STATE OF NORTH CAROLINA

UNC-GENERAL ADMINISTRATION

BANNER HOSTING SERVICES

DECEMBER 2013

INFORMATION TECHNOLOGY GENERAL CONTROLS

PERFORMANCE AUDIT

OFFICE OF THE STATE AUDITOR

BETH A. WOOD, CPA
STATE AUDITOR

EXECUTIVE SUMMARY

PURPOSE

This audit evaluated the policies and procedures of the University of North Carolina General Administration (UNC-GA) that govern the hosting services it provides to six university campuses to operate their financial systems. UNC-GA offers a package of hosting services, including system administration, database support, and hardware capacity, to UNC campuses.

BACKGROUND

UNC-GA is tasked with increasing operational efficiency across the UNC-system. Today, 14 of 17 UNC campuses use the Banner financial system to provide a consistent financial reporting system across the UNC system. While the system increases operational efficiency, there are costs associated with maintaining the infrastructure required by the system. To reduce these costs, UNC-GA offers a package of hosting services to UNC campuses.

During the audit period, six UNC campuses used this service: UNC-School of the Arts, Fayetteville State University, North Carolina Central University, Elizabeth City State University, UNC-Asheville, and Winston-Salem State University.

This audit covers the period from July 1, 2012, through June 13, 2013.

KEY FINDINGS

- UNC-GA has not defined and communicated key security and availability standards, creating an environment where hosting services may not meet the business requirements of the universities served.
- UNC-GA has not clearly defined responsibilities related to long-term preservation of data, creating an elevated risk of losing historical student and financial data campuses retain to service the needs of its students and employees.

KEY RECOMMENDATIONS

- UNC-GA should define information security standards for campus data and incorporate these in service level agreements with each campus receiving hosting services and also parties, such as North Carolina Information Technology Services, that UNC-GA relies upon to fulfill requirements of Banner Hosting Services.
- UNC-GA should work with each campus receiving hosted services to determine their long-term data retention requirements and assign personal responsibility for a plan to meet those requirements.

Key findings and recommendations do not include all findings and recommendations in this report.

STATE OF NORTH CAROLINA

Office of the State Auditor

Beth A. Wood, CPA
State Auditor

2 S. Salisbury Street
20601 Mail Service Center
Raleigh, NC 27699-0601
Telephone: (919) 807-7500
Fax: (919) 807-7647
Internet
http://www.ncauditor.net

December 19, 2013

The Honorable Pat McCrory, Governor
Members of the North Carolina General Assembly
Mr. Thomas Ross, President of the University of North Carolina
Mr. Peter Hans, Chairman of the University of North Carolina Board of Governors
Mr. John Leydon, Chief Information Officer of the University of North Carolina

Ladies and Gentlemen:

We are pleased to submit the results of our performance audit of information technology general controls at the University of North Carolina General Administration (UNC-GA) for the Banner Hosting Services.

The purpose of our audit was to review information technology general controls as they pertain to the hosting services provided to six universities within the University of North Carolina system covering the Banner application, which houses university financial data.

The results of our audit disclosed deficiencies that are considered reportable under Government Auditing Standards. The items regarding network security, due to their sensitivity, are reported by separate letter and should be kept confidential as provided in North Carolina G.S. 132-6.1(c).

The UNC-GA has reviewed the findings. Their responses to the findings in the public report are included.

We wish to express our appreciation to the UNC-GA staff for the courtesy, cooperation, and assistance provided us during the audit.

Beth A. Wood

Beth A. Wood, CPA
State Auditor

TABLE OF CONTENTS

PAGE

BACKGROUND

Shortly after the formation of the UNC System in 1971, campus administrators identified technology as an area where campuses could benefit from sharing knowledge and resources. To this end, the UNC System administrative office, known as UNC General Administration, sponsored an initiative called UNC-CAUSE in 1974. From the beginning, the objective of UNC-CAUSE was to *"establish a system-wide network of data processing professionals with the goals/objectives of sharing applications between campuses to reduce development costs associated with administrative applications."* [1]

In 2000, many UNC campuses were aware that their legacy financial systems were aging and vendor support was on the decline. That year, UNC-GA sponsored the development of the first UNC System-wide IT strategy. The UNC Shared Services Alliance was born to guide the search for an enterprise-wide system to integrate multiple business functions in a single application.

In 2002, the Alliance selected the Banner system. The Banner system processes financial data for the campuses, which may include payroll, student tuition and fees, student financial aid, accounts payable, and cash accounts. According to the Shared Services Alliance, the Banner Project has four objectives:

1. Transform business processes and leverage common processes across institutions
2. Facilitate development of shared vision through use of enterprise process methodology
3. Implement and maintain the systems in a collaborative manner
4. Enhance services through a single University-wide solution of integrated databases.

