flagged as inactive. By making it inactive, the user id cannot be used. If the termination is permanent the user id is deleted from the security system. The security system does log when a user last used their id.

We are putting a new process in place for timely notification from the departments on employee termination or access change requirement.

AUDIT FINDING 5: PASSWORD ADMINISTRATION

We found several weaknesses in password administration. Weaknesses over password administration limit the security of the system and may increase the risk that unauthorized persons can gain access to the system.

The process used to assign passwords provides individuals other than the account owner with knowledge of the password for the user account. The owner of an account should be the only one with knowledge of the account's password. Currently, system access is requested on a form that is sent to information systems services. This request form could go to five separate administrators for ids and passwords to be assigned. Each administrator establishes a user id and password for their respective system and then passes the form to the next administrator. The user does not change any of these passwords. Therefore each system's administrator has knowledge of a user's id and password for other systems. The school may not be able to hold individuals accountable for the action performed under their user ids since other people have knowledge of the password for the user accounts.

The user ids and passwords are not distributed in a secure and confidential manner. Passwords are assigned for the user id and sent to the user through interoffice mail in an envelope marked confidential. There is no confirmation that the proper individual received the ids and passwords.

Users are not forced to change passwords for mainframe and network accounts on a periodic basis. Users should be accountable for the actions of their user accounts. As such, individuals should control the passwords associated with their user accounts. Users should be forced to change the initially assigned password immediately and then forced to change their passwords on a periodic basis.

Recommendation: System access request forms should be sent to an information security officer who asks for user ids and initial passwords from each system's security administrator. The information office should then compile the user ids and passwords for the various systems and communicate these to the users in a secure method. There should be confirmation from the users that they received the ids and passwords. Where possible users should be forced to change their initial password before being able to log into their accounts.

Management should develop and implement policies to require that passwords be changed on a regular basis. At a minimum, users should be forced to change passwords every 90 days. Users with accounts that are highly privileged should be forced to change passwords every 30 days. Management should provide guidelines to users for selecting proper passwords.

Auditee Response: The College concurs with the finding. We will be working on a process to allow users to change their own passwords and to notify them that their password is about to expire. We will also attach a turnaround document to be sent back to ITS confirming the receipt of their user id. A procedure will be put in place to cover the rules for changing passwords. This procedure will be in place within 60 days. As stated earlier, the college does not have the funding to appoint a person specifically for security administration.

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.

The College has adopted adequate program change procedures. We did not note any significant weaknesses in program maintenance during our review.

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 College's physical security controls ensure that the computer service center is reasonably secure from foreseeable and preventable threats. Our audit did not identify any significant weaknesses in physical security.

OPERATIONS PROCEDURES

The operations of the computer center include all of the activities associated with running application systems for users. Procedures should be in place to control the scheduling and running of production jobs, restarting production jobs when problems occur, storing, handling and mounting tapes, and maintaining computer equipment.

The operations procedures at the College are adequate to ensure that computer processing is orderly and well controlled. We did not note any significant weakness in the operations procedures of the computer center during our review.

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 software at the College is properly approved and maintained by the computer service center. Our audit did not identify any significant weaknesses in systems software.

TELECOMMUNICATIONS

Telecommunications is the electronic transmission of any kind of information by radio, wire, fiber optics, microwave, laser, or any other electromagnetic system. It can be evaluated along several lines including the type of system, the geographical organization and the service environment.

The College has connected all departments to the campus-wide network. The network provides access to the Internet for campus users.

AUDIT FINDING 6: PROTECTION OF THE INTERNAL NETWORK

The College does not have a firewall to protect its internal network and system resources from unauthorized access by external users. If a connection to the Internet or other public network exists, a firewall should be installed to protect against denial of services attacks and unauthorized access to the internal network. Without an adequate firewall, there is a risk that denial of service attacks may cause interruption of computer services for authorized users and an increased risk of access to system resources by unauthorized persons from the outside.

Recommendation: The College should install a firewall between its internal network and its connection to the Internet. The firewall should allow only authorized traffic, as defined by the College's security policies, to pass through. The firewall itself should be protected from direct attack and should be structured to protect against denial of service attacks.

Auditee Response: The College concurs with the finding. We are currently investigating firewalls and a selection will be made by the end of December 2000.

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.

The College has developed disaster recovery plans for the Administrative Information Systems and the Distributed Technology Services units of Information Technology Services.

