



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

March 20, 2018 at 2:00 p.m.
University of North Carolina System Office
Spangler Center, Executive Conference Room
Chapel Hill, North Carolina

AGENDA

OPEN SESSION

- A-1. [Approval of the Minutes of January 25, 2018](#)Jim Holmes
- A-2. [Review of Draft Policies](#)Jim Holmes
 - a. Information Technology Governance
 - b. User Identity and Access Control
- A-3. [Review of Charters](#).....Joyce Boni and Lynne Sanders
 - a. Internal Audit Charter
 - b. CARMC Charter

CLOSED SESSION

- A-4. Approval of the Closed Session Minutes
of November 2, 2017; December 12, 2017; and January 25, 2018.....Jim Holmes
 - a. November 2, 2017
 - b. December 12, 2017
 - c. January 25, 2018
- A-5. Legal and Audit UpdateTom Shanahan and Lynne Sanders

OPEN SESSION

- A-6. Other BusinessJim Holmes
- A-7. Adjourn

DRAFT MINUTES

January 25, 2018
University of North Carolina System
Center for School Leadership Development, Room 119
Chapel Hill, North Carolina

This meeting of the Committee on Audit, Risk Management, and Compliance was presided over by Chair Jim Holmes. The following committee members, constituting a quorum, were also present in person: Kellie Hunt Blue, Carolyn Coward, and William Webb. The following committee members were absent: Walter Davenport.

Chancellors participating were Jose Sartarelli and Joseph Urgo.

Staff members present included Lynne Sanders, Tom Shanahan, and others from the UNC System Office.

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

Chair Holmes called the meeting to order at 3:50 p.m., on Thursday, January 25, 2018, and called for a motion to approve the open session minutes of December 12, 2017.

MOTION: Resolved, that the Committee on Audit, Risk Management, and Compliance approve the open session minutes of December 12, 2017, as distributed.

Motion: William Webb

Motion carried

2. UNC System Insurance Coverage (Item A-2)

Bryan Heckle, director of risk management at the NC Department of Insurance (NCDOL), presented to the committee an overview of the types of coverage available to state entities through the NCDOL. Mr. Heckle summarized how the University is insuring risks for UNC System institutions and activities.

3. Information Technology (Item A-3)

Steven Hopper, CIO transition advisor, provided the committee with an overview on information technology governance and risk management related to cybersecurity. The committee recommended that a special group be appointed to identify information technology security issues at the University.

4. UNC System Internal Audit Update (Item A-4)

Joyce Boni, chief audit officer, presented to the committee a status update on the 2017-18 internal audit projects that were initially approved by the committee in September 2017.

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; consult with our attorney to protect the attorney-client privilege; pursuant to Chapter 143-318.11(a)(1) and (3) of the North Carolina General Statutes.

Motion: William Webb

Motion carried

THE MEETING MOVED INTO CLOSED SESSION.

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

There being no further business, the meeting adjourned at 4:49 p.m.

William Webb, Secretary

AGENDA ITEM

A-2. Review of the Information Technology Governance PolicyJim Holmes

Situation: The University of North Carolina and each of the constituent institutions depend on strategic and coordinated governance and management of information technology to fulfill the University's mission. The University's information technology and information resource needs continually evolve as new challenges, opportunities, and technologies emerge.

Background: IT governance within the UNC System is grounded in the UNC System governance framework. Each chancellor is the executive head of the constituent institution, and responsible to the president for the administration of information technology governance in accordance with the policies established by the Board.

Assessment: The purpose of this policy is to foster the development and maintenance of strategically aligned information technology within known and acceptable levels of risk; to ensure an effective and consistent governance and management of information technology at each of the constituent institutions; and to encourage collaboration and shared service arrangements in areas of information technology management, where appropriate, among and between the constituent institutions and the UNC System Office. The policy provides that the president shall oversee an information technology governance program applicable to the UNC System and the constituent institutions. The program shall be developed, implemented, and maintained, subject to the president's approval, by the UNC System's chief information officer. Each constituent institution shall establish an information technology governance program with policies, processes, structures, and standards consistent with the UNC System's information technology governance program. The UNC System Office chief information officer shall work with the UNC System Office finance, audit, and legal staff, to establish the process and criteria by which a constituent institution shall demonstrate that it is operating in accordance with the UNC System's information technology governance program. The Board of Governors and the board of trustees of each constituent institution shall assign responsibility for oversight of IT governance to a standing committee of the board with audit responsibility.

Action: This item requires a vote by the committee, with a vote by the full Board of Governors through the consent agenda at the next meeting.

Information Technology Governance

I. Purpose. The University of North Carolina and each of the constituent institutions depend on strategic and coordinated governance and management of information technology to fulfill the University's mission. The University's information technology and information resource needs continually evolve as new challenges, opportunities, and technologies emerge. Consistent with the governance and oversight responsibilities of the Board of Governors, the executive and administrative responsibilities of the president and the chancellors of the constituent institutions, and the role of the boards of trustees, as described in *The Code of The University of North Carolina*, the Board adopts this policy delegating and allocating authorities and responsibilities concerning information technology governance within the University of North Carolina System.¹

The purpose of this policy is to foster the efficient development and maintenance of strategically aligned information technology within known and acceptable levels of risk; to ensure an effective and consistent governance and management of information technology at each of the constituent institutions; and to encourage collaboration and shared service arrangements in areas of information technology management, where appropriate, among and between the constituent institutions and the University of North Carolina System Office (UNC System Office).

II. Definitions

- A. "Board of Governors" or "Board" means the Board of Governors of the University of North Carolina.
- B. "Board of Trustees" means a board of trustees of a constituent institution of the University of North Carolina System.
- B. "Chancellor" means the administrative and executive head of a constituent institution of the University of North Carolina, as described in Section 502 of *The Code*.
- C. "Constituent Institution" means one of the 17-degree/diploma-granting institutions that comprise the University of North Carolina.
- D. "Information resources" means information owned or possessed by the University, or related to business of the University, regardless of form or location, and the hardware and software resources used to electronically store, process, or transmit that information.

*Supersedes Section 1400.1 originally entitled, "The Use of Information Technology," adopted November 12, 2004.

¹ G.S. 116-11(13); Section 203 A(9) of *The Code*.

E. “Information technology” means the hardware and software resources owned, leased, or used by the University and its partners to store, process, or transmit University information. Information technology is a subset of the University’s information resources.

F. “Information technology governance” within the UNC System refers to the framework, policies, rules, standards, structures, and processes established to ensure that the University’s information technology supports the missions, goals, and objectives of the UNC System and each constituent institution; that information technology and information resources are properly managed in accordance with rules and policies; and that risks and threats to information technology and information resources are appropriately and effectively identified and addressed. IT governance encompasses the planning, prioritization, funding, acquisition, implementation, maintenance, evaluation, auditing, and security of information technology and information resources at each constituent institution and across the UNC System.

G. “President” means the chief administrative and executive officer of the University of North Carolina, as described in Section 501 of *The Code*, who reports to the Board of Governors. The president is responsible for executing the board’s policies directly, through the chancellors, and through the staff who report to the president.

H. “University” or “University of North Carolina System” or “UNC System” means the University of North Carolina, a body politic and corporate defined as a single public multi-campus University composed of 17 constituent institutions, the UNC System Office, and other educational, research, and public service organizations.

III. UNC System IT Governance Program Development; Principles and Standards.

A. The president shall oversee the information technology governance program applicable to the UNC System and the constituent institutions.

B. The UNC System information technology governance program shall be developed, implemented, and maintained, subject to the president’s approval, by the UNC System’s chief information officer, who shall establish and update the program principles and standards on a regular basis in consultation with the UNC Chief Information Officer Council. The details of the information technology governance program and standards shall be confidential and not considered a public record to the extent permitted by North Carolina law.