As campuses within the UNC System implemented this enterprise-class solution, it became evident that smaller campuses lacked the resources needed to support such an enterprise-level system. In response, the UNC Shared Services Alliance developed hosted services to help campuses. Today, UNC-GA's Hosting Services provide a means to achieve highly available systems for the Banner modules used by UNC campuses.

The UNC-GA Shared Services Alliance offers Banner Hosting services as an option to all 17 constituent campuses of the UNC System. As of spring 2013, six UNC campuses used this service: UNC-School of the Arts, Fayetteville State University, North Carolina Central University, Elizabeth City State University, UNC-Asheville, and Winston-Salem State University.

As part of hosting services, UNC-GA provides system administration, database support, and hardware capacity for each hosted campus. Each campus retains ownership of its Banner enterprise system and therefore bears the responsibilities of defining the controls it deems necessary to provide for the availability, integrity, and confidentiality of their system.

With Banner Hosting Services, each campus explicitly delegates to UNC-GA the responsibilities of implementing, maintaining, and securing the infrastructure needed to support their Banner financial system. This arrangement delegates only tasks associated with administering the infrastructure required by the Banner system. UNC campuses using Banner

[1] http://unccause.org/

Hosting Services retain responsibility for the accuracy and completeness of their respective financial data. As custodian of campus data, UNC-GA manages data that continues to remain the property of each respective campus.

Banner Hosting Services is supported by the network and computing resources provided by MCNC and the North Carolina Office of Information Technology Services (ITS). MCNC is the private, non-profit operator of the North Carolina Research and Education Network (NCREN) that offers network connectivity to UNC-GA and all UNC campuses. ITS provides computing and network services to North Carolina state agencies and universities. UNC-GA receives both network connectivity and data center resources from MCNC and ITS in support of Banner Hosting Services.

Objectives, Scope, and Methodology

This audit evaluated the policies and procedures governing the Banner Hosting Services offered by the University of North Carolina General Administration (UNC-GA). The focus was on the hosting services provided to six UNC campuses that chose to use the hosting services. The audit's findings and recommendations apply to the Banner Hosting Services and not necessarily to UNC-GA as a whole.

Specifically, this audit evaluated information technology (IT) general controls for Banner Hosting Services that were designed, implemented, and operated throughout the period of July 1, 2012, through June 13, 2013. Since the hosted campuses are responsible for end-user processes and related internal controls supporting the completeness and accuracy of Banner data, this audit evaluated only system-level controls in place at UNC-GA and did not evaluate suitability of controls in place at each campus.

This audit sought to gain an understanding of the controls in place that support financial reports generated by the hosted universities. However, when assessing the overall level of security within the hosted environment, consideration was given to risks in both the financial and the public-access portions of the hosted environment.

The audit scope included the following IT general controls categories in relation to the hosted Banner systems:

- IT governance
- Access controls
- Program maintenance and change controls
- Operations procedures
- Physical security
- Help desk support
- Disaster recovery
- Network & virtualization security

To accomplish the audit objectives, auditors gained an understanding of UNC-GA Hosting Service's policies and procedures, interviewed key UNC-GA administrators and other personnel from hosted campuses, examined system configurations, tested select system controls, reviewed appropriate technical literature, and inspected computer-generated reports. The fieldwork phase of the audit lasted from March 6, 2013, through June 13, 2013.

As a basis for evaluating IT general controls, guidance contained in the *International Organization for Standardization (ISO) 27002 Information Technology - Security Techniques: Code of Practice for Information Security Management* was used. As allowed by state law[1], the University of North Carolina and its constituent institutions adopted ISO 27002 as the framework for information technology security standards. ISO 27002 is an information security standard that provides best practice recommendations on information security management for

[1] North Carolina General Statute §147-33.111(b)

use by those responsible for initiating, implementing, or maintaining information security management systems.

Additionally, auditors applied the guidance contained in the *Control Objectives for Information and Related Technology* (COBIT) framework issued by ISACA. COBIT is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks. COBIT enables clear policy development and good practice for IT control throughout organizations. COBIT emphasizes regulatory compliance and helps organizations increase the value of IT. COBIT standards state that management should implement controls to ensure that the organization's policies and procedures are designed to adequately protect critical and sensitive data from unauthorized access from both internal and external users.

