May 14, 2025 at 1:30 p.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 26, 2025 ..... Mark Holton

A-2. Summary of the UNC System FY 2025 Annual Audit Activities ..... Jennifer Myers

A-3. Research Security Update ..... Jennifer Gerz-Escandón
Angelica N. Martins

A-4. Annual Report on Implementation of UNC Information Technology Policies ..... Shannon Tufts

CLOSED SESSION

A-5. Approval of the Closed Session Minutes of February 26, 2025 ..... Mark Holton

A-6. Confidential Briefing on Campus Incident ..... Fred Sellers

OPEN SESSION

A-7. Adjourn

THE UNIVERSITY OF NORTH CAROLINA SYSTEM

MEETING OF THE BOARD OF GOVERNORS
Committee on Audit, Risk Management, and Compliance May 14, 2025

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).

MINUTES

February 26, 2025 at 11:30 a.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 Mark Holton. The following committee members, constituting a quorum, were also present in person or by phone: Woody White, Art Pope, Kirk Bradley, Carolyn Coward, and Kathryn Greeley.

Participating chancellors were Bonita Brown and Darrell Allison.

Staff members present included Fred Sellers, Jennifer Myers, Samantha Barbusse, 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 11:30 a.m. on Wednesday, February 26, 2025. The open session minutes from the November 13, 2024, meeting were approved by unanimous consent.

2. Purchase Cards Regulation (Item A-2)

President Peter Hans updated the committee with respect to purchase card usage on campuses. In November 2024, the president issued a new policy establishing requirements governing the use of purchase cards by UNC System employees. This new policy includes, among other things, specific procedures for issuing cards; annual training for all card holders; established monitoring, oversight, and reconciliation, and other provisions.

This item was for information only.

3. CARMC Charter and Internal Audit Committee Charter Updates (Item A-3)

Jennifer Myers presented the revised and updated charters for Internal Audit and CARMC. Effective January 9, 2025, the Institute of Internal Auditors revised their Global Internal Audit Standards. To comply with the new standards, revised charters for both CARMC and Internal Audit were reviewed and approved by the committee.

This item required a vote by the committee, with a vote by the full Board of Governors through the consent agenda.

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

Jennifer Myers presented on the audit reports issued to date by the Office of the State Auditor. The OSA released 13 financial statement audit reports related to the UNC System for Fiscal Year 2024. Of the completed reports, there were no audit issues found.

This item was for information only.

5. Summary of the UNC System FY 2025 Annual Audit Activities (Item A-5)

Ms. Myers further briefed on the UNC System Office Internal Audit Plan progress as of December 31, 2024. Six audits and special projects have been completed, and four audits and special projects are in process.

This item was for information only.

6. Cybersecurity Partnerships (Item A-6)

Chris Beal, chief information security officer at Microelectronics Center of North Carolina (MCNC), presented on the status of MCNC's cybersecurity partnerships with our UNC System institutions. The goal of MCNC is a partnership for protection that should be affordable and accessible. He illustrated how the partnership has helped our institutions identify and protect cyber assets, detect significant activity, and respond to identified threats. The UNC System has realized significant benefits from the MCNC partnership, especially at the smaller institutions.

This item was for information only.

7. 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 G.S. 143-748 of the North Carolina General Statues, 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.

Motion: Woody White
Motion carried

THE MEETING MOVED INTO CLOSED SESSION AT 12:06 p.m.
(The complete minutes of the closed session are recorded separately.)

THE MEETING RESUMED IN OPEN SESSION AT 12:31 p.m.

Adjourn

There being no further business, and without objection, the meeting adjourned at 12:32 p.m.

_____

Art Pope, Secretary

THE UNIVERSITY OF NORTH CAROLINA SYSTEM

MEETING OF THE BOARD OF GOVERNORS
Committee on Audit, Risk Management, and Compliance
May 14, 2025

AGENDA ITEM

A-2. Summary of the UNC System FY 2025 Annual Audit Activities..... Jennifer Myers

Situation: The Chief Audit Officer provides periodic updates on the UNC System Office's internal audit activities.

Background: In accordance with the committee charter and IIA's Global Internal Audit Standards, the committee is to receive periodic updates on the UNC System Office's internal audit activities. This allows the committee to assess Internal Audit's performance relative to the approved annual Audit Plan.

Assessment: The attached document identifies the status of the FY'25 Internal Audit projects as of April 30, 2025.