C. The information technology governance program shall:

1. Define a framework or frameworks to be implemented by constituent institutions;

2. Include a set of principles and standards addressing planning, prioritization, funding, acquisition, implementation, maintenance, evaluation, auditing, disaster recovery, privacy and security of information technology and information resources, risk assessments, risk management, oversight of distributed IT resources, organizational and staffing models, reporting and lines of authority, and such other areas as may be appropriate for the UNC System and the constituent institutions;

3. Include a set of standards and guidelines concerning information technology matters necessary to the teaching, research, and service missions of the UNC System and the constituent institutions, including but not limited to: security and encryption standards; software standards; hardware standards; acquisition of information technology consulting and contract services; disaster recovery standards; risk management and compliance; networking; wireless technologies; and personal devices; and

4. Include guidelines and priorities for decision-making for information technology that align with the University's strategic objectives.

D. The chief information officer, in consultation with leadership at the UNC System Office and the constituent institutions, shall make recommendations to the president at least annually concerning collaborations, shared services arrangements, staffing structures, and additional resources needed to assure that constituent institutions are able to achieve and maintain consistent and effective information technology governance programs.

IV. Each constituent institution and the UNC System Office shall establish an information technology governance program consistent with the UNC System's information technology governance program framework and principles.

A. The chancellor, or the president in the case of the UNC System Office, shall designate the institution's chief information officer or other member of the chancellor's senior staff, who will be responsible to the chancellor for oversight of information technology governance at the institution and implementation of the information technology governance framework and program as required by this policy.

B. The institution's chief information officer shall be vested with such authority as is necessary to successfully oversee the information technology governance program and ensure the establishment and proper implementation and operation of the information technology governance program framework and principles.

V. Oversight of Information Technology Governance.

A. 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 minimum criteria will include:

1. Demonstration of a comprehensive information technology governance program that encompass both centralized IT and distributed IT consistent with the framework, principles, and standards established in accordance with Part III of this policy;

2. Periodic self-monitoring and external monitoring of the institution's compliance with all principles, standards, and guidelines;

3. Periodic audits of information technology and information resource issues by qualified auditors with specialized expertise;
4. Regular information technology risk assessments;
5. Periodic consideration of information technology matters by the audit/compliance/risk management committee of the institution's board; and
6. Effective systems of accountability to identify and correct deficiencies.

B. The Board of Governors and the board of trustees of each constituent institution shall assign responsibility for oversight of IT governance to a standing committee of the board with audit responsibility.

1. Annual Audit Plan. The annual audit plans of the constituent institutions shall include audit activity focused on information technology matters, based on annual audit planning guidance to be issued by the CARMC and/or the UNC System Office.
2. Audits. The assigned committee with responsibility for IT governance shall review and discuss audit activity relating to information technology matters, and address issues of importance in information technology governance on a regular basis at its scheduled meetings.
3. Reporting. The assigned committee with responsibility for IT governance may request information and reporting related to the institution's IT governance program. All audit reports involving information technology governance matters will be shared with the CARMC.

VI. Other Matters

- A. Effective Date. The requirements of this policy shall be effective on the date of adoption by the Board of Governors.
- B. Relation to State Laws. The foregoing policies as adopted by the Board of Governors are meant to supplement, and do not purport to supplant or modify, those statutory enactments which may govern the activities of public officials.
- C. Regulations and Guidelines. These policies shall be implemented and applied in accordance with such regulations and guidelines as may be adopted from time to time by the president.

AGENDA ITEM

A-2. Review of User Identity and Access Control PolicyJim Holmes

Situation: This policy directs the University of North Carolina System Office and all University of North Carolina constituent institutions to evaluate and conduct risk-based implementation of appropriate identity confirmation and access control techniques, such as multi-factor authentication, to control access to University data.

Background: User identity confirmation and access controls help mitigate the risk of unauthorized access to University data and information systems. Multi-factor authentication, one form of identity confirmation, combines the requirement of using a password with another set of information or physical device to prove a user's identity. The UNC Information Security Council has strongly recommended that all UNC institutions adopt user identity confirmation and access controls, such as multi-factor authentication, as a standard IT security practice.

Assessment: The proposed policy requires each constituent institution to develop, in consultation with the University chief information officer, a strategy for the risk-based implementation of identity confirmation and access control measures. The measures must control access to sensitive and confidential information. The proposed policy also requires each chancellor and the president to designate a senior staff member who will be vested with the authority and responsibility to implement, maintain, and oversee all aspects of the user identity confirmation and access control program. The policy provides that the University chief information officer may identify constituent institutions that require additional resources or consultation to implement and maintain adequate identity confirmation and access control measures.

Action: This item requires a vote by the committee, with a vote by the full Board of Governors through the consent agenda at the next meeting.

User Identity and Access Control

I. Purpose. The security, privacy, and integrity of data and information systems is an operational priority for the University of North Carolina. Identity confirmation and access control techniques help mitigate the risk of unauthorized access to University data and information systems. This policy directs all University of North Carolina System constituent institutions to evaluate and conduct risk-based implementation of appropriate identity confirmation and access control techniques, such as multi-factor authentication, to control access to University data.

II. Risk-Based Implementation of Identity Confirmation and Access Control Measures. The UNC System chief information officer shall, in consultation with the Chief Information Officers Council, develop, maintain, and update standards for risk-informed identity confirmation and access control, such as multi-factor authentication, for use by constituent institutions and the UNC System Office. In the absence of multi-factor authentication, constituent institutions shall identify, implement, and document other appropriate measures to control access to sensitive data. Based on evaluation of the constituent institutions' identity confirmation and access control techniques, the University System chief information officer may identify constituent institutions that require additional resources or consultation to implement and maintain adequate measures and meet the requirements of this policy.

A. Each constituent institution and the UNC System Office shall implement and maintain risk-informed techniques to confirm user identity and control access to University information systems and resources in accordance with the standards developed and maintained by the UNC System chief information officer.

B. The chancellor, or the president in the case of the UNC System Office, shall designate the institution's chief information officer or other member of the senior staff, who will be responsible for the oversight of the implementation and maintenance of user identity confirmation and access control techniques as required by this policy. The institution's chief information officer shall be vested with such authority as is necessary to successfully oversee all aspects of the user identity confirmation and access control program as it applies to staff, faculty, students, and other individuals with access to the institution's information technology systems and information resources.

C. Each institution's user identification and access control measures must sufficiently control access to sensitive University data such as personally identifiable information, personal health information, and information subject to state or federal laws or regulations.

D. The timing and application of user identification and access control measures, such as multi-factor authentication and other techniques, shall be conducted in accordance with the standards maintained by the UNC System chief information officer, and guided by a risk-based evaluation of university data and information systems.

E. The standards developed and maintained by the UNC System chief information officer and the measures established by the constituent institutions in accordance with those

standards shall be confidential and not considered a public record to the extent permitted by North Carolina law.

F. 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 requirements of this policy.

III. Other Matters

A. **Effective Date.** The requirements of this policy shall be effective on the date of adoption of this policy by the Board of Governors.

B. **Relation to State Laws.** The foregoing policies as adopted by the Board of Governors are meant to supplement, and do not purport to supplant or modify, those statutory enactments which may govern the activities of public officials.

C. **Regulations and Guidelines.** These policies shall be implemented and applied in accordance with such regulations and guidelines as may be adopted from time to time by the president.

AGENDA ITEM

A-3. Review of Charters Joyce Boni

Situation: Proposed updates to the Charter for the Committee on Audit, Risk Management, and Compliance and the Internal Audit Charter are presented for review and approval.

