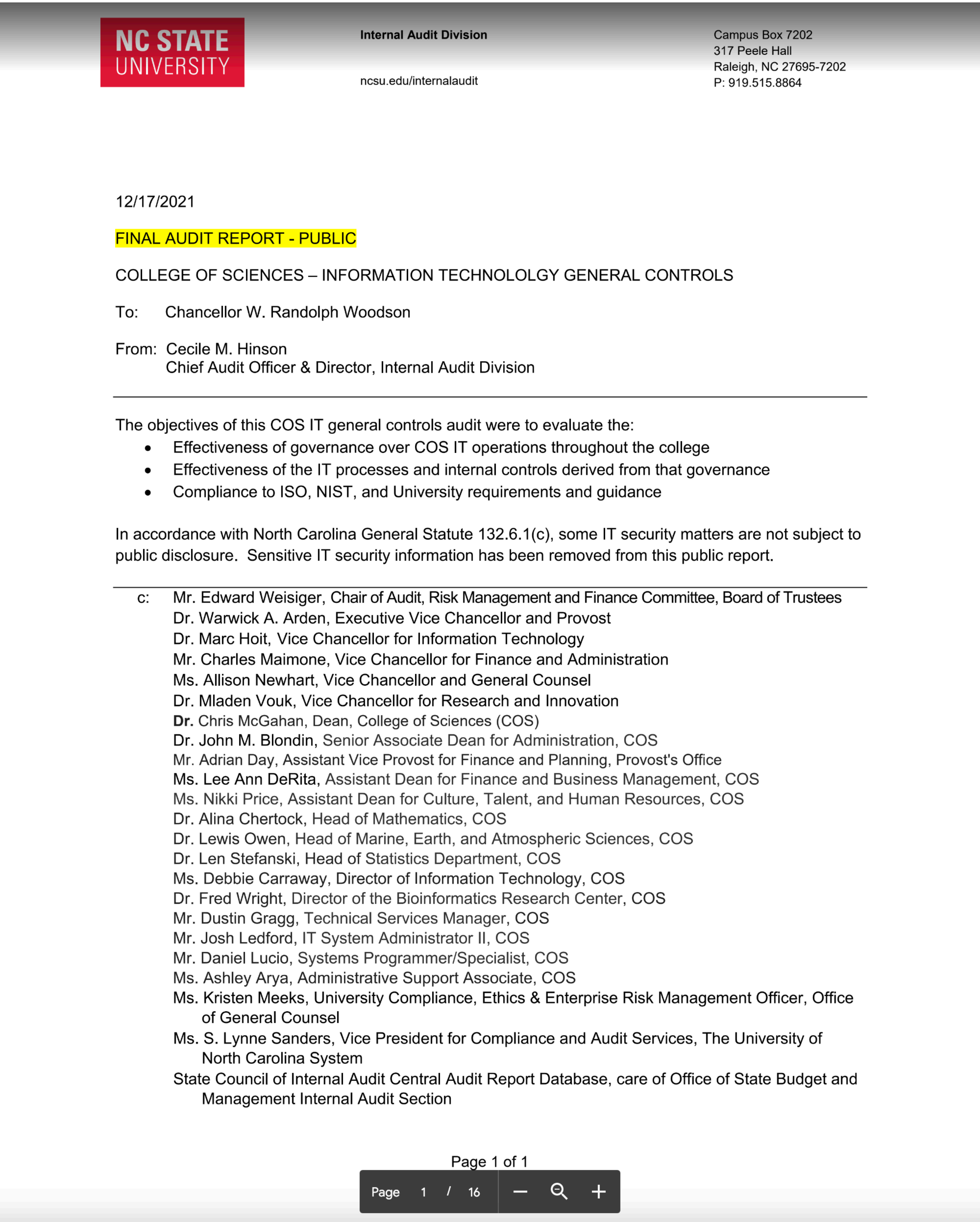

NC STATE UNIVERSITY

Internal Audit Division

ncsu.edu/internalaudit

Campus Box 7202
317 Peele Hall
Raleigh, NC 27695-7202
P: 919.515.8864

12/17/2021

FINAL AUDIT REPORT - PUBLIC

COLLEGE OF SCIENCES – INFORMATION TECHNOLOLGY GENERAL CONTROLS

To: Chancellor W. Randolph Woodson

From: Cecile M. Hinson
Chief Audit Officer & Director, Internal Audit Division

The objectives of this COS IT general controls audit were to evaluate the:

