May 24, 2023 at 10 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 and Closed Session Minutes of February 22, 2023	Terry Hutchens
A-2.	Presentation of Audit Reports from the Office of the State Auditor	Beth Wood, State Auditor
A-3.	Enterprise Risk Management Update a. UNC System Office Risk Register Process	Bryan Heckle
A-4.	Report on Strategic Pathways for Campus Law Enforcement Personnel a. EHRA LEO Implementation Status Update	Fred Sellers
A-5.	Cybersecurity Recommendations & System-wide Security a. Update on Cybersecurity Recommendations	Kim Smodic
A-6.	Annual Report on Implementation of UNC Information Technology Policies a. 2023 Annual Report on Implementation of UNC Information Technology Policies	Kim Smodic
A-7.	Adjourn	

DRAFT MINUTES

February 23, 2023 at 3 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: Jimmy D. Clark, Lee Roberts, Kirk Bradley, Art Pope, and Pearl Burris-Floyd.

Chancellors participating were Sharon L. Gaber and Darrell T. Allison.

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)

Chair Hutchens called the meeting to order at 3:02 p.m. on Wednesday, February 22, 2023, and called for a motion to approve the open session minutes of November 16, 2022.

MOTION: Resolved, that the Committee on Audit, Risk Management, and Compliance approve the open session minutes of November 16, 2022, as distributed.

Motion: Lee Roberts
Motion carried

2. UNC System Office Internal Audit Plan Revision (Item A-2)

Michael Ptasienski provided information to the committee on modifications that were made to the 2022-23 internal audit plan due to current staffing changes with the internship program.

This item was for informational only.

3. Audit Reports Issued by the Office of the State Auditor (Item A-3)

Mr. Ptasienski outlined to the committee that the Audit Report Issued by the Office of the State Auditor identified 16 financial statement audit reports on the UNC System for the 2022 fiscal year.

This item was for informational only.

4. Summary Report of Major Associated Entities (Item A-4)

Mr. Ptasienski provided the Summary Report of Major Associated Entities. As of June 30, 2021, there were 92 major Associated Entities subject to the reporting requirements in Section 600.2.5.2[R] of the UNC Policy Manual, *Regulation on Required Elements of University-Associated Entity Relationship*. All associated entities received opinions from audit firms that were in good standing with the NC State Board of CPA Examiners. All had unmodified opinions except one entity which had a modified opinion. Two associated entities had one or more audit findings.

This item was for informational only.

5. Report on Strategic Pathways for Campus Law Enforcement Personnel (Item A-5)

Fred Sellers reported that, over the past 18 months, the UNC System has worked strategically with all UNC System institutions campus police departments to redesign the classification and compensation system for campus police officers. This is an initiative previously briefed to the University of North Carolina Board of Governors to minimize an enterprise risk of campus safety due to high law enforcement vacancy rates. As of January 2023, six of the UNC campus police agencies have implemented the new classification and compensation program. Seven others are projecting to implement the new compensation program by March 31, 2023. The remaining campus police agencies will implement the new classification standards and compensation program by June 30, 2023.

This item was for informational 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) and (3) of the North Carolina General Statutes.

Motion: Lee Roberts
Motion carried

THE MEETING MOVED INTO CLOSED SESSION AT 3:38
(The complete minutes of the closed session are recorded separately.)

THE MEETING RESUMED IN OPEN SESSION AT 3:53 p.m.

There being no further business and without objection, the meeting adjourned at 3:54 p.m.

_____
Lee Roberts, Secretary

AGENDA ITEM

A-2. Presentation of Audit Reports from the Office of the State Auditor ..... Beth Wood, State Auditor

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 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 conducts annual financial statement audits at each institution, 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 FY2023, the Office of the State Auditor has released 18 financial statement audit reports related to UNC System institutions for the 2022 fiscal year. In addition, the Office of the State Auditor also released three statewide federal compliance audits. The audit results have been summarized for the committee in the attachment.

Action: This item is for information only.

