THE UNIVERSITY OF NORTH CAROLINA SYSTEM

MEETING OF THE BOARD OF GOVERNORS
Committee on Audit, Risk Management, and Compliance

April 21, 2021 at 3:30 p.m.
Via Videoconference and PBS North Carolina Live Stream
University of North Carolina System Office
Center for School Leadership Development, Board Room
Chapel Hill, North Carolina

AGENDA

OPEN SESSION

A-1. Approval of the Minutes of February 17, 2021 .... Mark Holton

A-2. Organizational Structure of Internal Audit - UNC System Office .... Jonathan Pruitt

A-3. Information Security Recommendations .... Keith Werner

A-4. 2021 Annual Report on Implementation of UNC Information Technology Policies .... Keith Werner

A-5. Summary of Audit Reports Issued by the Office of the State Auditor .... Lynne Sanders

CLOSED SESSION

A-6. Approval of the Closed Session Minutes of February 17, 2021 .... Mark Holton

A-7. Audit Update .... Lynne Sanders

OPEN SESSION

A-8. Adjourn

THE UNIVERSITY OF NORTH CAROLINA SYSTEM

MEETING OF THE BOARD OF GOVERNORS
Committee on Audit, Risk Management, and Compliance
April 21, 2021

Closed Session Motion

Motion to go into closed session to:

- Prevent the disclosure of information that is privileged or confidential under Article 7 of Chapter 126 and § 143-748 of the North Carolina General Statutes, or not considered a public record within the meaning of Chapter 132 of the General Statutes; and

- Consult with our attorney to protect attorney-client privilege.

Pursuant to: G.S. 143-318.11(a)(1) and (3).

THE UNIVERSITY OF NORTH CAROLINA SYSTEM

MEETING OF THE BOARD OF GOVERNORS
Committee on Audit, Risk Management, and Compliance

DRAFT MINUTES

February 17, 2021
Via Videoconference and PBS North Carolina Live Stream
University of North Carolina System Office
Center for School Leadership Development, Room 128
Chapel Hill, North Carolina

This meeting of the Committee on Audit, Risk Management, and Compliance was presided over by Chair Mark Holton. The following committee members, constituting a quorum, were also present: Pearl Burris-Floyd, James L. Holmes, Jr., Wendy Floyd Murphy, and Art Pope. The following committee member was absent: Terry Hutchens.

Chancellors participating were Nancy Cable and Sharon Gaber.

Staff members present included Lynne Sanders, Andrew Tripp, and others from the UNC System Office.

1. Call to Order and Approval of the Minutes of February 17, 2021 (Item A-1)

The chair called the meeting to order at 3:15 p.m., on Wednesday, February 17, 2021.

Chair Holton reminded all members of the committee that the meeting would be conducted pursuant to new amendments to the Open Meetings Act, which establish that all votes be taken by roll-call vote. The chair also reminded committee members of their duty under the State Government Ethics Act to avoid conflicts of interest and appearances of conflict of interest. The chair asked if there were any conflicts or appearances of a conflict with respect to any matter coming before the committee. No members identified any conflicts at the time.

The chair next called for a motion to approve the open session minutes of January 20, 2021.

MOTION: Resolved, that the Committee on Audit, Risk Management, and Compliance approve the open session minutes of January 20, 2021, as distributed.

Motion: James L. Holmes, Jr.
Motion carried

Roll Call Vote	
Holton	Yes
Burris-Floyd	Yes
Holmes	Yes
Hutchens	Absent
Murphy	Yes
Pope	Yes

2. Summary of Audit Reports Issued by the Office of the State Auditor (Item A-2)

Chair Holton called on UNC System Vice President for Compliance and Audit Services Lynne Sanders to present a summary of the 16 financial statement audit reports issued to date by the Office of the State Auditor for the 2020 fiscal year. There were no audit findings reported.

This item was for information only.

3. Property Insurance – Summary of Coverage and Exclusions (Item A-3)

Chair Holton welcomed Bryan Heckle from the NC Department of Insurance, who then provided the committee with an overview of exclusions and limitations to the all-risk special form property insurance coverage required at each of the constituent institutions.

This item was for information only.

4. Enterprise Safety and Security Risk: Campus Law Enforcement (Item A-4)

Chair Holton called on UNC System Senior Associate Vice President for Safety and Emergency Operations Fred Sellers to present to the committee potential solutions to the recruitment and vacancy rates at University police departments and the recommendations to address key enterprise risks in campus safety and security. Following the presentation, the chair called for a motion to approve the four recommendations presented to the committee.

MOTION: Resolved, that the Committee on Audit, Risk Management, and Compliance approve the recommendation to eliminate the cap on tuition waivers for campus law enforcement officers; and include this recommendation in the 2021 Board of Governors legislative policy priorities legislation amending Chapter 116-143(d) of the North Carolina General Statutes.

Motion: Art Pope
Motion carried

Roll Call Vote	
Holton	Yes
Burris-Floyd	Yes
Holmes	Yes
Hutchens	Absent
Murphy	Yes
Pope	Yes

MOTION: Resolved, that the Committee on Audit, Risk Management, and Compliance approve the recommendations to enhance the salary structure, career ladder, and organizational structure of campus law enforcement, develop plans to launch training programs at Samarcand Training Facility as well as identify equipment needs, and develop a system for dual employment to gap-fill critical vacancies.

