THE UNIVERSITY OF NORTH CAROLINA SYSTEM

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

May 21, 2018 at 2:00 p.m.
University of North Carolina System Office
Spangler Center, Conference Room C
Chapel Hill, North Carolina

AGENDA

OPEN SESSION

A-1. Approval of the Minutes of March 8, 2018 and March 20, 2018 ..... Jim Holmes
   a. March 8, 2018
   b. March 20, 2018

A-2. Internal Audit Update .....Joyce Boni

A-3. Approval of Charters .....Joyce Boni
   a. Internal Audit Charter
   b. CARMC Charter

A-4. Overview of Enterprise Risk Management ..... Lynne Sanders and Tim Wiseman

A-5. Update from the IT Security Working Group ..... Keith Werner
   a. Summary of Policies
   b. Summary of Recommendations
   c. MCNC Presentation

CLOSED SESSION

A-6. Approval of the Closed Session Minutes
   of March 8, 2018 and March 20, 2018 ..... Jim Holmes
   a. March 8, 2018
   b. March 20, 2018

A-7. Legal and Audit Update ..... Tom Shanahan and Lynne Sanders

OPEN SESSION

A-8. Other Business ..... Jim Holmes

A-9. Adjourn

Additional Information Available

A-4. Overview of Enterprise Risk Management Audio File (Access code: carmc)

DRAFT MINUTES

March 8, 2018
University of North Carolina System Office
Center for School Leadership Development, Room 128
Chapel Hill, North Carolina

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

Chancellor participating was Joseph Urgo.

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

---

1. Call to Order

Chair Holmes called the meeting to order at 2:30 p.m., on Thursday, March 8, 2018.

2. Update on the IT Security Working Group (Item A-1)

Keith Werner gave the committee an update on the IT Security Working Group (ITSWG). The ITSWG has been formed to address key risk areas and has already held two (2) meetings. The term of the ITSWG is 90 days from the initial meeting. The working group's initial recommendations focus on two policies: IT Governance, and User Identity and Access Control.

3. Review of the Information Technology Governance Policy (Item A-2)

Keith Werner reviewed with the committee the Information Technology Governance Policy (1400.1) that seeks to create a more robust policy to cover the information technology and information resource needs that continually evolve.

4. Review of the User Identity and Access Control Policy (Item A-3)

Keith Werner also reviewed with the committee the User Identity and Access Control Policy (1400.3), which directs the UNC System Office and constituent institutions to evaluate and conduct risk-based implementation of appropriate identity confirmation and access control, such as multi-factor authentication.

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 G.S. 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: Carolyn Coward
Motion carried

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

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

Motion: Carolyn Coward
Motion carried

THE MEETING RESUMED IN OPEN SESSION.

There being no further business, the meeting adjourned at 3:15 p.m.

_____
William Webb, Secretary

DRAFT MINUTES

March 20, 2018
University of North Carolina System Office
Spangler Center, Executive Conference Room
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 or by phone: Kellie Hunt Blue and William Webb. The following committee members were absent: Carolyn Coward and Walter Davenport.

Chancellor participating was 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 2:03 p.m., on Tuesday, March 20, 2018, and called for a motion to approve the open session minutes of January 25, 2018.

MOTION: Resolved, that the Committee on Audit, Risk Management, and Compliance approve the open session minutes of January 25, 2018, as distributed.

Motion: William Webb
Motion carried

2. Review of Draft Policies (Item A-2)

At the March 8, 2018 meeting, the committee discussed two new policies: the Information Governance policy and the User Identity and Access Control policy. There was discussion that the policies were under review by constituent institutions and that minor updates may be made to the policies as presented based on feedback. Chair Holmes asked the committee if there were any suggestions for changes to be made to the policy. There being no recommended changes by the committee, Chair Holmes asked for a motion to approve the policies with understanding that minor updates may be made to the final policies moving forward for full board approval in May.

MOTION: Resolved, that the Committee on Audit, Risk Management, and Compliance approve the Information Technology Governance policy and the User Identity and Access Control policy and recommend them to the full Board of Governors for a vote through the consent agenda at the next meeting.

Motion: William Webb
Motion carried

3. Review of Charters (Item A-3)

Joyce Boni, chief audit officer, presented the Charter for the Committee on Audit, Risk Management, and Compliance and the Internal Audit Charter for the UNC System Office for review. Updates to the charters were discussed briefly for the information of the committee members and will be presented to the committee for approval at the next meeting.

4. 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 G.S. 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: Kellie Hunt Blue
Motion carried

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

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

Motion: William Webb
Motion carried

THE MEETING RESUMED IN OPEN SESSION.

5. Other Business (Item A-6)

No further business matters were discussed in open session.

There being no further business, the meeting adjourned at 3:01 p.m.

_____

William Webb, Secretary

AGENDA ITEM

A-2. Internal Audit Update.....Joyce Boni

Situation: The chief audit officer is to provide periodic updates on the UNC System Office's internal audit activities.

Background: In accordance with the committee charter and the *International Standards for the Professional Practice of Internal Auditing (Standards*) issued by The Institute of Internal Auditors, the committee is to receive periodic updates on the UNC System Office's internal audit activities. Such updates help the committee to assess internal audit's performance relative to the annual audit plan.

Assessment: The attached document identifies the current status of the 2017-2018 internal audit projects that were initially approved by the committee in September 2017 as well as any significant changes to the plan.

