State of North Carolina

Office of the State Auditor
Beth A. Wood, CPA

The University of North Carolina System Office

Guidance for Information Technology Policies

Information Systems Audit
September 2020

NCOSA
The Taxpayers' Watchdog

EXECUTIVE SUMMARY

PURPOSE

The purpose of this audit was to determine if the University of North Carolina (UNC) System Office developed and issued information technology (IT) guidance in accordance with the UNC Policy Manual[1].

BACKGROUND

In 2018[2], the UNC Board of Governors adopted policies for *IT Governance[3], Information Security, and User Identity and Access Control.* The purpose of these policies was to create consistent standards and centralized guidance for IT practices at the UNC System Office and constituent institutions. The UNC System Office executes the policies of the UNC Board of Governors and provides System-wide leadership and support to the 17 constituent institutions that compose the UNC System.

The purpose of these policies is to (1) foster the efficient development and maintenance of strategically aligned IT within known and acceptable levels of risk; (2) ensure effective and consistent governance and management of IT at the UNC System Office and each constituent institution; (3) encourage collaboration and shared service arrangements in areas of IT between the constituent institutions and the UNC System Office; (4) preserve the security, confidentiality, accessibility, and integrity of information resources; and (5) ensure the risk of unauthorized access to University data and information systems is mitigated.

FINDING

- The UNC System Office has not fully developed and issued guidance for IT governance programs.

RECOMMENDATIONS

- The UNC System Office Chief Information Officer, in consultation with the UNC Chief Information Officer Council[4], should establish a plan and timeline to complete the development and issuance of the required guidance for IT governance in accordance with the UNC Policy Manual.
- The UNC System Office President should ensure the plan is followed and the required guidance for IT governance is issued in accordance with the UNC Policy Manual.

[1] UNC Policy Manual, Chapter 1400 Information Technology

[2] The UNC Board of Governors adopted a policy for *Information Security* in January 2018. The policies for *IT Governance and User Identity and Access Control* were adopted in May 2018.

[3] IT governance is a structural framework designed to ensure the effective and efficient use of IT to support the achievement of an organization’s mission and goals.

[4] The UNC Chief Information Officer Council is composed of the IT leaders from each constituent institution and the UNC System Office Chief Information Officer.

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 27699-0600
Telephone: (919) 807-7500
Fax: (919) 807-7647
http://www.auditor.nc.gov

AUDITOR'S TRANSMITTAL

The Honorable Roy Cooper, Governor
Members of the North Carolina General Assembly
Board of Governors, University of North Carolina System
Peter Hans, President, University of North Carolina System

Ladies and Gentlemen:

We are pleased to submit this information systems audit report titled *Guidance for Information Technology Policies*. The purpose of this audit was to determine if the University of North Carolina (UNC) System Office has developed and issued information technology (IT) guidance in accordance with the UNC Policy Manual.

The President reviewed a draft copy of this report. His written comments are included starting on page 9.

This audit was conducted in accordance with Chapter 147, Article 5A of the *North Carolina General Statutes*.

We appreciate the courtesy and cooperation received from management and the employees of the University of North Carolina System Office during our audit.

Respectfully submitted,

Beth A. Wood

Beth A. Wood, CPA
State Auditor

Beth A. Wood, CPA
State Auditor

TABLE OF CONTENTS

PAGE

Chapter 147, Article 5A of the *North Carolina General Statutes*, gives the Auditor broad powers to examine all books, records, files, papers, documents, and financial affairs of every state agency and any organization that receives public funding. The Auditor also has the power to summon people to produce records and to answer questions under oath.

BACKGROUND

The University of North Carolina

The University of North Carolina (UNC) campuses were placed under the UNC Board of Governors by the *Higher Education Reorganization Act of 1971*. The objectives of the UNC System are to foster the development of a well-planned and coordinated system of higher education, to improve the quality of education, to extend educational benefits beyond campus borders, and to encourage economic and effective use of the State's resources.[5] Today, the UNC Board of Governors and UNC System Office continue to support this mission by offering services, support, and guidance to the 17 constituent institutions of the University of North Carolina.

