UNC BOARD OF TRUSTEES

AUDIT, COMPLIANCE, AND RISK MANAGEMENT COMMITTEE

March 23, 2022, 9:00 a.m.
Chancellor's Ballroom, Carolina Inn

OPEN SESSION

FOR ACTION

1. Adoption of the Audit, Compliance, and Risk Management Committee Charter and amendments to the Office of Internal Audit Charter
   Dean Weber, Chief Audit Officer

FOR INFORMATION ONLY

(No formal action is requested at this time)

1. Office of Internal Audit Information Technology Audit Initiatives
   Dean Weber, Chief Audit Officer

2. Cyber Security Update
   Michael Barker, Vice Chancellor for Information Technology and Chief Information Officer
   Dennis Schmidt, Assistant Vice Chancellor for Information Security and Privacy and Chief Information Security Officer

*Some of the business to be conducted is authorized by the N.C. Open Meetings Law to be conducted in closed session.

COMMITTEE MEMBERS
Marty Kotis, Chair
Malcolm Turner, Vice Chair
Dave Boliek, ex-officio
Allie Ray McCullen **John Preyer**

CLOSED SESSION MOTION FOR AUDIT, COMPLIANCE, AND RISK MANAGEMENT COMMITTEE MEETING WEDNESDAY - 3/23/2022

Mr. Chairman, I move that the Audit, Compliance, and Risk Management Committee go into closed session pursuant to North Carolina General Statutes Section 143-318.11 (a)

(1) (to prevent the disclosure of privileged information under Section 126-22), (a) (3) (to consult with an attorney employed or retained by the public body in order to preserve the attorney-client privilege between the attorney and the public body), and (a) (7) (to plan, conduct, or hear reports concerning investigations of alleged criminal misconduct).

The University of North Carolina at Chapel Hill
Board of Trustees

Audit, Compliance, and Risk Management Committee
Wednesday, March 23, 2022

SUBJECT: Committee review and recommendation for approval of the Board of Trustees' *Audit, Compliance, and Risk Management Charter* and the *Office of Internal Audit Charter* (ACTION)

BACKGROUND:
The establishment of the University of North Carolina at Chapel Hill Board of Trustees' Audit, Compliance, and Risk Management Committee necessitates the development and approval of a charter detailing the Committee's oversight responsibilities and operating procedures. The newly developed and proposed *Audit, Compliance, and Risk Management Committee Charter* supports this agenda item.

Separately, the University of North Carolina at Chapel Hill maintains a comprehensive and effective internal audit program adhering to the *International Standards for the Professional Practice of Internal Auditing* of the Institute of Internal Auditors. Change in the Office of Internal Audit's reporting from the Board of Trustees' Finance, Infrastructure, and Audit Committee to the Audit, Compliance, and Risk Management Committee necessitates charter revisions. A track-change version of the O*ffice of Internal Audit Charter* identifying updated changes and the proposed revised document support this agenda item.

RECOMMENDED ACTION:

Motion to the University of North Carolina at Chapel Hill Board of Trustees for the approval and authorization of (1) The *Audit, Compliance, and Risk Management Charter* and (2) the *Office of Internal Audit Charter* and authorize the Committee Chairman's and the Chancellor's signatory endorsement of the documents.

THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

The University of North Carolina at Chapel Hill
Audit, Compliance, and Risk Management Committee Charter

Committee Oversight Responsibilities and Operating Procedures

I. Background and Authority

The Committee on Audit, Compliance, and Risk Management (Committee) is a standing committee of the University of North Carolina at Chapel Hill (University) Board of Trustees. The Committee is supported and staffed at the Chancellor's direction by the University's Office of Internal Audit, the Chief Audit Officer, and the Vice Chancellor for Institutional Integrity and Risk Management.[1]

The Committee has access through the Chancellor to other members of management and employees, and relevant information across the University as necessary to discharge its oversight responsibilities.

The legislation and policies relevant to the Committee's jurisdiction and oversight responsibilities are outlined in Appendix A.

The Committee's specific responsibilities concerning oversight of the University's Office of Internal Audit are outlined separately in the *Office of Internal Audit Charter*.

II. Purpose

The purpose of the Committee is to provide structured, systematic review and advice to the Chancellor on behalf of the Board concerning the University's audit, compliance, and risk management activities, as well as the University's internal control practices. It is the responsibility of University management under the direction of the Chancellor as the institution's executive and administrative head to maintain programs and systems of internal audit, compliance, risk management, and ethics. The Committee does not exercise decision-making authority on behalf of the University and the Committee's responsibilities do not replace or duplicate management's responsibilities. In addition to providing advice and guidance to management, the Committee sets broad policy for ensuring accurate, sound risk management and ethical behavior; exercises oversight responsibilities on behalf of the Board as defined herein; and makes reports and recommendations to the Board related to:

A. The integrity of the University's annual financial statements.
B. The internal audit function, external auditors, firms, and other providers of assurance.
C. The University's compliance with legal, regulatory, ethics, conflict of interest, and policy requirements.
D. The University's information governance and security program (Sections 1400.1 and 1400.2 of the UNC Policy Manual).
E. The required elements of the University's associated entities.
F. University-wide enterprise risk management and compliance processes.
G. Campus safety and emergency operations.
H. Additional matters that may implicate the University's interest in ensuring sound risk management and ethical behavior.

[1] See, Section 502 D of *The Code of The Board of Governors of The University of North Carolina*.

III. Organization

The chair of the Board of Trustees selects the Committee members and designates the Committee officers after evaluating the members' collective competencies and balance of skills. The Committee shall consist of no fewer than five (5) voting members appointed from the membership of the Board of Trustees. The Committee members:

A. Must be independent of the University and any University associated entity management and free of any relationship that would impair the members' independence.[2]
B. May not receive, directly or indirectly, consulting, advisory, or other fees from the University, associated entities of the University, the UNC System, or outside contractors hired to perform special engagements.
C. Should collectively possess sufficient knowledge of audit, finance, higher education, information technology, law, governance, risk management, compliance, and principles of internal control to respond to regulatory, economic, reporting, and other emerging developments and needs.
D. Must adhere to the UNC System's code of conduct and values and ethics established by the UNC System, including Sections 200.1 (Dual Memberships and Conflicts of Interest) and 200.7 (Duties, Responsibilities, and Expectations of Board Members) of the UNC Policy Manual, and University *Policy on Individual Conflicts of Interest and Commitment*. Consistent with UNC System policy and the North Carolina State Ethics Act, it is the responsibility of the Committee members to disclose any conflict of interest or appearance of a conflict of interest to the Committee chair.

IV. Meetings

The Committee shall meet no fewer than four times a year. The Committee will invite when needed, the Chancellor, external and internal auditors, representatives of the Office of the State Auditor, Office of Internal Audit staff, Institutional Integrity and Risk Management staff, 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 to staff. The Committee expects all communication with University management and staff, as well as external assurance providers, to be direct, open, and complete.

The Committee chair will collaborate with the Chancellor, the General Counsel, the Chief Audit Officer, and the Vice Chancellor for Institutional Integrity and Risk Management to establish meeting agendas that ensure the responsibilities of the Committee are properly scheduled and carried out. Meeting agendas and related materials will be prepared and provided in advance to members and meetings will be conducted in accordance with the Open Meeting Act. Minutes will be prepared following applicable law and policy.

V. Education

The Chancellor and the designated Committee staff are responsible for providing the Committee with educational resources related to auditing, compliance, risk management, accounting principles and practices, legal and regulatory requirements, ethics, conflicts of interest, and other information that the Committee may require. TheUniversity's Chief Audit Officer and the Vice Chancellor for Institutional Integrity and Risk Management will assist the Committee in maintaining literacy in the appropriate areas related to the Committee's function.

VI. Duties and Responsibilities

[2] The term "Associated Entity" is defined and describe in Section 600.2.5.2[R] of the UNC Policy Manual, and includes, "any foundation, association, corporation, limited liability company (LLC), partnership, or other nonprofit entity: (1) that was established by officers of the University; or (2) that is controlled by the University; or (3) that raises funds in the name of the University; or (4) that has a primary purpose of providing services or conducting activities in furtherance of the University's mission pursuant to an agreement with the University; or (5) that has a tax-exempt status that is based on being a support organization for the University."

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

A. General

1. Adopt and annually review and update the Committee's charter detailing the Committee's responsibilities and operating procedures for approval by the Board of Trustees. The operating procedures shall describe the scope of the duties and responsibilities of the Committee, the structure of the University's functions within the Committee's oversight responsibilities, and the basic responsibilities of management concerning each function.
2. Hold meetings following the requirements of the Open Meetings Act.
3. Report Committee oversight activities to the Board of Trustees, along with advice and recommendations as the Committee may deem appropriate.
4. Hear reports from management concerning investigations into any matters within the Committee's scope of oversight responsibility.
5. When deemed necessary by the Board of Trustees on the Committee's recommendation, advise the Chancellor and his or her delegate on the engagement of independent auditors.
6. Review and monitor implementation of management's response to recommendations by internal and external audits or other assurance providers.
7. Review and/or recommend policies to the Board that support the internal audit, compliance, and risk management functions.
8. Consider and advise the Chancellor regarding the effectiveness of the University's internal control system inresponding to risks, including information technology governance and security.
9. Receive legal reports from the General Counsel or the University's retained outside counsel.
10. Perform other oversight responsibilities assigned by the Board of Trustees.

B. Financial Statements

Management is responsible for the preparation, presentation, and integrity of the University's financial statements and the appropriateness of the accounting, internal control, and reporting policies used by the University. The Office of the State Auditor currently conducts the annual audit of the University's financial statements. The following shall be the principal duties and responsibilities of the Committee regarding the financial statements of the University:

1. Receive an annual overview from the State Auditor or a designated representative regarding the annual audits (financial and compliance) of the University. Review the results of the University's independent financial statement audit by the State Auditor, including any difficulties encountered and reportable issues.
2. Resolve any differences between management and the State Auditor regarding financial reporting and other matters.
3. Review with management and the University General Counsel any legal matters (including pending litigation) that may have a material impact on the University's financial statements and any material reports or inquiries from regulatory or governmental agencies.

C. External Audit/Outside Auditors

In addition to the annual financial statement audits (noted above), the Office of the State Auditor conducts federal compliance audits of select state institutions on an annual basis, and may, on occasion, conduct other audits or investigations of the University. Other external auditors may also be engaged by the UNC System Office or by the University for particular projects and matters. Concerning any such external audits, the Committee's responsibilities are as follows:

1. Review significant audit-related communications from the Office of the State Auditor or, as necessary, other external audit groups or firms concerning the University. Meet separately with the external auditors or firms, if necessary, to discuss sensitive and any other matters that the Committee or auditor believes should be discussed privately.
2. Review reports on the progress of implementing approved management action plans and audit recommendations resulting from completed audit engagements.
3. 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.