Action: This item is for information only.

UNC System Office
Internal Audit Plan Progress as of 4/30/2025
Fiscal Year 2025

Audit Activity	Budgeted Hours FY'25	*Actual Hours FY'25	% Utilized	Status
Prior Year Carry-Over				
PBS NC IT Contracting & Vendor Management Audit	80	77	96%	*Completed*
System Office IT Contracting & Vendor Management Audit	13	13	100%	*Completed*
Assurance Engagements				
ACH Change Processes Audit	160	57	36%	*Completed*
Campus Billing Processes Audit	240	0	0%	Not Started
Campus Data Quality Audit	720	142	20%	In-Process
Advisory Engagements				
Annual P-Card Compliance (System Office)	50	39	78%	*Completed*
Annual P-Card Compliance (PBS NC)	50	32	64%	*Completed*
Unplanned	0	3	-100%	As Needed
Follow-Up on Management Corrective Actions				
• PBS NC PCI Compliance Review • PBS NC IT Contracting & Vendor Management • System Office IT Contracting & Vendor Management • System Office ACH Change Processes	100	0	0%	Not Started
Investigations				
Unplanned/Various	50	0	0%	As Needed
Special Projects				
Annual Risk Assessment & FY'25 Audit Plan Development	100	103	103%	*Completed*
Annual Risk Assessment & FY'26 Audit Plan Development	0	16	-100%	In-Process
Charter Review & Update Policies to Align with New IIA Standards	80	314	393%	*Completed*
Other Special Projects	0	549	-100%	As Needed
Participation in OSBM Peer Review Process	120	0	0%	Not Started
Technical Assistance as Requested	50	92	184%	As Needed
UNCAA Conference Planning	20	13	65%	*Completed*
Other Hours				
Admin: Oversight, Hiring, MOU Updates, Misc.	207	533	257%	Ongoing
Holidays & Staff Leave	936	796	85%	Ongoing
Internal Audit Hotline Management	40	60	150%	Ongoing
NC Council on Internal Auditing Reporting Requirements	200	47	24%	Ongoing
Other Services: Routine Advisory Services, Assist External Auditors, QAIP Work, Other Projects as Determined, Misc.	100	187	187%	Ongoing
Outreach & Coordination with Other UNC System IA Groups	78	59	76%	Ongoing
Preparation for Board Meetings & Meeting Attendance	454	265	58%	Ongoing
Professional Development	120	361	301%	Ongoing
FY'25 Total Hours to UNC System Office:	3,968	3,758		
Internal Audit Shared Services				
Internal Audit Services to NCSEAA	760	451	59%	Ongoing
Internal Audit Services to NCSSM	1,512	858	57%	Ongoing
FY'25 Total Hours to MOUs:	2,272	1,309		
Total Hours:	**6,240**	**5,067**		

**Hours have been rounded to the closest whole number*

UNC System Office
Internal Audit Plan Progress as of 4/30/2025
Fiscal Year 2025

Highlights

Risk Assessment and Internal Audit Plan Development

The first part of fiscal year 2025 was spent performing risk assessments across the UNC System Office, North Carolina State Education Assistance Authority (*NCSEAA*), and North Carolina School of Science and Mathematics (*NCSSM*). This information was utilized to develop the FY'25 Internal Audit Plan, which was approved by the CARMC in September. However, due to the new P-Card regulations and requirements issued in November 2024, Internal Audit added this new annual engagement to the FY'25 Internal Audit Plan.

New Auditing Standards

Effective January 9, 2025, the Institute of Internal Auditors (*IIA*) implemented revised auditing standards known as the Global Internal Audit Standards (*Standards*). These Standards include 15 principles that are the worldwide guide for the professional practice of internal auditing. To conform to the new Standards, the Internal Audit team at the UNC System Office updated their charters, both the Internal Audit Charter and the CARMC Charter, revised the Internal Audit Manual, and updated all templates accordingly.

THE UNIVERSITY OF NORTH CAROLINA SYSTEM

MEETING OF THE BOARD OF GOVERNORS
Committee on Audit, Risk Management, and Compliance
May 14, 2025

AGENDA ITEM

A.3 Research Security Update ..... Dr. Jennifer Gerz-Escandón and Dr. Angelica Martins

Situation: The purpose of this item is to provide the Committee on Audit, Risk Management, and Compliance (CARMC) with a recap of activity to safeguard science Systemwide and an overview of the research security program at the University of North Carolina at Charlotte.