Motion: James L. Holmes, Jr.
Motion carried

Roll Call Vote	
Holton	Yes
Burris-Floyd	Yes
Holmes	Yes
Hutchens	Absent
Murphy	Yes
Pope	Yes

5. Closed Session

MOTION: Resolved, that the Committee on Audit, Risk Management, and Compliance move into closed session to prevent the disclosure of information that is privileged or confidential under Article 7 of Chapter 126 and § 143-748 of the North Carolina General Statutes, or not considered a public record within the meaning of Chapter 132 of the General Statutes; and to consult with our attorney to protect attorney-client privilege pursuant to Chapter 143-318.11(a)(1) and (3) of the North Carolina General Statutes.

Motion: James L. Holmes, Jr.
Motion carried

THE MEETING MOVED INTO CLOSED SESSION.

(The complete minutes of the closed session are recorded separately.)

MOTION: Resolved, that the Committee on Audit, Risk Management, and Compliance return to open session.

Motion: Wendy Floyd Murphy
Motion carried

THE MEETING RESUMED IN OPEN SESSION.

6. Adjourn

There being no further business and without objection, the meeting adjourned at 4:34 p.m.

____

Terry Hutchens, Secretary

THE UNIVERSITY OF NORTH CAROLINA SYSTEM

MEETING OF THE BOARD OF GOVERNORS
Committee on Audit, Risk Management, and Compliance
April 21, 2021

AGENDA ITEM

A-2. Organizational Structure of Internal Audit - UNC System Office ....Jonathan Pruitt

Situation: The University of North Carolina System Office is required to establish a program of internal auditing pursuant to North Carolina General Statute 143-746. The UNC System Office's internal audit function shall be accountable to the Board of Governors through the Committee on Audit, Risk Management, and Compliance and the president.

Background: The purpose of internal audit is to provide independent and objective assurance and consulting services to add value and improve operations of the UNC System Office. The mission of internal audit is to enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight. Internal audit helps the UNC System Office accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, internal control, compliance, and governance processes. It provides a central point for coordinating oversight of activities that promote accountability, integrity, efficiency, and compliance. Through individual Memorandums of Understanding, the chief audit officer and internal audit staff at the UNC System Office also provide internal audit services to the NC School of Science and Mathematics and the NC State Education Assistance Authority.

Assessment: To leverage resources, expertise, and promote efficiency in overseeing internal audit work for the University, leadership over the internal audit function for the System Office and its contracted affiliates will be streamlined and combined with current systemwide internal audit work across the University.

Action: This item requires a vote by the committee.

THE UNIVERSITY OF NORTH CAROLINA SYSTEM

MEETING OF THE BOARD OF GOVERNORS
Committee on Audit, Risk Management, and Compliance
April 21, 2021

AGENDA ITEM

A-3. Managing Risks Related to Information Management - Draft Recommendations.................. Keith Werner

Situation: The purpose of this item is to provide the Committee on Audit, Risk Management, and Compliance a set of recommendations to improve and mature the information technology controls and information security posture for each institution.

Background: CARMC has identified information governance and information security as areas of critical enterprise risk. The North Carolina Office of the State Auditor has indicated that IT controls audits will yield findings. In response, CARMC requested that the UNC System Office develop a set of recommendations to address this issue. The UNC System Office Risk Review Board, in consultation with the CIO Council, drafted a series of seven recommendations, with the programmatic goals of: (1) establish third-party validation of baseline controls, (2) improve the information security posture, (3) assure leadership is actively engaged in risk decision, (4) continuously monitor progress and exploit areas of improvement, (5) determine organizationally prioritized risks, (6) make targeted IT investments based on determined prioritization, and (7) ensure appropriate resource coverage.

Assessment: Information technology is a dynamic environment and challenged with frequent and new security attack vectors. All constituent institutions in the UNC System have agreed to the ISO 27002 framework and its associated 114 controls. The first recommendation is a third-party assessment of each institution against those 114 controls. This is an active engagement and one that will provide a solid baseline to measure and develop further sets of recommendations. In addition, each institution should leverage their Enterprise Risk Management Committee to ensure that organizational targets are set for each control and prioritization of risk is determined for information technology. The remaining recommendations include: utilize contract virtual information security officer services for institutions absent a CISO, maintain a dedicated budget specific to information security, and continue to follow and align to MCNC security services.

Action: This item is for information only.