4. Receive audit reports in those matters where the Board of Trustees or chancellor authorize or request an external audit or another independent review.
5. Where needed and appropriate, as determined by the chancellor or the chief audit officer, or the general counsel, receive audit reports in those matters where a board of trustees or the chancellor or affiliated entity authorizes or requests an external audit or another independent review.

D. Internal Audit

The Office of Internal Audit is responsible for the daily direction, oversight, and management of the University's internal audit work. Concerning any such work of the Office of Internal Audit, the Committee's responsibilities are as follows:

1. Monitor internal control systems at the University through activities of the internal and external auditors.
2. At the beginning of the audit cycle, review and recommend to the Board for approval the University's fiscal year internal audit work plan for the institution as prepared by the chief audit officer. At the end of the cycle, reviewing a comparison of the approved internal audit plan to internal audits performed.
3. Review internal audit reports and summaries of external and internal audit activities. Ensure that management is devoting adequate attention to issues raised.
4. Review all audits and management letters of University Associated Entities as defined in section 600.2.5.2[R] of the UNC Policy Manual.
5. Obtain annual assurance from the chief audit officer that all internal audits were conducted following IIA Professional Standards.
6. As needed, review and recommend to the Board for approval revisions to the Office of Internal Audit Charter.
7. Review and resolve any significant disagreement between University management and the Office of Internal Audit in connection with the preparation of internal audit reports and results.
8. Serve as the audit committee for the University's internal audit function. The Committee's oversight is defined in the charter for the UNC System Office internal audit function as outlined in Appendix B.
9. Review and recommend to the Board for approval, in consultation with the chancellor, the budget and resources for the Office of Internal Audit, including the chief audit officer's evaluation and remuneration.
10. The University's chief audit officer's appointment or termination of appointment shall be by the chancellor, after consultation and concurrence of the Board of Trustees.
11. Support Chapter 1400 of the UNC Policy Manual, *Information Technology*, including ensuring the following:

1400.1 *Information Technology Governance*:

1. Annual audit plans shall consider, as appropriate, audit activity focused on information technology matters, based on annual risk assessments.

2. The Committee shall review and discuss audit activity related to information technology matters and address issues of information technology governance on a regular basis.

3. The Committee 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 System's Committee on Audit, Risk Management, and Compliance.

1400.2 *Information Security*:

1. The Committee shall ensure that information security is addressed in the annual audit planning and risk assessments that are conducted by the institution's internal auditor.

2. The Committee shall periodically include an agenda item for emerging information security matters at its regularly scheduled meetings.

3. The designated senior officer with information security responsibility shall present a report to the Committee, at least annually, on the institution's information security program and information technology security controls.

E. Audit, Compliance, and Risk Management Committee

It is the responsibility of management, rather than the Committee and its members, to ensure adherence to laws, regulations, and policies. The responsibilities of the Committee regarding the University's compliance and risk management activities are as follows:

1. Support the efforts, establishment of, and collaboration among the risk management, ethics, and compliance programs within the University, including recommending to the Board University-wide policies regarding compliance and enterprise risk management.
2. Receive regular reports concerning enterprise risk management and compliance activities from the Vice Chancellor for Institutional Integrity and Risk Management, the Chief Audit Officer, and senior officers.
3. Provide general input regarding the University's adherence to laws, regulations, and policies that pertain to University operations.
4. Review the programs and policies of the University designed by management to assure compliance with applicable laws and regulations.
5. When necessary, meet privately with the General Counsel to discuss any matter that the Committee or the general counsel believes should be discussed privately.
6. Coordinate with other Board committees as appropriate on legal, risk management, and compliance matters.

F. Other Responsibilities

1. 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.
2. Consult with the General Counsel as necessary to review 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.
3. Take other actions, as necessary, to ensure that risk exposures are identified and effectively 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, in consultation with and the approval of the Chancellor in areas under the Chancellor's authority, modify or supplement these duties and responsibilities as needed.

The Committee may request a supplemental review or other audit procedures by the Chief Audit Officer, the State Auditor, or other advisors when the circumstances dictate that further review is required.

The Committee shall annually review and assess the adequacy of the Committee charter and the Office of Internal Audit charter with the assistance of University staff. The Committee chair will confirm annually that the relevant responsibilities in this charter have been carried out.

Approved:

_____ _____

Kevin M. Guskiewicz
Chancellor
University of North Carolina at Chapel Hill

Date

_____ _____

W.M. Kotis III
Chair, Audit, Compliance, and Risk Management Committee
University of North Carolina at Chapel Hill Board of Trustees

Date

THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

Appendix A

Committee on Audit, Compliance, and Risk Management

Statutory and Policy Authority

The legislation and policies relevant to the Committee on Audit, Compliance, and Risk Management's jurisdiction and oversight responsibilities 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 the recommendation ofthe president, shall adopt rules prescribing management staffing standards and internal financial controls and safeguards. UNC-Chapel Hill has been designated as a special responsibility constituent institution.
C. A special responsibility constituent institution is required by G.S. 116-30.8 to have an annual audit conducted by the North Carolina State Auditor.
D. The UNC System and each constituent institution 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. Section 1400.2 of the UNC Policy Manual assigns the responsibility for oversight of the University's information security program to the standing committee with audit responsibility.

THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

The University of North Carolina at Chapel Hill

Office of Internal Audit Charter

I. Background and Authority

A. The chief audit officer reports functionally to the Chair of the Audit, Compliance, and Risk Management (ACRM) Committee and administratively (i.e., day to day operations) to the Chancellor of the University.

II. Purpose & Authority

A. To establish, maintain, and assure that the University's internal audit department has sufficient authority to fulfill its duties, the ACRM Committee will govern the Department and:

1. Recommend to the Board for approval the internal audit charter;
2. Recommend to the Board for approval the risk-based internal audit plan;
3. Receive communications from the chief audit officer on the internal audit department's performance relative to its plan and other matters;
4. Review and recommend to the Board for approval, in consultation with the chancellor, the Department's budget and resources, including the chief audit officer's evaluation and remuneration;
5. Advise the Chancellor or the Board of Trustees regarding the chief audit officer's appointment and/or termination, and
6. Make appropriate inquiries of management and the chief audit officer to determine whether there are inappropriate scope or resource limitations.

B. The chief audit officer will have the unrestricted ability to communicate and interact directly with the Board, including in private meetings without management present.

C. The Board authorizes the internal audit department to:

1. Have full, free, and unrestricted access to all functions, records, property, and personnel necessary to carry out any engagement, provided the department complies with all applicable law and policy regarding the protection of confidential and/or sensitive records and information.
2. Allocate resources, set frequencies, select subjects, determine scopes of work, apply techniques required to accomplish audit objectives, and issue reports.
3. Obtain assistance from the necessary personnel of the University, as well as other specialized services from within or outside the University, to complete the engagement.

III. Independence and Objectivity

A. The chief audit officer will ensure that the internal audit department remains free from all conditions that threaten the ability of internal auditors to carry out their responsibilities in an unbiased manner, including matters of audit selection, scope, procedures, frequency, timing, and report content. If the chief audit officer determines that independence or objectivity may be impaired in fact or appearance, the details of such actual or apparent impairment will be disclosed to appropriate parties.

B. Internal auditors will maintain an unbiased mental attitude that allows them to perform engagements objectively and in such a manner that they believe in their work product, that no quality compromises are made, and that they do not subordinate their judgment on audit matters to others.

C. Internal auditors will have no direct operational responsibility or authority over any of the activities audited. Accordingly, internal auditors will not implement internal controls, develop procedures, install

systems, prepare records, or engage in any other department that may impair an internal auditor's judgment, including:

1. Assessing specific operations for which they had responsibility within the previous year.
2. Performing any operational duties for the University or its affiliates.
3. Initiating or approving transactions external to the internal audit department.
4. Directing the activities of any University employee not employed by the internal audit department, except to the extent that such employees have been appropriately assigned to auditing teams or to otherwise assist internal auditors.

D. Where the chief audit officer has or is expected to have roles and/or responsibilities that fall outside of internal auditing, safeguards will be established to limit impairments to independence or objectivity. Internal auditors will:

1. Disclose any impairment of independence or objectivity, in fact, or appearance, to appropriate parties.
2. Exhibit professional objectivity in gathering, evaluating, and communicating information about the department or process being examined.
3. Make balanced assessments of all available and relevant facts and circumstances.
4. Take necessary precautions to avoid being unduly influenced by their interests or by others in forming judgments.

E. The chief audit officer will confirm to the ACRM Committee, at least annually, the organizational independence of the internal audit department.

F. The chief audit officer will disclose to the ACRM Committee any interference and related implications in determining the scope of internal auditing, performing work, and/or communicating results.

IV. Scope of Internal Audit Activities

A. The scope of internal audit activities encompasses, but is not limited to, objective examinations of evidence to provide independent assessments to the ACRM Committee, management, UNC System Office, and outside parties on the adequacy and effectiveness of governance, risk management, and control processes for the University. Internal audit assessments include evaluating whether:

1. Risks relating to the achievement of the University's strategic objectives are appropriately identified and managed.
2. The University promotes governance, ethics, and integrity and communicates risk and control information.
3. The actions of the University's officers, directors, employees, and contractors comply with the University's policies, procedures, and applicable laws, regulations, and governance standards.
4. The results of operations or programs are consistent with established goals and objectives.
5. Operations or programs are being carried out effectively and efficiently.
6. Established processes and systems enable compliance with the policies, procedures, laws, and regulations that could significantly affect the University.
7. Information and the means used to identify, measure, analyze, classify, and report such information is reliable and has integrity.
8. Resources and assets are acquired economically, used efficiently, and protected adequately.

B. The chief audit officer will report periodically to senior management and the ACRM Committee regarding:

1. The internal audit department's purpose, authority, and responsibility.
2. The internal audit department's plan and performance are relative to its plan.
3. The internal audit department's conformance with The IIA's Code of Ethics and Standards, and action plans to address any significant conformance issues.
4. Significant risk exposures and control issues, including fraud risks, governance issues, and other matters requiring the attention of, or requested by, the ACRM Committee.
5. Results of audit engagements, special projects, investigations, or other activities.
6. Resource requirements.

