



**NORTH GEORGIA COLLEGE
& STATE UNIVERSITY**

**INTERNAL AUDIT REPORT
Presidential Transition
(DRAFT)**

January 4, 2005

Audit Number 05-41

Issued by:

**Board of Regents/University System of Georgia
Department of Internal Audit**

**Ronald B. Stark
Associate Vice Chancellor for Internal Audit**

Presidential Transition Audit Team
Michael Foxman, Auditor-in-Charge, Audit Supervisor
Scott Woodison, IT Audit Manager

TABLE OF CONTENTS

I.	AUDITOR'S APPRAISAL AND OPINION	Page 1
II.	EXECUTIVE SUMMARY	Pages 1 - 2
III.	OBSERVATIONS AND RECOMMENDATIONS	Pages 2 - 5

Overall Audit Rating Scale

Excellent = Few notable observations. No internal control weaknesses noted, good adherence to laws, regulations and policies. Excellent control environment.

Good = Several notable and/or one or two significant observations. Minor violations of policies and procedures. No violation of laws. Minor opportunities for improvement.

Fair = Many notable observations and/or few significant observations. Several notable violations of policy. Minor violations of regulations. No violations of laws. Moderate opportunities for improvement.

Poor = Several significant observations and no major observations. Controls were weak in one or more areas. Noncompliance with policies/regulations put the University/College at risk. Violation of law (not serious). Substantial opportunities for improvement.

Adverse = Several significant observations or one or more major observations. Significant risk for noncompliance with policies/regulations. Serious violation of laws. Significant opportunities for improvement.

Report Item Rating Scale

Insignificant = Nominal violations of procedures, rules or regulations. Not included in report. Corrective action suggested verbally, but not required.

Notable = Minor violation of policies and procedures; and/or weak internal controls; and/or opportunity to improve effectiveness and efficiency. Moderate risk identified. Corrective action recommended.

Significant = Significant violation of policies/procedures/laws; and/or poor internal controls; and/or significant opportunity to improve effectiveness and efficiency. Significant risk identified. Corrective action required.

Major = Major violation of policies/procedures/laws; and/or unacceptable internal controls; and/or high risk for fraud/waste/abuse; and/or major opportunity to improve effectiveness and efficiency. Major risk identified. Immediate corrective action required.

AUDITOR'S APPRAISAL AND OPINION

Overall Audit Opinion

Rating = Good

Although recommendations for improvement are provided in the areas of IT Controls and Financial Analysis, it is our opinion that the majority of internal control systems reviewed for these areas are adequate to safeguard assets and provide reliable data to management.

EXECUTIVE SUMMARY

North Georgia College & State University (NGCSU), located in Dahlonega, Georgia, was founded in 1873 and is known for its academic excellence and leadership development programs. The University offers baccalaureate and masters degrees in a variety of academic disciplines, as well as the education specialist degree in teacher leadership. Serving as a liberal arts university and as a military college for its Corps of Cadets, NGCSU is the only four-year public institution in northeast Georgia. A wide-range of educational opportunities, including more than 50 majors, attracts a highly qualified faculty and a student body of more than 4,500 students.

The information contained in this report was obtained from administrative and accounting records, budget documents, and through discussions with Institute personnel. The audit included examining, on a test basis, evidence supporting the data on financial and administrative records. The audit was primarily based on selected tests of sampled records/data and does not constitute a detailed review of all financial transactions. Therefore, it is possible that errors, irregularities and/or illegal acts, including fraud or defalcations, may go undetected. The observations and recommendations contained in this report were discussed with University officials and general agreement was reached on the audit conclusion. The recommendations represented are intended to assist management in the effective discharge of their responsibilities.

This executive summary provides an overview of the areas audited during a recent audit of North Georgia College & State University (The University). Fieldwork was conducted from November 29, 2004 through December 2, 2004. Deficiencies noted are explained in greater detail in the Observations and Recommendations section of this report. The following summary observations were noted for the areas reviewed:

IT Controls

A review of was conducted to ensure that North Georgia College & State University maintained adequate IT controls. The following observations were noted:

- **Report Item #1: Significant**
Banner user permissions provided data access greater than that required to perform assigned user tasks. This included the ability to change/modify grades.
- **Report Item #2: Notable**
The lack of a Domain Name Service (DNS) server on the NGCSU network created a significant single point of failure, which in turn, could impact the campus network if PeachNet network connectivity was lost.
- **Report Item #3: Notable**
Critical and sensitive servers (such as Banner and PeopleSoft servers), were connected to the NGCSU network, with no firewall protection from the general campus network.