THE UNIVERSITY OF NORTH CAROLINA SYSTEM

CARMC Recommendations & Updates

Information Security Recommendations
1400 Series Policy Updates

N★C THE UNIVERSITY OF
NORTH CAROLINA SYSTEM

Jonathan Pruitt
UNC System Office COO

Keith Werner
UNC System Office CIO

Kevin Lanning
UNC System Office CISO

2021

Relevant History

2011

- No single information security best practices approach
- US federal standard (NIST) did not exist yet.
- *18 separately developed infosec programs*

2012

- State of NC standard did not work in university environments
- ISO 27002 seemed a good baseline for UNC
- Every Chancellor and the System president endorsed 27002

2016

- Analyzing toolsets and sponsoring centralized purchases

2018

- Board of Governors approved 3 new policies: 1400.1-3

2020

- System president clarified "principles and guidelines" for 1400.1
- System Office CIO issued 1400.3 Standard
- Risk Review Board (RRB) chartered and meeting regularly

Board of Governors Policy Background

(1400.1, 1400.2 & 1400.3)

1400.1

Foster the development and maintenance of strategically aligned technology resources; consistent governance and management of IT; encourage collaboration; and, alignment with “principles and guidelines”

- Chancellor/System president assign responsibility
- Assign responsibility to standing committee with audit responsibility
- Annual Audit Plans & Risk Assessments

1400.2

Commit to an information security strategy, confirm core program and designate a responsible senior officer, accountable to chancellor/president

- Chancellor/System president assign responsibility
- Standing Committee with Audit Responsibility
- Audit Plan & Risk Assessments

1400.3

Risk-based implementation of identity confirmation and access control techniques, such as multi-factor authentication, to control access to sensitive University information

- Chancellor/System president assign responsibility
- Standard issued by UNC System CIO
- Every institution reported status and plan

Key Points

BACKGROUND

Different and disparate IT architectures & environments

Great foundational work over the past three years

Now have foundational Risk Review Board (RRB)

ERM, including information security, highly prioritized and sustainable

IT CONTROL AUDITS

114 control categories, w/ expected findings *(unlike financial audits)*

Prioritized maturity targets and continuous improvement is an effective, risk-based approach

More prioritization across the 114 controls will be more efficient and effective

Priorities and resources to meet them set by leadership at each institution

PROGRAMMATIC GOALS

Third party Baseline assessment

Improve information security posture

Assure leadership is engaged in risk decisions

Continuous monitoring and improvement

Organizational prioritization of enterprise risks

Targeted investments based on prioritization

Appropriate resource coverage based on leadership guidance

Recommendation/Action # 1

Outsourced, 3rd PARTY CYBER MATURITY ASSESSMENT [underway]

1. Third Party Cyber Maturity Assessment for all 18 UNC institutions [already in progress]

Contract with MCNC for a Third Party Cyber Maturity Assessment of all UNC institutions

- Provides a baseline using a uniform methodology and approach
- CFO's have been directed to use HEERF III funds per memo
- System Office facilitated system-wide contract
- UNC System Office is first review engagement
- Cross-reference with current/upcoming audit results
- System Office and CIO Council develops recommendations based on commonalities
- Appropriate actions prioritized by leadership to meet their risk targets
- Approximate MCNC timeline for completion is one year; some resulting, prioritized changes will take longer

Recommendation # 2

RISK MANAGEMENT *(Similar in function to the UNC System Office Risk Review Board)*

2. All institutions leverage their risk management functions, like ERM, to support IT Risk Management required by 1400.1

System leadership active engagement

- Leadership actively prioritizes cyber risks, guides risk treatment decisions, clarifies risk tolerances and sponsors risk management maturation via their Risk Review Board (RRB), for System Office = four leaders who report to the System president
- Sets organizationally approved maturity targets
- Sets expectations and priority for *resource and investmen*t allocation and can rapidly adjust to dynamic cyber security environment

Risk Register

- Annual submission of top 10 information security risks to UNC System Office CIO as a risk register

Recommendation # 3

VIRTUAL CHIEF INFORMATION SECURITY OFFICER (CISO) Availability

3. System Office has vetted optional vCISO contract consulting services for institutions absent a CISO

Recruitment and Retention Challenges

- Three CIOs doing double duty (CIO & CISO)
- Two UNC institutions actively seeking virtual CISO services now
- Recruitments for CISOs are taking months to years, creating sustained periods of time without a skilled resource
- Negotiated contracts in place for vCISO services

Recommendations # 4 - 7

4. Dedicated, reviewable budget specific to cyber security

- Identifiable cyber security budget that meets the institution's risk priorities and targets
- Priorities and investment are appropriately balanced on risk decisions by leadership

5. Coordinate with MCNC Security Services roadmap

- Excellent relationship with UNC over long history
- MCNC is in a unique position that ALL UNC and NCREN traffic goes through their facilities
- Mutually define incremental steps in service roadmap

6. CIO and CISO onboarding programs

7. Sharing of appropriate audit information at CIOC/ ISC

Continuous Monitoring & Improvement Cycle

Policy Statement from 1400.1: The UNC System Office chief information officer shall work with the UNC System Office finance, audit, and legal staff, and the Chief Information Officers Council, to establish the process and criteria by which each constituent institution and the UNC System Office shall demonstrate that it is operating in accordance with the UNC System's information technology governance program.