7. Any response to risk by management that may be unacceptable to the University.

C. The chief audit officer also coordinates activities, where possible, and considers relying upon the work of other internal and external assurance and consulting service providers as needed. The internal audit department may perform advisory (consulting) services, the nature and scope of which will be agreed to by the client, provided the internal audit department does not assume management responsibility. Examples include providing advice and information on internal controls, risk management, and sound business practices. This includes reviewing current practices, interpreting policies and procedures, participating in standing committees, attending ad-hoc meetings, and responding to routine questions. Additionally, this may include working with the UNC System Office, professional organizations, and serving as a liaison between the university and external auditors.

D. Opportunities for improving the efficiency of governance, risk management, and control processes may be identified during engagements. These opportunities will be communicated to the appropriate level of management.

V. Reporting and Monitoring

A. The chief audit officer or a designee will prepare a written report following the conclusion of each internal audit project, special project, and investigation, other than small consulting projects. Audit reports and close-out letters will be distributed to appropriate members of university management, all members of the Board, UNC System Office, and a redacted copy to the Council of Internal Auditing.

Internal audit reports will typically include management's response regarding corrective action taken or to be taken regarding the specific findings. Management's response should include a timetable for anticipated completion of planned corrective action and an explanation for any findings that will not be corrected. If management elects not to correct a finding, its response should include a statement accepting the risk from choosing not to address a reported condition.

VI. Responsibility

A. The chief audit officer has the responsibility to:

1. Submit, at least annually, to senior management and the ACRM Committee a risk-based internal audit plan for review and approval.
2. Communicate with senior management and the ACRM Committee the impact of resource limitations on the internal audit plan.
3. Review and adjust the internal audit plan, as necessary, in response to changes in the University's business, risks, operations, programs, systems, and controls.
4. Communicate with senior management and the ACRM Committee any significant interim changes to the internal audit plan.
5. Ensure each engagement of the internal audit plan is executed, including the establishment of objectives and scope, the assignment of appropriate and adequately supervised resources, the documentation of work programs and testing results, and the communication of engagement results with applicable conclusions and recommendations to appropriate parties.
6. Follow up on engagement findings and corrective actions, and report periodically to senior management and the ACRM Committee any corrective actions not effectively implemented.
7. Ensure the principles of integrity, objectivity, confidentiality, and competency are applied and upheld.
8. Ensure the internal audit department collectively possesses or obtains the knowledge, skills, and other competencies needed to meet the requirements of the internal audit charter.
9. Ensure trends and emerging issues that could impact the University are considered and communicated to senior management and the ACRM Committee as appropriate.
10. Ensure emerging trends and successful practices in internal auditing are considered.
11. Establish and ensure adherence to policies and procedures designed to guide the internal audit department.

12. Ensure adherence to the University's relevant policies and procedures unless such policies and procedures conflict with the internal audit charter. Any such conflicts will be resolved or otherwise communicated to senior management and the ACRM Committee.
13. Comply with Article 79 of Chapter 143 of the North Carolina General Statutes (NCGS) establishing the authority vested in the UNCH-CH Internal Audit function.
14. Ensure conformance of the internal audit department with the International Standards for the Professional Practice of Internal Auditing (Standards), with the following qualifications:
15. If the internal audit department is prohibited by law or regulation from conforming with certain parts of the Standards, the chief audit officer will ensure appropriate disclosures and will ensure conformance with all other parts of the Standards.
16. If the Standards are used in conjunction with requirements issued by the U.S. Government Accountability Office (GAO), often referred to as The Yellow Book, the chief audit officer will ensure that the internal audit department conforms with the Standards, even if the internal audit department also conforms with the more restrictive requirements of the GAO.

VII. Quality Assurance and Improvement Program

A. The internal audit department will maintain a quality assurance and improvement program that covers all aspects of the internal audit department. The program will include an evaluation of the internal audit department's conformance with the Standards and an evaluation of whether internal auditors apply the IIA's Code of Ethics. The program also assesses the efficiency and effectiveness of the internal audit department and identifies opportunities for improvement.

B. The chief audit officer will communicate to senior management and the ACRM Committee on the internal audit department's quality assurance and improvement program, including results of internal assessments (both ongoing and periodic) and external assessments conducted at least once every five years by a qualified, independent assessor or assessment team from outside the University.

Approved:

_____ _____
Kevin M. Guskiewicz Date
Chancellor
University of North Carolina at Chapel Hill

_____ _____
W.M. Kotis III Date
Chair, Audit, Compliance, and Risk Management Committee
University of North Carolina at Chapel Hill Board of Trustees

_____ _____
Dean A. Weber Date
Chief Audit Officer
University of North Carolina at Chapel Hill

THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

The University of North Carolina at Chapel Hill

Office of Internal Audit Charter

I. Background and Authority

A. The ~~Chief Audit Officer~~chief audit officer reports functionally to the Chair of the ~~Finance, Infrastructure~~Audit, Compliance, and ~~Audit~~ Risk Management (ACRM) Committee ~~(FIA)~~ and administratively (i.e., day to day operations) to the Chancellor of the University.

II. Purpose & Authority

A. To establish, maintain, and assure that the University's internal audit department has sufficient authority to fulfill its duties, the ~~FIA~~ACRM Committee will govern the Department and:

- 1. ~~Approve~~Recommend to the Board for approval the internal audit charter;
- 2. ~~Approve~~Recommend to the Board for approval the risk-based internal audit plan;
- 3. Receive communications from the ~~Chief Audit Officer~~chief audit officer on the internal audit department's performance relative to its plan and other matters;
- 4. Review and ~~approve~~recommend to the Board for approval, in consultation with the ~~Chancellor~~chancellor, the Department's budget and resources ~~for the Office of Internal Audit~~, including the ~~Chief Audit Officer's~~chief audit officer's evaluation and remuneration;
- 5. ~~Approve decisions~~Advise the Chancellor or the Board of Trustees regarding the chief audit officer's appointment and ~~removal of the Chief Audit Officer;~~/or termination, and
- 6. Make appropriate inquiries of management and the ~~Chief Audit Officer~~chief audit officer to determine whether there ~~is~~are inappropriate scope or resource limitations.

B. The ~~Chief Audit Officer~~chief audit officer will have the unrestricted ability to communicate and interact directly with the Board, including in private meetings without management present.

C. The ~~FIA Committee~~Board authorizes the internal audit department to:

- 1. Have full, free, and unrestricted access to all functions, records, property, and personnel ~~pertinent~~necessary to ~~carrying~~carry out any engagement, ~~subject to accountability for confidentiality~~provided the department complies with all applicable law and ~~safeguarding~~policy regarding the protection of confidential and/or sensitive records and information.
- 2. Allocate resources, set frequencies, select subjects, determine scopes of work, apply techniques required to accomplish audit objectives, and issue reports.
- 3. Obtain assistance from the necessary personnel of the University, as well as other specialized services from within or outside the University, ~~in order~~ to complete the engagement.

III. Independence and Objectivity

A. The ~~Chief Audit Officer~~chief audit officer will ensure that the internal audit department remains free from all conditions that threaten the ability of internal auditors to carry out their responsibilities in an unbiased manner, including matters of audit selection, scope, procedures, frequency, timing, and report content. If the ~~Chief Audit Officer~~chief audit officer determines that independence or objectivity may be impaired in fact or appearance, the details of such actual or apparent impairment will be disclosed to appropriate parties.

B. Internal auditors will maintain an unbiased mental attitude that allows them to perform engagements objectively and in such a manner that they believe in their work product, that no quality compromises are made, and that they do not subordinate their judgment on audit matters to others.

C. Internal auditors will have no direct operational responsibility or authority over any of the activities audited. Accordingly, internal auditors will not implement internal controls, develop procedures, install systems, prepare records, or engage in any other department that may impair an internal auditor's judgment, including:

1. Assessing specific operations for which they had responsibility within the previous year.
2. Performing any operational duties for the University or its affiliates.
3. Initiating or approving transactions external to the internal audit department.
4. Directing the activities of any ~~the~~ University employee not employed by the internal audit department, except to the extent that such employees have been appropriately assigned to auditing teams or to otherwise assist internal auditors.

D. Where the ~~Chief Audit Officer~~chief audit officer has or is expected to have roles and/or responsibilities that fall outside of internal auditing, safeguards will be established to limit impairments to independence or objectivity. Internal auditors will:

~~Internal auditors will:~~

1. Disclose any impairment of independence or objectivity, in fact, or appearance, to appropriate parties.
2. Exhibit professional objectivity in gathering, evaluating, and communicating information about the department or process being examined.
3. Make balanced assessments of all available and relevant facts and circumstances.
4. Take necessary precautions to avoid being unduly influenced by their ~~own~~ interests or by others in forming judgments.

E. The ~~Chief Audit Officer~~chief audit officer will confirm to the ~~FIA~~ACRM Committee, at least annually, the organizational independence of the internal audit department.

F. The ~~Chief Audit Officer~~chief audit officer will disclose to the ~~FIA~~ACRM Committee any interference and related implications in determining the scope of internal auditing, performing work, and/or communicating results.

IV. Scope of Internal Audit Activities

A. The scope of internal audit activities encompasses, but is not limited to, objective examinations of evidence ~~for the purpose of providing~~ to provide independent assessments to the ~~FIA~~ACRM Committee, management, UNC System Office, and outside parties on the adequacy and effectiveness of governance, risk management, and control processes for the University. Internal audit assessments include evaluating whether:

1. Risks relating to the achievement of the University's strategic objectives are appropriately identified and managed.
2. The University promotes governance, ethics~~.~~, and integrity and communicates risk and control information~~;~~.
3. The actions of the University's officers, directors, employees, and contractors ~~are in compliance~~comply with the University's policies, procedures, and applicable laws, regulations, and governance standards.
4. The results of operations or programs are consistent with established goals and objectives.
5. Operations or programs are being carried out effectively and efficiently.
6. Established processes and systems enable compliance with the policies, procedures, laws, and regulations that could significantly affect the University.
7. Information and the means used to identify, measure, analyze, classify, and report such information ~~are~~is reliable and ~~have~~has integrity.
8. Resources and assets are acquired economically, used efficiently, and protected adequately.

B. The ~~Chief Audit Officer~~chief audit officer will report periodically to senior management and the ~~FIA~~ACRM Committee regarding:

1. The internal audit department's purpose, authority, and responsibility.
2. The internal audit department's plan and performance are relative to its plan.
3. The internal audit department's conformance with The IIA's Code of Ethics and Standards, and action plans to address any significant conformance issues.
4. Significant risk exposures and control issues, including fraud risks, governance issues, and other matters requiring the attention of, or requested by, the ~~FIA~~ACRM Committee.
5. Results of audit engagements, special projects, investigations, or other activities.
6. Resource requirements.
7. Any response to risk by management that may be unacceptable to the University.