□ **Financial Analysis**

A review of the institution's most recently completed financial statements was conducted to determine accuracy and proper classification of accounts. The following observations were noted:

- **Report Item #4: Notable**
An amount for approximately \$24,000 was classified on the Statement of Net Assets as a negative liability, rather than as a receivable.
- ✓ • **Report Item #5: Notable**
There were capital assets that did not meet the established dollar thresholds for capitalization.

OBSERVATIONS AND RECOMMENDATIONS

Report Item #1

Assign Permissions to Banner Users Based on Job Responsibilities

Observation:

A number of users had the capability to change grades in Banner, even though they were not authorized to change grades. Also, there were other areas where a substantial number of users had access rights beyond their job requirements.

Banner security is accomplished through access to classes and their associated objects. A test was performed of the users authorized to change a student grade. Within Banner, the SHAINST object with modify capability is required to change grades. A listing of the Banner classes and their associated objects was obtained from the Department of Information and Instructional Technology (IIT). All classes which had access to the SHAINST object were identified. It was determined that four classes had MODIFY access to the SHAINST Banner object. These classes were: BAN_NCG_ADM_C, BAN_NCG_FIN_C, BAN_NCG_REG_C, and BAN_STUDENT_C.

Using these classes, it was determined that 51 unique people were contained in these classes and thus had modify access to the SHAINST object. Thus 51 people could make grade changes. These included six users which were described as work study students.

This access to grade changes was corrected while the audit team was on campus. User access was restricted to eight specific users in the Registrar's office and specific IIT employees. A draft plan was also developed to expand the level of review of user access.

In order to determine whether other processes had authorization greater than job requirements, a review was conducted of users who had the ability to withdraw a student from a meal plan. This withdrawal could cause a refund check to be created. The Banner object SLAMASG was required to withdraw a student from a meal plan. This object was found to be in the BAN_NCG_ADM_C, BAN_NCG_HOS_C, BAN_NCG_REG_C and BAN_STUDENT_C classes. Fifty-three unique users had modify access to these classes including work study students, an Assistant Professor and IIT staff. This was discussed with management and we were informed that action is being taken to reduce access.

Criteria:

Only University employees who have been authorized by University management to change grades should be given Banner access to change grades. Additionally, users should not have permissions which grant them access outside the scope of their job requirements.

Cause:

The permissions and risks which were attached to different Banner user classes were not fully understood by management. The Banner user classes had not been recently reviewed to determine whether the access was appropriate.

Risk/Effect:

- Inappropriately changed grades
- Academic Fraud
- Lost of critical controls

Recommendation:

The Department of Information and Instructional Technology should review the current Banner Classes and the permissions associated with each Class. Users should be assigned to Classes which allow them to perform their jobs but not be given access to areas outside their job requirement. A process should be put in place which will ensure that users are assigned to the proper Classes and that their access is reviewed on a periodic basis.

Report item #2

Install a DNS Server on the NGCSU Network to Reduce Single Points of Failure

Observation:

The NGCSU network used DNS services provided by Office of Information and Instructional Technology (OIIT) from two DNS servers located in Athens, GA. NGCSU users accessed these services via PeachNet. DNS services are required to resolve a network name to an IP address. Loss of PeachNet connectivity to Athens would cause loss of DNS services. Without DNS services, it is difficult to connect a terminal or application to another application by use of its name. Therefore, a web site address such as www.ncgsu.edu would not be usable on the NGCSU network.

There was also a single point of failure in the single fiber connection between the NGCSU network and the local telephone company, Alltel, central office. The fiber route provided by Alltel was on a telephone pole within two feet of a heavy volume roadway. The fiber faced the oncoming traffic and could be damaged by contact between a car and the pole.

Criteria:

Wherever possible, resources which provide critical services should not provide a single point of failure. There should be a secondary resource which could be used if the primary resource is unavailable. The identification and resolution of a critical point of failure should consider the cost to resolve the single point of failure compared to the impact of losing the function provided by the resource.