Closing and Q&A

- Annual Report

- Q&A

2021

Jonathan Pruitt
UNC System Office COO

Keith Werner
UNC System Office CIO

Kevin Lanning
UNC System Office CISO

THE UNIVERSITY OF NORTH CAROLINA SYSTEM

MEETING OF THE BOARD OF GOVERNORS
Committee on Audit, Risk Management, and Compliance
April 21, 2021

AGENDA ITEM

A-4. 2021 Annual Report on Implementation of UNC Information Technology Policies .... Keith Werner

Situation: The purpose of this item is to provide the Committee on Audit, Risk Management, and Compliance an update on institutional status of implementation of policies relating to information governance, information security, and data protection.

Background: CARMC has identified information governance and information security as areas of enterprise risk. In response, the Board adopted a policy on Information Security (Section 1400.2) in January 2018. Subsequently, in response to recommendations from the IT Security Working Group (ITSWG) and CARMC, the Board adopted two additional policies in May 2018: (1) the policy on Information Technology Governance (Section 1400.1), and (2) the policy on User Identity and Access Control (Section 1400.3). As a requirement to Section 1400.1 of the UNC Policy Manual, the CIO Council and Risk Review Board approved a new IT Governance Charter, with Principles and Guidelines, which was sent to the chancellors by President Hans. Providing an update on the status of implementation of these policies fulfills a request from CARMC, and satisfies the reporting requirement outlined in the policies.

Assessment: Information security is a complex issue and highlights the need for sound IT governance at each institution and the UNC System Office, as well as general security and system access controls. Per the reporting requirements detailed in the policies, status updates on the implementation of these policies is a requirement. A survey was sent to all institution CIOs in January 2021 to collect data and provide status on progress from the inception of the policies.

Action: This item is for information only.

2021 Annual Report on Implementation of UNC Information Technology Policies

UNC System Office

www.northcarolina.edu

THE UNIVERSITY OF NORTH CAROLINA SYSTEM

TABLE OF CONTENTS

FOREWARD

Pursuant to the requirements of policy, enclosed is the 2021 periodic report on the Implementation of UNC Information Technology Policies, specifically 1400.1 (IT Governance), 1400.2 (Information Security), and 1400.3 (User Identity and Access Control). The data collected is an annual survey that is provided to the institution Chief Information Officers (CIO) from the UNC System Office CIO. The CIO Council, a system-wide IT Governance structure, is responsible for the design, and ultimate approval of the survey. In 2021, 100% of the institutions responded to the survey.

In December 2020, the CIO Council updated the IT Governance Charter, including enhanced Principles and Guidelines. The Charter was approved by the UNC System Office Risk Review Board (RRB), culminating with the President signing and forwarding it to all the UNC System Chancellors. Per the CIO Council, the survey based the specific questions on the updated Principles and Guidelines. The survey was distributed in February 2021. This data will provide an excellent baseline and will enhance the monitoring of maturity and improvement. The results specific to this area are consistent with the new definitions, Principles and Guidelines, and abbreviated timeframes. In 2021, the CIO Council will contemplate maturity scores for the 2022 survey.

In 2020, the UNC System Office chartered the aforementioned Risk Review Board (RRB) and began meeting weekly to monthly to discuss enterprise risk, including information security risks, as well as to make risk treatment decisions. This foundational board is operating in an effective and sustainable manner, and will be critical to the on-going maturity and improvement of these policy requirements.

The results of the survey demonstrate maturity in this long-term exercise of effective governance. Notably,1400.2 compliance approaches 100% and 1400.3 compliance continue to grow. Given the newly updated Principles and Guidelines associated with 1400.1, the new baseline data illustrates the need for targeted maturity growth and improvement; however, effective foundational work has largely been completed. The Risk Review Board and CIO Council will continue to monitor compliance and any potential actions needed, per the requirements in 1400.1: *The UNC System Office chief information officer shall work with the UNC System Office finance, audit, and legal staff, and the Chief Information Officers Council, to establish the process and criteria by which each constituent institution and the UNC System Office shall demonstrate that it is operating in accordance with the UNC System's information technology governance program.*

EXECUTIVE SUMMARY

Background

In January-May 2018, the Board of Governors voted to establish three Information technology policies: 1400.1 – Information Technology Governance, 1400.2 – Information Security, and 1400.3 – User Identity and Access Control. These policies place emphasis on strategic and coordinated governance and management of information to fulfill the University's mission, assessments and risk management related to University information, and confirmation that responsibility is assigned to specific, named senior representatives of the Chancellors/System President The new policies also describe required assessments by UNC auditors and oversight activities that will be undertaken by the Board of Governors and the Boards of Trustees.

The UNC System Office Chief Information Officer (CIO) provides an annual update on the status of 1400.1 – 1400.3 policy series compliance to the Committee on Audit, Risk Management and Compliance (CARMC). The aims of the policies are as follows:

- 1400.1 - Foster the development and maintenance of strategically aligned technology resources; consistent governance and management of IT; encourage collaboration; and, in alignment with specified Principles and Guidelines
- 1400.2 - Commit to an information security strategy, confirm that core program components are in place and designate a responsible senior officer, accountable to Chancellor/President
- 1400.3 - Risk-based implementation of user identity and access control techniques, such as multi-factor authentication, to control access to sensitive University information

1400.1 – 1400.3 Series Policy Survey

The 1400.1 – 1400.3 Series Policy survey has been an annual survey conducted based on the requirements detailed in the 1400.1 – 1400.3 series policies as well as subsequent IT Governance charters and interpretations. The UNC System CIO conducted several collaborative meetings in advance of the annual survey to ensure all questions appropriately address the 1400.1 – 1400.3 policy series requirements as well as aim to meet our objectives detailed in the IT Governance Charter. A copy of the actual survey is available to the Board of Governors members on request to the System Office CIO.