Action: This item is for information only.

UNC System Office Internal Audit Plan

Fiscal Year 2017-2018

Description	Status
Prior Year Carry Over	
Compliance Audit: End User Data Storage & Security Awareness	Issued January 2018
Risk Assessment/2018 Audit Plan Development	Completed
Internal Control/Operational Procedures Review	
Go Global Expenditure Process & Procedures	Deferred
Design of the Vendor Payment Process at UNC-TV	Cancelled
Design of Independent Contract Evaluation Process	Not Started
Design of the Employee On-boarding/Off-boarding Process	Changed to Consult
Compliance Reviews	
NC New Teacher Support Program	Cancelled
Follow-up Reviews	
System Office Internal 2016 Travel & Purchase Card Follow-up, Plus Travel Review	In Process
OSA 2017 IT General Controls Audit Follow-up	Issued October 2017
System Office Internal 2017 GEAR-UP	Not Started
Investigations	
Unplanned/Various as occurs: Investigations of internal/external hotline reports and similar types of investigations	Not Started
Petty Cash Investigation	Issued August 2017
Special Projects/Consultations/Other	
Annual Risk Assessment/FY2019 Audit Plan Development	Not Started
Finance and IT Consults: Data Modernization, Enrollment Growth, Electronic Forms, Travel Procedures, Cybersecurity, IT policies	In Process
Academic Affairs Consult: Licensure Procedures Consult	Not Started
Strategy & Policy Consults: Program Development & Process Consult	Not Started
Academic & Student Affairs Consult: NC Pathways Agreements & Procedure Updates	Cancelled
UNC-TV Consults: New CRM System, FCC Tower Project, Cost Methodology, other	Not Started
Quality Assurance Review Preparation	In Process
Special Project: IA assistance at ECSU (added)	Completed
Board Meetings/Unit Oversight & Marketing	In Process
Other Consults/Committees: Routine consults for UNC-TV and System Office such as: Cheatham-White Scholars, Annual Self-Assessment of Controls, and other consults; Charter updates; Annual Certifications; CAO/OIA committee meetings; Clery Training Presenter; New Hire Interview Panel; External Audit Assistance and other projects.	In Process

Red denotes changes since the last update in January 2018.
This status update does not include audit projects for NCSSM or SEAA.

AGENDA ITEM

A-3. Approval 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 being 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 internal audit function should each have a charter to outline their respective roles and responsibilities. These charters must be periodically reviewed and updated if necessary.

Both charters were last updated in March 2017. Since then, The Institute of Internal Auditors has provided guidance on implementing the 2015 revised standards. In addition, the UNC System has adopted policies that impact the committee's duties. Both charters have been updated accordingly.

Assessment: The proposed revisions to the committee and internal audit charters are attached and include clean and marked versions.

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

THE UNIVERSITY OF NORTH CAROLINA SYSTEM

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, the Board of Governors of the University of North Carolina, 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 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 execution of 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 according 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 communication of 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 CARMC. The chief audit officer shall have direct and unrestricted access to the president and CARMC.

Administrative oversight includes day-to-day oversight such as approval of the chief audit officer's annual leave and travel. Functional oversight by 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 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 input from CARMC. Ensure the annual planning and risk assessment process addresses information security. Submit the plan to the president and 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 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 processes; 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, CARMC, and the appropriate levels of management.
    3. As appropriate, provide consulting and advisory services to management that add value and improve 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 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 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 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 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 to meet the requirements of this 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 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 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 as 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 May 2018

THE UNIVERSITY OF NORTH CAROLINA SYSTEM

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~~ the Board of Governors of the University of North Carolina, 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 in the~~ execution of assigned responsibilities to achieve the organization's goals and objectives. This may include~~s~~:

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~~ensure~~ 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 according ~~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 communication of 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 CARMC~~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 input 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 processes; 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 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 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 to meet the requirements of thise ~~C~~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~~to~~: 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 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~~ as 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~~

THE UNIVERSITY OF NORTH CAROLINA SYSTEM

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 (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 committee 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

The chair of the Board of Governors will select the committee chair, members, 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. Must be independent of the UNC System or associated entity management and free of any relationship that would impair the members' 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 committee expects all communication with UNC management and staff as well as external assurance providers to be direct, open, and complete.

The committee chair will collaborate with senior management and the chief audit officer to establish a work plan that ensures the responsibilities of 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 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 committee 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 Office of the State Auditor 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 and approve 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 or regulatory agencies and or information from management. This includes recommendations and planned actions in order to assess the adequacy and effectiveness of the organization's internal control systems in response to risks as well as updates on information technology security processes 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 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. These actions include 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 a 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., Chair of CARMC	Date
W. Louis Bissette, Jr., Chair of the Board of Governors	Date

Last updated and approved May 2018

THE UNIVERSITY OF NORTH CAROLINA SYSTEM

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 (the Board) that 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 committee 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.

III. Organization

~~The Committee on Audit, Risk Management, and Compliance will be a standing committee of the UNC Board of Governors.~~ The chair~~man~~ of the Board of Governors will select the ~~C~~committee chair, members, and determine the number of voting members. Continuance of committee members and their 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 m~~Must be independent of the UNC System or associated entity management and free of any relationship that would impair the members' independence.
B. ~~Committee members m~~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 Administration~~system 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 committee expects all communication with UNC management and staff as well as external assurance providers to be direct, open, and complete.