Cause:

Management failed to ensure that DNS services were available and accessible on campus. Management also failed to ensure that the connection between its network and the local telephone company was secured.

Risk/Effect:

- Loss of function within the NGCSU network
- Extra manpower needed to develop an alternate method of providing DNS services in case of failure

Recommendation:

1) NGCSU should build a server which will provide DNS services to the NGCSU network. This server could either function as the primary DNS server or as a secondary DNS server. The server should be active on the network and available in case of loss of DNS services from the OIIT DNS server. 2) NGCSU should evaluate the cost of providing a second connection to PeachNet or increasing protection for the existing fiber connection.

Report item #3

Protect Critical and Sensitive Servers on a Separate Network Segment Behind a Firewall

Observation:

The NGCSU network had a perimeter firewall between PeachNet and the campus network. There also were internal firewalls between the campus network and selected network segments such as Physics and Computer Science (Hitz Lab). However, the Banner and People Soft servers were not behind an internal firewall and could be directly accessed from the campus network. This left critical servers open to attack and scanning by terminals located on the campus network.

Criteria:

Critical servers should be protected from attack by use of a firewall and other security defenses.

Cause:

Management failed to ensure that critical servers were protected by a firewall.

Risk/Effect:

- Loss or corruption of data
- Loss of availability

Recommendation:

Place critical servers, such as Banner and PeopleSoft servers, on their own network segment. Place this segment behind a firewall which will only allow selective access to these servers. Develop firewall policies to protect access to these servers.

Report item #4

Ensure Receivables are Correctly Classified on Financial Statements

Observation:

A review of the institution's financial statements was conducted to ensure that items were properly reflected. It was noted that third party contractor tuition reimbursements for sponsored programs totaling \$24,560.89 were listed as a negative liability on the Statement of Net Assets. Since the institution at fiscal year-end was waiting for payment, this amount should be classified as a receivable.

Criteria:

Money that is due to the University within a twelve month time frame should be treated as a current asset receivable on the Statement of Net Assets.

Cause:

- Incorrect classification of a receivable as a negative liability

Risk/Effect:

- Misclassification of financial statement amount

Recommendation:

Amounts due from third party sponsors at year-end should be treated as a receivable on the Statement of Net Assets.

Report Item #5

Ensure that Capitalized Items Meet the Stated Capitalization Threshold

Observation:

A review was conducted of capital assets as of 6/30/2004, to ensure capitalization thresholds were met. It was noted that assets were capitalized below the threshold amounts. For instance, Building asset numbers 3452 and 3453 were capitalized in the amounts of \$58,383 and \$98,387, respectively. (Threshold for Building assets is \$100,000). Facility asset numbers 3395, 3396, 3397, 3412, and 3479 were capitalized in the amounts of \$6,119, \$11,006, \$26,520, \$7,365 and \$68,065, respectively. (Threshold for Facilities is \$100,000). Infrastructure asset number 4104 was capitalized in the amount of \$90,395. (Threshold for Infrastructure is \$1,000,000). The above are examples only and may not include other assets that were below capitalization thresholds as well.

Criteria:

Capitalization guidelines are detailed in *Board of Regents Business Procedures Manual, Section 7.0 Capitalization*. All University System of Georgia entities are required to use thresholds as stated in *Subsection 7.1.2*:

Class of Asset	Threshold
Land/land improvements	Capitalize All
Buildings/building improvements	\$100,000
Facilities & other improvements	\$100,000
Infrastructure (Major Systems)	\$1,000,000
Equipment / Leased Equipment	\$5,000
Library books/materials (collections)	Capitalize All
Works of art/historical treasures	Capitalize All
Software developed or obtained for internal use	\$1,000,000
Capital Leases - Buildings	\$100,000

Cause:

Assets were capitalized that did not meet established criteria.

Risk/Effect:

- Overstatement of capital assets in financial reports

Recommendation:

Management should review capital assets to ensure all assets within each category meet the capitalization thresholds. Assets that do not meet the threshold and are not a part of a larger system as identified by Board of Regents policy should be: 1) written off in the current year and 2) shown in the FY2005 Annual Financial Report as a prior year adjustment.