The constituent institutions are composed of 16 universities and the North Carolina School of Science and Mathematics, the country's first public residential high school for gifted students. Each of the 17 institutions plays a role in fulfilling the UNC System's mission; however, there are many differences among them. While combined student enrollment for the 16 public universities was almost 240,000 in 2019, enrollment counts at individual universities ranged from 1,086 to 36,304.[6] Certain universities participated in shared information technology (IT) services while others operated independently. The UNC System accounted for nearly $600 million of the State's IT expenditures in fiscal year 2019, while individual institutional spending ranged from just over $1 million to nearly $165 million.[7] Technological solutions that work for one institution may not work for another; however, each institution must manage all applicable operational risks including those associated with IT.

Purpose of Information Technology Policies

In 2018 , the UNC Board of Governors adopted three IT policies to create consistent standards for IT practices among the UNC System Office and constituent institutions. These policies included *Information Security*, which was adopted in January 2018, and *IT Governance*[8] and *User Identity and Access Control*, which were adopted in May 2018. The UNC System Office issued guidance for the *Information Security* and *User Identity and Access Control* policies in September 2019 and March 2020, respectively.

The collective purpose of these policies is as follows:

- To foster the efficient development and maintenance of strategically aligned IT within known and acceptable levels of risk;
- To ensure effective and consistent governance and management of IT at each constituent institution;
- To encourage collaboration and shared service arrangements in areas of IT between the constituent institutions and the UNC System Office;
- To preserve the security, confidentiality, accessibility, and integrity of information resources; and

[5] https://www.northcarolina.edu University of North Carolina mission statement

[6] https://dev.northcarolina.edu/news/unc-system-announces-second-year-of-record-enrollment/

[7] https://www.osc.nc.gov/public-information/reports/it-expenditures-report

[8] IT governance is a structural framework designed to ensure the effective and efficient use of IT to support the achievement of an organization's mission and goals.

- To ensure the risk of unauthorized access to UNC System data and information systems is mitigated.

The three policies require the UNC System Office to develop and issue guidance as follows:

- **Information Security** – The UNC System Office and each constituent institution must designate a senior officer with information security responsibility and establish an information security program.
- **User Identity and Access Control** – The UNC System Office Chief Information Officer (CIO), in consultation with the Chief Information Officer Council (CIOC), must develop, maintain, and update standards for identity and access controls for the UNC System Office and constituent institutions.
- **Information Technology Governance** – The UNC System Office CIO shall develop, implement, and maintain an IT governance program for the UNC System. The IT governance program must include a defined framework, or frameworks, to guide the development and implementation of the individual constituent institution IT governance programs. Additionally, the UNC System Office CIO, in consultation with the CIOC, shall develop a set of principles and guidelines addressing specific IT areas defined in the policy.

Importance of Information Security and User Identity and Access Control

Information security is necessary to ensure the confidentiality, integrity, and availability of State information and information systems. An information security program implements standard security management practices and controls over information systems that collect, process, transmit, store, and share university data. Ineffective information security increases the risk of data resources being disclosed, destroyed, or denied by unauthorized individuals. These outcomes often lead to reputational damage, legal ramifications, and increased costs.

A core element of an effective information security program is restricting data access to authorized individuals. User identity and access controls ensure individuals are properly identified and allowed access to only the data necessary to fulfil one’s job responsibilities. Similar to ineffective information security, ineffective user identity and access control increases the risk of unauthorized disclosure, modification, or denial of data.

Importance of Information Technology Governance

To ensure that students and citizens have confidence in the UNC System’s governance of IT, governance processes that protect student information, research data, and IT systems must be implemented and maintained. IT governance requires formalized processes and programs to ensure IT activities are consistently performed, responsive to risk, and auditable.