- Effectiveness of governance over COS IT operations throughout the college
- Effectiveness of the IT processes and internal controls derived from that governance
- Compliance to ISO, NIST, and University requirements and guidance

In accordance with North Carolina General Statute 132.6.1(c), some IT security matters are not subject to public disclosure. Sensitive IT security information has been removed from this public report.

---

c: Mr. Edward Weisiger, Chair of Audit, Risk Management and Finance Committee, Board of Trustees
Dr. Warwick A. Arden, Executive Vice Chancellor and Provost
Dr. Marc Hoit, Vice Chancellor for Information Technology
Mr. Charles Maimone, Vice Chancellor for Finance and Administration
Ms. Allison Newhart, Vice Chancellor and General Counsel
Dr. Mladen Vouk, Vice Chancellor for Research and Innovation
Dr. Chris McGahan, Dean, College of Sciences (COS)
Dr. John M. Blondin, Senior Associate Dean for Administration, COS
Mr. Adrian Day, Assistant Vice Provost for Finance and Planning, Provost's Office
Ms. Lee Ann DeRita, Assistant Dean for Finance and Business Management, COS
Ms. Nikki Price, Assistant Dean for Culture, Talent, and Human Resources, COS
Dr. Alina Chertock, Head of Mathematics, COS
Dr. Lewis Owen, Head of Marine, Earth, and Atmospheric Sciences, COS
Dr. Len Stefanski, Head of Statistics Department, COS
Ms. Debbie Carraway, Director of Information Technology, COS
Dr. Fred Wright, Director of the Bioinformatics Research Center, COS
Mr. Dustin Gragg, Technical Services Manager, COS
Mr. Josh Ledford, IT System Administrator II, COS
Mr. Daniel Lucio, Systems Programmer/Specialist, COS
Ms. Ashley Arya, Administrative Support Associate, COS
Ms. Kristen Meeks, University Compliance, Ethics & Enterprise Risk Management Officer, Office of General Counsel
Ms. S. Lynne Sanders, Vice President for Compliance and Audit Services, The University of North Carolina System
State Council of Internal Audit Central Audit Report Database, care of Office of State Budget and Management Internal Audit Section

PUBLIC AUDIT REPORT

COLLEGE OF SCIENCES – INFORMATION TECHNOLOGY GENERAL CONTROLS

December 17, 2021

AUDITING STANDARDS

This audit conforms to the definition of internal auditing, the Code of Ethics, and the International Standards for the Professional Practice of Internal Auditing as defined in the Institute of Internal Auditors' International Professional Practice Framework, 2017 Edition.

BACKGROUND

Information Technology (IT) staff in the College of Sciences' (COS) provide services that support achievement of the COS mission and goals including general IT support for faculty, staff, and students; research computing support and consulting; emerging technology research and development; classroom support; and information security. The college relies heavily on IT services to support extensive research activities related to contracts and grants that totaled $162M in fiscal year (FY) 2020. Effective IT governance and controls over IT services and data can ensure the college successfully achieves its goals while still meeting Federal, State, UNC System, and NC State University requirements.

The IT governance and control framework employed by the UNC System and NC State University is based on the International Organization for Standardization (ISO) 27002 information security standard. Additionally, the National Institute of Standards and Technology (NIST) Special Publication (SP) 800 series provides detailed requirements for federal research data. The two frameworks complement each other by requiring senior management support, a continual improvement process, and a risk based approach.

An IT general controls audit evaluates IT governance, processes, and internal controls against standard framework requirements and best practices to ensure the structures and controls over IT organizations and services are best aligned with and beneficial to the entity served.

