THE UNIVERSITY OF
NORTH CAROLINA SYSTEM

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

May 22, 2024 at 9:00 a.m.
Via Videoconference and PBS North Carolina Livestream
UNC System Office
223 S. West Street, Board Room
Raleigh, North Carolina

AGENDA

OPEN SESSION

A-1. Approval of the Open Session Minutes of February 28, 2024 .... Terry Hutchens

A-2. Presentation of Audit Reports from the Office of the State Auditor .... Jordan Chippewa, OSA

A-3. Enterprise Risk Management Progression ....Bryan Heckle

A-4. Annual Report on Implementation of UNC Information Technology Policies .... Kim Smodic

CLOSED SESSION

A-5. Approval of the Closed Session Minutes of February 28, 2024 .... Terry Hutchens

A-6. Investigative Audit Update ....Michael Ptasienski

A-7. Adjourn

THE UNIVERSITY OF NORTH CAROLINA SYSTEM

MEETING OF THE BOARD OF GOVERNORS
Committee on Audit, Risk Management, and
Compliance
May 22, 2024

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), (3), and (6).

THE UNIVERSITY OF NORTH CAROLINA SYSTEM

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

DRAFT MINUTES

February 28, 2024 at 3:15 p.m.
Via Videoconference and PBS North Carolina Livestream
UNC System Office
223 S. West Street, Room 1809
Raleigh, North Carolina

This meeting of the Committee on Audit, Risk Management, and Compliance was presided over by Chair Terry Hutchens. The following committee members, constituting a quorum, were also present in person or by phone: Pearl Burris-Floyd, Kirk Bradley, Jimmy D. Clark, and Art Pope.

Chancellor participating was Todd Roberts.

Staff members present included Fred Sellers, Brad Trahan, and others from the UNC System Office.

1. Call to Order and Approval of OPEN Session Minutes (Item A-1)

The chair called the meeting to order at 3:15 p.m. on Wednesday, February 28, 2024. The open session minutes from the November 15, 2023, meeting were approved by unanimous consent.

2. Update on Research Security Activity (Item A-2)

Mary Millsaps from NC State University and Quinton Johnson from the University of North Carolina at Chapel Hill briefed on the recent research security update standards targeting the security of federally funded research. These regulations or standards will impact several compliance areas, including export controls, international travel, standard disclosure requirements, and cybersecurity.

This item was for information only.

3. UNC System Office Internal Audit Update (Item A-3)

Michael Ptasienski presented an update on the progress of the UNC System Office Internal Audit Plan that identifies the current status of the 2023-24 internal audit projects.

This item was for information only.

4. Audit Reports Issued by the Office of the State Auditor (Item A-4)

Mr. Ptasienski further presented a report on the audits issued by the Office of the State Auditor that included 13 financial statement audit reports on the UNC System for the 2023 fiscal year. Several reports had yet to be issued.

This item was for information only.

5. Appalachian State University Campus Safety Update (Tentative (Item A-5)

Campus Police Chief Andy Stephenson of Appalachian State University presented on the need to improve the 911 system for the university. Their path includes efforts to design a system that will allow timely responses for the campus police department to respond to 911 calls to include fire or emergency medical assistance. This effort will immediately improve the safety of the campus.

This item was for information only.

6. 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 pursuant to Chapter 143-318.11(a)(1), (3), and (6) of the North Carolina General Statutes.

Motion: Kirk Bradley
Motion carried

THE MEETING MOVED INTO CLOSED SESSION AT 4:10 p.m.
(The complete minutes of the closed session are recorded separately.)

THE MEETING RESUMED IN OPEN SESSION AT 4:37 p.m.

7. Adjourn

There being no further business and without objection, the meeting adjourned at 4:38 p.m.

____
Kirk Bradley, Secretary

MEETING OF THE BOARD OF GOVERNORS
Committee on Audit, Risk Management, and
Compliance
May 22, 2024

AGENDA ITEM

A-2. Presentation of Audit Reports from the Office of the State Auditor..........................Jordan Chippewa, OSA

Situation: The committee will receive an update on the audit reports issued by the Office of the State Auditor.

Background: All constituent institutions and the University of North Carolina 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 conducts annual financial statement audits at each institution and annual federal compliance audits at select institutions, and periodically performs other audits, such as investigations and information technology general controls audits at select institutions.