C. The ~~Chief Audit Officer~~chief audit officer also coordinates activities, where possible, and considers relying upon the work of other internal and external assurance and consulting service providers as needed. The internal audit department may perform advisory (consulting) services, the nature and scope of which will be agreed to by the client, provided the internal audit department does not assume management responsibility. Examples include providing advice and information on internal controls, risk management, and sound business practices. This includes reviewing current practices, interpreting policies and procedures, participating ~~on~~in standing committees, attending ad-hoc meetings, and responding to routine questions. Additionally, this may include ~~work~~working with the UNC System Office, professional organizations, and serving as a liaison between the university and external auditors.

D. Opportunities for improving the efficiency of governance, risk management, and control processes may be identified during engagements. These opportunities will be communicated to the appropriate level of management.

V. Reporting and Monitoring

A. The ~~Chief Audit Officer~~chief audit officer or a designee will prepare a written report following the conclusion of each internal audit project, special project, and investigation, other than small consulting projects. Audit reports and close-out letters will be distributed to appropriate members of university management, all members of the Board, UNC System Office, and a redacted copy to the Council of Internal Auditing ~~(redacted).~~.

Internal audit reports will typically include management's response regarding corrective action taken or to be taken ~~in regard to~~regarding the specific findings. Management's response should include a timetable for anticipated completion of planned corrective action and an explanation for any findings that will not be corrected. If management elects not to correct a finding, its response should include a statement accepting the risk from choosing not to address a reported condition.

VI. Responsibility

A. The ~~Chief Audit Officer~~chief audit officer has the responsibility to:

1. Submit, at least annually, to senior management and the ~~FIA~~ACRM Committee a risk-based internal audit plan for review and approval.
2. Communicate ~~to~~with senior management and the ~~FIA~~ACRM Committee the impact of resource limitations on the internal audit plan.
3. Review and adjust the internal audit plan, as necessary, in response to changes in the University's business, risks, operations, programs, systems, and controls.
4. Communicate ~~to~~with senior management and the ~~FIA~~ACRM Committee any significant interim changes to the internal audit plan.
5. Ensure each engagement of the internal audit plan is executed, including the establishment of objectives and scope, the assignment of appropriate and adequately supervised resources, the

documentation of work programs and testing results, and the communication of engagement results with applicable conclusions and recommendations to appropriate parties.

6. Follow up on engagement findings and corrective actions, and report periodically to senior management and the ~~FIA~~ACRM Committee any corrective actions not effectively implemented.
7. Ensure the principles of integrity, objectivity, confidentiality, and competency are applied and upheld.
8. Ensure the internal audit department collectively possesses or obtains the knowledge, skills, and other competencies needed to meet the requirements of the internal audit charter.
9. Ensure trends and emerging issues that could impact the University are considered and communicated to senior management and the ~~FIA~~ACRM Committee as appropriate.
10. Ensure emerging trends and successful practices in internal auditing are considered.
11. Establish and ensure adherence to policies and procedures designed to guide the internal audit department.
12. Ensure adherence to the University's relevant policies and procedures unless such policies and procedures conflict with the internal audit charter. Any such conflicts will be resolved or otherwise communicated to senior management and the ~~FIA~~ACRM Committee.
13. Comply with Article 79 of Chapter 143 of the North Carolina General Statutes (NCGS) establishing the authority vested in the UNCH-CH Internal Audit function.
14. Ensure conformance of the internal audit department with the International Standards for the Professional Practice of Internal Auditing (Standards), with the following qualifications:
15. If the internal audit department is prohibited by law or regulation from ~~conformance~~conforming with certain parts of the Standards, the ~~Chief Audit Officer~~chief audit officer will ensure appropriate disclosures and will ensure conformance with all other parts of the Standards.
16. If the Standards are used in conjunction with requirements issued by the U.S. Government Accountability Office (GAO), often referred to as The Yellow Book, the ~~Chief Audit Officer~~chief audit officer will ensure that the internal audit department conforms with the Standards, even if the internal audit department also conforms with the more restrictive requirements of the GAO.

VII. Quality Assurance and Improvement Program

A. The internal audit department will maintain a quality assurance and improvement program that covers all aspects of the internal audit department. The program will include an evaluation of the internal audit department's conformance with the Standards and an evaluation of whether internal auditors apply the IIA's Code of Ethics. The program also assesses the efficiency and effectiveness of the internal audit department and identifies opportunities for improvement.

B. The ~~Chief Audit Officer~~chief audit officer will communicate to senior management and the ~~FIA~~ACRM Committee on the internal audit department's quality assurance and improvement program, including results of internal assessments (both ongoing and periodic) and external assessments conducted at least once every five years by a qualified, independent assessor or assessment team from outside the University.

The University of North Carolina at Chapel Hill
Board of Trustees

Audit, Compliance, and Risk Management Committee
Wednesday, March 23, 2022

SUBJECT: Office of Internal Audit Information Technology Audit Initiatives (INFORMATION)

BACKGROUND:
The Office of Internal Audit completes various engagements within the information technology space, necessary to evaluate operations, assess internal controls, and mitigate risks. The University of North Carolina System Board of Governors actively supports evaluation of information technology enterprise risks and provides clear expectations that member institutions mature their information technology controls and that internal audit consider core prioritized Enterprise Risk Management and technology risks of the institution.

The Office of Internal Audit has developed a strong working relationship with information technology leadership and personnel. An informational update is provided highlighting the Office of Internal Audit's engagement activity, consulting initiatives, and collaboration addressing information technology matters.

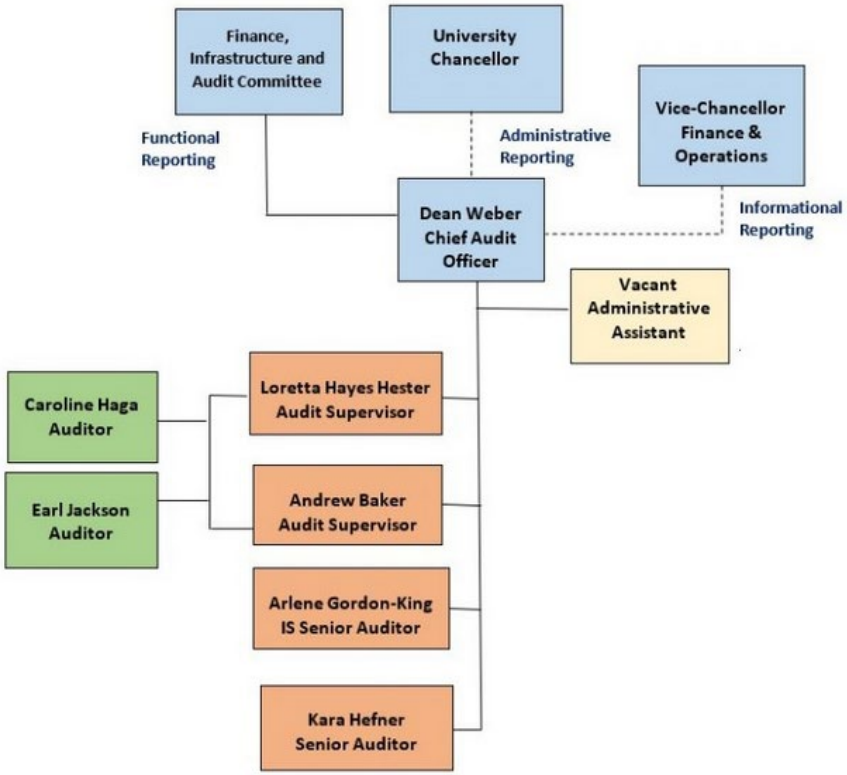
Office of Internal Audit Information Technology Audit Initiatives

UNIVERSITY of NORTH CAROLINA
at CHAPEL HILL

Arlene Gordon-King
IT Auditor
March 23, 2022

Presentation - Agenda

- Audit Themes Related to IT (UNC System Office)
  - IT Audit Findings (OSA)
  - Enterprise Risk (UNC-CH)
- OIA – Internal IT Auditing – Vision
  - OIA Future -- Integrated Audits When Able
  - Why OIA Consults and Collaborates With ITS
- IT Consultation for Internal Auditing
  - ITS Support of OIA Audit Work
  - System Administration Initiative Engagement
  - OIA Business Intelligence Audit Tool
  - Nessus Professional - Configuration Scans
  - IT Self-Assessment of PCI and SSN Using Nessus
  - OIA Annual Security Audit



Major Professional Certifications Held by Staff

3 - Certified Fraud Examiner (CFE)
2 - Certified Internal Auditor (CIA)
1 - Certified Internal Controls Auditor (CICA)
1 - Certified Information Systems Auditor (CISA)
1 - Certified Information Security Manager (CISM)
1 - Certified Information System Security Professional (CISSP)
1 - Certified Public Accountant (CPA)
1 - Certified Risk Management Assurance (CRMA)
1 - EC-Council Certified Security Analyst (ECSA)

OIA Staff Avg Time in OIA is **2.5 years**

Only **1** IT Systems Auditor
(new to higher ed)

Years	Arlene's Experience
15	**Audit** Information Systems & Security; External Audit Liaison; Internal Review Supervisor
8	**Information Technology** Systems Administrator; Business Intelligence Analyst; IT Specialist Manager
9	**Analysis** (Building, Equipment, & Fleet Maintenance Control Clerks; Accounting and Marketing Clerks
5	**Customer Service**

Master in Business Administrations (MBA)
Master of Science in Information Systems (MSIS)
BS in Computer Technology

Memo to Chancellors
From: Peter Hans, President
July 13, 2021

Sharing of Appropriate Audit Information
While the details of IT security audits are confidential, the CIO Council and Information Security Council will share relevant broad categories of findings for the System's collective benefit. Campuses should use this information to proactively address areas likely to receive audit scrutiny. This information should also inform campus ERM decisions and internal audit priorities after comparing with internally prioritized information security risks. The System Office will also use this information to compare audit findings with top risk rankings to inform potential enterprise shared service or procurement needs.

Memo To: UNC System Chancellors
From: Peter Hans, President
Date: January 27, 2022
Subject: Information Technology Controls

Information Technology Control Audit Themes:

The Office of the State Auditor has completed audits at System University with common themes:

1. Sensitive data inventories
2. Vulnerability and configuration management
3. Log repositories (at least 1 year), with analytics and notifications
4. Vendor/supplier risk management
5. Access management
6. Need for metrics to demonstrate status on the above themes.