UNC-GA management, pursuant to state law,[2] bears full responsibility for establishing and maintaining a proper system of internal control, which includes IT general controls. A proper system of internal control is designed to provide reasonable, rather than absolute, assurance that relevant objectives are achieved. Because of inherent limitations in internal controls, unauthorized access to data, for example, may nevertheless occur and not be detected. Projections of the auditors' evaluation in this report of general controls to future periods are subject to the risk that, for example, conditions at UNC-GA Hosting Services may change or compliance with policies and procedures may deteriorate.

This performance audit was conducted in accordance with generally accepted government auditing standards. Those standards require that auditors plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for findings and conclusions based on the audit objectives. The Office of the State Auditor believes that the evidence obtained provides a reasonable basis for the findings and conclusions based on the audit objectives.

This audit was conducted under the authority vested in the State Auditor of North Carolina by *North Carolina General Statute §147.64.*

[2] North Carolina General Statute §143D-7

AUDIT FINDINGS, RECOMMENDATIONS AND RESPONSES

The results of our audit disclosed deficiencies considered reportable under *Government Auditing Standards*. Findings regarding network security, due to their sensitive nature, are reported to UNC-GA management by separate letter and should be kept confidential as provided in North Carolina G.S. 132-6.1(c).

The auditors found deficiencies related to information technology (IT) governance practices by UNC-GA that could increase the risk of inadequate performance by Banner Hosting Services' employees and contractors. Specifically, auditors found:

FINDING #1: KEY DATA SECURITY AND SYSTEM AVAILABILITY STANDARDS ARE NOT DEFINED AND INCLUDED IN WRITTEN AGREEMENTS

Security Standards for Information Systems are guided by three main principles:

Availability: Allows authorized users to depend on systems to access needed data in a timely manner, even after a system failure or occurrence of a natural disaster.

Integrity: Allows authorized users to trust that data is both unaltered and accurate.

Confidentiality: The prevention of unauthorized information disclosure using appropriate security safeguards.

Service level agreements (SLA's) between Banner Hosted Services and the six universities receiving services do not define and include key standards involving data security and availability of the Banner system. The lack of standards and failure to monitor compliance against those standards elevates the risk of incidents that could adversely affect the confidentiality, integrity, and availability of hosted data, affecting the ability of campuses to rely on the Banner system. The Banner system processes financial data for campuses, which may include payroll, student tuition and fees, student financial aid, accounts payable, and cash accounts.

Existing SLA's Do Not Adequately Address Key Areas:

- Disaster Recovery—Key metrics involving availability are not formally defined. Without clearly defined expectations, there is a risk of data loss and unexpected downtime from disasters affecting primary data centers. For example, SLAs lack provisions to help UNC-GA facilitate disaster recovery testing with campuses. In addition, agreements fail to specify recovery time objectives and recovery point objectives. A recovery time objective is the amount of time needed to restore systems after a disaster occurs. A recovery point objective is the amount of data lost after a disaster, measured by how far back in time the system is restored.
- Security Monitoring, Incident Response, and Reporting—SLA's did not define levels of security monitoring of hosted services or describe appropriate incident response procedures, including how campuses are notified of such incidents. Without monitoring and reporting of incidents, UNC-GA and campuses receiving hosted services may not be

able to appropriately respond to incidents affecting the confidentiality, integrity, or availability of hosted data. Not only does this increase the risk of non-compliance with state and federal requirements, it increases the difficulty of UNC-GA preventing similar incidents from recurring in the future.

- Dispute Resolution—SLA's lacked details on how campuses can resolve disputes involving hosted services, including problems that may arise from data loss and system availability.

Missing or Ineffective Service Level Agreements (SLA's):

- Western Data Center—UNC-GA lacked a signed SLA with the North Carolina Office of Information Technology Services (ITS) for its use of the Western Data Center to support Hosted Banner Services. Without an enforceable agreement, UNC-GA accepts undue risks in relying upon the Western Data Center to support availability of Banner Hosted Services.
- Elizabeth City State University (ECSU)—although UNC-GA has an SLA defined with ECSU, UNC-GA failed to review the agreement for effectiveness. Throughout the document, the ECSU campus is referred to as "East Carolina State University" instead of Elizabeth City State University.

Recommendations

- Update existing service level agreements with campuses with specific provisions that current agreements do not adequately address, including:
  - Disaster recovery - continue disaster recovery testing with hosted campuses to define reasonable recovery point objectives and recovery time objectives.
  - Security monitoring - define security events to monitor on hosted servers. The definition should clarify the frequency of associated security reports provided to campuses as well as a description of incident response procedures and notification.
  - Dispute resolution - define an agreed to dispute resolution process with hosted campuses to handle disagreements or other incidents, such as data loss.