According to the UNC Policy Manual, the IT governance program should include a framework, or frameworks, for developing and implementing IT governance programs at each constituent institution. Additionally, the program must include principles and guidelines for planning, prioritization, funding, evaluation, auditing, disaster recovery, privacy, and security of IT and information resources, risk assessments, risk management, oversight of distributed IT resources, organizational and staffing models, reporting, and lines of authority.[9]

[9] UNC Policy Manual § 1400.1 Information Technology Governance

Proper IT governance over the UNC System means:

- The UNC System President ensures that each constituent institution is provided a framework, principles, and guidelines for the development and implementation of consistent IT governance programs.
- The UNC System Office CIO, in consultation with the CIOC, establishes a process and criteria by which each constituent institution and the UNC System Office demonstrate that it is operating in accordance with the UNC System's IT governance policy.

Establishing consistent plans and policies for IT governance activities improves an institution's ability to prevent and respond to incidents, manage known vulnerabilities, protect data, and keep IT resources available to users. Consistent IT governance requires each university, and the UNC System as a whole, to establish and implement rules and guidelines for the use of its information resources and data.

Effective governance over IT is essential because IT supports mission-critical business functions. Benefits of effective IT governance include: strategic alignment between IT and university objectives, appropriate risk management, optimized IT investments that contribute value to a university's mission, meaningful metrics for IT reporting, and effectively managed IT resources.[10] The absence of effective IT governance could lead to negative consequences. These may include recurring IT issues, unplanned system downtime, and increased susceptibility to cyber-attacks. Any of these outcomes may lead to increased costs, reputational damage, and significant impediments to an institution's ability to achieve its mission and goals.

[10] Institute of Internal Auditors Global Technology Audit Guide 17, "Auditing Information Technology Governance"

Objective, Scope, and Methodology

We conducted this information systems 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 objective.

The audit objective was to determine whether the University of North Carolina (UNC) System Office has developed and issued information technology (IT) guidance in accordance with the UNC Policy Manual.[11]

To achieve the audit objective, we performed the following procedures:

- Interviewed key UNC System Office managers and staff.
- Interviewed the Chair of the Committee on Audit, Risk Management, and Compliance of the UNC Board of Governors.
- Interviewed external stakeholders.
- Reviewed policies and best practices.
- Reviewed state laws.
- Examined documentation of controls and processes.
- Examined documentation supporting the activities executed by the UNC System Office, including activities executed in consultation with the 17 constituent institutions.
- Evaluated processes and documentation against policy requirements and best practices.

Our audit scope included activities executed by the UNC System Office between January 2018 and April 2020. We conducted the fieldwork from March 2020 to May 2020.

Because of the test nature and other inherent limitations of an audit, together with limitations of any system of internal and management controls, this audit would not necessarily disclose all performance weaknesses or lack of compliance.

As a basis for evaluating internal control, we applied the guidance contained in professional auditing standards. These standards require auditors to identify internal control components that are deemed significant to our audit objective (see Appendix on page 8). While internal control guidance contained in those standards was followed, our audit does not provide a basis for rendering an opinion on internal control, and consequently, we have not issued such an opinion.

[11] UNC Policy Manual, Chapter 1400 Information Technology

Results and Conclusions

Based on the results of audit procedures described in the *Objective, Scope, and Methodology* section of this report, we identified a deficiency in the University of North Carolina (UNC) System Office's internal control over developing and issuing guidance for information technology (IT) governance that is considered reportable under *Government Auditing Standards*. Specifically, the UNC System Office has not fully developed and issued guidance for IT governance[12] programs.

This deficiency is described in more detail in the *Finding and Recommendations* section of this report. Management's response is presented in the *Response from the University of North Carolina System Office* section of this report. We did not audit the response, and accordingly, we express no opinion on it.

[12] IT governance is a structural framework designed to ensure the effective and efficient use of IT to support the achievement of an organization's mission and goals.

Finding and Recommendations

IT GOVERNANCE PROGRAM GUIDANCE NOT FULLY DEVELOPED AND ISSUED

The University of North Carolina (UNC) System Office has not fully developed and issued guidance for information technology (IT) governance[13] programs.