2021 Survey Results Highlights

Compliance with 1400.1 – 1400.3 continues to improve in maturity, given the updated Principles and Guidelines is very recent. Despite an unusual year with COVID negatively impacting our institutions, the institutions across the UNC System have continued to evolve program maturities. In 2020, the CIO Council updated the IT Governance Charter, including updated Principles and Guidelines. The Charter was approved by the UNC System Office Risk Review Board, culminating with the President approving and forwarding to all the UNC System Chancellors. The survey based the specific questions on the updated Principles and Guidelines. Some key highlights related to 1400.1 – 1400.3 series are shown below:

77%

Avg. Systemwide Yes/In Process

1400.1

Accomplished fulfilling the principles and guidelines described in the IT Governance Charter

97%

1400.2 Information Security Compliance

1400.2

Compliance rate based on survey assessments

18

All Institutions updated written status on Standard

1400.3

More MFA than ever with gaps clarified and written compliance paths published

Key Takeaways

1400.1

- President Hans sent updated supplemental "Principles and Guidelines" to Chancellors in late 2020. The results are consistent with the abbreviated timeframe from the updated Principles and Guidelines and the survey date.
- The System Office Enterprise Risk Review Board has been chartered and is meeting and taking action weekly to monthly.

1400.2

- CIOs continue to indicate they are compliant with the requirements of this policy.
- The baseline Maturity Assessment outsourced to MCNC will help validate **(Maturity Assessment)**

1400.3

- UNC institutions have more MFA in place than ever before.
- In March 2020, the System Office CIO issued the Standard as required by the policy.
- All UNC institutions reported their compliance status to the System Office CIO in writing as required by the Standard.
- Most institutions had gaps; all provided a written remediation plan update and most reported resource level deficits to close their remaining gaps.

1400.1 – IT GOVERNANCE

Overview

The two following questions are based on the 1400.1 policy:

- Are you the chancellor-named designate for oversight of information technology governance and implementation of the information technology governance framework and program as required by 1400.1 at your institution?
- Can your organization produce an artifact that documents that designation?

Chancellor-named designate	Designation documented
100 PERCENT	82.4 PERCENT

Ownership and Accountability Structure-and-Process

All of the institutions already are in process of defining the IT governance oversight structure, approval processes, reporting lines and organizational structure required by the above charter. Most institutions indicated that they would be compliant with this within a 12-month timeframe. Below are additional questions associated with Ownership and Accountability.

100

PERCENT

Access to Senior Leadership – Yes/In Process/Maturing

Does your IT governance include the lines of authority to include access to senior leadership?

100

PERCENT

Project Prioritization– Yes/In Process/Maturing

Does your institution document its IT project prioritization?

100

PERCENT

Strategic Plan Alignment – Yes/In Process/Maturing

Does the governance align with your institution's strategic plan?

77

PERCENT

Funding Approach – Yes/In Process/Maturing

Does your institution document its IT funding approach?

For all of the above questions, the estimated timeframe's to completion were within a 12-month period. IT governance is a continuous and maturing foundational element to proper IT decision-making, prioritization and investment strategies. The CIO Council views IT governance as a modelling activity that benefits from a cycle of continuous assessment, modifications and improvements.

Transparency and Collaboration

All of the institutions have worked with the CIOC and its subcommittees through timely collaboration defining and reducing gaps, needs, and potential Shared Service opportunities.

That collaboration is demonstrated via institutional involvement in the CIO Council and it's subcommittees: Shared Services for Hosted ERP Services/RemoteDBAs (HISSC), Information Security Council (ISC), Shared Enterprise Applications & Services Committee (SEASC) and the Infrastructure and Operations Committee (I&O). The above IT governance structure continues to see positive membership participation across all the institutions.

Evaluation and Self-Monitoring

The institutions surveyed responded to this series of questions as follows:

88.2
PERCENT

BOG Assessments - 2021

Are you planning to conduct required 'Board of Governors (BOG) 1400* series policies' assessments within the 2021 calendar year?

88.2
PERCENT

ISO 27002 Self-Assessment

Did your institution complete an annual self-assessment based on ISO 27002 in 2020?