- Complete a service level agreement for the Western Data Center to ensure that the North Carolina Office of Information Technology Services can adequately support intended availability metrics of Banner Hosting Services.

- Correct the service level agreement for Elizabeth City State University to incorporate the proper legal name of the campus.

UNC-GA Response

Disaster Recovery:

- We agree with the findings and recommendations. The UNC-GA hosting staff is currently completing a draft of a new service level agreement (SLA) that will clearly state the disaster recovery testing schedule, recovery time objectives and recovery point objectives. We expect the draft to be completed no later than January 15, 2014, and then forwarded to the hosted campuses for further review. Upon completion of the review, the new SLA will be sent to the campuses for signature.

Security Monitoring, Incident Response, and Reporting:

- We agree with the findings and recommendations. The UNC-GA hosting staff team is currently completing a draft of a new SLA that will clearly state the expected levels and process for security monitoring of the systems within the hosted environment. The draft will also include the expected incident response procedure and campus notification process. We expect the draft to be completed no later than January 15, 2014, and then forwarded to the hosted campuses for further review. Upon completion of the review, the new SLA will be sent to the campuses for signature.

Dispute Resolution:

- We agree with the findings and recommendations. The UNC-GA hosting staff is currently completing a draft of a new SLA that will clearly state the dispute resolution procedure. We expect the draft to be completed no later than January 15, 2014, and then forwarded to the hosted campuses for further review. Upon completion of the review, the new SLA will be sent to the campuses for signature.

Missing or Ineffective Service Level Agreements:

- Western Data Center: We agree with the finding and recommendation. The finding has been corrected; a Memorandum of Understanding has been signed with the Western Data Center.

- Elizabeth City State University: We agree with the finding and recommendations. The finding has been corrected; the current SLA executed with Elizabeth City State University has been updated.

FINDING #2: LONG-TERM PRESERVATION OF FINANCIAL DATA NOT MADE

Backups of data from information systems can be produced in a variety of ways depending on the intended purpose of the backup. Data backups fall into one of two categories:

- Active backups—copies of data that are readily accessible to restore systems in the event the primary system goes offline. Often, these backups are maintained for a short period and are overwritten by a more current backup on a regular basis.
- Archival backups—copy of data representing a point-in-time snapshot stored in a secured, offline location for many years. Archives are often used to address regulations governing the long-term preservation of data, but they can also play an integral part in restoring systems to a specific point-in-time.

The current backup configuration is not designed to address long-term **archival** needs. Given the inherent limitations of capacity of online backup systems, the active backups maintained online by UNC-GA Hosting Services are overwritten multiple times within each accounting cycle. Therefore, the current backup configuration is not designed to address long-term archival needs. If data were to become corrupted and go unnoticed until after all active backups are overwritten, the current system provides no means to restore systems to a point-in-time prior to the corruption event.

UNC-GA Hosting Services currently maintains multiple copies of data in an online system to address the need to have **active** backups supporting system restoration. These backups are stored both locally at the primary site and are replicated to the backup site, allowing for system to switch processing to the backup site in the event the primary sites goes offline.

This system does not adequately address policies or regulations requiring campuses to preserve point-in-time snapshots of data for multiple years. To comply with federal and state regulations for data, UNC campuses are required to maintain long-term archives of data for multiple years.

UNC-GA has not communicated with campuses to determine each campus’ specific **archival** needs. Because each campus may house different types of data in the Banner Hosting Environment, each campus has unique data archive requirements. Without defining these needs, UNC-GA is not able to devise plans or assign responsibilities designed to assist campuses with regulatory compliance requirements pertaining to data archives.

Recommendations

Communicate with each hosted campus to determine its long-term data retention requirements. Document an agreement with each campus that defines:

- The frequency in which data archives need to be created and storage media to be used.
- The security requirements of the archives, including physical security, use of encryption, and management of any encryption keys used.
- The party responsible for physically maintaining offline data archives. This responsible party can be a representative from UNC-GA, a representative from the hosted campus, or a representative from a third-party vendor. Regardless of the responsible party, archives should be stored in a secured location that is geographically separate from the data centers used by UNC-GA.

UNC-GA Response

- We agree with the findings and recommendations. The UNC-GA hosting staff is currently completing a draft of a new SLA that will clearly state the campus's responsibility for the long-term archiving and offsite storage of campus financial data. We expect the draft to be completed no later than January 15, 2014, and then forwarded to the hosted campuses for further review. Upon completion of the review, the new SLA will be sent to the campuses for signature.