Assessment: Thus far in FY2024, the Office of the State Auditor has released 16 financial statement audit reports related to UNC System institutions for the 2022 fiscal year. In addition, the Office of the State Auditor also released six statewide federal compliance audits. The audit results have been summarized for the committee in the attachment.

Action: This item is for information only.

Financial Statement Audits for FY2023

Financial Statement Audits for FY2023 (as of 5/2/2024)				
Institution Name	**Report Link**	**Report Number**	**Release Date**	**# of Findings**
Appalachian State University	/2023-12/FIN-2023-6080.pdf?Version	FIN-2023-6080	12/8/2023	0
East Carolina University	s/2023-11/FIN-2023-6065.pdf?Versio	FIN-2023-6065	11/20/2023	0
Elizabeth City State University	2024-01/FIN-2023-6086_0.pdf?Versi	FIN-2023-6086	1/26/2024	0
Fayetteville State University			STILL PENDING	
North Carolina Agricultural and Technical State University	2023-12/FIN-2023-6070.pdf?VersionI	FIN-2023-6070	12/14/2023	0
North Carolina Central University	/2024-04/FIN-2023-6090.pdf?Versio	FIN-2023-6090	4/22/2024	**1**
North Carolina State University	2023-11/FIN-2023-6030.pdf?Version	FIN-2023-6030	11/29/2023	0
North Carolina School of Science and Mathematics			STILL PENDING	
University of North Carolina at Asheville	/2023-10/FIN-2023-6055.pdf?Versio	FIN-2023-6055	10/24/2023	0
University of North Carolina at Chapel Hill	2023-12/FIN-2023-6020.pdf?Version	FIN-2023-6020	12/1/2023	0
University of North Carolina at Charlotte	s/2023-11/FIN-2023-6050.pdf?Versio	FIN-2023-6050	11/9/2023	0
The University of North Carolina at Greensboro	/2023-11/FIN-2023-6040.pdf?Version	FIN-2023-6040	11/15/2023	0
The University of North Carolina at Pembroke	s/2023-11/FIN-2023-6082.pdf?Versio	FIN-2023-6082	11/22/2023	0
University of North Carolina School of the Arts	/2023-12/FIN-2023-6092.pdf?Versio	FIN-2023-6092	12/8/2023	0
University of North Carolina System Office	2024-03/FIN-2023-6010.pdf?VersionI	FIN-2023-6010	3/19/2024	0
University of North Carolina Wilmington	s/2023-11/FIN-2023-6060.pdf?Versio	FIN-2023-6060	11/20/2023	0
Western Carolina University	2023-11/FIN-2023-6075.pdf?Version	FIN-2023-6075	11/29/2023	0
Winston-Salem State University	/2024-02/FIN-2023-6084.pdf?Versio	FIN-2023-6084	2/21/2024	0

THE UNIVERSITY OF NORTH CAROLINA SYSTEM

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

AGENDA ITEM

A-3. Enterprise Risk Management Progression .... Bryan Heckle

Situation: The purpose of this item is to provide the Committee on Audit, Risk Management, and Compliance an update on enterprise risk management in the University of North Carolina System.

Background: In adopting the policy on University Enterprise Risk Management and Compliance, the University of North Carolina Board of Governors provided for the establishment of UNC Systemwide and institution-based enterprise risk management and compliance processes. The policy aims to address enterprise risk management, including risks related to compliance with laws and ethical standards at the system level, and to complement and support the risk management and compliance processes and activities of the constituent institutions.

Assessment: The committee will receive an update on the enterprise risks progression ongoing at the constituent institutions and the UNC System Office.

Action: This item is for information only.

THE UNIVERSITY OF NORTH CAROLINA SYSTEM

ENTERPRISE RISK MANAGEMENT

Bryan Heckle, CIC, CPCU, CRM
Director of Enterprise Risk Management

ERM Progression

- System Office Maturity

  More mature with the inclusion of PBS North Carolina, NC Arboretum and NCSEAA risks

  Dedicated resources to capture emerging risks across the constituent institutions and the System Office

  Consistent and robust dialogue with the Risk Review Board on current and emerging risks

ERM Progression

- Constituent Institutions Maturity
  - Constituent institutions are becoming more mature in their processes

- All constituent institutions have staff dedicated to enterprise risk management