Background: As required by North Carolina General Statutes, the North Carolina Council of Internal Auditing, and the standards prescribed by The Institute of Internal Auditors, both the committee and the Office of Internal Audit should have a charter to outline their respective roles and responsibilities. These charters must be periodically reviewed and updated as necessary.

Both charters were last updated in March 2017. Since then, The Institute of Internal Auditors has provided guidance on implementing the new standards. Our charters have been updated accordingly.

Assessment: The proposed revisions to both the committee and internal audit charters are attached and include a clean and marked version of each.

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



UNIVERSITY OF NORTH CAROLINA SYSTEM OFFICE

Internal Audit Charter

I. Mission and Purpose

The mission and purpose of the internal audit function at the University of North Carolina System Office (UNC System Office) is to provide independent, objective assurance and consulting services designed to add value and improve the organization's operations. Internal audit strives to provide risk-based services that help the organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, internal control, and governance processes.

The internal audit function is dedicated to:

- Conforming to The Institute of Internal Auditor's code of ethics and demonstrating the highest level of integrity, objectivity, confidentiality, and competency.
- Building strong and effective working relationships with the UNC System Office personnel, UNC Board of Governors, and other stakeholders through mutual respect and teamwork.
- Providing risk-based and objective assurance and consulting services to the UNC System Office and its affiliated organizations.

II. Role

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

Internal audit partners and consults with management to help the UNC System Office achieve its goals and to support compliance with policies, rules, and regulations. The internal audit scope encompasses, but is not limited to, examining and evaluating the adequacy and effectiveness of the organization's governance, risk management, and internal controls as well as the quality of executing assigned responsibilities to achieve the organization's goals and objectives. This may include:

- A. Evaluating risks associated with achieving the organization's goals and objectives and whether the risk management process is appropriately identifying and managing the risk exposure.
- B. Evaluating if resources are acquired economically, used efficiently, and are adequately protected.
- C. Evaluating reliability and integrity of significant financial, managerial, and operating information and the means used to identify, measure, classify, and report such information.
- D. Evaluating the actions of UNC System Office employees, as well as the processes and systems used, to assess compliance with policies, procedures, governance standards, and applicable laws and regulations which could significantly impact the organization.
- E. Evaluating specific operations or programs to assess if results are consistent with established objectives and goals and whether those operations or programs are being carried in an efficient and effective manner.
- F. Monitoring and evaluating the governance processes and assessing if quality and continuous improvement are fostered in the organization's processes.
- G. Performing consulting and advisory services related to governance, risk management, and controls.

- H. Reporting periodically on the internal audit's purpose, authority, and responsibility; performance of its audit plan; and the sufficiency of internal audit's resources.
- I. Reporting significant risk exposures and control issues, including fraud risks, governance issues, and other matters needed or requested by the president or CARMC.
- J. Evaluating specific operations at the request of management, the president, or CARMC, as appropriate.

III. Professional Standards

The internal audit function will strive to govern itself by adherence to The Institute of Internal Auditors' mandatory guidance, which includes the core principles for the profession, the definition of internal auditing, the code of ethics, and the *International Standards for the Professional Practice of Internal Auditing (Standards)*. This mandatory guidance constitutes the fundamental requirements for the professional practice of internal auditing and the principles against which to evaluate the effectiveness of the internal audit function. The chief audit officer will report at least annually to the president and CARMC regarding the internal audit function's conformance to the code of ethics and the *Standards*.

As applicable, the following will also be used to guide internal audit operations: The Institute of Internal Auditors' implementation and supplemental guidance; *Government Auditing Standards* issued by the Comptroller General of the United States; relevant state and University policies and procedures; and the internal audit function's standard operating procedures manual.

IV. Independence and Objectivity

All internal audit activities will remain free from interference in determining the internal audit plan, scope, performance of procedures, frequency, timing, and communicating results.

The audit staff will exhibit the highest level of professional objectivity in gathering, evaluating, and communicating information about the activity being examined. In addition, a balanced assessment will be made of all the relevant circumstances and the internal audit function will not be unduly influenced by personal interests or by others in forming judgments.

To maintain necessary independence and objectivity, the internal audit function reports administratively to the president or the president's designee and functionally to the Committee on Audit, Risk Management, and Compliance (CARMC). The chief audit officer shall have direct and unrestricted access to the president and the CARMC.

Administrative oversight includes day-to-day oversight such as approval of the chief audit officer's annual leave and travel. Functional oversight by the CARMC includes:

- A. Approve the annual risk-based internal audit plan and monitor progress at least quarterly.
- B. Review and accept internal audit reports when issued.
- C. Periodically review and approve the internal audit charter.
- D. Confirm and assure the independence of the internal audit function.
- E. Receive communications regarding the status and/or results of audit activities, approve any significant deviations from the audit plan, and assure the internal audit function has appropriate budget and staff resources.
- F. Meet privately with the chief audit officer as deemed necessary.
- G. Monitor the effectiveness of the internal audit function, including the efforts made to comply with The Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing (Standards)* and the code of ethics.

- H. Make appropriate inquiries of management and the chief audit officer to determine whether there are inappropriate scope or resource limitations.
- I. Resolve disagreements between internal audit and management concerning audit findings and recommendations.

If the chief audit officer is assigned roles and/or responsibilities that fall outside of internal auditing, necessary disclosures and/or safeguards will be established to limit impairments to independence or objectivity. If the chief audit officer determines that independence or objectivity may be impaired in fact or appearance, details of impairment will be disclosed to the president and CARMC. In addition, the effect of any interference with determining the internal audit scope, performing work, and/or communicating results will be disclosed to the appropriate parties.

The chief audit officer will confirm to the CARMC, at least annually, the organizational independence of the internal audit function.

V. Responsibility

Internal audit has the responsibility to:

- A. Develop a flexible annual audit plan using appropriate risk-based methodology, considering any risks or control concerns identified by management and any input or recommendations from CARMC. Ensure the annual planning and risk assessment process addresses information security. Submit the plan to the president and the CARMC for review and approval.
- B. Implement the annual audit plan as approved, including as appropriate, any special tasks or projects requested by management and/or the CARMC, to include:
 - 1. Conduct and coordinate audits, investigations, and reviews related to the programs and operations of the organization. These services may assess the adequacy of the organization's internal control, risk management, and governance process; the economy and efficiency of the policies and procedures governing the organization's programs and operations; and the organization's compliance with policies, laws, or regulations.
 - 2. Assist and/or conduct the investigation of suspected fraud or abuse within the organization and share the results with the president, the CARMC, and the appropriate levels of management.
 - 3. As appropriate, provide consulting and advisory services to management that add value and improve the governance, risk management, control processes, and operating procedures without the internal auditor assuming management responsibility. This may include evaluating and assessing significant functions as well as new or changing services, processes, operations, and control processes as deemed necessary.
 - 4. When necessary, solicit from management corrective actions taken or to be taken on significant findings and recommendations. Management's response should include a timetable for completion or an explanation for any recommendations that will not be implemented. After a reasonable time, conduct an appropriate follow-up on significant findings and report on the progress made by management to implement the corrective actions. In addition, any management response to a risk exposure that may be unacceptable to the organization will be communicated to the president and the CARMC.
 - 5. At the conclusion of an engagement, prepare a written report that communicates the engagement's objective, scope, and significant results. When applicable, recommendations and management's response and planned corrective action should be provided. Reports are to be appropriately distributed and the results communicated to the CARMC.
 - 6. When applicable, identify opportunities for improving the efficiency of governance, risk management, and control processes and communicate such information to the appropriate

level(s) of management.