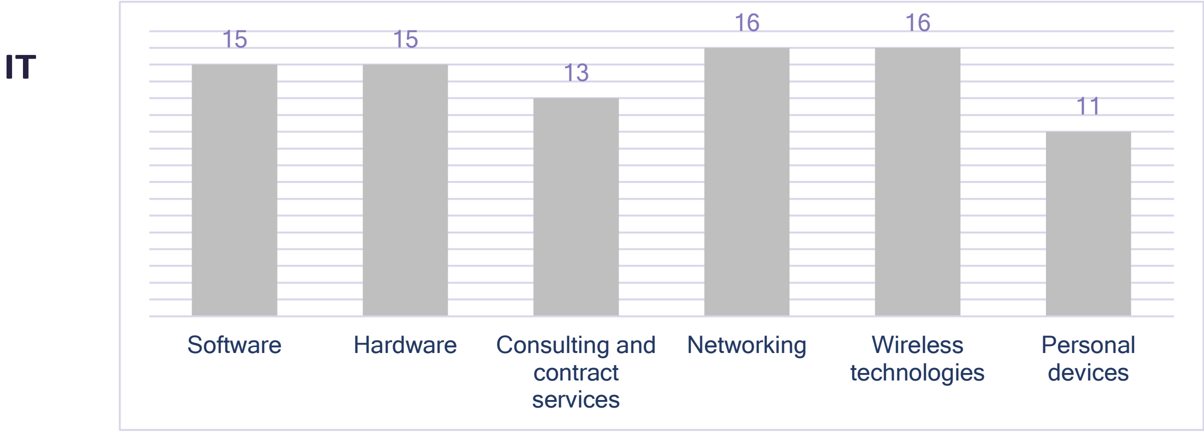
Policies, Standards and Procedures

The policy, standards and procedures section of the survey addressed whether an institution followed the Principles and Guidelines detailed in the IT Governance Charter. The specific survey question was asked as follows:

"Under the control of the University CIO (or chancellor-designated responsible campus party) and following your institution's approved risk management approach, does your institution follow the IT Governance charter regarding principles and guidelines on the following topics: software, hardware, acquisition of information technology including consulting and contract services; networking; wireless technologies and personal devices."

The chart below is consistent with the recently published Principles and Guidelines:

Table 1. Policies, Standards and Procedures Survey Results



The CIO Council will prioritize this discussion of these topics in the upcoming July 2021 meeting.

Policy Survey Additional Questions

Additional questions pertained to conducting periodic self-monitoring and external monitoring, internal audits as well as maintaining systems of accountability and additional questions covered by 1400.1 – 1400.3 Series BOG Policies. Below is a snapshot of those responses.

70.6

PERCENT

Periodic self- and external monitoring – Yes/In Process/Maturing

Does your IT Governance program provide periodic self-monitoring and external monitoring of the institution's compliance with the language of 1400.1?

81.3

PERCENT

Specialized expertise audits – Yes/In Process/Maturing

Does your IT Governance program include periodic audits of information technology and information resource issues by qualified auditors with specialized expertise?

94.1

PERCENT

Periodic audit/compliance/risk management to Board– Yes/In Process/Maturing

Does your IT Governance program provide periodic consideration of information technology matters by the audit/compliance/risk management committee of your institution's board?

88.2

PERCENT

Effective systems of accountability – Yes/In Process/Maturing

Does your IT Governance program maintain effective systems of accountability to identify and correct deficiencies?

IT Policy Survey Additional Questions – Survey Results continued.

94.1
PERCENT

Oversight of IT Governance – Yes/In Process/Maturing

Has the board of trustees of your institution assigned responsibility for oversight of IT governance to a standing committee of the board with audit responsibility?

94.2
PERCENT

Annual Audit Plan – Yes/In Process/Maturing

Does your institution have an annual audit plan that considers possible audit activity for the year focused on information technology matters, based on annual risk assessments?

82.4
PERCENT

Regular IT Governance Review – Yes/In Process/Maturing

Has the assigned committee with responsibility for IT governance reviewed and discussed audit activity relating to information technology matters, and addressed issues of importance in information technology governance on a regular basis at its scheduled meetings?

100
PERCENT

CIO Council and associated committees' participation – Yes/In Process/Maturing

Does your institution participate in IT governance activities regarding planning, funding, evaluation, auditing, prioritization and information security via the CIO Council and associated committees as described.
the IT Governance Program Charter?

88.3
PERCENT

Disaster Recovery Plan (Yes within 12 months) – Yes/In Process/Maturing

Does your institution have a written, approved disaster recovery plan as described in the IT Governance Program Charter?

82.3
PERCENT

Privacy Requirements followed described in IT Governance Program – Yes/In Process/Maturing

Does your institution follow privacy requirements described in the IT Governance Program Charter?

88.3
PERCENT

Risk Management requirements followed – Yes/In Process/Maturing

Does your institution follow risk management requirements described in the IT Governance Program Charter?

94.1
PERCENT

Defined IT oversight structure – Yes/In Process/Maturing

Has your institution defined the IT governance oversight structure, approval processes, reporting lines, oversight of distributed IT, organizational structure and staffing as required in the IT Governance Program Charter?

Additional questions related to encryption standards and strategic alignment:

- Does your institution have published encryption standards as described in the IT Governance Program Charter? Approximately half have fully published the standards.
- Has your institution published guidelines and priorities that align with the University's strategic objectives? Given the recent publication of the Principles and Guidelines, formalizing this alignment is an area that is currently in process.