OBJECTIVE AND SCOPE

The objectives of this COS IT general controls audit were to evaluate the:

- Effectiveness of governance over COS IT operations throughout the college
- Effectiveness of the IT processes and internal controls derived from that governance
- Compliance to ISO, NIST, and University requirements and guidance

We used Control Objectives for Information Technology (COBIT) to coordinate the multiple frameworks in order to provide consistent risk management recommendations to the COS.

The scope of the audit was college-wide IT activities performed by the COS IT Team and IT staff in each individual department and center within the COS.

EXECUTIVE SUMMARY OF RESULTS

We reviewed IT strategic decision-making, organization and administration of IT functions, and policies and procedures as these areas provide the foundation for effective IT controls. Those IT controls included contingency planning, physical and environmental security of server rooms, backups, disaster recovery, and business continuity. This audit identified a number of positive observations in COS IT operations as well as issues requiring corrective action by COS management.

<u>Positive Observations</u>

- As part of a self-initiated orientation to the college, the college IT Director analyzed IT activities throughout the college, departments, and units to gain a preliminary understanding of IT personnel, operations, and infrastructure. This resulted in the identification of several challenges to the effectiveness of IT support throughout the college such as:
  - misalignment between IT personnel skills and expertise in comparison to the needs of the college
  - little to no training for IT staff
  - limited communication between the college IT Director, college, and departmental IT staff

This analysis facilitated the IT Director's development of a roadmap tying IT services to the College's IT needs and addressing opportunities when changes arose. The roadmap facilitated hiring resources with expertise to meet the College IT needs.

- In audit interviews, the majority of IT staff communicated and demonstrated their commitment to improving the IT services and operations within the college. For example, IT staff:
    - Incorporated both ISO and NIST standards into IT processes implementing the standards' best practices and requirements, such as:
        - Maintaining and monitoring server room access lists
        - Assigning responsibilities for the operation of server rooms and maintenance of servers and equipment
        - Utilizing staff departure checklists when employment ends to ensure access to University resources and data is removed
    - Moved servers from the rooms, maintained by other units, with higher physical and environmental risks to a location where the college can implement controls to mitigate these risks
    - Collaborated with other campus IT units in developing virtual desktop services for future use

<u>Audit Issues</u>

Issue 1 – Lack of Clear IT Vision, Strategy, and Direction

There is no college-level vision or strategy to ensure that IT decisions, activities, and resourcing throughout the decentralized IT organization support the college's overall goals and objectives. Additionally, IT functions are siloed in departments so there is currently no effective way to comprehensively identify IT resources and expertise available or needed throughout the college.

Issue 2 – Insufficient IT Support Throughout the College

There is insufficient IT support throughout the college for faculty, staff, and students. IT personnel are required to perform responsibilities outside their expertise or skill set with little to no training. For example, individuals with responsibilities for supporting hardware, software, and other technologies do not always have adequate IT security experience to ensure University data is protected and may not have certifications required by projects/grants to support the IT services required. Additionally, some IT staff have non-IT responsibilities which limits their ability to adequately provide the necessary IT support and reduces time available for understanding, developing, or implementing new IT initiatives or requirements.

Issue 3 – Inadequate IT Policies and Procedures

The College of Sciences does not have adequate IT policies or procedures at either the college or departmental level documenting day-to-day IT functions and operations. This includes such activities as IT: support, inventory, security, storage, backup, and disaster recovery.

Issues 4 – 11 contain detailed sensitive security information about University information technology. In accordance with the North Carolina General Statute §132-6.1 (c), the IT security matters in issues 4 – 11 are not subject to public disclosure. Those issues, recommendations, and related management corrective action plans have been provided exclusively to University executive leadership and management directly responsible for addressing the issues.

See the Audit Issues and Management Responses section below for further details of the issues, our recommendations, and COS's planned corrective actions for Issues 1 – 3.