Background: Since the issuance of National Security Presidential Memorandum 33 (NSPM 33) in January 2020, federal agencies have issued new and updated regulations targeting the security of federally funded research. These regulations impact several compliance areas, including export controls, international travel, standard disclosure requirements, and cybersecurity. Constituent universities within the UNC System that receive at least $50 million in annual federal science and engineering support will be required to implement a formal research security program, but all universities within the System can benefit from implementing elements of a research security program that apply to their research portfolio and the associated risks.

Assessment: Research security program standards consist of broadly applicable existing laws and regulations, as well as new requirements. UNC System chief research officers have shown exemplary leadership in implementing these standards and safeguarding scientific discovery and innovation by fostering informed and accountable campus cultures, implementing robust processes, and promoting collaborative efforts to ensure research security and federal regulatory compliance. Constituent institutions are dedicated to maintaining partnerships that leverage both internal expertise and external collaborations.

Action: This item is for information only.

CHARLOTTE
DIVISION OF RESEARCH

Research Security Overview: Collaborating to Safeguard Science

Angelica N. Martins, Ph.D.

Assistant Vice Chancellor for Research Protections and Integrity

May 14, 2025

THE UNIVERSITY OF NORTH CAROLINA SYSTEM

Research Security Program Areas

UNC Charlotte

Foreign Travel Security

- International Travel Pre-Review
- Personal International Travel with University-Owned Equipment Review

Cybersecurity

- CUI Compliant Environment (NIST 800-171)

Conflict of Interest and Commitment

- COI and COC Disclosures in NR
  - Paid and Unpaid Relationships and Affiliations Since 2020
- Research Security Review of External Professional Activities and Foreign Financial Support
- Prohibition to Participate in MFTRP
- Revision of COI/COC Policy

Export Control

- Visa Sponsorship Review
- Technology Control Plans
- Sponsored Guest Accounts Review (FN)
- University-Owned Equipment Taken Abroad Review
- International Collaborations Review
- Restricted Party Screening

Training

- Export Control
- International Travel
- Undue Foreign Influence
- Research Security

- Prohibition to Engage or Enter Agreements with Entities of Concern
- International Shipping and Materials Transfer

Current Practice
Under Development

Thank you! It Takes a Village

Foreign Travel Security

- Academic Affairs
  - Office of International Programs
- Institutional Integrity
- Business Affairs
- OneIT

Conflict of Interest and Commitment

- Academic Affairs
  - J. Murrey Atkins Library
- Institutional Integrity
- University Advancement
- OneIT

Export Control

- Academic Affairs
  - Office of International Programs
  - International Student and Scholar Office
- Business Affairs
  - Materials Management
- Institutional Integrity
- University Advancement
  - University Communications
- OneIT

Training

- Academic Affairs
- OneIT

Cybersecurity

- OneIT

Division of Research

- Office of Research Services (ORS)
- Office of Research Protections and Integrity (ORPI)
  - Mr. Saul Sotolongo (Research Security Coordinator)
  - Ms. Lacy Kitchin (Export Control Officer)
  - Ms. Sherry Loyd (COI Officer)

THE UNIVERSITY OF NORTH CAROLINA SYSTEM

MEETING OF THE BOARD OF GOVERNORS
Committee on Audit, Risk Management, and Compliance
May 14, 2025

AGENDA ITEM

A-4. Annual Report on Implementation of UNC Information Technology Policies .....Dr. Shannon Tufts

Situation: This item presents the Committee on Audit, Risk Management, and Compliance (CARMC) with the annual report on the implementation status of the UNC System's 1400 Series Information Technology policies. The briefing provides a summary of institutional compliance, a year-end review of cybersecurity investments and improvements, and future considerations for IT and cybersecurity investment across the UNC System

Background: Chapter 1400 of the UNC Policy Manual includes three primary policies: Section 1400.1, *Information Technology Governance*; Section 1400.2, *Information Security*; and Section 1400.30, *User Identity and Access Control*. In 2024, Section 1400.1[R], *Regulation Regarding Anonymous, Hyperlocal Platforms*, was adopted to ensure UNC System institutions blocked access to specified high-risk anonymous, hyperlocal sharing platforms. These policies were developed to ensure a Systemwide approach to managing enterprise IT and cybersecurity risks, aligning governance with strategic objectives, and safeguarding university information assets.