The committee chair will collaborate with senior management and the chief audit officer to establish a work plan that ensures the responsibilities of 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 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 committee 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 Office of 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 and approve 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 or regulatory agencies and information from management. This includes recommendations and planned actions in order to assess the adequacy and effectiveness of the organization's internal control systems in response to risks as well as updates on 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. These actions include 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.

Joyce D. Boni, Chief Audit Officer Date

James Holmes, Jr., Chair of CARMC Date

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

Last updated and approved ~~March 2017~~

AGENDA ITEM

A-4. Overview of Enterprise Risk Management..... Lynne Sanders and Tim Wiseman

Situation: The narrated presentation of Enterprise Risk Management communicates the importance of how enterprise risk is defined, why and how risk is managed, and the governance structure required for the establishment of a successful program.

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

Assessment: Having accomplished some initial ERM development work at the UNC System level, we are now ready to develop the first iteration of the UNC System risk register. The risk register is an easily understandable listing and map of the major enterprise risks and issues. It is prepared with the strategic plan goals of the organization in mind and intended to inform the thinking, goal setting, and strategy of UNC System leaders and the Board.

Action: This item is for information only.

AGENDA ITEM

A-5. Update from the IT Security Working Group ..... Keith Werner

Situation: The University of North Carolina System is committed to maintaining sound operations and practices relating to information governance, information security, and data protection. Roles and responsibilities that support proper oversight and accountability for all components of the information system environment should be defined at each institution and the UNC System Office.

Background: The Committee on Audit, Risk Management, and Compliance (CARMC) has identified information governance and information security as areas of enterprise risk. Recent audit work completed by the Office of the State Auditor (OSA) and internal auditors within the UNC System have pinpointed certain deficiencies in IT security that institutions are working to address. The IT Security Working Group (ITSWG) has been formed with membership drawn from across the UNC System to address key risk areas and to keep the president and the chair of CARMC apprised of progress and institutional needs relating to these matters. The term of the ITSWG is 90 days from inception.

Assessment: The ITSWG has detailed the foundational pieces of information security and IT governance. Notably, these include the Information Security Policy (1400.2) and the ISO 27002 Standards and Guidelines. Information security is a complex issue and highlights the need for sound IT governance at each campus and the UNC System Office, as well as general security and system access controls. The ITSWG's initial recommendations focused on two policies: IT Governance (1400.3), and User Identity and Access Control (1400.3).

In addition, the ITSWG was tasked with an evaluation of each security control related to ISO 27002 for each constituent institution. The ITSWG has developed the following recommendations: (1) Adopt the IT Governance Guiding Principles set forth by the IT Governance (1400.1) policy, (2) Convene each campus CIO and senior leadership to document resource and service needs, review existing vacancies and budget for immediate needs, and document gaps for budgetary requests in the long session, (3) Identify the appropriate funding to meet the User Identity and Access Control Requirement, (4) Identify the appropriate funding for each campus to maintain a minimum $1 million coverage level in cybersecurity insurance to cover response services, legal and public relations consultation, and call center expenses, (5) Identify the appropriate funding for the standardization and procurement of annual security awareness training, integrated into existing learning management systems or other delivery means at the campus level, (6) Broaden the existing partnership with MCNC to

deliver security services to the campuses, (7) Utilize the existing system level IT governance structure (CIO Council and Information Security Council) for continued recommendations, with an initial charge of investigating risk assessment automation and a security awareness toolkit, and (8) Broadly publish the policies and recommendations from the ITSWG to all key stakeholders.

Action: This item is for information only.


N★C
THE UNIVERSITY OF
NORTH CAROLINA SYSTEM

THE UNIVERSITY OF NORTH CAROLINA SYSTEM

Information Technology Security Working Group (ITSWG)

ITSWG Background

- Scope
- Membership
- Goals
- Workgroup Actions

Policies

- Information Technology Governance (1400.1)
- User Identity and Access Control (1400.3)

IT Governance Guiding Principles

UNC System Office will be responsible for the IT governance core set of principles; each campus will own the implementation of the IT governance program, which aligns to the following:

- Actively Design IT Governance
  - Review/redesign process and schedule
  - Approval process requirement that includes broad campus support
  - Continuous monitoring
  - Exception handling
- Governance Framework
  - Ownership and accountability
  - Business and IT synergy
  - Account for all IT, including distributed IT
  - CIO access to senior leadership

IT Governance Guiding Principles

- Implement Policies and Procedures
  - Awareness and training
  - Gaps and associated action plans
  - Policies, guidelines and standards
  - Process to verify compliance
- Information Security Program
  - Oversight
  - Training and awareness
- Transparency
  - Reporting requirements set forth by president or Board of Governors
  - Timely collaboration with UNC System on gaps, needs, or shared service opportunities

ITSWG Recommendations

Campus Resource Needs Process

- Use new IT Governance Policy (1400.1)
- Broker communication between CIO and campus senior leadership
  - Document needs for resources and/or services
  - Review existing vacancies/budget for immediate needs
  - Document gaps, develop budget requests for long session

User Identity and Access Control Requirement ($282,872 annual estimate)