AUDIT ISSUES AND MANAGEMENT RESPONSES

ISSUE 1: Lack of Clear IT Vision, Strategy, and Direction

ISSUE NOTED

There is no college-level vision or strategy to ensure that IT decisions, activities, and resourcing throughout the decentralized IT organization support the college's overall goals and objectives. IT staff throughout the college interviewed were not aware of how their IT work is incorporated to support the college-wide goals and objectives.

IT functions are siloed in departments so there is currently no effective way to comprehensively identify IT resources and expertise available or needed throughout the college. IT activities and decisions are made with little to no interaction between the COS IT Team, departments and centers. Without collaboration and communication, individual IT staff do not have a clear direction on where to focus energy and resources for college-wide initiatives.

Additionally, there has not been a full, in-depth assessment to identify what the IT needs are throughout the college in order to effectively support the college. Some examples of IT needs include training, policies and processes, and security of server equipment. A broad set of skills and knowledge are needed to adequately support the IT activities throughout the college (see Issue 2). A clear IT vision would help identify expertise in areas and weaknesses in other areas. This knowledge could be leveraged to improve both the effectiveness and efficiency of IT support by sharing skills in areas that need assistance.

IMPACT OF THE ISSUE

Proper IT alignment helps faculty, staff and IT support understand the goals and objectives of all IT functions. Without a clear IT vision or strategy, IT staff are reactive in nature instead of being proactive and understanding what is needed to work together to complete tasks that support the college's goals and objectives. Without a formal IT vision, strategy, and direction, the college cannot produce measurable results toward achieving goals and objectives. It also makes it difficult to create budgets for special projects or understand the personnel and funding resources necessary to be successful.

RECOMMENDATION

We recommend the Dean for the College of Sciences ensure the College of Sciences Director of Information Technology develop and implement an IT strategy to support both the college and departments' goals and objectives. The IT strategy for the college and departments should also align with the University IT Strategy. This IT strategy should include but not be limited to identification of:

- Goals and objectives and the conditions needed to achieve them
- Needs of the college and departments to support the IT vision, strategy and direction
- Opportunities and limitations of IT throughout the college and departments

MANAGEMENT RESPONSE FROM COS

Cultural issues have prevented the College of Sciences from fully integrating IT across all college departments and centers. Historically, departments have been separately responsible for all operational matters and operated autonomously, resulting in silos. Currently, Math, Statistics, the Bioinformatics Research Center and the Center for Research in Scientific Computing continue to operate independently of Sciences IT.

The College of Sciences plans to reorganize the IT function so that all college IT staff report to IT supervisors in the college's central IT unit led by the Director of Information Technology as indicated in the management response to Issue 2.

In addition, the College of Sciences will adopt Standard Operating Procedures (SOPs) that guide the acquisition and management of all IT resources in the college so that the college's IT strategy can be operationalized (see the management response to Issue 3).

Currently, the Dean is leading the College of Sciences in the development of strategic and culture plans facilitated by a consulting company, Tidal Equality. The Director of Information Technology will develop a whole-college IT vision and strategic plan after this process is complete. It will align with both the College's and University's overall strategic goals, as well as the campus' IT strategic plan.

Development of this strategic plan will involve an overall needs and risk assessment that includes the input of administration, faculty, staff and students, which will be developed by the Director of Information Technology.

The overall needs and risk assessment will be reviewed with the college's IT Advisory Committee (ITAC) prior to delivery to the Dean for approval. The IT Advisory Committee includes faculty and staff representatives from all departments.

Once complete and approved by the Dean, the IT vision and strategic plan will be communicated to college leadership and the IT Advisory Committee and will be published on the College's website.