AUDIT FINDING 7: DISASTER RECOVERY PLANNING

We found that the Disaster Recovery plans for the Administrative Information Systems unit and Distributed Technology Services unit are not complete. The plans were deficient in the following areas.

- The plans do not estimate the time necessary to restore the full computing resources to campus users in the event of a disaster.
- User departments are not required to define alternate procedures to manage their workloads until computer services are restored. Consequently, none of the user departments have prepared a Business Continuity Plan that describe procedures necessary to do their work manually in the event of a disaster.
- The disaster recovery plans do not set priorities for restoring applications and services if resources are limited.
- We could not determine if the President of the College has approved the plans.
- There are no provisions for the testing and updating of the plans.

The absence of a complete disaster recovery plan reduces the ability of the College to effectively restore computer resources. Without a defined business continuity plan, user departments may not be able to continue to provide services in the event of the loss of computer processing.

Recommendation: Management should review the existing disaster recovery plans and ensure that the plans are complete and updated. Each user department should have a business continuity plan to give direction as to how the department will carry out its duties without computer processing until the computer center completely restores computer services. The disaster recovery plans and user department procedures should be tested and updated on a regular basis. The President of the College should approve the disaster recovery plans and user department procedures. In addition, each department or unit within the College with

computer systems should have a written disaster recovery plan for recovering their computer resources in the event of a disaster.

Auditee Response: The College concurs with the finding. Administrative Computing Services and Distributed Technology Services will be working on improving their disaster recovery plans in the next fiscal year. Other departments at the College will be encouraged to develop a business continuity plan to carry out their duties when technology resources are not available.

We will also be reviewing the disaster recovery plan for the State of NC. This could be a very good guide for us in completing this plan.

DISTRIBUTION OF AUDIT REPORT

In accordance with G.S. § 147-64.5 and G.S. § 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 James B. Hunt, Jr.	Governor of North Carolina
The Honorable Dennis A. Wicker	Lieutenant Governor of North Carolina
The Honorable Harlan E. Boyles	State Treasurer
The Honorable Michael F. Easley	Attorney General
Mr. Marvin K. Dorman, Jr.	State Budget Officer
Mr. Edward Renfrow	State Controller
Mr. H. Martin Lancaster	President, North Carolina Community College Systems Office
Dr. Anthony Zeiss	President, Central Piedmont Community College

LEGISLATIVE BRANCH

Appointees to the Joint Legislative Commission on Governmental Operations

Senator Marc Basnight, Co-Chairman	Representative James B. Black, Co-Chairman
Senator Frank W. Ballance, Jr.	Representative Martha B. Alexander
Senator Patrick J. Ballantine	Representative E. Nelson Cole
Senator Roy A. Cooper, III	Representative James W. Crawford, Jr.
Senator James Forrester	Representative W. Pete Cunningham
Senator Wilbur P. Gulley	Representative Ruth M. Easterling
Senator David W. Hoyle	Representative Joe Hackney
Senator Howard N. Lee	Representative Thomas C. Hardaway
Senator Fountain Odom	Representative Martin L. Nesbitt
Senator Beverly M. Perdue	Representative Edd Nye
Senator Aaron W. Plyler	Representative William C. Owens, Jr.
Senator Anthony E. Rand	Representative Liston B. Ramsey
Senator Robert G. Shaw	Representative E. David Redwine
Senator Ed N. Warren	Representative Stephen W. Wood
Senator Allen H. Wellons	Representative Thomas E. Wright

Appointees to the Joint Select Committee on Information Technology

Senator Austin M. Allran	Representative Joe P. Tolson
Senator Charles Carter	Representative Russell Edwin Tucker
Senator Daniel G. Clodfelter	Representative William L. Wainwright
Senator Eric Miller Reeves	Representative Trudi Walend
Mr. Dwight Allen	Mr. Rufus Edmisten
Mr. Curtis Clark	Ms. Diana Oblinger
Ms. Darleen Johns	Ms. Janet Smith

Other Legislative Officials

Representative Phillip A. Baddour, Jr.	Majority Leader of the N.C. House of Representatives
Representative N. Leo Daughtry	Minority Leader of the N.C. House of Representatives
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

Telephone: 919/807-7500

Facsimile: 919/807-7647

E-Mail: reports@ncauditor.net

A complete listing of other reports issued by the Office of the North Carolina State Auditor is available for viewing and ordering on our Internet Home Page. To access our information simply enter our URL into the appropriate field in your browser: **http://www.osa.state.nc.us**