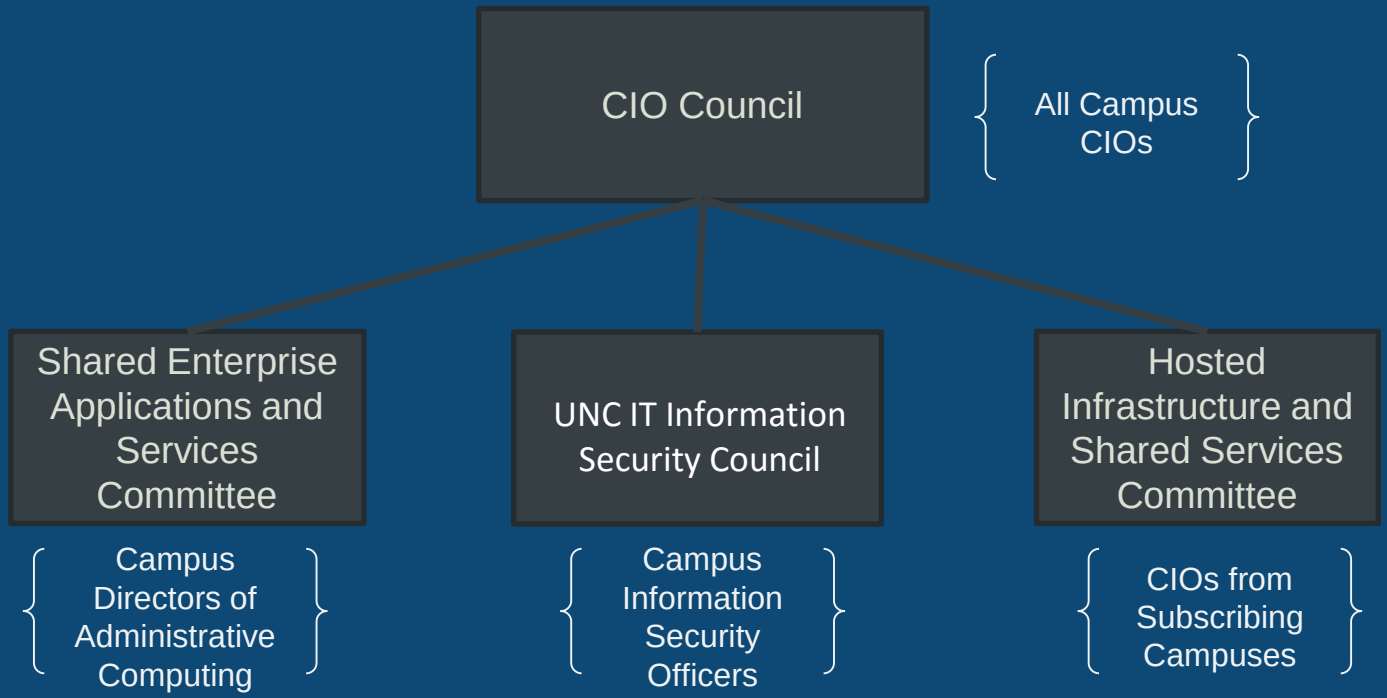
Cyber Insurance ($425,000 annual estimate)

- Each campus will maintain a minimum $1 million coverage level for: response services, legal & PR consult, notification, call center expenses

ITSWG Recommendations

- Annual Security Awareness Training ($100,000 annual estimate)
  - SCORM compliant awareness materials to be integrated into learning management systems or other delivery means at the campus level
  - Standardize/procure
- Partner with MCNC for Security Services
- Reporting and Oversight
  - Executive and Board briefing(s)
- Utilize Existing IT Governance Structure – ISC, CIO Council
  - Charge ISC/CIOC with risk assessment automation review
  - Develop and implement a security awareness toolkit
- Publish Recommendations from CARMC/ ITSWG

CIO Governance



QUESTIONS?

Security Services Update

May 2018

Who We Serve Today

Founded in 1980 as a non-profit research institute based in Research Triangle Park