PERSON RESPONSIBLE FOR IMPLEMENTING CORRECTIVE ACTION

COS Director of Information Technology
COS Dean

DATE CORRECTIVE AND PREVENTIVE ACTION WILL BE IMPLEMENTED

- Completion and acceptance of College of Sciences strategic and culture plans – December 31, 2021
- Director of IT develops draft of whole-college IT vision and strategic plan, including an overall needs and risk assessment and ITAC/stakeholder input – July 30, 2022
- Director of IT provides final draft of IT strategic plan to Dean for review – August 15, 2022
- Dean provides final approval of IT strategic plan and it is published on the College website – September 15, 2022

ISSUE 2: Insufficient IT Support Throughout the College

ISSUE NOTED

There is insufficient IT support throughout the College of Sciences for faculty, staff, and students. IT staff in the college have varying levels of skills and expertise as it relates to providing IT support and have received little to no training on the technologies, hardware, and software for which they are required to support. Additionally, some IT staff have non-IT responsibilities which limits time available for IT support and new IT initiatives. Some departmental IT staff report to non-technical individuals, who may not have the technical knowledge and expertise to ensure IT staff are performing their IT responsibilities fully and appropriately. They may have difficulty in directing and supporting technical staff due to a lack of knowledge in areas including, but not limited to:

- IT vision, strategy, direction (see Issue 1)
- IT policies and procedures (see Issue 3)
- Technology being used or evaluated
- Security risks and threats (see Issues 4-9)
- Federal, State, and University requirements

In addition, students (undergraduate and graduate), postdocs, and faculty provide IT support in areas without IT staff. These individuals may not have adequate IT security experience to ensure University data is protected and may not meet education or certification requirements stated by projects/grants to support IT services. Consistency and sustainability of services are diminished as these students graduate.

IMPACT OF THE ISSUE

An effective and solid IT support function is critical to the college's operational infrastructure, academic mission, and commitment to research. Effective IT support should also align with the college's IT vision, strategy and direction. Training for the current IT resources is essential to improve their understanding and effective use of current and emerging technologies. Training will help the IT resources fulfill the requirements of the college and be more productive and effective in their positions. IT support provided by undergraduate and graduate students does not provide for consistency and sustainability of services in those departments. Students may also fall short of project/grant requirements that a full-time resource would be required to have to start a position, for example, an applicable undergraduate degree, background check, certification, or years of experience.

RECOMMENDATION

We recommend the Dean for the College of Sciences ensure the College of Sciences Director of Information Technology complete a risk assessment to identify the IT support needs within each department and center, particularly in relation to the college's vision and strategy. This would include, but not be limited to, identifying:

- IT points of contact for departments that do not have dedicated IT support
- Training needs for IT staff to fulfill IT functions including technical expertise and security
- Customer service expectations and needs of college personnel
- Existing skillsets that could be matched to current needs
- Gaps in compliance to Federal, State and University IT requirements

MANAGEMENT RESPONSE FROM COS

Since the date the audit occurred, we have implemented the following corrective actions:

- The reporting lines for IT staff from Chemistry, Physics, Biological Sciences, MEAS, and the State Climate Office have changed and staff now report to the college's Sciences IT Technical Services Manager.
- The Math IT position now has a dotted line report to the IT Director.
- All Sciences IT staff are now in professional IT classifications.
- While skills gaps remain, Sciences IT staff have received training in relevant areas and this is a continuing effort.

However, current staffing levels continue to be inadequate to provide sufficient general IT support, much less meet the pressing needs for research support, security and compliance despite the College of Sciences being arguably the most computationally intensive college at NC State. The ratio of IT staff to faculty/staff/students is far lower than CALS or Engineering and even lower than less computationally intensive colleges such as CHASS.

Because of historically low investments in IT and staff salaries, the college is at high risk of losing current staff. Insufficient funding for salaries is exacerbated by the highly competitive market for skilled IT staff in the Research Triangle area which is driving labor costs up rapidly. The College has limitations on its ability to compete effectively and retain experienced staff due to difficulties with funding competitive salaries, the inability to offer salary increases, and less remote work flexibility than our corporate competitors, particularly in the face of rapidly rising housing prices in the Triangle area.

To address this issue, The Director of IT will provide an analysis of IT staffing level and other IT support resource needs along with a risk assessment (including skills gap analysis) for the Dean's review as part of the overall IT needs and risk assessment as noted in the management response to Issue 1. The Dean will identify funding resources necessary to address the IT support needs required by the college.