- C. Adjust the plan, as necessary, in response to changes in the organization's business, risks, operations, programs, systems, and controls.
- D. Provide quarterly updates to the president and the CARMC summarizing internal audit's activity relative to its plan and/or results of audit activities, including communicating any significant changes to the approved audit plan and the impact of resource limitations.
- E. Keep the president, management, and the CARMC informed concerning significant risk exposures; governance issues; internal control deficiencies; noncompliance; fraud; abuse or misuse of state property; significant complaints; and emerging trends or issues that could impact the organization.
- F. Consider the scope of work by other monitoring and compliance functions, as well as the external auditors and regulators, as appropriate, for the purpose of coordinating activities, evaluating if the work of others can be relied upon, and/or avoiding duplication to provide optimal services to the organization.
- G. As needed, serve as a liaison between management and external auditors and regulators.
- H. Ensure the audit team collectively possesses, obtains and maintains sufficient knowledge, skills, competencies, and professional certifications necessary to meet the requirements of the Charter and the internal audit Standards. Consider emerging trends and successful internal audit practices.
- I. Ensure the requirements are met with regard to internal audit activities set forth by the UNC Board of Governors and the North Carolina Council of Internal Auditing.
- J. Ensure adherence to the organization's relevant policies and procedures, unless they conflict with the internal audit charter, and establish and ensure adherence to policies and procedures designed to guide the internal audit function.
- K. Maintain a quality assurance and improvement program that covers all aspects of the internal audit function and includes: evaluating conformance with The Institute of Internal Auditors' *Standards*, core principles, definition of internal auditing, and code of ethics; assessing the efficiency and effectiveness of the internal audit function; and identifying opportunities for improvement. The chief audit officer will communicate to the CARMC and senior management significant results from the quality assurance and improvement program, including, if necessary, plans to address significant issues noted from ongoing internal assessments, as well as from external assessments that are conducted at least every five years.

VI. Authority

With strict accountability for confidentiality and safeguarding records and information, the internal audit function is authorized to:

- Have full, free, and unrestricted access to all functions, records, property, and personnel pertinent to any engagement.
- Provide consulting services to management as deemed appropriate.
- Allocate resources, set frequencies, select subjects, determine scopes of work, and apply the techniques required to accomplish audit objectives, and issue reports.
- Obtain the necessary assistance of personnel in units of the organization where audits are performed, as well as other specialized services from within or outside the organization, if needed to fulfill the internal audit roles and responsibilities.

The internal audit function is not authorized to:

- Have direct operational responsibility or authority over any of the activities to be audited.
- Initiate or approve accounting transactions external to the internal audit function.

- Direct the activities of any UNC System Office employee not employed within internal audit function, except to the extent such employees have been appropriately assigned to auditing teams or to otherwise assist the chief audit officer.
- Implement internal controls, develop procedures, install systems, prepare records, or engage in any other activity that may impair internal auditor’s judgment; including assessing operations for which they had responsibility within the previous year.

Joyce D. Boni, Chief Audit Officer

Date

James Holmes, Jr., Chair of CARMC

Date

Margaret Spellings, President

Date

Last updated and approved March ~~2017~~



UNIVERSITY OF NORTH CAROLINA SYSTEM OFFICE

Internal Audit Charter

I. Mission and Purpose

The mission and purpose of the internal audit function at the University of North Carolina System Office (UNC System Office) is to provide independent, objective assurance and consulting services designed to add value and improve the organization's operations. Internal audit strives to provide risk-based services that help the organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, internal control, and governance processes.

The internal audit function is dedicated to:

- Conforming to The Institute of Internal Auditor's code of ethics and demonstrating the highest level of integrity, objectivity, confidentiality, and competency.
- Building strong and effective working relationships with the UNC System Office personnel, UNC Board of Governors, and other stakeholders through mutual respect and teamwork.
- Providing risk-based and objective assurance quality auditing and consulting services to the UNC System Office and its affiliated organizations.

II. Role

The University of North Carolina is required to establish a program of internal auditing pursuant to N.C.G.S. § 143-746. The UNC System Office's internal audit function shall be accountable to the UNC Board of Governors through the Committee on Audit, Risk Management, and Compliance (CARMC) and the president.

Internal audit partners and consults with management to help the UNC System Office achieve its goals and to support compliance with policies, rules, and regulations. ~~The internal audit staff seeks to proactively focus on the risk exposures that have the greatest impact on UNC-GA while being flexible to react to changing conditions.~~ The internal audit scope encompasses, but is not limited to, examining and evaluating the adequacy and effectiveness of the organization's governance, risk management, and internal controls as well as the quality of executing in the execution of assigned responsibilities to achieve the organization's goals and objectives. This may includes:

- A. Evaluating risks associated with achieving the organization's goals and objectives and whether the risk management process is appropriately identifying and managing the risk exposure.
- B. Evaluating if resources are acquired economically, used efficiently, and are adequately protected.
- C. Evaluating reliability and integrity of significant financial, managerial, and operating information and the means used to identify, measure, classify, and report such information is accurate, reliable, and timely.
- D. Evaluating the actions of UNC System Office employees, as well as the processes and systems used, to assess compliance with policies, procedures, governance standards, and applicable laws and regulations which could significantly impact the organization.
- E. Evaluating specific operations or programs to assess if results are consistent with established objectives and goals and whether those operations or programs are being carried ~~out as planned~~ in an efficient and effective manner.
- F. Monitoring and evaluating the governance processes and assessing if quality and continuous improvement are fostered in the organization's processes.
- G. Performing consulting and advisory services related to governance, risk management, and controls.

- H. Reporting periodically on the internal audit's purpose, authority, and responsibility; performance of its audit plan; and the sufficiency of internal audit's resources.
- I. Reporting significant risk exposures and control issues, including fraud risks, governance issues, and other matters needed or requested by the president or CARMC.
- J. Evaluating specific operations at the request of management, the president, or CARMC, as appropriate.

III. Professional Standards

The internal audit function will strive to govern itself by adherence to The Institute of Internal Auditors' mandatory guidance, which includes the core principles for the profession, the definition of internal auditing, the code of ethics, and the *International Standards for the Professional Practice of Internal Auditing* (Standards). This mandatory guidance constitutes the fundamental requirements for the professional practice of internal auditing and the principles against which to evaluate the effectiveness of the internal audit function. The chief audit officer will report at least annually to the president and CARMC regarding the internal audit function's conformance to the code of ethics and the Standards.

As applicable, the following will also be used to guide internal audit operations: The Institute of Internal Auditors' implementation and supplemental guidance ~~(practice guides)~~; *Government Auditing Standards* issued by the Comptroller General of the United States; relevant state and University policies and procedures; and the internal audit function's standard operating procedures manual.

IV. Independence and Objectivity

All internal audit activities will remain free from interference in determining the internal audit plan, scope, performance of procedures, frequency, timing, and communicating results~~report content~~.

The audit staff will exhibit the highest level of professional objectivity in gathering, evaluating, and communicating information about the activity being examined. In addition, a balanced assessment will be made of all the relevant circumstances and the internal audit function will not be unduly influenced by personal interests or by others in forming judgments.

To maintain necessary independence and objectivity, the internal audit function reports administratively to the president or the president's designee and functionally to the Committee on Audit, Risk Management, and Compliance (CARMC). The chief audit officer shall have direct and unrestricted access to the president and the CARMC.