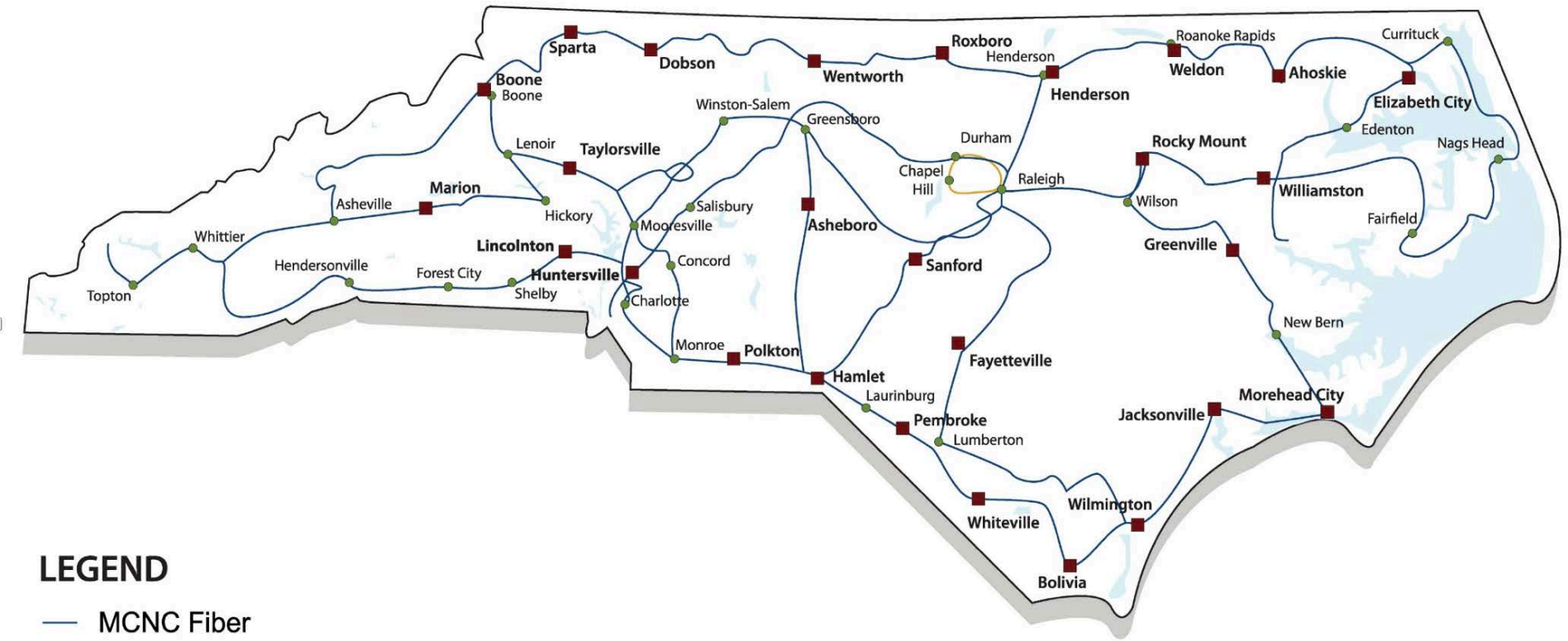
NCREN Serves

- 17 UNC System Institutions
- 26 of 36 ICUs
- 58 Community Colleges
- 115 K-12 LEAs
- 76 Charter / Other Public K-12
- 37 Hospitals
- 55 County Health Agencies / Clinics
- 15 NC State Highway Patrol Locations