This analysis will be repeated on an annual basis with the input of the College's IT Advisory Committee. The Dean will consider this analysis in budget planning each year.

The noted problems with IT staff reporting to non-technical supervisors are significant. Because it is not feasible to train non-technical supervisors to develop the level of knowledge necessary to supervise IT staff in the areas indicated in this issue, the College plans to restructure the IT function so that all IT staff in the College report to supervisors with the College's IT unit.

The issue that some IT staff have non-IT responsibilities will be addressed in two ways: College administration will work with the affected departments to identify alternative ways to achieve the non-IT tasks, and the Director of IT will develop a standard operating procedure that defines the scope of IT activities and the extent to which College IT will normally assist with non-IT tasks.

The issue that faculty, postdocs and students are providing IT support without adequate knowledge, certification or IT security expertise will be addressed in three ways:

- First, through the staffing level remediation mentioned above
- Second, through the development and implementation of standard operating procedures (SOPs) to address purchasing, installation, configuration and management practices required to implement the university's IT PRRs and security best practices (see Issue 3) in order to implement a security baseline for new systems by default
- Third, through implementing the university's IT PRRs and security best practices following these SOPs on existing systems. This will include working with OIT to identify alternative solutions, security controls, or architectures in cases where implementation of these requirements creates a significant adverse impact on system performance or productivity.

PERSON RESPONSIBLE FOR IMPLEMENTING CORRECTIVE ACTION

COS Director of Information Technology
COS Dean

DATE CORRECTIVE AND PREVENTIVE ACTION WILL BE IMPLEMENTED

The Director of IT will provide an initial analysis of IT staffing level and other IT support resource needs along with a preliminary risk assessment (including skills gap analysis) for the Dean's review This analysis will be presented to the Dean for review by November 30, 2021.

The Dean will consider the risk levels and will identify funding for IT staff positions and other IT support resources needed, prioritizing areas of high risk and/or high impact, considering budget availability and compliance requirements. The Dean will collaborate with the Director of IT to develop an action plan for staffing level and IT support corrective action by January 31, 2022.

The Dean and the College's assistant deans for HR and finance & business and the senior associate dean for administration will work with the IT director and affected units to transition IT staff in departments and centers to College IT where they will be assigned to IT supervisors. This transition will be completed by February 15, 2022.

See Issue 3 for timelines regarding the development and implementation of the necessary Standard Operating Procedures.

Future ongoing efforts:
The Director of IT will provide an updated staffing level and skills gap assessment and a risk analysis to the Dean by February 15th each year for review and incorporation into budget planning, beginning in 2023.

ISSUE 3: Inadequate IT Policies and Procedures

ISSUE NOTED

The College of Sciences does not have adequate IT policies or procedures at either the college or departmental level documenting day-to-day IT functions and operations. When conducting interviews with IT staff, little to no documentation was provided around IT policies and procedures. This includes IT support, inventory, security, storage, backup, and disaster recovery. Without college and department level IT policies and procedures, compliance with Federal, State, and University IT requirements is more difficult. Examples, include but are not limited to:

- Maintaining up-to-date inventories of data and equipment reflecting current information systems with a level of granularity necessary to assist in resolving problems and securing University assets (see Issues 4-9)
- Ensuring secure configurations for equipment accessing the University's network to protect data
- Ensuring environmental protections are in place for University resources (see Issues 4-9)
- Documenting physical access controls to detail the access authorizations in place, verify who has access, and control the ingress/egress points to server rooms (see Issues 4-9)
- Monitoring and analyzing IT activity for vulnerabilities and implementing remediation plans to address risks
- Implementing and testing backup procedures to ensure that data is recoverable (see Issue 10)

IMPACT OF THE ISSUE

IT policies and procedures ensure that processes are documented and in alignment with the college IT strategy. They assist college users in fulfilling their requirement to protect and secure data residing in or on assigned University accounts or other University and non-University IT resources. Policies and procedures also assist IT staff with enforcement of meeting the requirements outlined in them. Consistent procedures that can be replicated throughout the college assists IT staff in providing dedicated, consistent support to users.