Office of Internal Audit
ERM Survey – Technology was Highest Concern

Question #	Risk Category	Risk Topic	Survey Questions	Ranking
4.1	Technology	Cybersecurity	Struggle to stay on top of the wide array of cyber security threats, this includes novel ways to exploit criminal activity, ransomware and denial of service attacks.	High
4.2	Technology	Cybersecurity	Insufficient resources necessary to plan ahead for new regulatory requirements to handle student data, research information, intellectual property, and fulfill other privacy commitments.	Moderate
4.3	Technology	Data Privacy/Management	With the university's decentralized operational environment, failure to ensure a common understanding of how sensitive data is to be properly maintained likely exists, and action to ensure appropriate data privacy safeguards have been applied is a requirement.	Moderate
4.4	Technology	Data Privacy/Management	Failure to address international data privacy requirements impacting research, study abroad, and international recruitment.	Moderate
4.5	Technology	Widening of the Digital Divide Among Students	Ineffectively addressing digital inequalities that exist between students sharing the same course enrollment. Lack of awareness of the struggle to gain access to devices and network necessities suffered by disadvantaged students.	Moderate

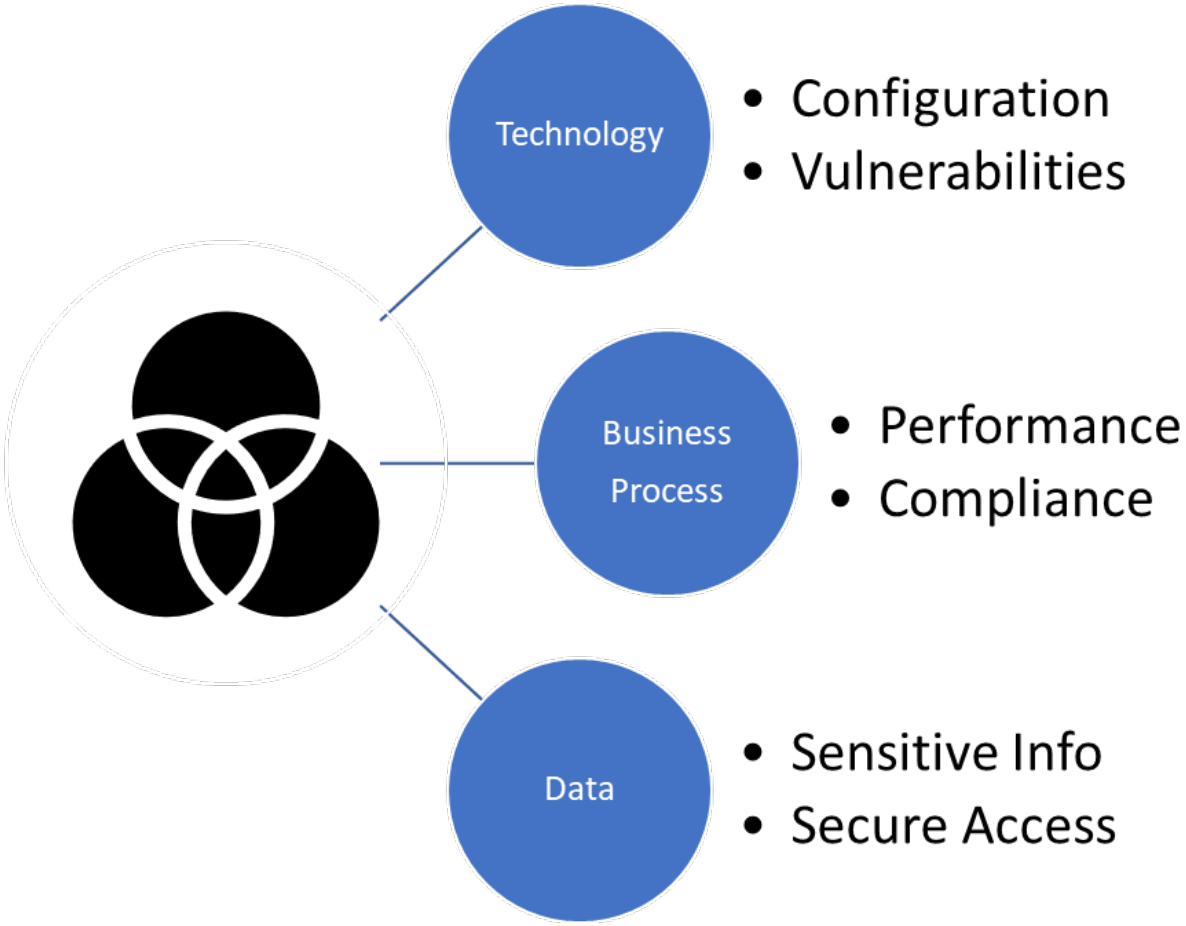
FY 2021-2022 Internal Audit Projects

	Audit Engagement Title	Achievements
1	ITS Consultation for Internal Audit	• Information was shared between OIA and ITS • Tools were used by ITS and OIA • Access control processes were improved, and ITS was granted access to the OIA Business Intelligence (BI) Audit Tool • The Nessus Professional vulnerability scanning tool was purchased jointly by the UNC System Office and the UNC Chapel Hill Office of Internal Audit. Nessus is approved for offline configuration audit work performed by the OIA.
2	System Administration Initiative (SAI)	• Designed and developed the OIA Business Intelligence Audit Tool • Reported observations for ITS awareness
3	IT Self-Assessment of PCI and SSN using Nessus	• A collaborative project for vulnerability assessment • Nessus for offline configuration audits to check against standards
4	OIA Annual Security Audit (OIA Access Control)	• Manually document information security and access controls • Collaborating to semi-automate review and documentation processes
5	Presentations About OIA and IT Audit	• School of Medicine (SOM) IT All Hands Meeting on 09/23/2021 • Information Security Liaison Meeting on 12/02/2021

OIA – Internal IT Auditing - Vision

OIA Foundational IT Work for Audit	Desired Future Value to University
Control Self-Assessment – OIA Corrected former employees' access	**Requests for Control Self-Assessments** Units may want processes reviewed
OIA Annual Security Review Review Compliance to Info Sec Standard	**Info Security Standard Reviews** Semi-automated; Specific/Broad Scope
Designed Internal Audit Business Intelligence Splunk enterprise data for scope based on SAI registered systems and risks	**Enterprise Data-driven Reviews** Less burden on operations; faster; multiple data sources; visualizations
OIA Requested ITS Consultation Collaboration to obtain information for OIA knowledge base for audit teams	**Integrated Reviews** Audit projects can review related processes, systems, and data.
Promoting Collaboration Networking, ISL meetings,	**Partnering with Units** New innovations; security controls; and improved processes

OIA Future -- Integrated Audits When Able



Why OIA Consults and Collaborates With ITS

To add more value to the University, by working smarter and broader

Internal Audit is business intelligence & decision-support analysis

- OIA and ITS share information for mutual benefits/perspectives

Information Systems are computerized, manual, & automated

- All audits involve information.
- All auditors can evaluate systems.
- ITS knowledge of systems, data & processes informs OIA risk analysis and scope identification

Technology supports business processes & financial transactions

- ITS shares technical info for OIA to relate to University business

Technology is the highest ranked topic of concern for enterprise risk

- ITS walks OIA through the IT risk assessment steps
- ITS explains the controls at multiple levels of defense in depth

IT Consultation for Internal Auditing
Objective

The engagement letter distributed on July 9, 2021, stated the objective of the 2-year audit engagement:

- "To provide value-added auditing, …
- The OIA seeks to build a foundation of relevant information for efficient knowledge management to support effective audit engagements…
- Together we can build the foundation for exclusive business intelligence tools meeting a variety of objectives for our separate departments."

The consulting service is intended to:

- Obtain University information related to systems, technology, security, and data
- Learn about relevant processes and procedures
- Understand tools, techniques, and practices related to audit activities

ITS Support of OIA Audit Work

Information Security Office

- Primary contact for System Administration Initiative (SAI)
- ITS liaison for coordinating communications between OIA and various ITS departments
- Provided data and information regarding SAI Portal, Qualys, monitoring, vulnerability scans; patch management, and general information security

Middleware Services and I&O OPSEC

- Provided data flow processes related to Splunk, SAI Portal, Tableau, and Qualys
- Provided guidance for the OIA on software applications
- Customized business intelligence objects for OIA use

ITS Support of OIA Audit Work - Continued

Enterprise Applications

- Extracted data from the SAI Portal
- Considered new fields to be added to SAI Portal
- Provided OIA access to the test environment of the SAI Portal

Enterprise Reporting and Analytics

- Collaborated with Middleware to create data extraction
- Connected data sources to OIA Tableau site
- Provided guidance for using Tableau and enterprise data

ITS Policy

- Explained the tiers for sensitive information

Managed Desktop Services

- Serves as technical support liaison for OIA
- Meets to discuss resources available to OIA
- Troubleshoots technical OIA issues

System Administration Initiative Engagement
Identifying Important Systems in SAI

Internal audit activities were divided into three stages with specific objectives:

- **Stage 1** was to explore information and data related to the System Administration Initiative (SAI) to determine if the available data is sufficient, adequate, and reliable for management and auditors to monitor key information effectively
- **Stage 2** was to evaluate data sources, data elements, and data flows needed before efficient analytical processes and dynamic reporting can be relied upon
- **Stage 3** was to design and develop the prototype for the OIA business intelligence tool in the OIA Tableau site

OIA Developed Business Intelligence Audit Tool

This is a proof of concept for using business intelligence for internal auditing.