MCNC

MCNC Fiber Infrastructure

Enabling the Operation of the North Carolina Research and Education Network



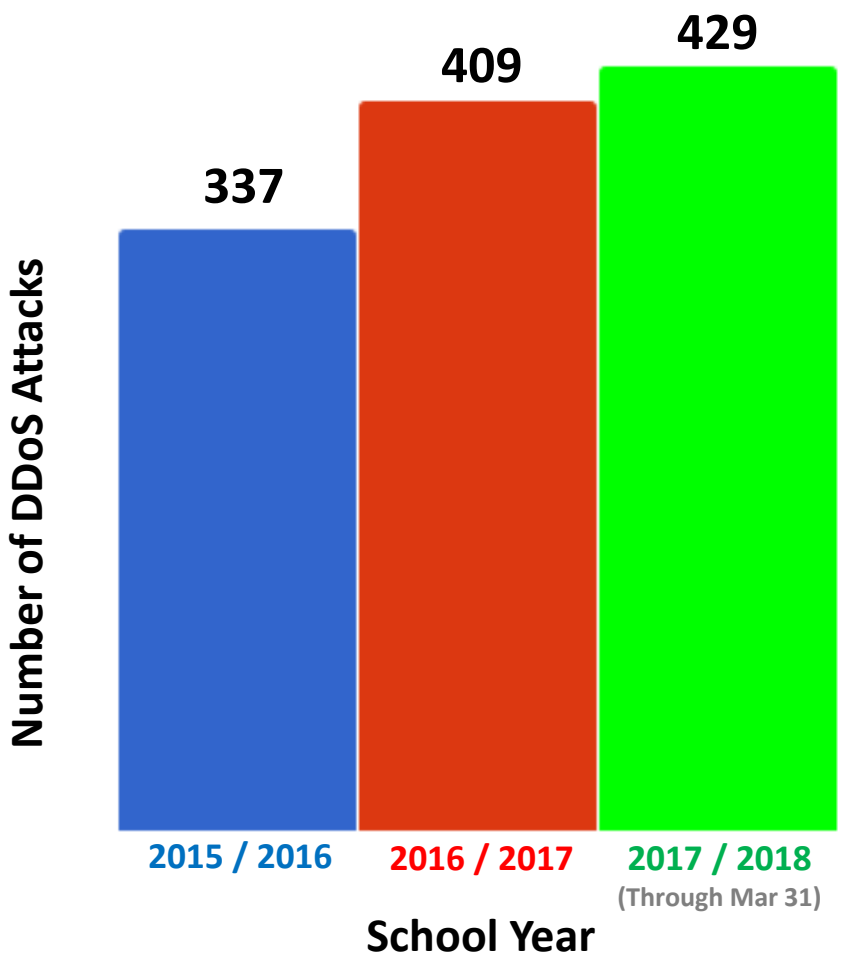
LEGEND

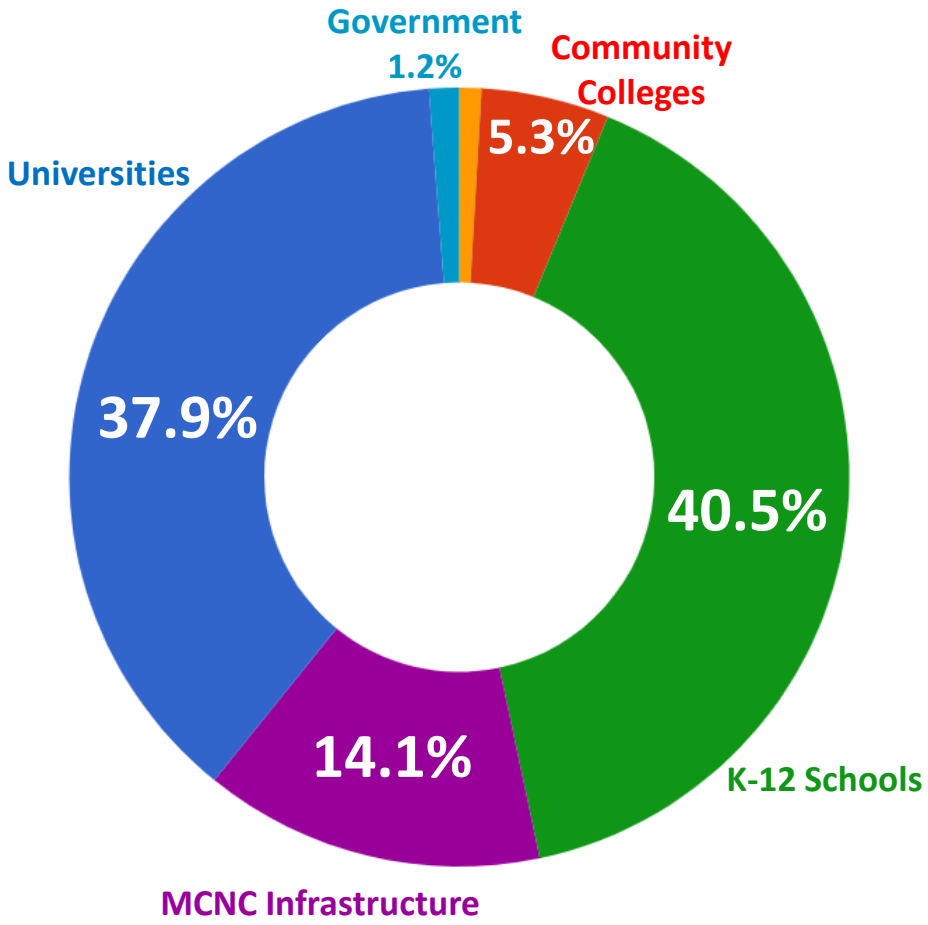
- MCNC Fiber
- MCNC Co-location Facility
- MCNC Fiber (Triangle Ring)
- City

As of July 2017

MCNC®
Connecting North Carolina's Future Today

DDoS Attack Protection





DDoS Attacks on NCREN
Sep 2014 – Mar 2018

Automatic Protection