Administrative oversight includes day-to-day oversight such as approval of the chief audit officer's annual leave and travel. Functional oversight by the CARMC includes:

- A. Approve the annual risk-based internal audit plan and monitor progress at least quarterly.
- B. Review and accept internal audit reports when issued.
- C. Periodically review and approve the internal audit charter.
- D. Confirm and assure the independence of the internal audit function.
- E. Receive communications regarding the status and/or results of audit activities, approve any significant deviations from the audit plan, and assure the internal audit function has appropriate budget and staff resources.
- F. Meet privately with the chief audit officer as deemed necessary.
- G. Monitor the effectiveness of the internal audit function, including the efforts made to comply with The Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing* (Standards) and the code of ethics.
- H. Make appropriate inquiries of management and the chief audit officer to determine whether there are inappropriate scope or resource limitations.
- I. Resolve disagreements between internal audit and management concerning audit findings and recommendations.

If the chief audit officer is assigned roles and/or responsibilities that fall outside of internal auditing, necessary disclosures and/or safeguards will be established to limit impairments to independence or objectivity. If the chief audit officer determines that independence or objectivity may be impaired in fact or appearance, details of impairment will be disclosed to the president and CARMC. In addition, the effect of any interference with determining the internal audit scope, performing work, and/or communicating results will be disclosed to the appropriate parties.

The chief audit officer will confirm to the CARMC, at least annually, the organizational independence of the internal audit function.

V. Responsibility

Internal audit has the responsibility to:

- A. Develop a flexible annual audit plan using appropriate risk-based methodology, considering any risks or control concerns identified by management and any input or recommendations from CARMC. ~~and~~ Ensure the annual planning and risk assessment process addresses information security. ~~Submit the~~ plan to the president and the CARMC for review and approval.
- B. Implement the annual audit plan as approved, including as appropriate, any special tasks or projects requested by management and/or the CARMC, to include:
 1. Conduct and coordinate audits, investigations, and reviews related to the programs and operations of the organization. These services may assess the adequacy of the organization's internal control, risk management, and governance process; the economy and efficiency of the policies and procedures governing the organization's programs and operations; and the organization's compliance with policies, laws, or regulations.
 2. Assist and/or conduct the investigation of suspected fraud or abuse within the organization and share the results with the president, the CARMC, and the appropriate levels of management.
 3. As appropriate, provide consulting and advisory services to management that add value and improve the governance, risk management, control processes, and operating procedures without the internal auditor assuming management responsibility. This may include evaluating and assessing significant functions as well as new or changing services, processes, operations, and control processes as deemed necessary.
 4. When necessary, solicit from management corrective actions taken or to be taken on significant findings and recommendations. Management's response should include a timetable for completion or an explanation for any recommendations that will not be implemented. After a reasonable time, conduct an appropriate follow-up on significant findings and report on the progress made by management to implement the corrective actions. In addition, any management response to a risk exposure that may be unacceptable to the organization will be communicated to the president and the CARMC.
 5. At the conclusion of an engagement, prepare a written report that communicates the engagement's objective, scope, and significant results. When applicable, recommendations and management's response and planned corrective action should be provided. Reports are to be appropriately distributed and the results communicated to the CARMC.
 6. When applicable, identify opportunities for improving the efficiency of governance, risk management, and control processes and communicate such information to the appropriate level(s) of management.
- C. Adjust the plan, as necessary, in response to changes in the organization's business, risks, operations, programs, systems, and controls.
- D. Provide quarterly updates to the president and the CARMC summarizing internal audit's activity relative to its plan ~~the status~~ and/or results of audit activities, including communicating any significant changes to deviation from the approved audit plan and the impact of resource limitations.
- E. Keep the president, management, and the CARMC informed concerning significant risk exposures; governance issues; internal control deficiencies; noncompliance; fraud; abuse or misuse of state property; ~~and~~ significant complaints; and emerging trends or issues that could impact the organization.
- F. Consider the scope of work by other monitoring and compliance functions, as well as the external auditors and regulators, as appropriate, for the purpose of coordinating activities, evaluating if the work of others can be relied upon, and/or avoiding duplication to provide optimal services to the organization.
- G. As needed, serve as a liaison between ~~UNC-GA~~ management and external auditors and regulators.
- H. Ensure the audit team collectively possesses, obtains and maintains sufficient knowledge, skills,

competencies, and professional certifications necessary to meet the requirements of the Charter and the internal audit Standards. Consider emerging trends and successful internal audit practices.

- I. Ensure the requirements are met with regard to internal audit activities set forth by the UNC Board of Governors and the North Carolina Council of Internal Auditing.
- J. Ensure adherence to the organization's relevant policies and procedures, unless they conflict with the internal audit charter, and establish and ensure adherence to policies and procedures designed to guide the internal audit function.
- K. Maintain a quality assurance and improvement program that covers all aspects of the internal audit function and includes: evaluating conformance with The Institute of Internal Auditors' *Standards*, core principles, definition of internal auditing, and code of ethics; assessing the efficiency and effectiveness of the internal audit function; and identifying opportunities for improvement. The chief audit officer will communicate to the CARMC and senior management significant results from the quality assurance and improvement program, including, if necessary, plans to address significant issues noted from ongoing internal assessments, as well as from external assessments that are conducted at least every five years.

VI. Authority

With strict accountability for confidentiality and safeguarding records and information, the UNC GA's internal audit function is authorized to:

- Have full, free, and unrestricted access to all functions, records, property, and personnel pertinent to any engagement in accordance with North Carolina General Statutes.
- Provide consulting services to management as deemed appropriate.
- Allocate resources, set frequencies, select subjects, determine scopes of work, and apply the techniques required to accomplish audit objectives, and issue reports.
- Obtain the necessary assistance of personnel in units of the organization where audits are performed, as well as other specialized services from within or outside the organization, if needed to fulfill the internal audit roles and responsibilities.

The internal audit function is not authorized to:

- Have direct operational responsibility or authority over any of the activities to be audited.
- Initiate or approve accounting transactions external to the internal audit function.
- Direct the activities of any UNC System Office employee not employed within internal audit function, except to the extent such employees have been appropriately assigned to auditing teams or to otherwise assist the chief audit officer.
- Implement internal controls, develop procedures, install systems, prepare records, or engage in any other activity that may impair internal auditor's judgment; including assessing operations for which they had responsibility within the previous year.

Joyce D. Boni, Chief Audit Officer

Date

James Holmes, Jr., Chair of CARMC

Date

Margaret Spellings, President

Date

Last updated and approved March ~~2017~~



Committee Charter for the Board of Governors

Committee on Audit, Risk Management, and Compliance

I. Background and Authority

The Committee on Audit, Risk Management, and Compliance (CARMC) is a standing committee of the Board of Governors of the University of North Carolina System (the Board) and provides independent oversight of the University's governance, risk management, compliance and internal control practices. This charter sets out the authority of the committee to carry out the responsibilities established by the Board. In discharging its responsibilities, the committee will have unrestricted access to members of management, employees, and relevant information it considers necessary to discharge its duties. Related authoritative legislation and policies include:

- A. All constituent institutions, affiliated entities, and the University of North Carolina System Office (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 (G.S.).
- B. Under the authority of G.S. 116-30.1, the Board of Governors may designate a special responsibility constituent institution, by expressly finding that each institution to be so designated, has the management staff and internal financial controls that will enable it to administer competently and responsibly all additional management authority and discretion to be delegated to it. The Board, on recommendation of the president, shall adopt rules prescribing management staffing standards and internal financial controls and safeguards.
- C. A special responsibility constituent institution of the University of North Carolina is required by G.S. 116-30.8 to have an annual audit conducted by the North Carolina State Auditor.
- D. The University of North Carolina is required to establish a program of internal auditing pursuant to G.S. 143-746.
- E. Chapter 600 of the UNC Policy Manual establishes financial, reporting, and audit policies, regulations, and guidelines for the University of North Carolina, University-related private foundations, and associated entities.
- F. UNC Policy Manual 1400.2 assigns the responsibility for oversight of the UNC System Office's information security program to the standing committee with audit responsibility.