ATTACHMENT

Office of the State Auditor (OSA) Reports issued in FY2023 (to-date)

Financial Statement Audits for FY2022			
Institution Name	**Report Link**	**Release Date**	**# of Findings**
Appalachian State University	FIN-2022-6080	12/8/2022	0
East Carolina University	FIN-2022-6065	11/16/2022	0
Elizabeth City State University	FIN-2022-6086	12/9/2022	0
Fayetteville State University	FIN-2022-6088	12/2/2022	0
North Carolina Agricultural and Technical State University	FIN-2022-6070	12/9/2022	0
North Carolina Central University	FIN-2022-6090	1/13/2023	0
North Carolina State University	FIN-2022-6030	11/15/2022	0
North Carolina School of Science and Mathematics	FIN-2022-6094	3/9/2023	0
University of North Carolina at Asheville	FIN-2022-6055	10/28/2022	0
University of North Carolina at Chapel Hill	FIN-2022-6020	11/29/2022	0
University of North Carolina at Charlotte	FIN-2022-6050	11/16/2022	0
The University of North Carolina at Greensboro	FIN-2022-6040	11/9/2022	0
The University of North Carolina at Pembroke	FIN-2002-6082	12/14/2022	0
University of North Carolina School of the Arts	FIN-2022-6092	11/30/2022	0
University of North Carolina System Office	FIN-2022-6010	3/23/2023	0
University of North Carolina Wilmington	FIN-2022-6060	11/10/2022	0
Western Carolina University	FIN-2022-6075	11/14/2022	0
Winston-Salem State University	FIN-2022-6084	12/15/2022	0

Federal Compliance Audit Reports			
Institution Name	**Report Link**	**Release Date**	**# of Findings**
The University of North Carolina at Pembroke	FSA-2022-6082	4/13/2023	0
Western Carolina University	FSA-2022-6075	4/12/2023	0
The University of North Carolina at Charlotte	FSA-2022-6050	4/11/2023	0

AGENDA ITEM

A-3. Enterprise Risk Management Update .....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 UNC 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 process ongoing at the UNC System Office and the constituent institutions.

Action: This item is for information only.

THE UNIVERSITY OF NORTH CAROLINA SYSTEM

ENTERPRISE RISK MANAGEMENT

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

UNC Policy Manual

(1300.7)

Subject to the direction of the president, each constituent institution shall establish an enterprise risk management process that aligns with the institution's programs, activities, and management systems and that supports the institution's strategic and other goals.

The enterprise risk management processes established at each constituent institution shall include components and appropriate procedures for:

- ✓ Identifying risks that impact the constituent institution's goals
- ✓ Developing plans to monitor and mitigate risks
- ✓ Providing periodic updates to the chancellor and the board of trustees
- ✓ Reporting significant enterprise risks to the president, and with the president's guidance, to the Board of Governors

<u>UNC System Enterprise Risk Management Process</u>

1. Annual Identification of Risks
2. Ranking to Identify the Top Risks
3. Submission to the System Office
4. Compilation of Results
5. Grouping and Summarization of Risk Topics
6. Annual Reporting to the President and CARMC
   - The listed risk were reported to the CARMC in September 2022
     - Cyber Security
     - Talent Management
     - Student Retention
     - Financial
     - Facilities Maintenance
     - Regulatory Compliance
     - Business Process
     - Mental Health & Public Safety

System Office Risk Register Process

1. Meetings with Senior VP's and risk owners to discuss existing risk register and new or emerging risks
2. Provide a summary of risks as reported by divisions to the Risk Review Board for approval
3. Develop and present the approved Risk Register for the System Office risks to the CARMC

UNC Constituent University Process

1. Each university reports their top 5 risks to the System Office once approved by the BOT
2. Top 5 risks from each university is 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

AGENDA ITEM

A-4. Report on Strategic Pathways for Campus Law Enforcement Personnel ....Fred Sellers

Situation: Each UNC System institution maintains a police department staffed by sworn officers and headed by a police chief. In addition to performing traditional law enforcement functions, university police departments require special training and skills to work in and meet the unique public safety needs of the academic communities in which our students, faculty, and staff collaborate and interact.

Background: Preserving public safety on our university campuses requires adequate staffing, resources, training, and ensuring each campus has the operational readiness for the daily rigors of law enforcement activities. UNC System institutions continually seek ways to collaborate and leverage the benefits of the UNC System in these areas. With support from the committee in February 2021, the UNC System Office implemented several initiatives and strategies as options to attract and preserve the necessary public safety resources needed for each university police department.

Assessment: Over the past 18 months, the UNC System has worked strategically with all UNC System institutions with a Campus Police Department to redesign the classification and compensation system for campus police officers. This is an initiative briefed and supported by the University of North Carolina Board of Governors to minimize an enterprise risk of campus safety due to high law enforcement vacancy rates.

Action: This item is for information only.