Protection starts within seconds

Highly Effective

Part of Standard MCNC Network Service

DDoS Attacks No Longer a Major Security Risk for MCNC Customers

MCNC

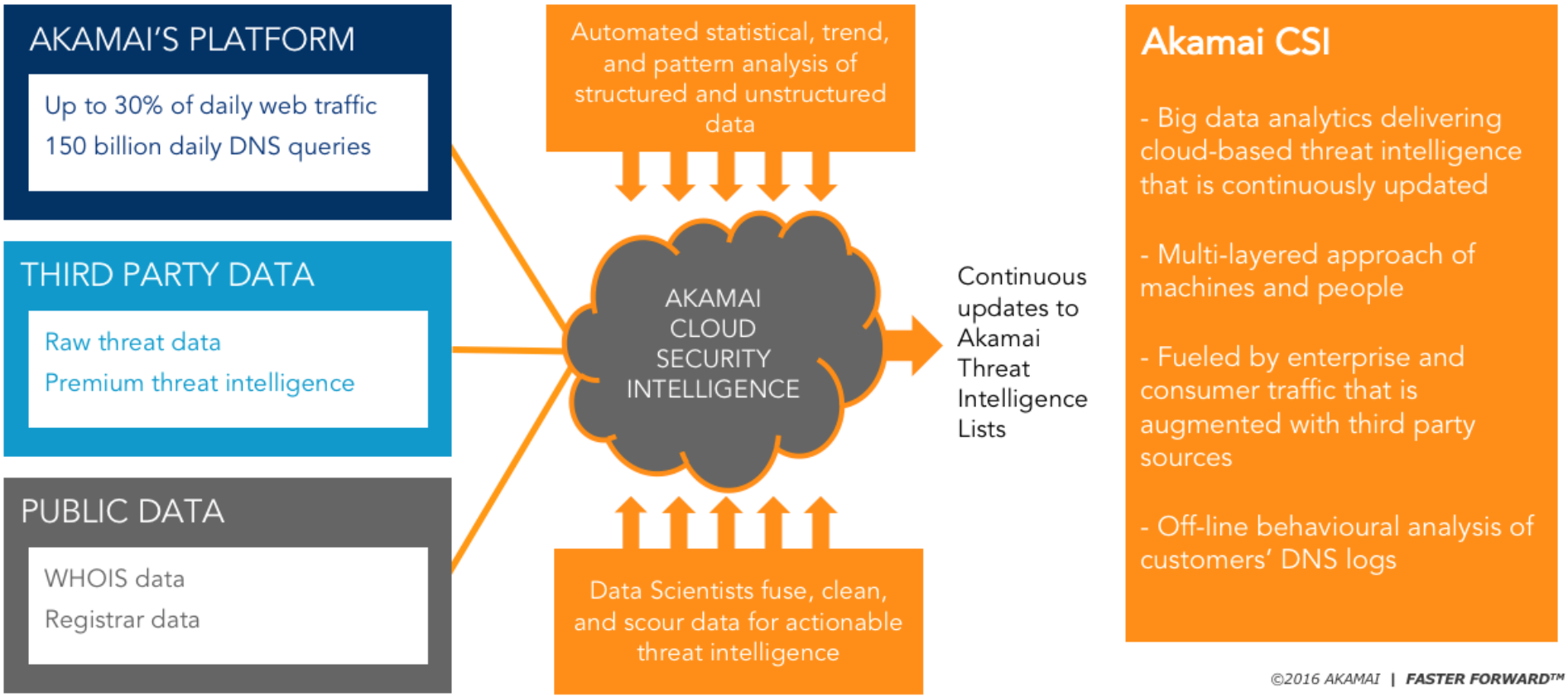
I just wanted to take a moment to thank you and your team for the DDoS Auto-Mitigation service you provide that we have subscribed to after it became available this year. It has been enacted twice in the last 5 days.