The UNC System Office had not issued an IT Governance framework as of May 2020, two years after the adoption of the IT Governance policy. After we began audit related inquiry in January 2020, the UNC System Office contracted with a consultant to compose an IT Governance Program Charter (or Charter). This contract was executed in February 2020, and the draft Charter was delivered by the consultant in April 2020. This Charter will serve as the defined IT governance program framework that is designed to ensure that IT operations and IT projects are effectively managed and meet the needs of each constituent institution.

The UNC System Office had developed and issued a set of principles and guidelines; however, our audit found that these principles and guidelines did not fully address each area specified in the UNC Policy Manual. Specifically, the principles and guidelines did not address non-security matters for the areas as follows:

- **Disaster Recovery** – creating a plan for restoring data and information systems after a natural or man-made disaster[14]
- **Risk Assessment** – actively identifying risks and threats[15] to the IT environment and evaluating the likelihood and impact of those risks occurring
- **Risk Management** – continuously responding to risks through mitigation strategies[16]

Because the UNC System Office has not issued the IT Governance Program Charter, staff of the constituent institutions lack the framework necessary to develop and implement their IT governance programs consistent with the UNC System expectations. Without guidance, the IT governance programs may be ineffective and lead to negative outcomes such as increased costs, reputational damage, and unexpected service interruptions. Additionally, if the principles and guidelines do not fully address each area specified in the UNC Policy Manual, constituent institutions may fail to include these areas in their IT governance programs. If the aforementioned areas are not addressed, there is an increased risk of the following:

- An event[17] damages IT resources and causes loss of university data
- IT risks are not identified or addressed, leading to unplanned downtime[18]

[13] IT governance is a structural framework designed to ensure the effective and efficient use of IT to support the achievement of an organization's mission and goals.

[14] Disasters may be natural such as a hurricane or tornado physically damaging an IT facility. Disasters can also be man-made such as someone digging and cutting a cable, starting a fire, or making untested changes to IT settings that result in IT becoming temporarily unavailable.

[15] A threat refers to a new or newly discovered incident that has the potential to harm a system or an institution overall. There are three main types of threats: (1) natural threats, such as floods, hurricanes, or tornadoes; (2) unintentional threats, such as an employee mistakenly accessing the wrong information; (3) intentional threats, such as spyware, malware, adware companies, or the actions of a disgruntled employee. Risk is defined as the potential for loss or damage when a threat exploits a vulnerability. Examples of risk include financial losses, loss of privacy, reputational damage, legal implications, and even loss of life.

[16] Mitigation strategies are activities performed to reduce the chance of risks and threats occurring.

[17] Any natural or man-made disaster that causes disruption or damage to IT resources.

[18] Unplanned downtime means IT resources become unexpectedly unavailable for use.

- Identified risks are not appropriately prioritized or managed[19]

According to the UNC System Office Chief Information Officer (CIO), he prioritized the development and issuance of guidance for the Information Security and User Identity and Access Control policies over the guidance on the IT governance policy. This decision was made due to the complexity and length of time required to develop guidance for IT governance programs. The UNC System Office issued guidance for Information Security and User Identity and Access Control in September 2019 and March 2020, respectively. Additionally, the UNC System Office CIO considered the areas of disaster recovery, risk assessment, and risk management to be addressed by the UNC System Office's information security program. However, these areas also impact non-security related IT operations such as the availability of IT resources to business users when needed.

The UNC Policy Manual[20] requires the UNC System Office CIO to develop, implement, and maintain an IT governance program, subject to the UNC System President's approval, for the UNC System Office and the 17 constituent institutions to follow. This governance program includes a defined framework, or frameworks, to guide development and implementation of the individual governance programs at constituent institutions. The UNC Policy Manual also specifies a minimum set of principles and guidelines to be included in each program which are to be updated on a regular basis by the UNC System Office CIO in consultation with the UNC Chief Information Officer Council.[21]

RECOMMENDATIONS

The UNC System Office Chief Information Officer, in consultation with the UNC Chief Information Officer Council, should establish a plan and timeline to complete the development and issuance of the required guidance for IT governance in accordance with the UNC Policy Manual.