THE UNIVERSITY OF NORTH CAROLINA SYSTEM

LAW ENFORCEMENT INITIATIVE UPDATE

UNC BOG Committee on Audit & Risk Management

Fred Sellers

VP Safety & Enterprise Risk Management

May 24, 2023

Goal

- With direction from the Board of Governors, help address campus police department recruitment and retention challenges through:
  1. Major redesign of classification and compensation system for campus police officers
  2. Career progression ladders
  3. Additional educational benefits
- July 1, 2023: All UNC police officers will become EHRA employees and no longer governed by the state agency personnel system which provides us with significantly enhanced HR flexibility

Recap

- **June 2020** – General Assembly authorized EHRA classification for campus law enforcement officers (S.L. 2020-56, Sec. 7)
- **February 2021** –
  - CARMC briefed on need for major redesign of LEO classification and compensation structure to help address campus police department recruitment and retention challenges
  - Board of Governors approved $30 increase in campus security fee to support LEO salaries, student counseling and suicide intervention, and other campus safety initiatives
- **CY 2021** – System Office developed LEO EHRA classification and compensation structure based on extensive market research and campus input
- **May 2022** – Board of Governors delegated authority to President to implement LEO EHRA program
- **July 2022** –
  - President Hans issued implementing regulation (300.2.21[R])
  - SO issued final LEO EHRA classification and compensation structure **with implementation deadline of 6/30/2023**

Status and Next Steps

- As of May 19, 2023, **12** of the UNC campus police agencies have implemented the new compensation program
  - NC Arboretum receives no funding from the Board of Governors approved $30 increase in campus security fee to support LEO salaries; however, they moved forward with the major redesign of classification and compensation system for campus police officers
- **Five** campuses are projecting to implement the new compensation program by either June 1 or June 30, 2023
- **100% implementation by all 16 campuses and NC Arboretum.**
- As of June 2023, the *average* starting salary for entry-level officers will be **$45.5K** prior to graduating the police academy and **$51K** for those who have completed academy training and are state certified

QUESTIONS?

AGENDA ITEM

A-5. Update on Cybersecurity Recommendations…… ..... Kim Smodic

Situation: The purpose of this item is to provide the Committee on Audit, Risk Management, and Compliance (CARMC) an update on the May 2022 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 NC Office of the State Auditor has concluded six IT control audits on student data that have yielded consistent findings. Additionally, the UNC System brokered a systemwide third party assessment with MCNC to develop baselines. In response, the CARMC requested that the UNC System Office develop a set of recommendations to address this issue with appropriate corrective actions. The UNC System Office Risk Review Board, in consultation with the CIO Council, drafted a series of recommendations presented in open and closed sessions in May 2022. These recommendations were approved and subsequently included in the legislative budget request.

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. This portion of the presentation focuses on the cybersecurity budget and proposed action in the following areas: vendor risk management, incident response, continuous monitoring, log collection and management, on-going improvements, and available resources.

Action: This item is for information only

THE **UNIVERSITY** OF
NORTH CAROLINA SYSTEM

A-5: Information Security Maturity Model

Update on Cybersecurity Recommendations

Kim Smodic
UNC System Office
Chief Information Security Officer

2023

Informing Recommendations and Budget

Recommendations designed to strategically and tactically improve cybersecurity posture, based on the following:

- Improve cybersecurity maturity of lower resourced institutions
- Learnings from OSA Audit and Compliance reports, themes include:
  - *Sensitive/Confidential Data Inventories (Classify Data)*
  - *Vulnerability Management*
  - *Configuration Management*
  - *Data Log Management*
  - *Vendor/Supplier Risk Management*
- Advanced persistent threats (APTs) by hackers
- Identified security deficiencies in systems
- Leverage/broker shared services

* ***Position UNC System and institutions to be proactive and cyber resilient***

CARMC Approved Recommendations	Additional Information
1. Cybersecurity Budget and CARMC Support	Annual exercise, aligned with legislative/budget cycles
2. Vendor Risk Management Program	Assessing risk of vendors in a shared and efficient manner
3. Training	Cybersecurity awareness training for faculty, staff and students. Professional development for information security staff.
4. Partnering and Managing Incident Response	Cyber Insurance and partnering with the NC Joint Cyber Task Force
5. Structured Information Sharing/ Shared Repository	Collaborative and structured approach to information sharing for policies, baselines, rules and regulations, vendor risk management assessments, and training
6. Continuous Monitoring (Detect and Prevent)	Security assessments, vulnerability scanning, threat management, testing and baselines
7. Data Log Management System	Collection of data/network logs for legal requirements, forensics, threat detection and monitoring