The service worked so quickly and so well, if we had not received the notification provided by the DDoS Auto-Mitigation service that the service had been enabled for the particular destination address, we would not even have known that anything had occurred.

Thank you for your continued support for our organization and others in the State of North Carolina

- NCREN K-12 customer. April 2018

DNS Security Filtering



MCNC

DNS Security Filtering

No Hardware or Software to Deploy or Manage

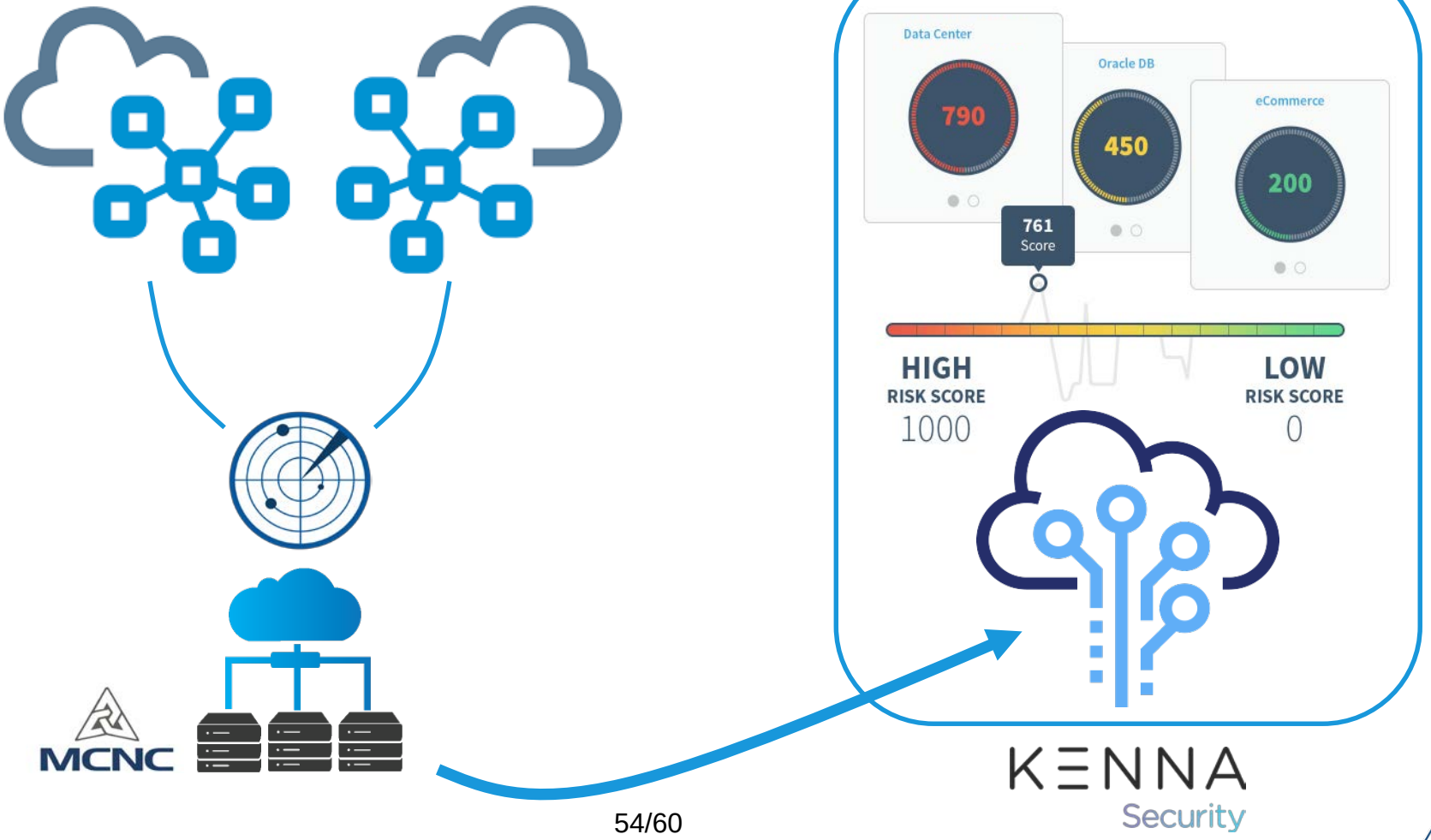
Lightweight Service

Simple to Setup / Operate

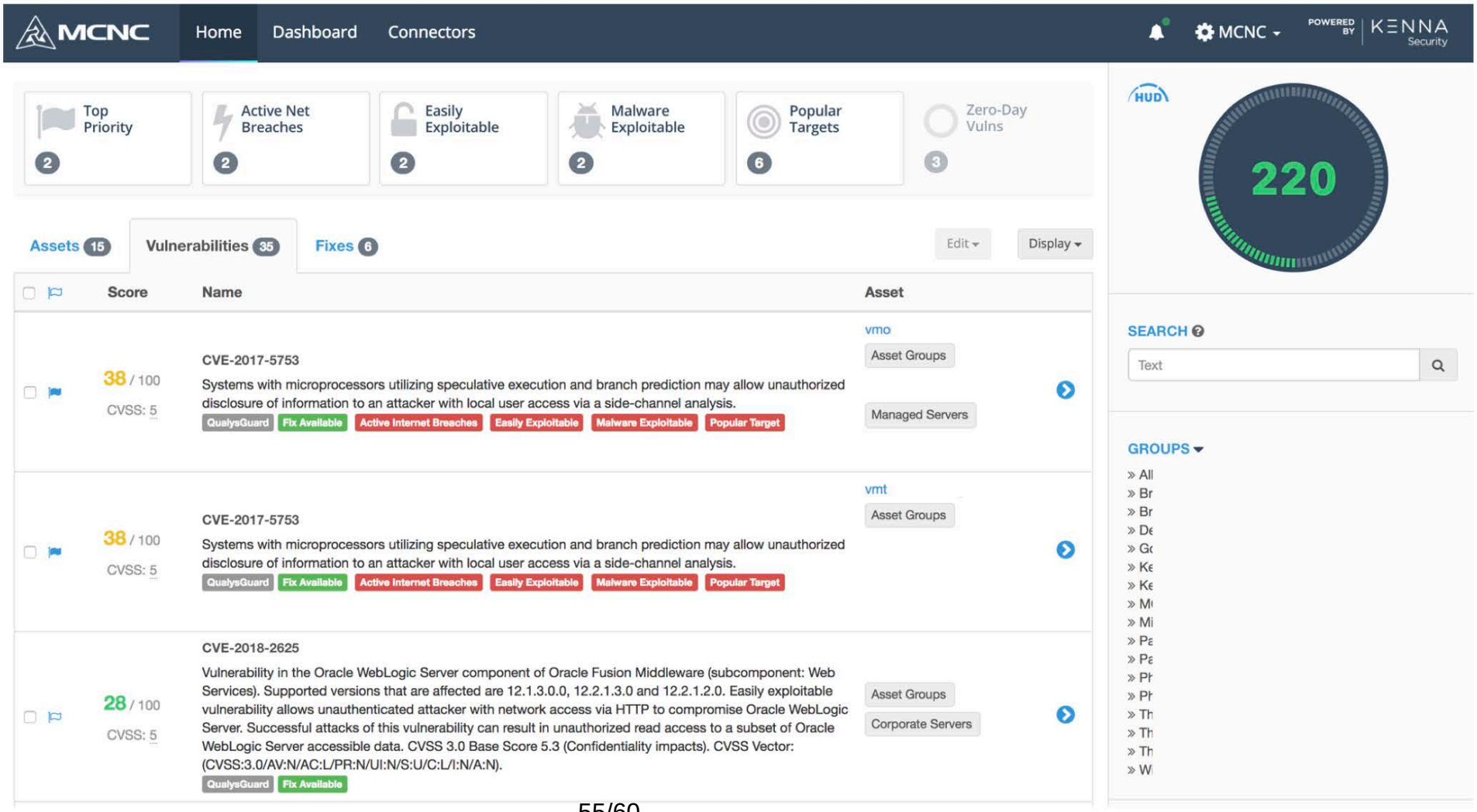
Significant Price Advantage

MCNC

Continuous Monitoring
and Risk Assessment



Continuous Monitoring
and Risk Assessment



MCNC

Continuous Monitoring
and Risk Assessment

MCNC

Continuous Monitoring

and Risk Assessment

No Hardware or Software to Deploy or Manage

Scanning is Fully Managed

Continuously Updated View of Risk Posture

Risk Scores Tell You What to Fix First

(and how to fix it)

Executive Reporting Dashboards

MCNC

Advisory Consulting Services

Security Program Assessments

Risk Assessments

Audit Finding Remediation

Application / System Security Testing

Security Policy Creation

Security Technology Evaluation

Staff Augmentation (Virtual CISO)

MCNC

Advisory Consulting Services

Significant Demand Across NC Schools

Economies of Scale with Centralized Capability

MCNC History of Success

- Network Services
- K-12 Consulting Services
- Existing Security Services

MCNC is Trusted Partner to NC Schools

MCNC

MCNC SECURITY

MCNC