The UNC System Office President should ensure the plan is followed and the required guidance for IT governance is issued in accordance with the UNC Policy Manual.

[19] Risk prioritization allocates resources to activities that reduce threats with the highest liklihood and/or negative impact if they were to occur before allocating resources to less impactful or likely threats.

[20] UNC Policy Manual § 1400.1 IT Governance

[21] The UNC Chief Information Officer Council is composed of IT leaders from each constituent institution and the UNC System Chief Information Officer.

APPENDIX

Internal Control Components and Principles Significant to the Audit Objective

The purpose of this audit was to determine whether the University of North Carolina (UNC) System Office has developed and issued guidance for information technology (IT) in accordance with the UNC Policy Manual.

Internal control components and underlying principles that were significant to our audit objective are identified as follows:

Control Environment

- The oversight body should oversee the entity's internal control system.
- Management should establish an organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives.

Risk Assessment

- Management should define objectives clearly to enable the identification of risks and define risk tolerances.
- Management should identify, analyze, and respond to significant changes that could impact the internal control system.

Control Activities

- Management should design control activities to achieve objectives and respond to risks.
- Management should design the entity's information system and related control activities to achieve objectives and respond to risks.
- Management should implement control activities through policies.

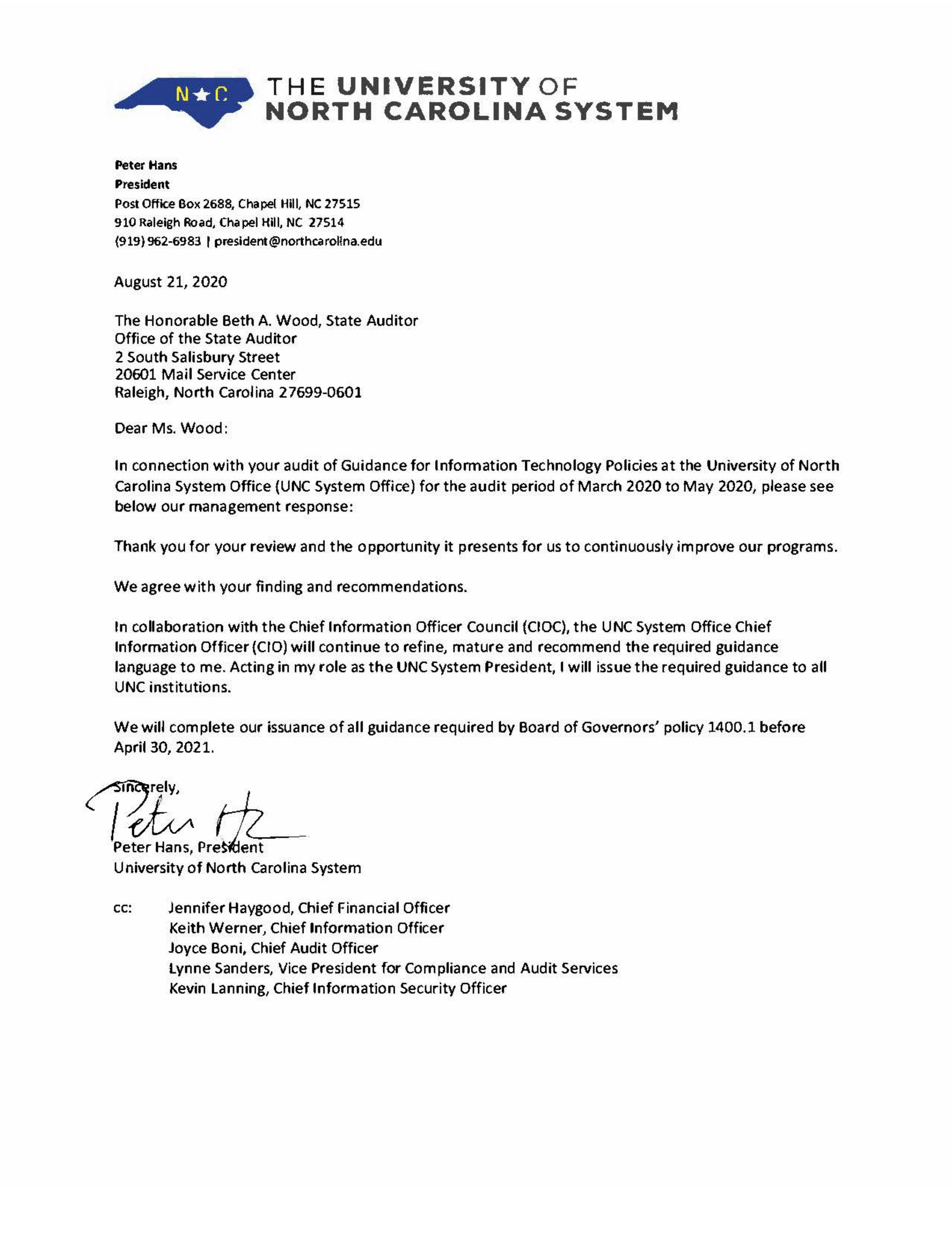
Information and Communication

- Management should internally communicate the necessary quality information to achieve the entity's objectives.
- Management should externally communicate the necessary quality information to achieve the entity's objectives.

Monitoring Activities

- Management should establish and operate monitoring activities to monitor the internal control system and evaluate the results.
- Management should remediate identified internal control deficiencies on a timely basis.

RESPONSE FROM UNIVERSITY OF NORTH CAROLINA SYSTEM OFFICE