Services/Components to Protect Against Cyber Threats

- Vendor Risk Management (outsourcing services can expose us to potential adverse events such as data breach, operational disruption or reputational disruption – another company has our sensitive data)
- Systemwide Cyber Command
  - Central Log Management System
  - External/Perimeter Network Monitoring (24x7x365)
  - Internal Network Monitoring (IDS/IPS)
  - Threat Intelligence Feeds
  - Endpoint Detection and Response (EDR)
  - SIEM (Event Monitoring System)
- Cybersecurity Awareness Training (Staff/Faculty/Students)

2. Improving Vendor Risk Management Program

What: Vendors are increasing exponentially that store or transact with sensitive data within an organization. IT Departments are required to evaluate each vendor to ensure that the appropriate security controls are in place (SOC2 Type 2, FedRAMP, etc.). These reviews are to be continuously monitored, often annually.

Issue: This critical work requires extensive man-hours at every organization, with many struggling to equal the demand. Often there are extensive backlogs and extended timeframes for review, leaving the business unit anxious and impatient. The security resources that perform this work would be better served on true security related tasks. Often there is a considerable amount of back-and-forth communication from the organization to the vendor to acquire the necessary information. Institutions have historically stored all of their data on premise, however, with the introduction of cloud services and moving our data off premise, there are extensive risks that come with relinquishing control and protection of our most sensitive data and moving it from our data center to a vendor's data center. The vendor's data center may not be as secure as ours and may not meet compliance with UNC System policies, federal regulations, and state statutes UNC System is required to abide by.

Status: ***Pilot authorized for a centralized shared service VRM program. Specifically, this would include the acquisition of a VRM business automation tool, implementation of the tool and staff support.***

AUDIT THEME

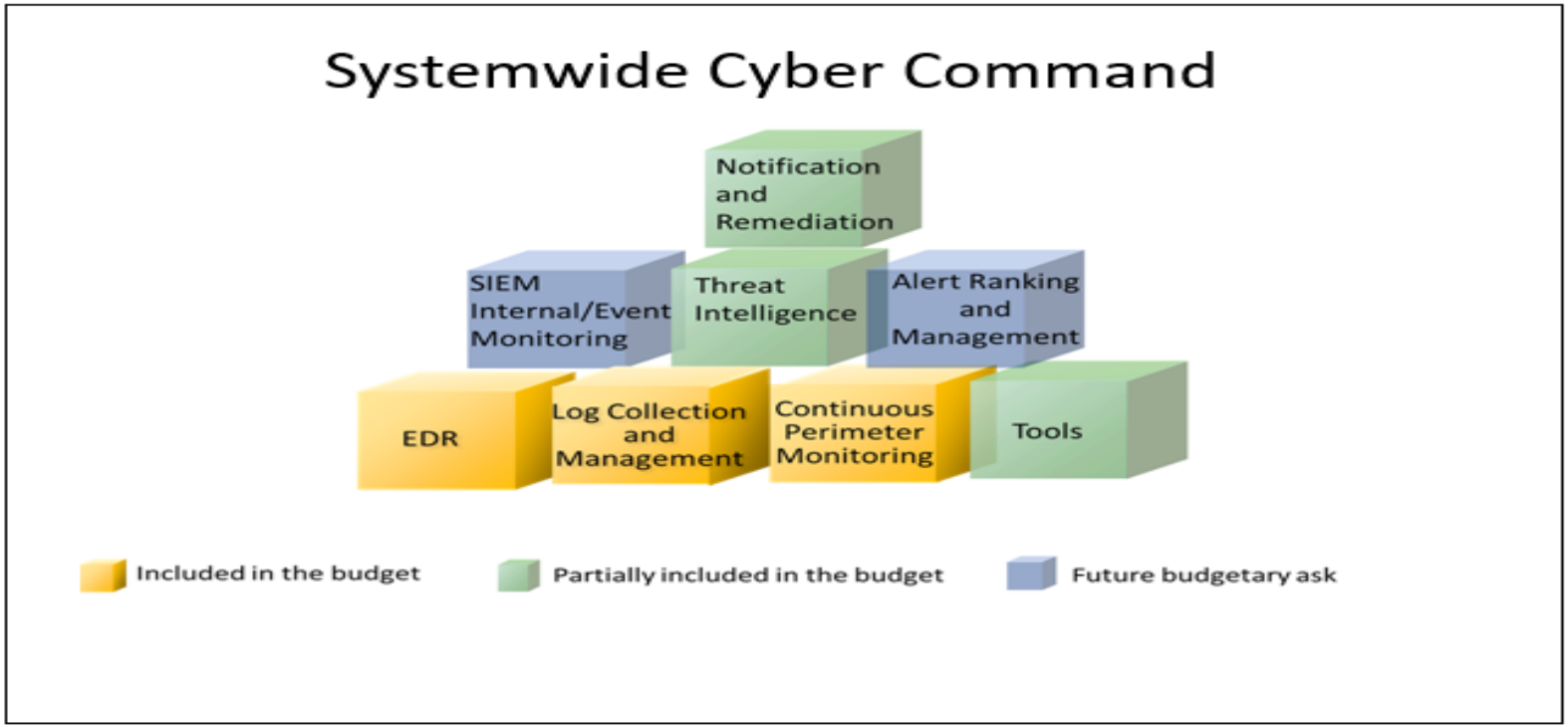
ISO27002 Control #15 Supplier Relationships