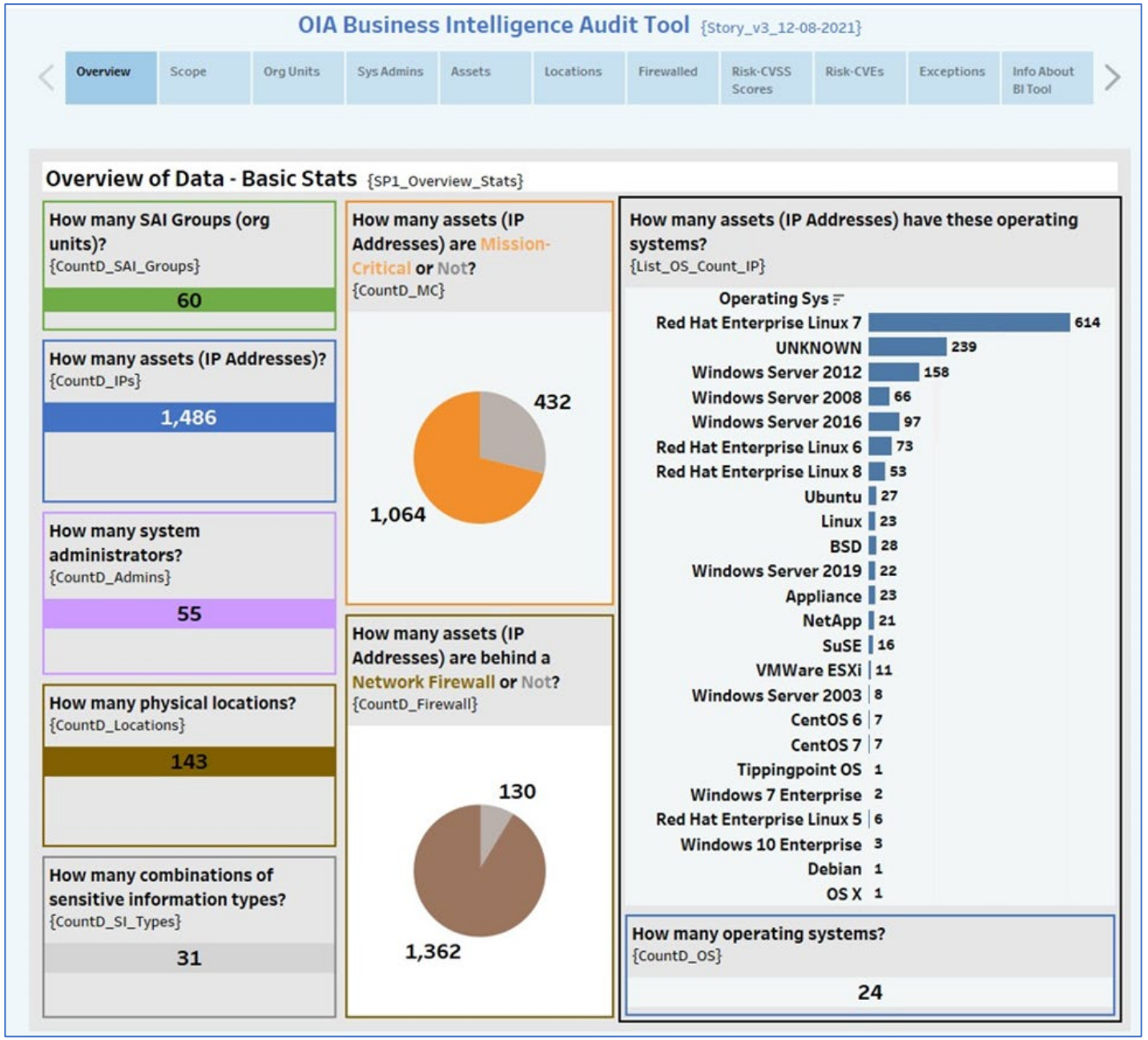
Auditors may use it for scoping audits and identifying risks associated with mission-critical systems or sensitive information.

The ITS Information Security Office (ISO) may use the dashboards to help SAI administrators improve data within the SAI portal.

Enterprise Applications may use the audit tool to show data design features that consider visual analytics for incorporating review and monitoring functions in future IT data/application projects. Four ITS staff were granted access to the OIA audit tool.

Benefits

- Risk assessment
- Scope identification
- Visual analytics
- Dynamic reporting


OIA Business Intelligence Audit Tool {Story_v3_12-08-2021}
Overview
Scope
Org Units
Sys Admins
Assets
Locations
Firewalled
Risk-CVSS Scores
Risk-CVEs
Exceptions
Info About BI Tool
Overview of Data - Basic Stats {SP1_Overview_Stats}
How many SAI Groups (org units)?
{CountD_SAI_Groups}
60
How many assets (IP Addresses)?
{CountD_IPs}
1,486
How many system administrators?
{CountD_Admins}
55
How many physical locations?
{CountD_Locations}
143
How many combinations of sensitive information types?
{CountD_SI_Types}
31
How many assets (IP Addresses) are Mission-Critical or Not?
{CountD_MC}
432
1,064
How many assets (IP Addresses) are behind a Network Firewall or Not?
{CountD_Firewall}
130
1,362
How many assets (IP Addresses) have these operating systems?
{List_OS_Count_IP}
Operating Sys
Red Hat Enterprise Linux 7 614
UNKNOWN 239
Windows Server 2012 158
Windows Server 2008 66
Windows Server 2016 97
Red Hat Enterprise Linux 6 73
Red Hat Enterprise Linux 8 53
Ubuntu 27
Linux 23
BSD 28
Windows Server 2019 22
Appliance 23
NetApp 21
SuSE 16
VMWare ESXi 11
Windows Server 2003 8
CentOS 6 7
CentOS 7 7
Tippingpoint OS 1
Windows 7 Enterprise 2
Red Hat Enterprise Linux 5 6
Windows 10 Enterprise 3
Debian 1
OS X 1
How many operating systems?
{CountD_OS}
24

Partnering with the UNC System Office
Nessus Professional - Configuration Scans

The OIA partnered with the UNC System Office to purchase a network vulnerability scanning tool for internal audit use.

- One-year license for Nessus Professional
- Offline configuration audit - no active scanning of network devices
- Configuration files extracted, stored, scanned, and evaluated
- Corrected configurations for more security

ITS staff were liaisons: meeting with vendor and UNC System Office

ITS navigated the data protection and risk assessment process

- Data Protection Checklist
- ISO Risk Assessment Customer Engagement (RACE) form
- **Data Flow Diagram** – explaining OIA plans for Nessus
- ITS approved Nessus for offline configuration audits

IT Self-Assessment of PCI and SSN Using Nessus
More Value: Configuration & Process Improvement

Traditional Audit – Compliance

- Tests – Pass or Fail
- Results are final
- Auditor organizes results to develop findings based on failures
- Auditor performs root-cause analysis, via interviews and research, to make recommendations
- Auditee responds to findings and recommendations with plans of action and milestones
- Auditor reports on findings, recommendations, and potential impact of vulnerabilities.
- Auditors' follow-up later

Collaborative Audit – Assurance

- Checks – Pass or Fail
- Results are reviewed
- Failures cause conversations
- **Auditor and Auditee share security analysis techniques and info**
- Auditee takes corrective actions
- **Auditor and Auditee identify gaps between results, policy, and practices**
- Auditee promotes process improvement by informing decision-makers of gaps, and providing knowledge from the business perspective
- Auditor reports on controls, corrective actions, plans, accepted risks, remaining findings, and actual impact of controls in place.

OIA Annual Security Audit
OIA User Access Controls

Starting fiscal year 2020-2021, OIA reports annually on our information security-related activities and shows relevance of the Information Security Controls Standard issued by ITS.

ITS resources are valuable to OIA.

ITS executives coordinated:

- Accurate templates for efficient and consistent access to ConnectCarolina data for OIA staff
- Appropriate assignment of OIA administrator role for the OIA SharePoint site

Additional Information Security Tasks

OIA IT Auditor is a member of:

- Information Security Liaisons Monthly Meetings
- EDCC – subgroup Software Inventory
- Qualys Vulnerability Management Detection and Response (VMDR) Focus Group

OIA IT Auditor attended SANS Stay Sharp: Nov 2021

- SEC 440: CIS Critical Controls - A Practical Introduction
- Course material was downloaded and is available to share

Questions/Comments

Cyber Security Update

J. Michael Barker, Ph.D.
Vice Chancellor for Information Technology and
Chief Information Officer

Dennis Schmidt
Assistant Vice Chancellor for Information Security and
Privacy and Chief Information Security Officer

March 2022

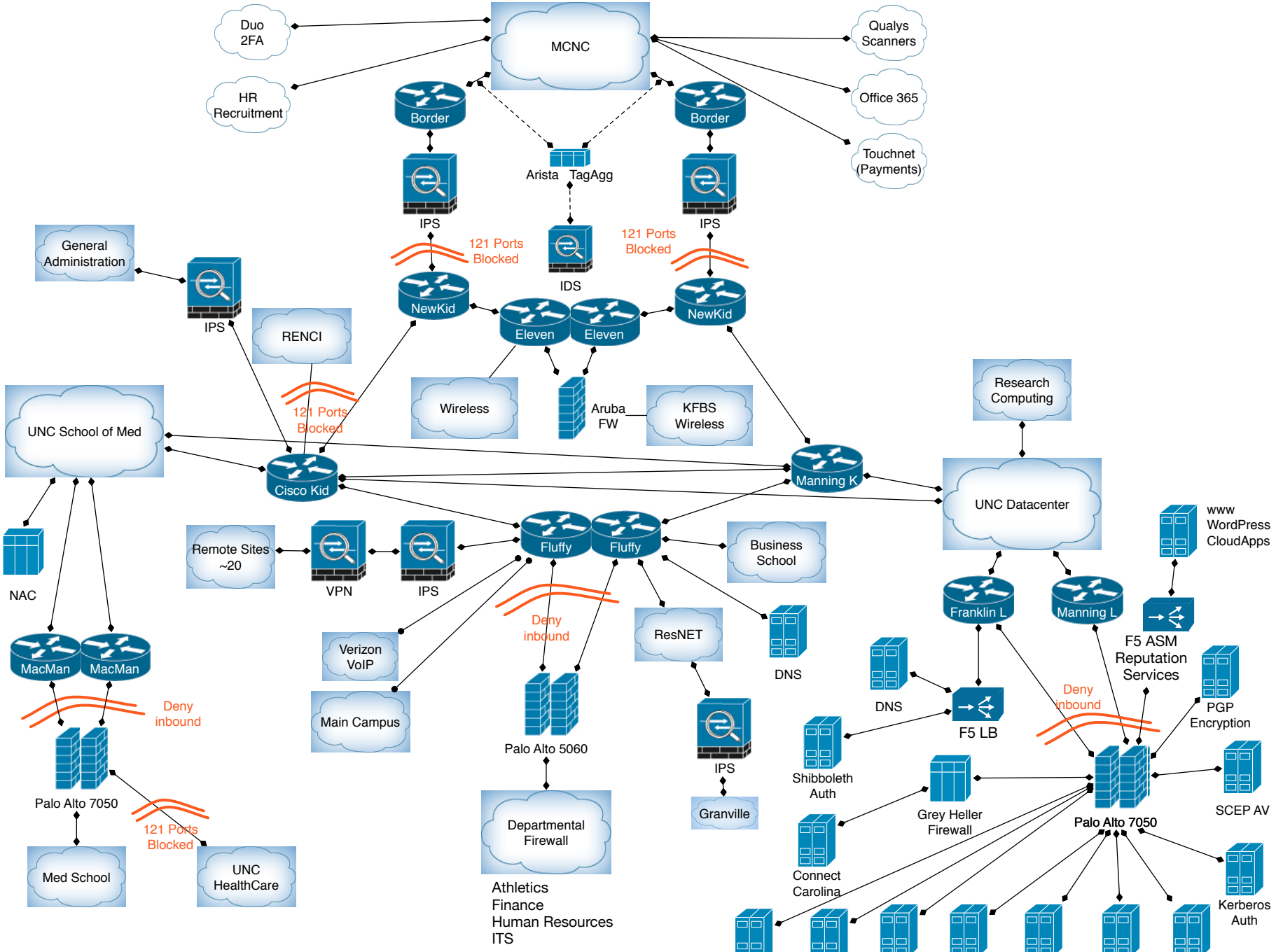
UNC
INFORMATION
TECHNOLOGY SERVICES

Outline

1. Orientation to How We Protect the University
2. The Threats We Face
3. Top Ten Threats/Risks
4. Discussion, Question, Answer