Staffing

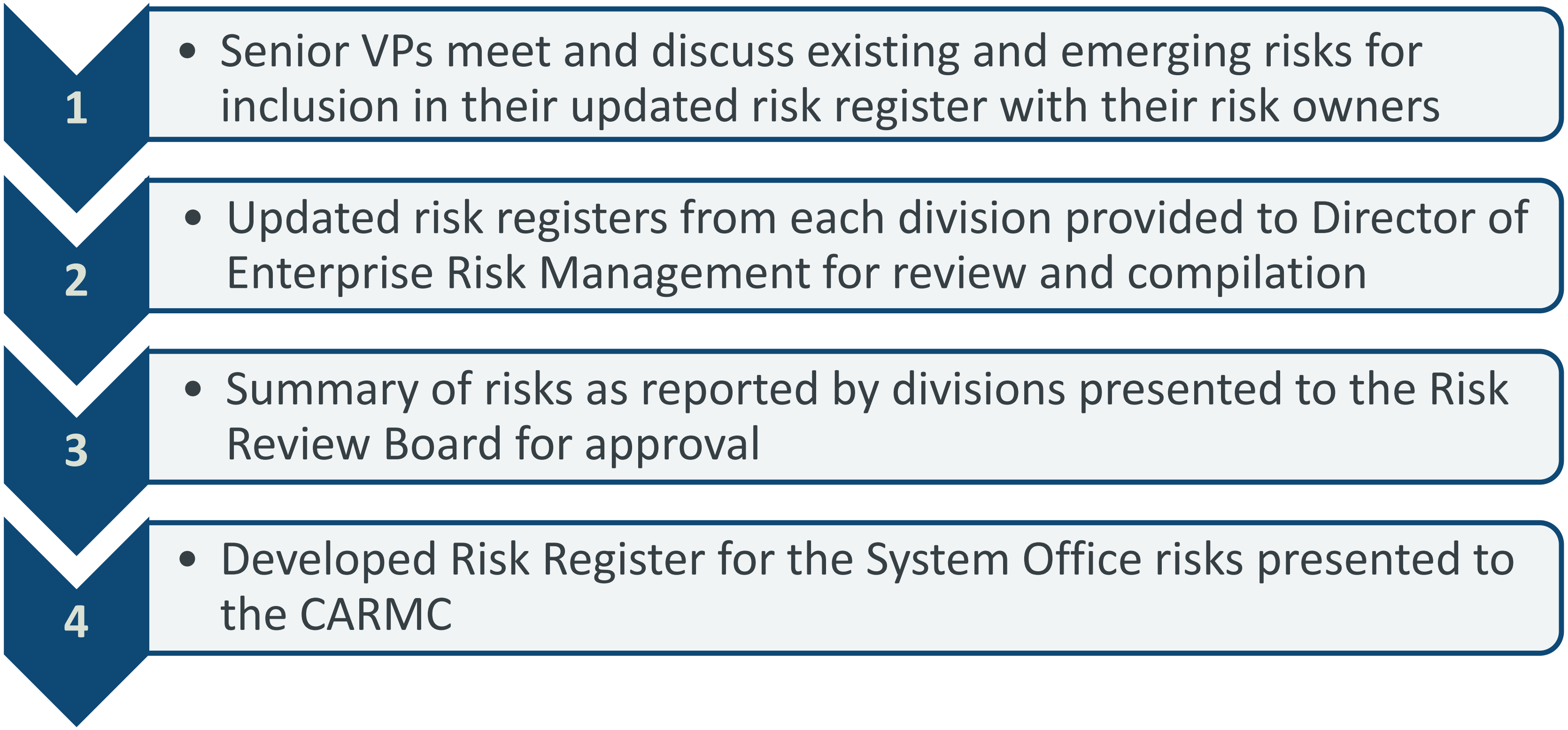
- All constituent institutions are researching for technology to better collect and provide risk mitigation recommendations

Technology

- Risk owners are more collaborative with their risk managers to ensure their enterprise risks are being leveraged with cabinet members and trustees

Collaboratio
n

System Office Risk Register Process



1

- Senior VPs meet and discuss existing and emerging risks for inclusion in their updated risk register with their risk owners

2

- Updated risk registers from each division provided to Director of Enterprise Risk Management for review and compilation