4. Partnership with Joint Cybersecurity Task Force (JCTF)

- In-process or completed security assessments and/or penetration tests – 7 institutions
- Number of incidents – 1 institution

- Working to get more institutions scheduled
- Extended lead times
- Alternatively, receiving scope/ quote from MCNC to augment JCTF network security assessments

6. Continuous Monitoring
7. Data Log Management System



THE UNIVERSITY OF NORTH CAROLINA SYSTEM

MEETING OF THE BOARD OF GOVERNORS
Committee on Audit, Risk Management, and Compliance
May 24, 2023

AGENDA ITEM

A-6. 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) with 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 IT Security Working Group (ITSWG) and CARMC, the Board adopted two additional policies in May 2018: Section 1400.1 of the UNC Policy Manual, *Information Technology 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 CIO Council and Risk Review Board approved a new IT Governance Charter, with Principles and Guidelines, that was sent to the Chancellors by President 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 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 are a requirement. A survey was sent to all institution CIOs in January 2023 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.

TABLE OF CONTENTS

FOREWARD

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 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 forwarding to all the UNC System chancellors.

In 2020, the UNC System Office chartered the Risk Review Board (RRB) and 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 2023 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 to confirm that an information security program is in place and that a senior officer, accountable to the chancellor, is responsible for information security. The new policies also describe oversight activities that will be undertaken by the UNC Board of Governors and the b oards 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; consistent governance and management of IT; encourage collaboration; and, 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 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 is an annual survey conducted based on the 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 aim to meet our objectives detailed in the IT Governance Charter.

2022 Survey Results Highlights

Compliance with 1400.1 – 1400.3 series policy continues to improve in maturity. In 2020, the CIO Council (CIOC) updated the IT Governance Charter, including updated 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. 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 multi-factor 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

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.

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?

70.

76.

Funding Approach – Yes/In Process/Maturing

Does your institution document its IT funding approach?

Strategic Plan Alignment – Yes/In Process/Maturing

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

93.

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 CIO Council (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, internal audits as well as the maintaining systems of accountability and additional questions covered by 1400.1 – 1400.3 series is a policy. Below is a snapshot of those responses.

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?

70.

100
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?

75
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.

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.

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

87.

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.

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

Does your institution follow privacy requirements described in the IT

76.

Risk Management requirements followed – Yes/In Process/Maturing

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

100

76.

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

relating to information technology matters, and addressed issues of importance in information technology governance on a

100
PERCENT

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. All but one have that as a written artifact.

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 multi-factor 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, 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 CIO Council (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 CIO Council 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.


N★C
THE UNIVERSITY OF
NORTH CAROLINA SYSTEM

A-6: 2023 Annual Report on IT Policy Implementation

Report in Board Materials

Kim Smodic
UNC System Office
Chief Information Security Officer

2023

2023 Annual CIO Survey Update

Executive Summary

1400.1 (IT Governance)

1400.2 (Information Security)

1400.3 (Identity & Access Mgmt.)

Note: Written Report in Board Materials

THE UNIVERSITY OF NORTH CAROLINA SYSTEM

- 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

Q&A

2023

Kim Smodic
Chief Information Security Officer

THE UNIVERSITY OF NORTH CAROLINA SYSTEM

Questions?