STATE OF NORTH CAROLINA

THE UNIVERSITY OF NORTH CAROLINA AT CHAPEL HILL

INFORMATION TECHNOLOGY GENERAL CONTROLS

MAY 2010

PERFORMANCE AUDIT

OFFICE OF THE STATE AUDITOR

BETH A. WOOD, CPA

STATE AUDITOR

THE UNIVERSITY OF NORTH CAROLINA AT CHAPEL HILL

INFORMATION TECHNOLOGY GENERAL CONTROLS

MAY 2010

PERFORMANCE AUDIT

STATE OF NORTH CAROLINA
Office of the State Auditor

Beth A. Wood, CPA
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.ncauditor.net

AUDITOR'S TRANSMITTAL

May 17, 2010

The Honorable Beverly Eaves Perdue, Governor
The General Assembly of North Carolina
Dr. Holden Thorp, Chancellor

This report presents the results of our performance audit of information technology general controls at the University of North Carolina at Chapel Hill. Our audit was performed by authority of Article 5A of Chapter 147 of the *North Carolina General Statutes* and was conducted in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States.

The objective of this audit was to review the general controls as they pertain to the University's information technology. The results of our audit disclosed deficiencies that are considered reportable under *Government Auditing Standards.* These items are described in the Audit Findings and Responses section of this report, except those regarding access controls which due to their sensitivity are reported to you by separate letter pursuant to *North Carolina G.S. 147-64.6(c)(18).*

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.

Beth A. Wood, CPA
State Auditor

TABLE OF CONTENTS

BACKGROUND

The University of North Carolina at Chapel Hill is a public research university located in Chapel Hill, North Carolina. Authorized by the N.C. Constitution in 1776, the University was chartered by the N.C. General Assembly on Dec. 11, 1789. First enrolling students in 1795, UNC-Chapel Hill is the oldest public university in the United States and is one of the original eight schools known as a Public Ivy.

UNC-Chapel Hill enrolls more than 28,000 students from all 100 North Carolina counties, the other 49 states, and 47 other countries. State law requires that the percentage of students from North Carolina in each freshman class meets or exceeds 82%. UNC-Chapel Hill offers more than 250 undergraduate, graduate, and professional programs including law and medicine which consists of 71 bachelor's 107 master's, and 74 doctoral degree programs.

[This Page Left Blank Intentionally]

OBJECTIVES, SCOPE, AND METHODOLOGY

As authorized by Article 5A of Chapter 147 of the *North Carolina General Statutes*, we have conducted a performance audit at the University of North Carolina at Chapel Hill. The objective of this audit was to determine the effectiveness of general controls which influence the overall organization and operation of the University's information technology (IT). Our audit was conducted between September 21, 2009 and February 19, 2010.

The scope of our audit included the following IT general controls categories: general security, access controls, program maintenance, systems software, systems development, physical security, operations procedures, and disaster recovery, which directly affect UNC-Chapel Hill's computing operations.

To accomplish our audit objectives, we gained an understanding of University policies and procedures, interviewed key University administrators and other personnel, examined system configurations, tested on-line system controls, reviewed appropriate technical literature, and reviewed computer-generated reports.

As a basis for evaluating general controls, we applied the guidance contained in *Control Objectives for Information and Related Technology* (COBIT), created by the Information Systems Audit and Control Association and the IT Governance Institute. COBIT contains a widely accepted set of best practices in the field of information technology management.

University management, pursuant to North Carolina General Statute §143D-7, bears full responsibility for establishing and maintaining a proper system of internal control which includes IT general controls. A proper system of internal control is designed to provide reasonable, rather than absolute, assurance that relevant objectives are achieved. Because of inherent limitations in internal controls, unauthorized access to data, for example, may nevertheless occur and not be detected. Also, projections of our evaluation in this report of general controls to future periods are subject to the risk that, for example, conditions at the University may change or compliance with University policies and procedures may deteriorate.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

RESULTS

The results of our audit disclosed general control deficiencies that are considered reportable under *Government Auditing Standards*. Deficiencies noted are as follows:

1. Failure to maintain a centralized information technology environment.
2. Failure to develop a risk assessment.
3. Failure to develop technology plans and standards.
4. Failure to finalize and approve security policies.
5. Failure to require staff to undergo annual security awareness training.
6. Failure to establish standards for information published on web pages.
7. Failure to develop an effective disaster recovery plan.
8. Failure to implement access controls in five critical areas.

Details about the deficiencies noted above are described in the Audit Findings and Responses section of this report, except those regarding access controls (number 8 above) which due to their sensitive nature were conveyed to University management in a separate letter pursuant to North Carolina G.S. 147-64.6(c)(18).

1. FAILURE TO MANAGE A CENTRALIZED INFORMATION TECHNOLOGY ENVIRONMENT

The responsibility for managing information technology (IT) resources has not been appropriately restricted to the UNC-Chapel Hill Chief Information Officer (CIO). The University allows faculty and auxiliary departments to manage their own IT resources without being subject to the UNC-Chapel Hill CIO standards and policies.