A Large and Complex Enterprise

- Millions of Personally Identifiable Records
- Billions of intrusion attempts
- Hundreds of unique phishing campaigns
- 1,500 sensitive servers on campus and in the cloud
- 65 departments have registered sensitive data servers
- $81M in credit card transactions
- 2972 Wired network switches, 175,278 ports, 150,000 devices
- 10,035 Wireless Access points, 15,700 peak connections
- 3 Billion connections via the Internet per day



1 – Orientation to How We Protect the University

Multilayered Defense

- Multiple layers of defense, with varying technologies and controls requiring different skillsets to penetrate.
- Think: Castle with high stone walls, deep moat, hot oil, arrows, etc.
- Within the castle are walled areas with gates to control internal movement.
- No single layer is infallible. Getting through multiple layers is more difficult for attackers.

Layered Defense for the Network

- Akamai DNS Filtering – Blocks bad links.
- Firewalls at the front door and internal
- Intrusion Detection/Prevention Systems
- Segmented Networks – Prevent lateral movement
- Mandiant Managed Defense Service – Monitors all in/out traffic 24X7X365
- Incident Response Team – on call 24X7
- Ability to respond to changing world situations.
  - Expect increased Russian cyber attacks during Ukrainian crisis.

Layered Defense for Systems

- System Administration Initiative (SAI) – Proactive vulnerability scans of servers
- Multifactor or separate credential for privileged accounts
- Quarterly review of privileged access
- Firewall protection for sensitive machines
- Remote backup of critical systems
- Redundancy/failover of critical systems
- Automated monitoring of logs and alerts

Layered Defense for Applications

- Collaboration with Security Office during development
- Penetration testing to look for holes
- Formal risk assessments
- Vendor Risk Management Process
- Multifactor authentication for strong access
- Web Application Firewalls or Intrusion Detection for extra defense layers

Layered Defense for End Points

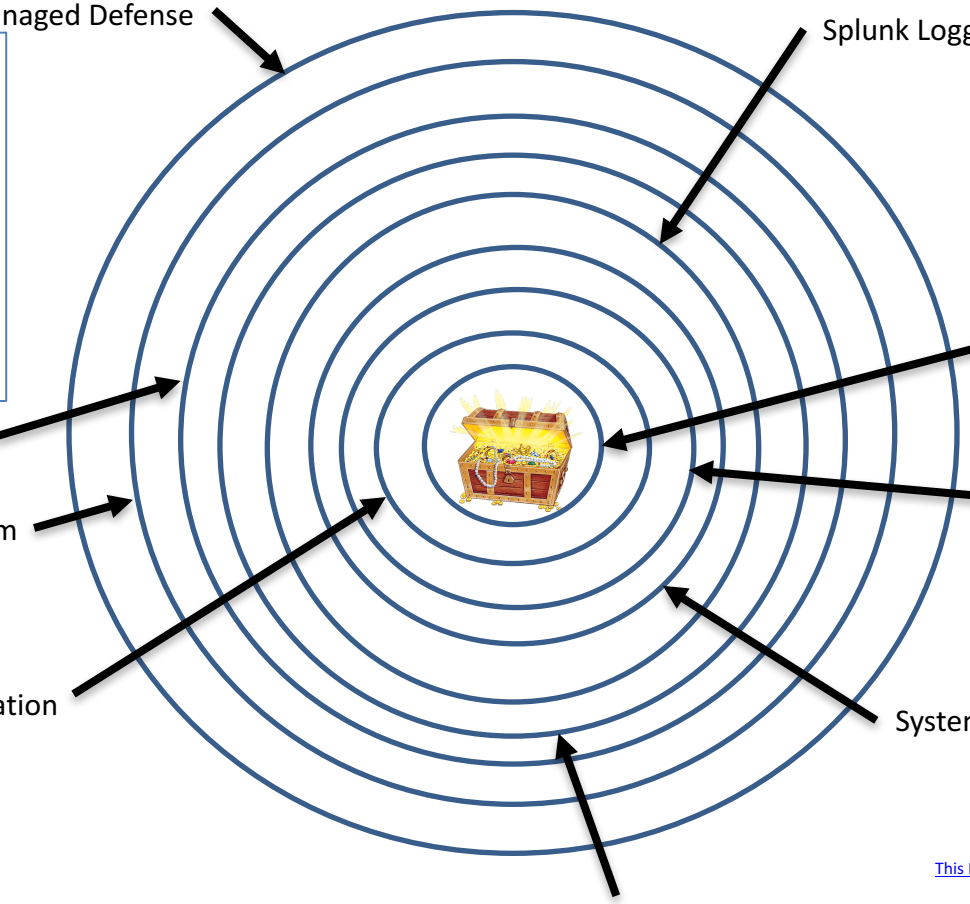
- Microsoft Anti-Malware, FireEye Detection and Response
- BitLocker and FileVault encryption
- Strong identity controls
- User awareness training and outreach
- Configuration management through SCCM/Active Directory (Windows) and JAMF (Macs)

Layered Defense for Governance

- Data Governance Oversight Group
- IT Executive Council (ITEC)
- IT Security Liaisons Program
- Enterprise Data Coordinating Committee
- ITEC/CIO Advisory Committee
- IT Infrastructure Coordinating Committee
- IT Security Coordinating Committee

Layered Defense

Each Layer is a different technology, requiring a different skillsets to penetrate.



Relevant Security Frameworks

- ISO 27002 - All UNC System schools
  - Annual self-assessment, peer-reviewed by UNC CISOs
  - Maturity assessment by MCNC - Sept 2021 – Jan 2022
- NIST 800-53 required for Federal contracts
- NIST 800-171 required by most Federal contracts
- NC State Information Security Manual for state contracts (Based on NIST 800-53)
- CMMC will be required soon for DoD contracts - based upon NIST 800-171

MCNC ISO 27002 Maturity Assessment

ISO 27002 MATURITY ASSESSMENT

To measure UNC Chapel Hill's ISO 27002 maturity, this assessment examined fourteen security control clauses containing thirty-five main security categories and one hundred fourteen controls. The Secure Controls Framework *Security and Privacy Capability Maturity Model (SP-CMM)*[3] criteria was used to evaluate each control. The maturity score was calculated based on IT staff interviews, analysis of evidence and a self-assessment submitted by UNC Chapel Hill.

The overall maturity score was calculated by taking the average SP-CCM level for each control and dividing by the total number of controls in the ISO 27002 framework. Each control clause maturity score was calculated by taking the average SP-CMM level for each control and dividing by the total number of controls in that control clause.

LEVEL	SP-CMM DESCRIPTION
0	Not Performed
1	Performed Informally
2	Planned and Tracked
3	Well-Defined
4	Quantitatively Controlled
5	Continuously Improving

ISO 27002 MATURITY - MCNC VALIDATED

3.22

ISO 27002 MATURITY - SELF-ASSESSMENT

3.86

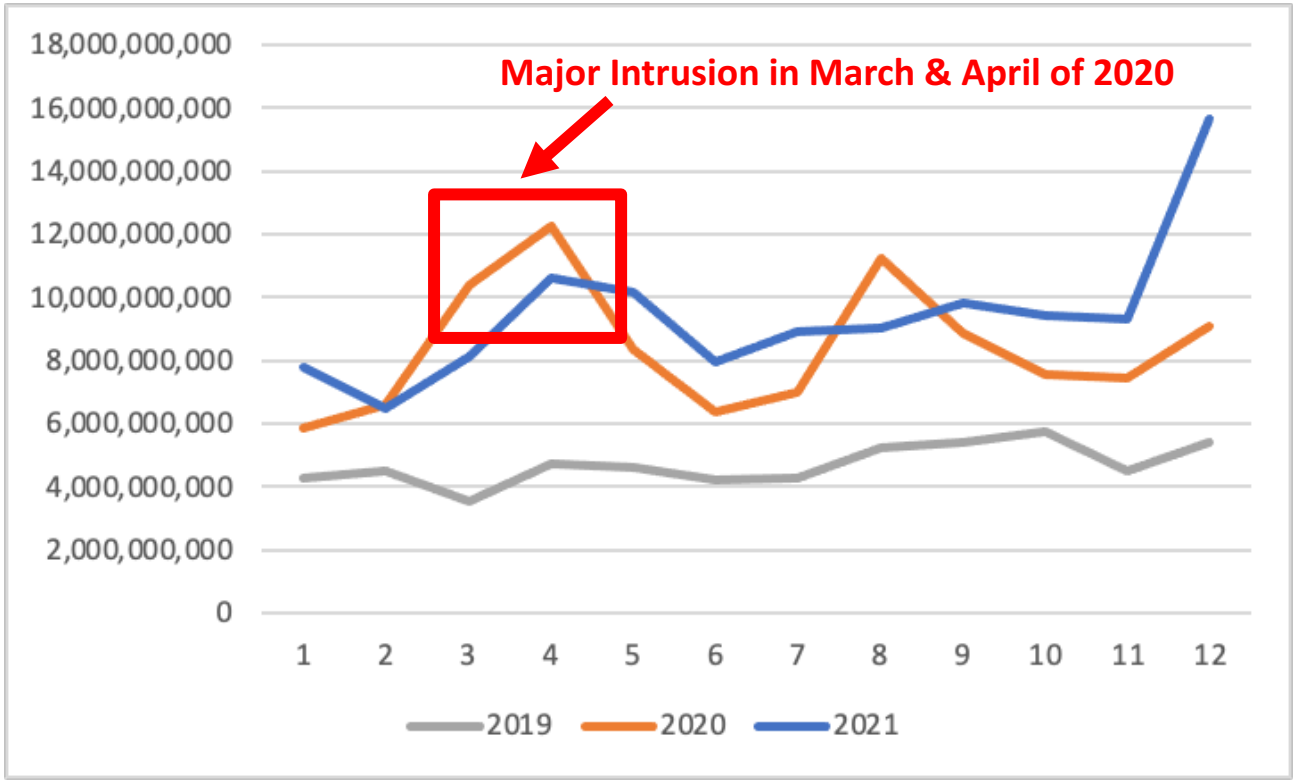
1 – Orientation to How We Protect the University