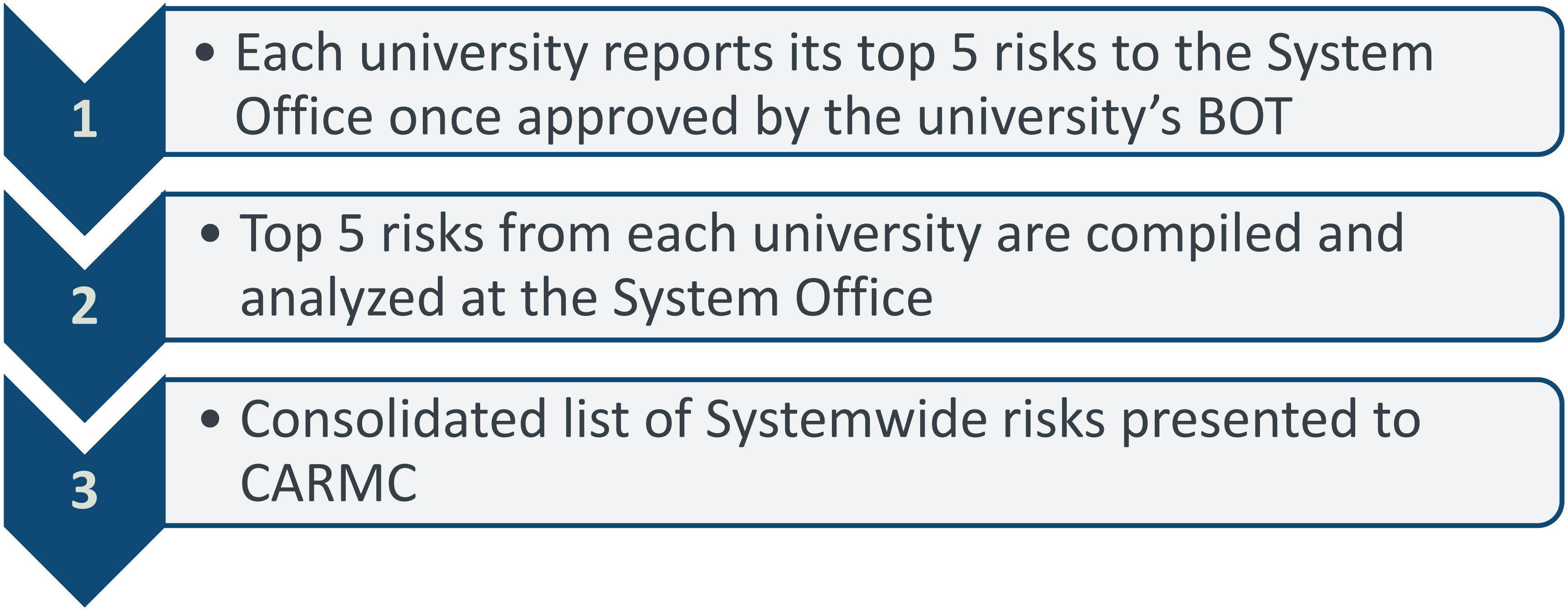
3

- Summary of risks as reported by divisions presented to the Risk Review Board for approval

4

- Developed Risk Register for the System Office risks presented to the CARMC

UNC Constituent University Process



1

- Each university reports its top 5 risks to the System Office once approved by the university’s BOT

2

- Top 5 risks from each university are compiled and analyzed at the System Office

3

- Consolidated list of Systemwide risks presented to CARMC

QUESTIONS?

THE UNIVERSITY OF
NORTH CAROLINA SYSTEM

MEETING OF THE BOARD OF GOVERNORS
Committee on Audit, Risk Management, and
Compliance
May 22, 2024

AGENDA ITEM

A-4. Annual Report on Implementation of UNC Information Technology Policies.............................Kim Smodic

Situation: The purpose of this item is to provide the Committee on Audit, Risk Management, and Compliance (CARMC) 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 Section 1400.2 of the UNC Policy Manual, *Information Security*,in January 2018. In response to recommendations from the Information Technology Security Working Group (ITSWG) and CARMC, the Board adopted two additional policies in May 2018: (1) Section 1400.1 of the UNC Policy Manual, *Information Tehchnology Governance*, and (2) Section 1400.3 of the UNC Policy Manual, *User Identity and Access Control*. As a requirement to Section 1400.1 of the UNC Policy Manual, the Chief Information Officer Council (CIOC) and Risk Review Board approved a new Information Technology Governance Charter, with Principles and Guidelines, that was sent to the chancellors by President Peter Hans. Providing an update on the status of implementation of these policies fulfills a request from the 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 University of North Carolina 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 are required. A survey was sent to all institution CIOs in 2024 to collect data and provide status on progress from the inception of the policies. The detailed written report is in the board materials.