This document may be subject to the North Carolina Public Records Act (NC General Statute 132.1 and NC General Statute 116-40.7). The Office of Record for this document is the NC State University Internal Audit Division. Please refer all requests (internal or external) for release of this document or copies to the Internal Audit Division Chief Audit Officer & Director at (919) 515-8862.

Inadequate IT policies and procedures creates gaps in the level of service provided to end users. Without these policies and procedures, there are no clear guidelines or steps to follow when responding to a request and ensuring the response aligns to the IT strategy of the college. Without policies and procedures, it is difficult to be consistent in making informed decisions and providing efficient resolutions to problems. IT policies and procedures are needed to keep the activities in the college and IT departments running smoothly and ensure consistency and alignment with the IT vision, strategy, and direction.

RECOMMENDATION

We recommend the Dean for College of Sciences ensure that the College of Sciences Director of Information Technology, the Department Heads and Directors create, document, communicate, and implement college and departmental IT policies and procedures consistent with Federal, State, and University requirements. The guidance from the policies and procedures should include, but not be limited to:

- Inventory of data equipment
- Configuration management
- Environmental controls
- Physical access controls
- Vulnerability assessment and remediation
- Backup and recovery

MANAGEMENT RESPONSE FROM COS

The Director of IT will ensure that Standard Operating Procedures (SOPs) are developed that address the operational procedures and policies necessary to support effective delivery of day-to-day functions, ensure compliance with university PRRs and other applicable IT policies, meet compliance requirements, implement security best practices, and operationalize IT strategy. The college's Technical Services Manager will perform a gap analysis to identify operational areas in need of SOPs and develop and SOP portfolio.

The Director of IT will work with the Assistant Dean for Finance and Business to create SOPs and policies governing the acquisition and lifecycle of IT resources, including but not limited to purchasing, shipping and receiving, and IT surplus processes.

An IT asset inventory project is in progress, including the introduction of asset tagging in preparation for a future automated inventory management system. Currently, this inventory effort includes all departments and centers other than Mathematics, Statistics, and the Bioinformatics Research Center. With the centralization of IT staffing (Issue 2) and implementation of a whole-college IT strategy (Issue 1) this effort will expand to encompass all IT resources in the college. Future phases will include software inventory and cloud services.

The College will comply with data inventory requirements as specified by university PRRs. The Director of IT will collaborate with OIT Security & Compliance and the Campus IT Directors group (CITD) to help identify a manageable and effective process to accomplish the requirements. If necessary, the Dean will discuss any related resource needs with the Provost.

The College of Sciences is streamlining its process for approving Standard Operating Procedures (SOPs) through updating the "SOP on SOPs". Once this is complete, the Director of IT will ensure that all approved SOPs are published on the college web site.

PERSON RESPONSIBLE FOR IMPLEMENTING CORRECTIVE ACTION

COS Director of Information Technology
COS Technical Services Manager
COS Assistant Dean for Finance

DATE CORRECTIVE AND PREVENTIVE ACTION WILL BE IMPLEMENTED

- SOP gap analysis for IT operations – December 1, 2021
- "SOP on SOPs" approval and publication – November 30, 2021
- SOP development for identified gaps – January 31, 2022
- SOP development for IT purchasing and related processes – March 15, 2022

ISSUES 4 - 11

We identified 8 issues that contain detailed sensitive security information about University information technology. In accordance with the North Carolina General Statute §132-6.1 (c), the IT security matters are not subject to public disclosure; thus, these issues, recommendations, and related management corrective action plans have not been provided here.

The College of Sciences is actively working with the Provost Office, OIT, and Office of Finance and Administration to identify funding sources for the corrective actions for these issues. According to the college, these corrective actions cannot begin until funding is provided. It is estimated that it will take three years to implement these corrective actions once funded.