II. Purpose

The purpose of the Committee on Audit, Risk Management, and Compliance (CARMC) is to provide a structured, systematic oversight of the University of North Carolina System's governance, risk management, and internal control practices. The CARMC will assist the Board in performing its responsibilities and oversight related to:

- A. The integrity of financial statements.
- B. Governance, systems of internal control, values and ethics.
- C. The internal audit function, external auditors, and other providers of assurance.
- D. Compliance with laws and policies.
- E. System-wide enterprise risk management and compliance processes.
- F. Designation of special responsibility constituent institutions.
- G. The required elements of University associated entities.

III. Organization

As a standing committee of the UNC Board of Governors, the chairman of the Board will select the CARMC chair and members, as well as determine the number of voting members. Continuance of committee members and their overall, collective competencies and skills will be reviewed annually. A quorum for the committee will be a majority of the voting members.

The CARMC members:

- A. Must be independent of the UNC System or associated entity management and free of any relationship that would impair the member's independence.
- B. May not receive consulting, advisory, or other fees from any of the constituent institutions, affiliated entities, associated entities, or the UNC System Office.
- C. Should collectively possess sufficient knowledge of audit, finance, higher education, information technology, law, governance, risk and control in order to respond to regulatory, economic, reporting and other emerging developments and needs.
- D. Should adhere to the UNC System's code of conduct and values and ethics established by the UNC System. It is the responsibility of the committee members to disclose any conflict of interest or appearance of conflict of interest to the CARMC chair.
- E. Are obligated to prepare for and participate in committee meetings.

IV. Meetings

The committee shall meet no fewer than four times a year. The committee will invite representatives of the constituent institutions, external and internal auditors, representatives of the Office of the State Auditor, legal counsel, and others to attend the meetings and provide pertinent information as required and requested. The committee will communicate its information requirements, including the nature, extent, and timing of information. The CARMC expects all communication with UNC management and staff as well as external assurance providers will be direct, open, and complete.

The CARMC chair will collaborate with senior management and the chief audit officer to establish a work plan that ensures the responsibilities of the CARMC are properly scheduled and carried out. Meeting agendas and related materials will be prepared and provided in advance to members. Minutes will be prepared in accordance with applicable requirements.

V. Duties and Responsibilities

It is the responsibility of the CARMC to provide the Board with independent, objective advice on the adequacy of the University's governance processes, values and ethics, risk management, prevention and detection of fraud, compliance monitoring, and internal control practices. The committee will also review observations and conclusions of the internal auditor, external auditor, or other regulatory agencies. The CARMC will regularly report to the Board a summary of the committee's significant activities and recommendations.

The following shall be the principal oversight duties and responsibilities of this committee:

- A. External Audit
 - 1. Receive an annual overview from the State Auditor or a designated representative regarding the annual audits (financial and compliance) of the constituent institutions. Review the results of the UNC System Office's independent audit, including any difficulties encountered and reportable issues.
 - 2. Review other significant audit-related communications from the State Auditor's Office or other external audit groups or firms. Meet separately with the external auditors to discuss sensitive and

any other matters that the committee or auditor believes should be discussed privately.

3. Review reports on the progress of implementing approved management action plans and audit recommendations resulting from completed audit engagements.
4. Be available to meet during the year with external auditors (the State Auditor, engaged CPA firm, or audit staff) for consultation purposes or to discuss the auditor's judgment about the quality, not just the acceptability, of any accounting principles and underlying estimates in the preparation of a financial statement and other matters required to be communicated to the committee under generally accepted auditing standards.
5. Request, as needed, that the State Auditor rotate the Audit Manager or that the engaged CPA firm rotate the partner assigned to a constituent institution, affiliated entity, or the UNC System Office financial statement audit.
6. Provide a direct channel of communication to the full Board of Governors for the State Auditor and the results of external audits.

B. Internal Audit

1. Review an annual summary of the internal audit plans submitted by each constituent institution and the UNC System Office.
2. Review an annual summary of the internal audit activities overseen by the audit committee of each constituent institution's boards of trustees. This report will incorporate a summary of audits, reviews, investigations, or special assignments completed by the internal audit department of each constituent institution and the UNC System Office, and will note material reportable conditions and the status of their resolution.
3. Serve as the audit committee for the UNC System Office's internal audit function. In this oversight capacity, the committee will:
 - a. Review and approve the Internal Audit Charter, ensuring it accurately reflects internal audit's purpose, authority, and responsibility.
 - b. Review and approve the annual risk-based internal audit plan and all significant changes to the plan. If necessary, provide input and make recommendations concerning the planned audit projects and the resources necessary to achieve the plan.
 - c. Confirm that internal audit coordinates with external auditors and regulators to provide optimal audit coverage, reduce duplication of work, and use audit resources effectively.
 - d. Review internal audit reports to management and periodic summaries of external and internal audit activities, including internal audit's performance relative to its annual plan.
 - e. Consider the scope and results of the internal audit activity and evaluate the adequacy of internal audit resources to ensure there are no budgetary or scope limitations that impede internal audit from executing its responsibilities. If necessary, review and approve proposals to outsource internal audit activities.
 - f. Review the organizational structure of the internal audit function to assure its independence and that no unjustified restrictions or limitations are placed upon the internal audit function.
 - g. Review reports on significant findings and recommendations, along with management's responses. Review and resolve any significant disagreement between management, external auditors, or internal audit over audit related matters.
 - h. Review reports regarding the progress of implementing approved management action plans and audit recommendations resulting from completed audit engagements.
 - i. Meet privately with the chief audit officer, as deemed necessary, to discuss sensitive or other matters that the committee or auditor believes should be discussed privately.
 - j. Monitor the effectiveness of the internal audit function, including adherence to The Institute of Internal Auditors' mandatory guidance, which includes the core principles for the profession, definition of internal auditing, code of ethics, and the *International Standards for the Professional Practice of Internal Auditing*. Ensure the chief audit officer complies with all reporting requirements of the NC Office of Internal Audit and UNC policies related to the internal audit function.

- k. Monitor to ensure the internal audit function has a quality assurance and improvement program and that the results of these periodic assessments are presented to the committee.
- l. Monitor to ensure the internal audit function has an independent external quality assurance review every five years. Review the results of this external quality assurance review and monitor the implementation of internal audit's action plans to address any recommendations. Advise the Board about any recommendations for continuous improvement of the internal audit function.
- m. Provide a direct channel of communication to the full Board of Governors regarding relevant internal audit activities. Report committee activities and forward with recommendations to the full Board significant management initiatives resulting from internal/external audit activities.

C. Enterprise Risk Management and Compliance

- 1. Support the efforts, establishment of, and collaboration among the risk management, ethics, and compliance programs at the constituent institutions, including recommending to the Board University-wide policies regarding internal audit, enterprise risk management, and compliance.
- 2. Monitor through regular reports from the UNC System Office's general counsel and senior officers the system-wide risk management and compliance processes.