Action: This item is for information only.

2024 Annual Report on Implementation of UNC Information Technology Policies

UNC System Office

www.northcarolina.edu

THE UNIVERSITY OF NORTH CAROLINA SYSTEM

TABLE OF CONTENTS

FOREWORD

Pursuant to the requirements of policy, enclosed is the Annual Report on the Implementation of UNC Information Technology Policies, Section 1400.1 of the UNC Policy Manual, *Information Technology Governance*, Section 1400.2 of the UNC Policy Manual, *Information Security*, and Section1400.3 of the UNC Policy Manual, *User Identity and Access Control.* The data collected is an annual survey that is provided to the institution chief information officers (CIO) from the University of North Carolina System Office CIO. The CIO Council (CIOC), the Systemwide IT governance structure, is leveraged for the design and ultimate approval of the survey.

In 2020, the CIOC 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 forwarding to all the UNC System chancellors.

In 2020, the UNC System Office chartered the RRB, and the board began meeting regularly to discuss enterprise risk and available treatments, including information management. This foundational board is operating in an effective and sustainable manner and is critical to the ongoing maturity and improvement of these policy requirements.

The results of the 2024 annual survey demonstrate positive maturity in this long-term exercise of effective governance. Notably, both Sections 1400.2 and 1400.3 of the UNC Policy Manual have seen tremendous improvement and compliance. Given the updated Principles and Guidelines associated with Section 1400.1 of the UNC Policy Manual, the expected new baseline data illustrates the need for targeted maturity 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, per the requirement in Section 1400.1 of the UNC Policy Manual: *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

Beginning in January 2018, the University of North Carolina Board of Governors voted to establish three information technology policies: Section 1400.1, *Information Technology Governance*; Section 1400.2, *Information Security*; and Section 1400.3, *User Identity and Access Control*. These policies emphasize strategic and coordinated information technology governance and management to fulfill the UNC System's mission, risk management related to unauthorized access to University data and information systems, and confirmation that an information security program is in place and that a senior officer, accountable to the chancellor, is responsible for information security. The policies also describe oversight activities that will be undertaken by the UNC Board of Governors and the boards of trustees.

The UNC System Office chief information officer (CIO) provides an annual update on the status of Section 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, ensure consistent governance and management of IT, encourage collaboration, and operate in alignment with “Guiding Principles”;
- 1400.2 - Commit to an information security strategy, confirm core program, and designate a responsible senior officer, accountable to chancellor/president;
- 1400.3 - Risk-based implementation of identity confirmation and access control techniques, such as multifactor authentication, to control access to sensitive University information.

1400.1 – 1400.3 Series Policy Survey

The 1400.1 – 1400.3 series policy survey is an annual survey conducted based on the Board of Governors reporting requirements detailed in the 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 addressed the series requirements, as well as aimed to meet our objectives detailed in the IT Governance Charter.

2024 Survey Results Highlights

Compliance with 1400.1 – 1400.3 series policy continues to improve in maturity. In 2020, the CIOC updated the IT Governance Charter, including updated Principles and Guidelines. The charter was approved by the UNC System Office RRB, culminating with the president forwarding to all the UNC System chancellors. Some key highlights related to 1400.1 – 1400.3 series policy are included below:

Key Takeaways

1400.1

- In early 2021, UNC System President Peter Hans sent updated supplemental “Principles and Guidelines” to UNC System chancellors.
- The System Office RRB has been chartered and is operating for the UNC System Office and elements throughout the entire System.
- Each institution submitted their RRB charters to the UNC System Office

1400.2

- CIOs continue to indicate they are compliant with the requirements of this policy.

1400.3

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

1400.1 – IT GOVERNANCE

Overview

The two following questions are based on Section 1400.1 of the UNC Policy Manual:

- 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 Section 1400.1 at your institution?
- Can your organization produce an artifact that documents that designation?