Assessment: The 2025 compliance review confirmed continued efforts to adhere to the Chapter 1400 policies in the UNC Policy Manual. Under Section 1400.1, every institution has appointed a senior leader responsible for IT governance, with continuous improvements and structural adjustments actively underway. Regarding Section 1400.1[R], all institutions have implemented either formal user acceptance policies or technical controls to block access to anonymous, hyperlocal platforms. For Section 1400.2, all campuses have designated an information security officer (i.e., CIO, CISO, etc.) and are actively progressing with formalized security programs aligned with System expectations. Similarly, Section 1400.3 demonstrates widespread implementation of core identity and access management (IAM) components across all institutions, including widespread adoption of multifactor authentication (MFA). Further expansion of identity and privileged access management capabilities is currently in progress.

Across the System, institutions have made meaningful advancements in key cybersecurity domains. Campuses have broadly deployed next-generation endpoint protection and network management tools and increased the use of security information and event management (SIEM) solutions for log aggregation and analysis.

There has been an increase in Systemwide threat intelligence sharing and incident response efforts, including improved handling of malware, credential compromise, business email compromise (BEC), and token hijacking. All institutions have adopted Systemwide baseline requirements pursuant to ISO 27002:2022, and several are utilizing governance, risk & compliance (GRC) tools, along with specific IT contract terms and conditions. Institutions have implemented targeted strategies to enhance defenses against phishing and BEC attacks. Security awareness and education efforts have expanded significantly, with broad participation in simulated phishing campaigns, student outreach, and training for faculty and staff. Finally, campuses have strengthened their incident response plans and penetration testing capabilities, while the UNC System Office continues to offer threat hunting, forensic support, policy development, and coordination assistance.

Looking forward, both individual institutions and the UNC System Office are evaluating future cybersecurity efforts with an emphasis on assessing return on investment from existing initiatives, while capitalizing on opportunities to leverage collaborative security solutions. Strategic decisions are also being shaped by the CIO Council and the Information Security Council, findings from internal and external IT audits, the need to adapt to changing regulatory requirements, and the necessity to respond effectively to a continuously evolving threat landscape.

Action: This item is for information only.

THE UNIVERSITY OF NORTH CAROLINA SYSTEM

A-4: Annual Report on Implementation of UNC Information Technology Policies

Shannon Tufts, Ph.D.
Senior Advisor on Cybersecurity, UNC System
NC Joint Cybersecurity Task Force Member
Professor, UNC School of Government

2025

1400 Series Compliance Review

1400.1. Information Technology (IT) Governance

- **100%** designated senior leader responsible for IT Governance

1400.1[R]. Regulation Regarding Anonymous, Hyperlocal Platforms

- **100%** implementation of user acceptance policies and/or technical controls to block access to specified anonymous, hyperlocal platforms

1400.2. Information Security

- **100%** designated senior officer responsible for IT security (i.e., CIO, CISO) with ongoing adoption & maintenance of security programs

1400.3. User Identity and Access Control

- **100%** implemented components of identity & access management, including widespread use of multifactor authentication and layered defense strategies

Year in Review

UNC System + Institutional-Specific Efforts

Endpoint & Network Security

- ✓ Broad deployment of advanced endpoint & network security solutions, allowing for proactive, rapid response

Threat Detection & Monitoring

- ✓ Improved threat intelligence, awareness & mitigation
- ✓ Increased use of security event analytic solutions

Email & Communication Security

- ✓ Enhanced defenses against malicious emails, including phishing and spam

Incident Response

- ✓ Maturing incident response plans & practices with real-time testing and validation
- ✓ Supplemental incident response support via UNC System & NC JCTF

Security Awareness & Education

- ✓ Widespread adoption across all campus populations

Governance, Policy & Risk

- ✓ Expansion of shared services & resources
- ✓ Continued partnership with institutional risk management

Future Efforts for Consideration

Guiding Investment Strategies

- Response to shifting threat landscape
- Changing compliance requirements and regulations
- Demand for shared services
- Identified institutional needs
- IT audit findings
- Evaluation of existing investments

System-Wide Status Platform

Continuous Security Assessments

GRC Solutions

Shared Cybersecurity Staff

Enterprise Agreements

Shared Repositories

Advanced Threat Protection