This condition increases the risk that security vulnerabilities will exist and that critical computer resources and data will be compromised. Also, decentralization in the IT environment increases the risk that uniform policies and procedures are not followed. Furthermore, it renders security controls ineffective if enforcement of policies do not apply to all areas of UNC-Chapel Hill.

COBIT standards state that implementing a highly centralized IT staffing function allows management to exercise control over strategy, resources, budget and process.

Recommendation: Management should ensure that the UNC-Chapel Hill CIO has direct authority and control over all IT resources for the University. The CIO typically reports directly to the Chancellor to ensure standards are consistently applied throughout the University.

Agency Response: Management of The University of North Carolina at Chapel Hill (UNC-Chapel Hill) agrees that more control must be exercised on the security of University IT resources, no matter where direct support responsibility resides.

The Chancellor will mandate that the UNC-Chapel Hill Chief Information Officer has the authority to enforce all policies and standards necessary for the protection of UNC-Chapel Hill data and IT resources. As an immediate implementation step, the CIO will require that all schools and departments identify their IT resources along with responsibility for management of systems, so that additional controls—such as more stringent access and server management requirements—can be imposed. Localized IT support is strategically important to meet the distinct and evolving research and teaching missions of the College, the Schools and certain administrative departments. Therefore, in the opinion of University management, complete centralization of IT support is not the most viable option to reduce the risk of security vulnerabilities.

2. FAILURE TO DEVELOP A RISK ASSESSMENT

UNC-Chapel Hill has not identified and assessed risks to its information technology assets. Without an adequate risk assessment, the University cannot adequately anticipate and address threats and vulnerabilities to its assets nor design appropriate controls to mitigate risk.

COBIT standards state that an organization should maintain a current business risk assessment to identify, evaluate, and prioritize risks which could significantly impact the organization's computer operations. These standards recommend the risk assessment be

reviewed regularly and updated for changes in computer operations. The risk assessment for computer operations should be a part of the overall business risk assessment for the entire organization.

***Recommendation*:** UNC-Chapel Hill management should develop a risk assessment that will assist the University in anticipating and mitigating threats and vulnerabilities to its assets, especially information technology assets. Management should design controls appropriately to mitigate risk.

***Agency Response*:** Management of UNC – Chapel Hill agrees with the finding.

The University issued RFP# 65-RFP02042010 on February 2, 2010 and has selected Illumant, LLC, to perform an Enterprise IT Risk Assessment for the entire campus. This work will begin shortly and is expected to take two months to complete.

3. Failure To Develop And/Or Formalize Technology Plans and Standards

UNC-Chapel Hill has not developed and/or formalized the following:

- Technology infrastructure plan - This plan includes contingency arrangements and acquisition plans for operating systems, databases, and network devices.
- Technology standards - These are standards that will guide management in purchasing uniform technology to support learning, teaching, and educational goals.

Inadequately developed, formalized, or defined technology plans and standards could impair the operating effectiveness of the University and result in poorly designed information technology controls.

COBIT standards state that an organization should maintain long and short-range information technology plans, technology infrastructure plans, and technology standards to allow management to maintain proper controls over its information technology assets and provide direction to staff.

***Recommendation*:** The University should develop a technology infrastructure plan, and formalize its technology standards.

***Agency Response*:** Management of UNC – Chapel Hill agrees with the finding.

<u>Technology Infrastructure Plans</u>

Three principal IT infrastructure planning initiatives are underway:

1. IT infrastructure architecture is a primary strategic focus of developing a comprehensive IT strategy for the campus, per recently-developed ITS goals and strategies.
2. The design and deployment of high-priority key infrastructure services to campus organizations is a key goal of the Carolina Counts IT projects.

3. Consolidation and standardization of the infrastructure that delivers core business functions is a focus of in-progress internal ITS efficiency and process improvements. Internal process improvements underway also include an implementation of ITIL-based processes, the creation of an infrastructure lifecycle plan, and establishment of a project management office in ITS.

These three initiatives support one another in that a capably defined and managed IT architecture establishes a framework within which infrastructure to deliver core business functions can also deliver high-value services to the community, thus maximizing the return on investment for resources so allocated.

Technology Standards

Initial areas of focus for architectural review include the following:

- Commodity x86 platform systems, and virtualized x86 hosting
- Commodity high volume network delivered storage
- Identity and resource management systems (e.g., Active Directory, Shibboleth, LDAP)
- ITS Storage Area Network consolidation
- Establishing ITS infrastructure standards

Working groups have been established to document and set requirements, codify efforts already completed, and outline steps from current state to desired state. The output of these working groups, and follow-on activities in other technology focus areas, will constitute three- and five-year infrastructure technology plans.

4. FAILURE TO FINALIZE AND APPROVE SECURITY POLICIES

UNC-Chapel Hill has not finalized its information security policy or its information security standards policy. These policies remain in draft form. These policies provide the security standards that the users of the University network must follow.