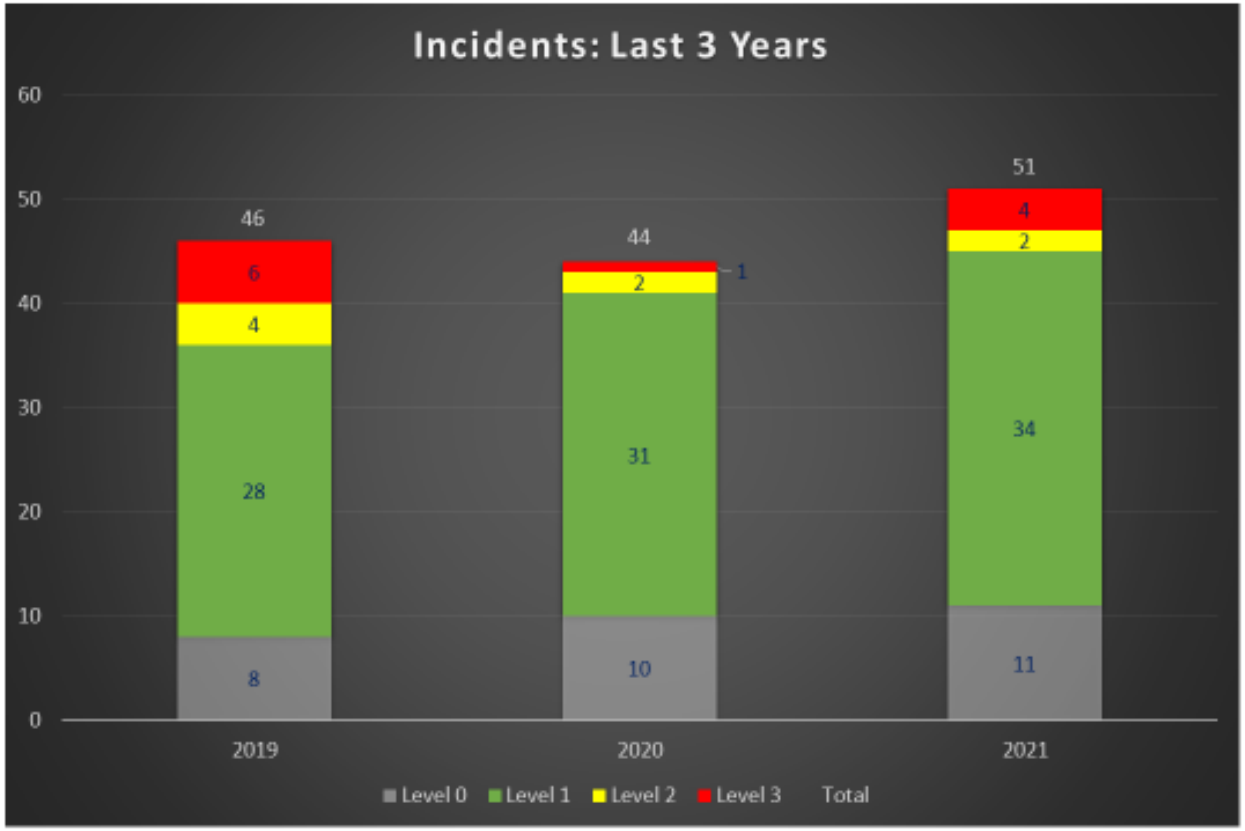
Current Landscape

Threats and attacks continue to grow dramatically, but our protections are improving and more effective, and our response to incidents is robust, resulting in fewer incidents and exposures of sensitive University data.

Attacks Blocked Automatically: Firewall (Monthly totals) *Higher than ever*

2019: 56 billion blocks | 2020: 100 billion blocks | 2021: 113 billion blocks

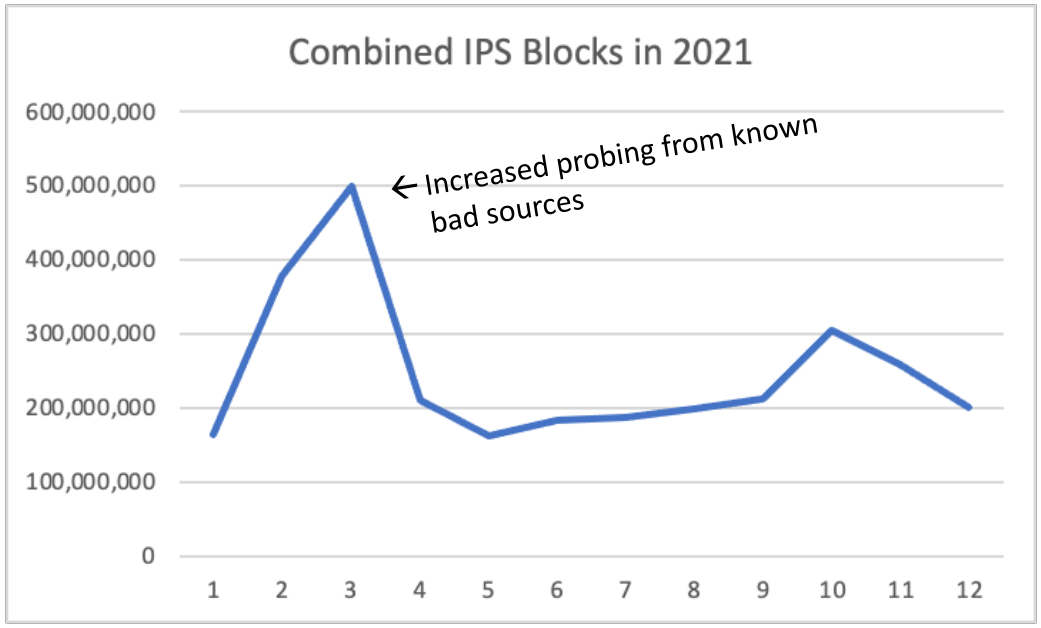




Level 3 – confirmed SI
Level 2- potential SI
Level 1 – no SI
Level 0 - request

Intrusion Prevention By the numbers…

- ✓ In 2020 we blocked 2.5 billion attacks using border and firewall-based intrusion prevention systems.
- ✓ In 2021 we blocked 2.95 billion attacks



Our Top 10 Security Threats/Risks

1. Phishing Attacks
2. Advanced Persistent Threats
3. Ransomware
4. Incomplete Inventory of Sensitive Data
5. Inadequate protection for remote/home machines
6. Inadequate end user security awareness
7. Obscure University systems in the cloud
8. Loss of talent to outside job market
9. Unmanaged IT, especially Internet of Things
10. University data on unmanaged mobile devices

Phishing

- Phishing attacks from professional teams of criminals continue to plague us
  - Targeted spear phishing is very common
  - Emails can arrive from a known acquaintance
  - "Impersonation phishing" persists
    - Ex: chancellor.unc.edu@yahoo.com
  - Continually change tactics to thwart protections
- User training has not been effective. Recent campaign results:
  - 33% of faculty & staff provided credentials.
  - 25% of IT staff provided credentials!

Phishing Mitigation

- Multifactor most effective defense to date
  - 12 compromised accts since December 2018
  - Down from hundreds per month in 2017/18!
- Purchased enhanced Microsoft security
  - Detailed logs to track most phisher activity
  - Additional anti-phishing tools
    - Block malicious links across the M365 tenant
    - Sandbox – tests attachments for malware
    - More aggressive detection of phishing messages
  - Expanded conditional access capability

Advanced Persistent Threats

- Evolving, sophisticated, targeted attacks
- Cybercriminals, Nation States
- Our Mitigations
  - Firewall coverage for entire network (Complete 6/22)
    - Firewalls perform deep packet inspection
    - Default: Deny access
  - Mandiant Managed Defense Service – Round the clock monitoring of all network traffic
  - Domain Names Service (DNS) filtering (Akamai) - Blocks malicious links

Ransomware

- On the rise – targeting all industries.
  - Double Jeopardy – Pay to get data back and pay to not have sensitive data publicly released
- Our Mitigations:
  - Protected backups (ability to restore)
  - Segmented network (limits spread e.g. firewall)
  - Expanded internal firewall coverage
  - Managed Defense focus on ransomware signatures. 22,000+ active FireEye agents.
  - Two tabletop exercises focused on ransomware
  - 3rd party review (SOM).

Incomplete Inventory of Sensitive Data

- Foundational security best practice – You can't protect what you don't know! Sensitive data is scattered across institution on decentralized systems
  - System administrators often have little knowledge of what users store on their systems or where users store data
- Decentralization makes this difficult
- Extremely resource intensive to compile and maintain.
- We currently do not have a good solution for this.

Inadequate Protection for Remote Machines

- COVID forced us into a remote workforce
- Little time to prepare
- Users brought machines home or use personal devices
- No campus network protections for endpoints
- Some workers are still at home
- Mitigation: FireEye and Microsoft Defender provide more advanced protection

Inadequate End User Security Awareness Training

- Annual training is required by policy, but not easily enforced.
- Compliance averages 64%
- Annual training is supplemented with robust outreach program
- Phishing click rates still average 30%

University Systems in the Cloud

- Servers under the desk 2.0
- Only takes a credit card to build a system
- No easy way to detect or enforce
- Must rely on administrative policies and cooperation of our users and researchers
- Risk increases when sensitive data is in scope

Loss of Talent to Outside Job Market

- State salaries have remained stagnant for years
- Extended freezes on promotions and merit increases
- Reduced staffing levels & increased requirements = increased workload
- External job market is exploding, particularly in Information Security
- We have lost two (out of 12) in the last 6 months
- Mitigation: Very limited options available

Unmanaged Internet of Things

- Market is flooded with IOT devices
- IOT capability embedded in common products, such as video projectors
- Most devices are not patched by vendor
- Attackers target devices with unpatched vulnerabilities
- Mitigation: Block direct access from internet

University Data on Unmanaged Mobile Devices

- BYOD is prevalent in our environment
- Users prefer portability and convenience of having single device
- Mobile management tools are costly and intrusive on personal devices
- Users resistant to controls on personal devices
- Policy alone is inadequate

Questions?