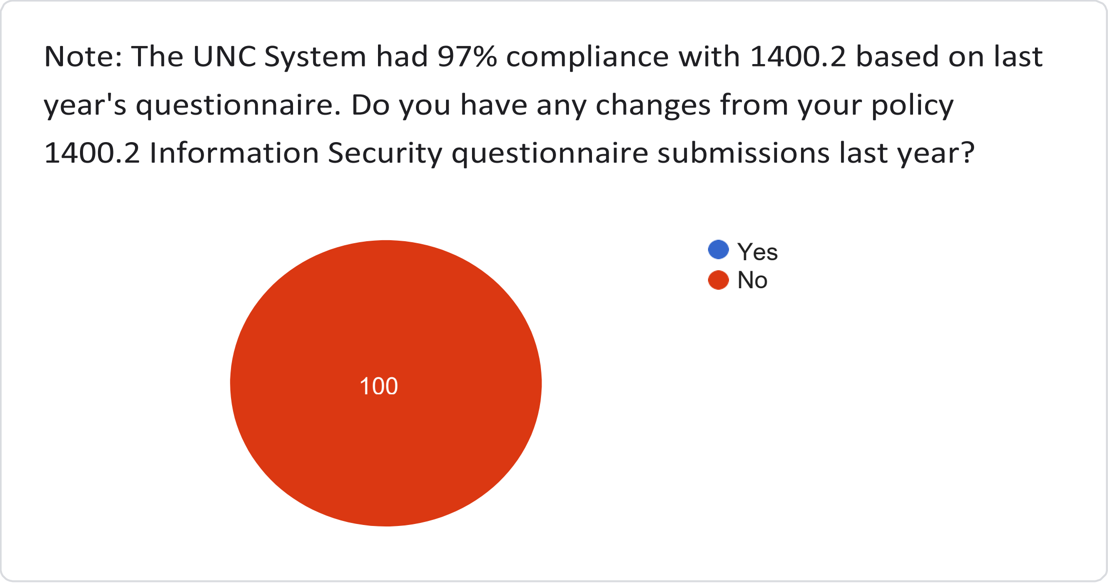
1400.2 – INFORMATION SECURITY

The 1400.2 portion of the survey questions focuses on assessing whether an institution follows all 1400.2 policy components.

- Has your institution designated a senior officer, accountable to the president or chancellor who is responsible for information security?" And, do you have a written artifact to document designation?
- The UNC System had 97% compliance with 1400.2 based on last year's questionnaire. Do you have any changes from your policy 1400.2 Information Security questionnaire submissions last year?

100% of all institutions for the UNC System have designated a senior officer, accountable to the president or chancellor who is responsible for information security. All but one has that as a written artifact.

Additionally, all institutions responses indicate having no changes since last year’s 1400.2 Information Security questionnaire.



Note: The UNC System had 97% compliance with 1400.2 based on last year's questionnaire. Do you have any changes from your policy 1400.2 Information Security questionnaire submissions last year?