THE UNIVERSITY OF
NORTH CAROLINA SYSTEM

Peter Hans
President
Post Office Box 2688, Chapel Hill, NC 27515
910 Raleigh Road, Chapel Hill, NC 27514
(919) 962-6983 | president@northcarolina.edu

August 21, 2020

The Honorable Beth A. Wood, State Auditor
Office of the State Auditor
2 South Salisbury Street
20601 Mail Service Center
Raleigh, North Carolina 27699-0601

Dear Ms. Wood:

In connection with your audit of Guidance for Information Technology Policies at the University of North Carolina System Office (UNC System Office) for the audit period of March 2020 to May 2020, please see below our management response:

Thank you for your review and the opportunity it presents for us to continuously improve our programs.

We agree with your finding and recommendations.

In collaboration with the Chief Information Officer Council (CIOC), the UNC System Office Chief Information Officer (CIO) will continue to refine, mature and recommend the required guidance language to me. Acting in my role as the UNC System President, I will issue the required guidance to all UNC institutions.

We will complete our issuance of all guidance required by Board of Governors' policy 1400.1 before April 30, 2021.

Sincerely,

Peter Hans, President
University of North Carolina System

cc: Jennifer Haygood, Chief Financial Officer
Keith Werner, Chief Information Officer
Joyce Boni, Chief Audit Officer
Lynne Sanders, Vice President for Compliance and Audit Services
Kevin Lanning, Chief Information Security Officer

ORDERING INFORMATION

COPIES OF THIS REPORT MAY BE OBTAINED BY CONTACTING:

Office of the State Auditor
State of North Carolina
2 South Salisbury Street
20601 Mail Service Center
Raleigh, North Carolina 27699-0600

Telephone: 919-807-7500
Facsimile: 919-807-7647
Internet: http://www.auditor.nc.gov

To report alleged incidents of fraud, waste or abuse in state government contact the
Office of the State Auditor Fraud Hotline: **1-800-730-8477**
or download our free app.

REPORT FRAUD

https://play.google.com/store/apps/details?id=net.ncstateauditor.ncauditor&hl=en_US

REPORT FRAUD

https://itunes.apple.com/us/app/nc-state-auditor-hotline/id567315745

For additional information contact the
North Carolina Office of the State Auditor at:
919-807-7666

NC$OSA
The Taxpayers' Watchdog

This audit was conducted in 1,040 hours at an approximate cost of $108,160.