The *Statewide Information Security Manual* states: "The *Statewide Information Security Manual* is the foundation for information technology security in North Carolina. It sets out the standards required by G.S. §147-33.110, which directs the State Chief Information Officer (State CIO) to establish a statewide set of standards for information technology security to maximize the functionality, security, and interoperability of the State's distributed information technology assets."

The *Security Manual* further states: "The *Statewide Information Security Manual* sets forth the basic information technology security requirements for state government. Standing alone, it provides each executive branch agency with a basic information security manual. Some agencies may need to supplement the manual with more detailed policies and standards that relate to their operations and any applicable statutory requirements, such as the Health Insurance Portability and Accountability Act of 1996 and the Internal Revenue Code. While this Manual is the foundation for information technology security in state government, simply adopting these standards will not provide a comprehensive security program. Agency management should emphasize the importance of information security throughout their organizations with ongoing training and sufficient personnel, resources and support."

Without finalized and approved security policies in place, the University may not be able to adequately address security challenges and opportunities as they arise. This may result in a poorly controlled environment that is susceptible to increased security risks.

***Recommendation*:** The University should finalize and formally adopt a set of security policies that will assist in anticipating the University's security needs.

***Agency Response*:** Management of UNC – Chapel Hill agrees with the finding.

The UNC – Chapel Hill security policies are in the final stages of editing and will be announced to the campus and implemented this academic year. The overarching "Information Security Policy" has now been approved and the remaining policies will follow quickly. As a follow up to the release of the existing policies there is a "Carolina Counts" project that will undertake a gap analysis to identify any areas in the *Statewide Information Security Manual* that are not addressed by UNC – Chapel Hill IT security policies. Once the gaps are known, changes to existing policies will be proposed or additional policies developed to cover these gaps.

5. FAILURE TO REQUIRE STAFF TO UNDERGO ANNUAL SECURITY AWARENESS TRAINING

The University does not require users to annually recertify that they have read and understand the University's security policies and procedures. By not requiring an annual recertification, users may not be aware of the security policies and procedures in place, and the University increases the risk that users will become complacent or simply unaware of security measures they should adhere to.

COBIT standards state that management should have procedures in place that require users to annually recertify that they have read and understand management's security policies and procedures.

***Recommendation*:** The University should first formalize and approve security policies and then require users to annually recertify that they have read and understand the University's security policies and will adhere to them.

***Agency Response*:** Management of UNC – Chapel Hill agrees with the finding.

A security awareness training module containing information about security policies and their impact on day-to-day proper usage of IT resources and protection of University data has been created and piloted. The University intends to create a new policy that requires all University employees to annually certify that they have read and understand the University's security policies and will adhere to them.

6. FAILURE TO ESTABLISH STANDARDS FOR INFORMATION PUBLISHED ON WEB PAGES

The University does not have policies and procedures in place that establish standards for what is appropriate content for the University's web site. UNC-Chapel Hill management relies on two draft policies to prevent the inadvertent publication of critical or sensitive information on its web site. Both policies have not been approved by UNC-Chapel Hill management and do not address criteria for web site content. By not implementing web site content policies and procedures, the University increases the risk that critical or sensitive information may be inadvertently divulged on its web pages.

The *Statewide Information Security Manual* states: "The State's information, data and documents shall be handled in a manner that will protect the information, data and documents from unauthorized or accidental disclosure, modification or loss. All information, data and documents must be processed and stored in accordance with the classification levels assigned to those data in order to protect their integrity, availability and, if applicable, confidentiality."

Management is responsible for designing controls over the access to critical and sensitive data. This access extends to the data that is placed on web sites.

***Recommendation*:** The University should implement policies and procedures to ensure critical and sensitive information is not inadvertently disclosed on its web site. University management should communicate web site content standards in an approved policy.

***Agency Response*:** Management of UNC – Chapel Hill agrees with the finding.

We will ensure that the information security and data governance policies specifically address web content.

7. FAILURE TO DEVELOP AN EFFECTIVE DISASTER RECOVERY PLAN

UNC-Chapel Hill's disaster recovery plan is outdated and does not support the current information technology infrastructure. The disaster recovery plan refers to personnel who are no longer employed at the University, and the plan does not address the new technology the University recently acquired. As a result, the current plan may not enable the University to restore all of its critical functions if a disaster were to occur.

COBIT standards state that without a formal process for periodic review and approval of changes, it will be difficult to properly maintain the disaster recovery plan to ensure continued service in the event of a disaster.

***Recommendation*:** University management should revise the current disaster recovery plan to include the new technolgy that exists in its current environment and test the plan to ensure that critical functions and services can be restored if a disaster occurs. Additionally, the disaster recovery plan should be reviewed and approved by executive management to ensure it has campus-wide support.

***Agency Response*:** Management of UNC – Chapel Hill agrees with the finding.

Information Technology Services included in its budget submission earlier this year a request for funding for a Business Impact Analysis in order to begin the disaster recovery planning process. In response to the audit report, the University has funded this request.

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