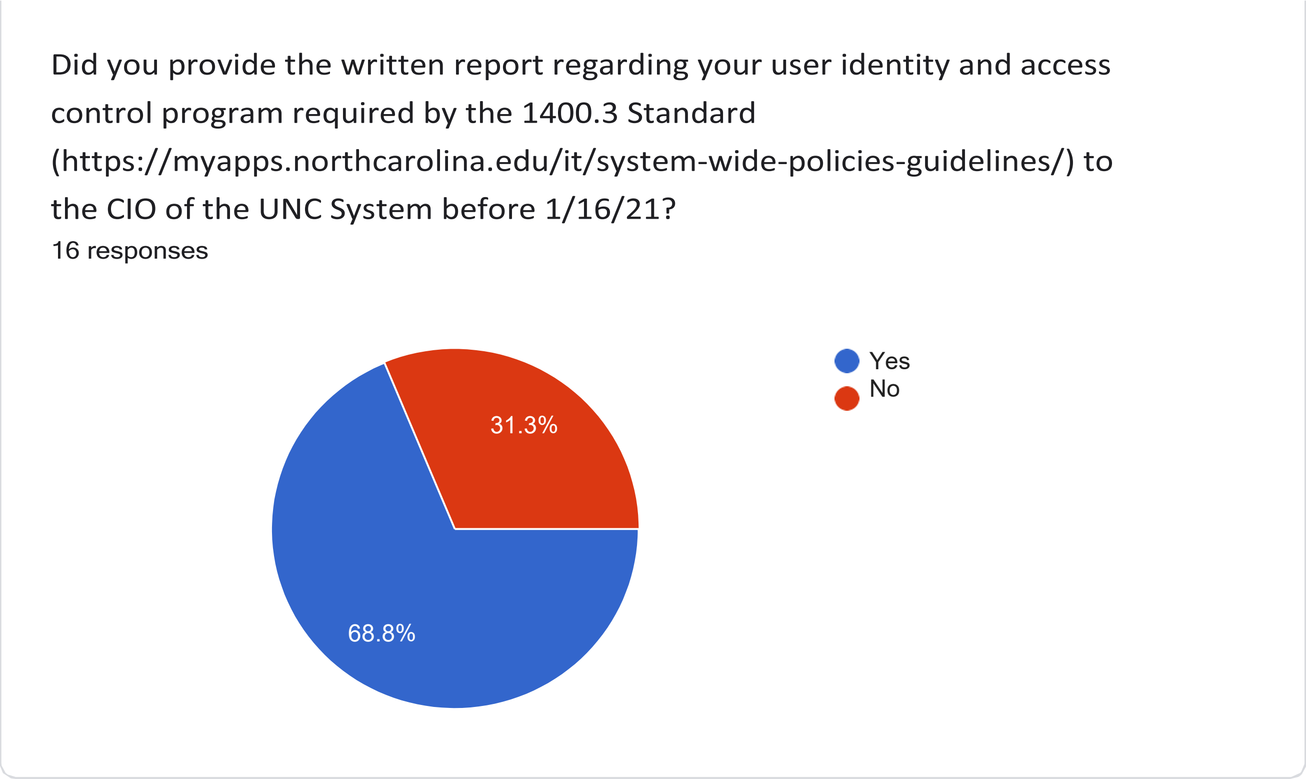
1400.3 – USER IDENTITY & ACCESS CONTROL

Did you provide the written report regarding your user identity and access control program required by the 1400.3 Standard (https://myapps.northcarolina.edu/it/system-wide-policies-guidelines/) to the CIO of the UNC System before 1/16/21?

68% responded that they provided the written report regarding your user identity and access control program required by the 1400.3 Standard.

Additional Information

System Office staff worked intensively with the CIOs resulting in all CIOs providing a written report to the System Office CIO by the early April, 2021.



Did you provide the written report regarding your user identity and access control program required by the 1400.3 Standard (https://myapps.northcarolina.edu/it/system-wide-policies-guidelines/) to the CIO of the UNC System before 1/16/21?

16 responses

COMPLIANCE AND MONITORING

The Risk Review Board and CIO Council will continue to monitor compliance and promote any needed actions, per the requirements in 1400.1: *The UNC System Office chief information officer shall work with the UNC System Office finance, audit, and legal staff, and the Chief Information Officers Council, to establish the process and criteria by which each constituent institution and the UNC System Office shall demonstrate that it is operating in accordance with the UNC System's information technology governance program.*

The newly updated Principles and Guidelines of the IT Governance Charter indicate:

Actively Designing IT Governance

The UNC System Office and all UNC institutions will participate in creating, reviewing, monitoring and supporting one another:

- To actively design and maintain the framework defined by this charter
- To adhere to the framework for IT Governance
- To subsequently follow the UNC System policies
- To subsequently provide guidance to each institution, allowing it to develop a campus-specific IT governance program that supports its unique structure

Each IT governance effort will be subject to regular review not only by each institution but also collectively by the UNC CIO Council (CIOC). These reviews will be conducted to ensure adherence to best practices, to the CIOC Strategic Plan, and to the policies from both the Board of Governors and each relevant Institution.

The CIO Council will include this as an on-going agenda item for the quarterly meetings, with the July meeting serving as the more in-depth and directional meeting.

System leadership will participate via System Office CIO updates to the System Office Risk Review Board.

THE UNIVERSITY OF NORTH CAROLINA SYSTEM

MEETING OF THE BOARD OF GOVERNORS
Committee on Audit, Risk Management, and Compliance
April 21, 2021

AGENDA ITEM

A-5. Summary of Audit Reports Issued by the Office of the State Auditor .... Lynne Sanders

Situation: The committee will receive an update on audit reports issued since the February CARMC meeting by the Office of the State Auditor for the 2020 fiscal year.

Background: All constituent institutions and the UNC System Office are subject to audit by the North Carolina State Auditor under Article 5A of Chapter 147 of the North Carolina General Statutes. The State Auditor's Office conducts annual financial statement audits at each institution, annual federal compliance audits at select institutions, and periodically performs other audits, such as information technology general controls audits at select institutions.

Assessment: The Office of the State Auditor has released ten reports between March 30, 2021, and April 12, 2021, for the 2020 fiscal year. Out of the ten reports, two are financial statement audits and eight are statewide federal compliance audits. The audit results are summarized for the committee in the attachment.

Action: This item is for information only.

Financial Statement Audit Reports			
Institution Name	Report Link	Release Date	# of Findings
North Carolina School of Science and Mathematics	FIN-2020-6094	3/31/2021	0
University of North Carolina System Office	FIN-2020-6010	3/30/2021	0

Statewide Federal Compliance Audit Reports			
Institution Name	Report Link	Release Date	# of Findings
Appalachian State University	FSA-2020-6080	4/9/2021	0
East Carolina University	FSA-2020-6065	4/7/2021	0
Elizabeth City State University	FSA-2020-6086	4/9/2021	2
Fayetteville State University	FSA-2020-6088	4/12/2021	2
North Carolina Agricultural and Technical State University	FSA-2020-6070	4/9/2021	1
North Carolina State University	FSA-2020-6030	4/6/2021	0
University of North Carolina at Chapel Hill	FSA-2020-6020	4/6/2021	0
University of North Carolina at Charlotte	FSA-2020-6050	4/8/2021	0