Chancellor-named designate

100

PERCENT

Designation documented

100

PERCENT

Ownership and Accountability Structure-and-Process

All UNC System institutions are in the process of defining the IT governance oversight structure, approval processes, reporting lines, and organizational structure required by the IT Governance Charter. Almost all institutions felt they would be compliant 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?

70.6

Project Prioritization– Yes/In Process/Maturing

Does your institution document its IT project prioritization?

93.8

Strategic Plan Alignment – Yes/In Process/Maturing

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

76.5

PERCENT

Funding Approach – Yes/In Process/Maturing

Does your institution document its IT funding approach?

For all of the above questions, the majority of the estimated timeframes 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 CIOC views IT governance as a continuous improvement model.

Transparency and Collaboration

All UNC System institutions have worked with the CIOC and its subcommittees to define and reduce gaps, needs, and potential shared service opportunities. That collaboration is shown through institution involvement in the CIOC and its subcommittee structure: Shared Services for Hosted ERP Services/Remote DBAs (HISSC), Information Security Council (ISC), Shared Enterprise Applications & Services Committee (SEASC), and the Infrastructure and Operations Committee (I&O). This IT governance structure continues to see positive membership participation across all the institutions.

IT Policy Survey Additional Questions

Additional questions pertained the institutions conducting periodic self-monitoring and external monitoring, and internal audits, as well as the maintaining systems of accountability, and additional questions covered by 1400.1 – 1400.3 series policy. 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?

75
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?

100
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?

75
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?

88.2
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?

76.5
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 in the IT Governance Program Charter?

87.5
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?

76.5
PERCENT

Risk management requirements followed – Yes/In Process/Maturing

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

100
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?

1400.2 – INFORMATION SECURITY

Section 1400.2 of the UNC Policy Manual portion of the survey questions focuses on assessing whether an institution follows all 1400.2 policy components.

- 4.1) Has your institution designated a senior officer, accountable to the president or chancellor, who is responsible for information security? Do you have a written artifact to document designation?
- 5.1) 100 percent of the institutions received a final report of the MCNC Information Security Assessment of ISO 27002 controls in 2022.

100 percent of all UNC System institutions have designated a senior officer, accountable to the president or chancellor, who is responsible for information security.

1400.3 – USER IDENTITY & ACCESS CONTROL

3.1) In 2021, every UNC System institution reported user identity and access control program status in written form as required by the 1400.3 Standard (https://myapps.northcarolina.edu/it/system-wide-policies-guidelines/) to the CIO of the UNC System Office. Are you still on track with your roadmap produced to the UNC System Office CIO in 2022?

94.1 percent responded that they answered yes or commented that progress or incremental improvements have been made.

The policy requirement mandates multifactor authentication (MFA) for systems that access sensitive data. The UNC System institutions have more MFA implemented than ever before and this continues to improve. In March 2020, the System Office CIO issued the Standard as required by the policy. All institutions reported their compliance status to the System Office CIO as required by the Standard. Most institutions had gaps, often due to budgetary needs, but all have provided a written remediation plan and most reported resource and budget level deficits to close their remaining gaps.

COMPLIANCE AND MONITORING

The Risk Review Board (RRB) and CIO Council (CIOC) will continue to monitor compliance and any potential actions, per the requirement in Section 1400.1 of the UNC Policy Manual: *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.*

In the newly updated Principles and Guidelines of the IT Governance Charter, it states:

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 CIOC. These reviews will be conducted to ensure adherence to best practices, to the CIOC Strategic Plan, and to the policies of both the Board of Governors and each relevant Institution.

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

THE UNIVERSITY OF
NORTH CAROLINA SYSTEM

THE UNIVERSITY OF NORTH CAROLINA SYSTEM

2024 Annual Report on IT Policy Implementation

Report in Board Materials

Kim Smodic
UNC System Office
Chief Information Security Officer

2024

2024 Annual CIO Survey Update

Executive Summary

1400.1 (IT Governance)

1400.2 (Information Security)

1400.3 (Identity & Access Mgmt.)

- Annual Reporting required by policy to CARMC
- All institutions submitted timely
- Full compliance with 1400.2
- Institutions leveraging risk management functions for IT
- Substantive IT Governance maturity continues

Note: Written Report in Board Materials

QUESTIONS?