D. Other Responsibilities

- 1. Monitor the internal control and audit-finding resolution requirements for special responsibility constituent institutions.
- 2. Review a summary of the annual financial audit reports of the University's major associated entities.
- 3. Review the required elements of a University associated entity relationship.
- 4. Participate, when necessary, in training sessions related to system-wide internal controls, enterprise risk management and compliance, and internal/external audit issues.
- 5. Oversee the UNC System Office's information security program, including but not limited to: obtaining confirmation from the chief audit officer that the annual audit planning and risk assessment process addresses information security; periodically including emerging information security matters on the committee's meeting agenda; and receiving a report, at least annually, from the senior officer responsible for information security regarding the UNC System Office's information security program and information technology security controls.
- 6. Review the results from auditors, regulatory agencies, or information from management, including any recommendations and planned actions in order to assess the adequacy and effectiveness of the organization's internal control systems in response to risks, including information technology security and controls and the systems for monitoring compliance with laws and policies.
- 7. Receive briefings from management or internal audit regarding any significant complaints, internal control deficiencies, noncompliance, fraud, abuse, or misuse of State property in order to oversee the University's mechanisms for receiving, resolving, and retaining records of complaints regarding accounting, internal control, and operating matters.
- 8. Oversee management's procedures for the prevention and detection of fraud by challenging management and auditors to ensure appropriate antifraud programs and controls are in place to identify potential fraud and to take appropriate action if fraud is detected.
- 9. Consult with the UNC System Office's general counsel to review any legal matters that may have a significant impact on a financial statement, overall financial performance, enterprise risk management, or compliance with applicable state, local, or federal laws and regulations. Review and provide advice on systems, practices, policies and standards of ethical conduct. Identify and manage any legal or ethical violations.
- 10. Take other actions, as necessary, to ensure that risk exposures are identified and properly managed to assure the integrity of the finances, operations, and controls of the University; including, reviewing the established governance processes and advising on related policies and procedures that should be in place.

The committee may modify or supplement these duties and responsibilities as needed.

The committee shall have the authority to engage independent counsel or other advisors as necessary to carry out its duties, in accordance with State rules and regulations. The committee may also request supplemental review or other audit procedures by internal audit, the State Auditor, or other advisors when the circumstances dictate that further review is required. The UNC System Office shall provide appropriate funding, as determined by the committee, for payment to advisors employed by the committee.

The committee shall annually review and assess the adequacy of the committee charter, with the assistance of staff at the UNC System Office. The committee chair will confirm annually that the relevant responsibilities in this charter have been carried out.

Joyce D. Boni, Chief Audit Officer

Date

James Holmes, Jr., Committee Chair

Date

W. Louis Bissette, Jr., Chair of the Board of Governors

Date

Last updated and approved March 2018



Committee Charter for the Board of Governors
Committee on Audit, Risk Management, and Compliance

I. Background and Authority

The Committee on Audit, Risk Management, and Compliance (CARMC) is a standing committee of the Board of Governors of the University of North Carolina System (the Board) and provides independent oversight of the University's governance, risk management, compliance and internal control practices. This charter sets out the authority of the committee to carry out the responsibilities established by the Board. In discharging its responsibilities, the committee will have unrestricted access to members of management, employees, and relevant information it considers necessary to discharge its duties. Related authoritative legislation and policies include:

- A. All constituent institutions, affiliated entities, and the University of North Carolina System Office (UNC System Office) ~~General Administration of the University of North Carolina~~ are subject to audit by the North Carolina State Auditor under Article 5A of Chapter 147 of the North Carolina General Statutes (~~N.C.~~G.S.).
- B. Under the authority of ~~N.C.~~G.S. §—116-30.1, the Board of Governors may designate a special responsibility constituent institution, by expressly finding that each institution to be so designated, has the management staff and internal financial controls that will enable it to administer competently and responsibly all additional management authority and discretion to be delegated to it. The Board ~~of Governors~~, on recommendation of the president, shall adopt rules prescribing management staffing standards and internal financial controls and safeguards.
- C. A special responsibility constituent institution of the University of North Carolina is required by ~~N.C.~~G.S. §-116-30.8 to have an annual audit conducted by the North Carolina State Auditor.
- D. The University of North Carolina is required to establish a program of internal auditing pursuant to ~~N.C.~~G.S. §-143-746.
- E. Chapter 600 of the UNC Policy Manual establishes financial, reporting, and audit policies, regulations, and guidelines for the University of North Carolina, University-related private foundations, and associated entities.
- F. UNC Policy Manual 1400.2 assigns the responsibility for oversight of the UNC System Office's information security program to the standing committee with audit responsibility.

II. Purpose

The purpose of the Committee on Audit, Risk Management, and Compliance (CARMC) is to provide a structured, systematic oversight of the University of North Carolina System's governance, risk management, and internal control practices. The CARMC will assist the ~~UNC Board of Governors (Board)~~ in performing its responsibilities and oversight related to:

- A. The integrity of financial statements.
- B. Governance, systems of internal control, ~~and the audit process~~ values and ethics.
- C. The internal audit function, external auditors, and other providers of assurance.
- D. Compliance with laws and policies.
- E. System-wide enterprise risk management and compliance processes.
- F. Designation of special responsibility constituent institutions.
- G. The required elements of University associated ~~entities~~ entities.

III. Organization

~~The Committee on Audit, Risk Management, and Compliance will be a~~ As a standing committee of the UNC Board of Governors. ~~The chairman of the Board of Governors will select the CARM Committee chair and members, as well as and~~ determine the number of voting members. Continuance of committee members and their overall, collective competencies and skills will be reviewed annually. A quorum for the committee will be a majority of the voting members.

The CARMC members:

- A. ~~Committee members must~~ be independent of the UNC System or associated entity management and free of any relationship that would impair the member's independence.
- B. ~~Committee members may~~ not receive consulting, advisory, or other fees from any of the constituent institutions, affiliated entities, associated entities, or the UNC System Office General.
- C. ~~If practicable, at least one member of the committee should be a financial expert. A financial expert is someone who has an understanding of generally accepted accounting principles and financial statements, preferably relative to higher education; experience in applying such principles; experience in preparing, auditing, analyzing, or evaluating financial information; experience with internal controls and procedures for financial reporting; or an understanding of the audit committee function~~Should collectively possess sufficient knowledge of audit, finance, higher education, information technology, law, governance, risk and control in order to respond to regulatory, economic, reporting and other emerging developments and needs.
- D. Should adhere to the UNC System's code of conduct and values and ethics established by the UNC System. It is the responsibility of the committee members to disclose any conflict of interest or appearance of conflict of interest to the CARMC chair.
- ~~C.E. Are obligated to prepare for and participate in committee meetings.~~
- D. ~~—— If a financial expert is not available from the members of the Board of Governors, the committee may request the appointment of an independent financial expert in an advisory capacity, upon approval from the full Board of Governors.~~
- E. ~~—— An appointed financial expert may not receive consulting, advisory, or other fees from any of the constituent institutions, affiliated entities, associated entities, or the UNC General Administrationsystem office, other than fees related to the committee appointment.~~
- F. ~~—— If feasible, the role of financial expert will be rotated on an annual basis.~~

IV. Meetings

The committee shall meet no fewer than four times a year. The committee will invite representatives of the constituent institutions, external and internal auditors, representatives of the Office of the State Auditor, legal counsel, and others to attend the meetings and provide pertinent information as required and requested. The committee will communicate its information requirements, including the nature, extent, and timing of information. The CARMC expects all communication with UNC management and staff as well as external assurance providers will be direct, open, and complete.

The CARMC chair will collaborate with senior management and the chief audit officer to establish a work plan that ensures the responsibilities of the CARMC are properly scheduled and carried out. Meeting agendas and related materials will be prepared and provided in advance to members. Minutes will be prepared in accordance with applicable requirements.

V. Duties and Responsibilities

It is the responsibility of the CARMC to provide the Board with independent, objective advice on the adequacy of the University's governance processes, values and ethics, risk management, prevention and detection of fraud, compliance monitoring, and internal control practices. The committee will also review observations and conclusions of the internal auditor, external auditor, or other regulatory agencies. The CARMC will regularly report to the Board a summary of the committee's significant activities and recommendations.

The following shall be the principal oversight duties and responsibilities of this committee:

A. External Audit

1. Receive an annual overview from the State Auditor or a designated representative regarding the annual audits (financial and compliance) of the constituent institutions. Review the results of the UNC System Office's~~General Administration's~~ independent audit, including any difficulties encountered and reportable issues.
2. Review other significant audit-related communications from the State Auditor's Office or other external audit groups or firms. Meet separately with the external auditors to discuss sensitive and any other matters that the committee or auditor believes should be discussed privately.
3. Review reports on the progress of implementing approved management action plans and audit recommendations resulting from completed audit engagements.
4. Be available to meet during the year with external auditors (the State Auditor, engaged CPA firm, or audit staff) for consultation purposes or to discuss the auditor's judgment about the quality, not just the acceptability, of any accounting principles and underlying estimates in the preparation of a financial statement and other matters required to be communicated to the committee under generally accepted auditing standards.
5. Request, as needed, that the State Auditor rotate the Audit Manager or that the engaged CPA firm rotate the partner assigned to a constituent institution, affiliated entity, or the UNC System Office~~General Administration~~ financial statement audit.
6. Provide a direct channel of communication to the full Board of Governors for the State Auditor and the results of external audits.

B. Internal Audit

1. Review an annual summary of the internal audit plans submitted by each constituent institution and the UNC System Office General Administration.
2. Review an annual summary of the internal audit activities overseen by the audit committee of each constituent institution's boards of trustees. This report will incorporate a summary of audits, reviews, investigations, or special assignments completed by the internal audit department of each constituent institution and UNC General Administration the UNC System Office, and will note material reportable conditions and the status of their resolution.
3. Serve as the audit committee for the UNC System Office's General Administration internal audit function. In this oversight capacity, the committee will:
 - a. Review and approve the Internal Audit Charter, ensuring it accurately reflects internal audit's purpose, authority, and responsibility.
 - b. Review and approve the annual risk-based internal audit plan and all significant changes to the plan. If necessary, provide input and make recommendations concerning the planned audit projects and the resources necessary to achieve the plan.
 - c. Confirm that internal audit coordinates with external auditors and regulators to provide optimal audit coverage, reduce duplication of work, and use audit resources effectively.
 - d. Review internal audit reports to management and periodic summaries of external and internal audit activities, including internal audit's performance relative to its annual plan.
 - e. Consider the scope and results of the internal audit activity and evaluate the adequacy of internal audit resources to ensure there are no budgetary or scope limitations that impede internal audit from executing its responsibilities. If necessary, review and approve proposals to outsource internal audit activities.
 - f. Review the organizational structure of the internal audit function to assure its independence and that no unjustified restrictions or limitations are placed upon the internal audit function.
 - g. Receive Review reports on significant findings and recommendations, along with management's responses. Review and resolve any significant disagreement between management, external auditors, or internal audit over audit related matters.
 - h. Review reports regarding the progress of implementing approved management action plans and audit recommendations resulting from completed audit engagements.
 - i. Consider the adequacy and effectiveness of the internal control systems, including information technology security and controls, and the system of monitoring compliance with laws and policies. Review the results from auditors, regulatory agencies, or management, including any recommendations and planned actions.
 - j. Oversee the institution's mechanisms for receiving, resolving, and retaining records of complaints regarding accounting, internal control, and operating matters. Receive briefings from management or internal audit regarding any significant complaints, internal control deficiencies, noncompliance, fraud, abuse, or misuse of State property.
 - k. Meet privately with the chief audit officer, as deemed necessary, to discuss sensitive or other matters that the committee or auditor believes should be discussed privately.
 - l. Monitor the effectiveness of the internal audit function, including adherence to The Institute of Internal Auditors' mandatory guidance, which includes the core principles for the profession, definition of internal auditing, code of ethics, and the *International Standards for the Professional Practice of Internal Auditing*. Ensure the chief audit officer complies with all reporting requirements of the NC Office of Internal Audit and UNC policies related to the internal audit function.
 - m. Monitor to ensure the internal audit function has a quality assurance and improvement program and that the results of these periodic assessments are presented to the committee.
 - n. Monitor to ensure the internal audit function has an independent external quality assurance review every five years. Review the results of this external quality assurance review and monitor the implementation of internal audit's action plans to address any recommendations. Advise the

Board about any recommendations for continuous improvement of the internal audit function.

- o. Provide a direct channel of communication to the full Board of Governors regarding relevant internal audit activities. Report committee activities and forward with recommendations to the full Board significant management initiatives resulting from internal/external audit activities.

C. Enterprise Risk Management and Compliance

1. Support the efforts, establishment of, and collaboration among the risk management, ethics, and compliance programs at the constituent institutions, including recommending to the Board University-wide policies regarding internal audit, enterprise risk management, and compliance.
2. Monitor through regular reports from the UNC System Office's ~~the UNC General Administration's~~ general counsel and senior officers the system-wide risk management and compliance processes.

D. Other Responsibilities

1. Monitor the internal control and audit-finding resolution requirements for special responsibility constituent institutions.
2. Review a summary of the annual financial audit reports of the University's major associated entities.
3. Review the required elements of a University associated entity relationship.
4. Participate, when necessary, in training sessions related to system-wide internal controls, enterprise risk management and compliance, and internal/external audit issues.
5. Oversee the UNC System Office's information security program, including but not limited to: obtaining confirmation from the chief audit officer that the annual audit planning and risk assessment process addresses information security; periodically including emerging information security matters on the committee's meeting agenda; and receiving a report, at least annually, from the senior officer responsible for information security regarding the UNC System Office's information security program and information technology security controls.
6. Review the results from auditors, regulatory agencies, or information from management, including any recommendations and planned actions in order to assess the adequacy and effectiveness of the organization's internal control systems in response to risks, including information technology security and controls and the systems for monitoring compliance with laws and policies.
7. Receive briefings from management or internal audit regarding any significant complaints, internal control deficiencies, noncompliance, fraud, abuse, or misuse of State property in order to oversee the University's mechanisms for receiving, resolving, and retaining records of complaints regarding accounting, internal control, and operating matters.
8. Oversee management's procedures for the prevention and detection of fraud by challenging management and auditors to ensure appropriate antifraud programs and controls are in place to identify potential fraud and to take appropriate action if fraud is detected.
9. Consult with ~~UNC General Administration~~ the UNC System Office's general counsel to review any legal matters that may have a significant impact on a financial statement, overall financial performance, enterprise risk management, or compliance with applicable state, local, or federal laws and regulations. Review and provide advice on systems, practices, policies and standards of ethical conduct. Identify and manage any legal or ethical violations.
10. Take other actions, as necessary, to ensure that risk exposures are identified and properly managed to assure the integrity of the finances, operations, and controls of the University; including, reviewing the established governance processes and advising on related policies and procedures that should be in place.

The committee may modify or supplement these duties and responsibilities as needed.

The committee shall have the authority to engage independent counsel or other advisors as necessary to carry out its duties, in accordance with State rules and regulations. The committee may also request supplemental review or other audit procedures by internal audit, the State Auditor, or other advisors when the circumstances dictate that further review is required. ~~The UNC System Office - General Administration~~ shall provide appropriate

funding, as determined by the committee, for payment to advisors employed by the committee.

The committee shall annually review and assess the adequacy of the committee charter, with the assistance of staff at the UNC System Office~~General Administration~~. The committee chair will confirm annually that the relevant responsibilities in this charter have been carried out.

<u>Joyce D. Boni, Chief Audit Officer</u>	<u>Date</u>
---	-------------

<u>James Holmes, Jr., Chair of CARMC</u>	<u>Date</u>
--	-------------

<u>W. Louis Bisette, Jr., Chair of the Board of Governors</u>	<u>Date</u>
---	-------------

Last updated and approved March ~~2017~~