- The UNC-GA hosting staff will conduct a survey and review process to identity campus processes, options, expectations and retention requirements in this area. This survey will be completed by January 31, 2014, and if it is determined this service needs to be offered within the hosted environment, the UNC-GA hosting staff will develop a solution with an appropriate business model, and submit the proposal to the campuses for review. The solution will clearly state the performance goals related to frequency of archiving, the identification of any security measures required for the archived data, and the identification of responsible parties for the maintenance of off-site storage. Upon campus approval, the proposed solution will be implemented. A description of the service, along with its performance metrics and responsibilities, will be clearly stated as an addendum to the existing SLA, or, depending on the adopted business model, a separate SLA covering the archival storage of data will be developed.

FINDING #3: NO FORMAL TRAINING PROCESS AND CONFIDENTIALITY AGREEMENT

UNC-GA does not provide formal technical or security awareness training to employees working with Banner Hosting Services. These same employees also do not receive information regarding the confidentiality of data stored within the hosted environment nor are they required to sign a confidentiality agreement covering information they may see in their normal course of duties. Without formal training and agreement by employees, employees supporting Banner Hosting Services may make decisions that compromise the security of hosted data.

Formal Training and Security Awareness

Employees supporting Banner Hosting Services need to remain aware of the risks associated with a rapidly changing IT landscape. New threats to data security evolve each day and employees supporting Banner Hosting Services must be aware of these threats in order to guard against them. Without formal training conducted on a regular basis, employees may be unaware of risks and inadvertently make decisions that compromise security, causing hosted services to become vulnerable to exploitation and data loss.

Confidentiality Agreements

In providing Banner Hosted Services to campuses within the UNC System, UNC-GA and its support personnel accept responsibility for being custodians of campus data. This responsibility requires UNC-GA management to ensure that sufficient administrative controls are in place to safeguard the integrity and confidentiality of hosted data.

An important administrative control involves training employees about confidentiality rules related to the data under their care. Such training should conclude by gathering explicit acceptance of these rules. Without formal employee training and subsequent receipt of understanding and acceptance of rules regarding confidentiality, staff members may not understand the data they work with is confidential. This increases the risk that employees may inadvertently share it with other parties, possibly in violation of laws and regulations.

Recommendations

- Develop a formal security awareness program for staff supporting Banner Hosting Services. The program should include both general security training as well as risks specific to the hosted environment, as identified in the internal risk assessment. Training to communicate these updates to staff should occur annually or after major changes to the hosted environment.
- Provide annual training to staff on state and federal regulations for data that resides on the hosted servers. At the conclusion of such training, staff should agree to and sign a confidentiality agreement covering student and financial data housed within the hosted environment.

UNC-GA Response

Formal Training and Security Awareness:

- We agree with the findings and recommendations. The UNC-GA Division of Information Technology is currently developing a UNC-GA program to cover general annual security awareness and sensitive data handling, and this program will include the personnel who support and use data from the hosted environment. We have procured training videos from the SANS “Securing the Human” program, as well as the “application developer” modules, and will deploy these videos as part of our training program. We will work with UNC-GA Division of Human Resources to develop our enterprise plan, and if the rollout of the general plan is delayed beyond March 15, 2014, we will roll out a targeted effort to the technical staff within the hosted environment prior to that date. We will supplement the formal effort with occasional web ex presentations (or similar) from experts and vendors who operate in the data security awareness and policy space (FBI cyber security program, etc.).

Confidentiality Agreements:

- We agree with the findings and recommendations. As part of the general security awareness training outlined above, the UNC-GA Division of Information Technology will develop a blanket confidentiality agreement for the employees at UNC-GA, and if the rollout of the general confidentiality agreement is going to be delayed beyond March 15, 2014, we will roll out a specific confidentiality agreement to the technical staff within the hosted environment prior to that date.

FINDING #4: FEEDBACK FROM CAMPUSES NEEDED TO ASSESS PERFORMANCE AND MINIMIZE RISKS

UNC-GA did not seek feedback from campuses on Banner Hosted Services and did not include hosted services in its most recent information technology (IT) risk assessment. Consequently, the opportunities to identify and improve hosted services were not maximized. In providing Banner Hosting Services to campuses within the UNC System, UNC-GA assumes the responsibility of maintaining an active dialog with each hosted campus to determine what each campus defines as acceptable performance related to availability, integrity, and confidentiality of hosted data.

Policy Review and Campus Feedback

Although UNC-GA has a well-established system for tracking feedback on specific support issues, written feedback was not collected from campuses related to the overall performance of hosting services. Without this written feedback, UNC-GA cannot perform an effective review of data security and system availability of its systems. This is significant because UNC-GA intends to promote these services to more UNC campuses.

Risk Assessment

UNC-GA performs an annual IT risk assessment, but the most recent assessment, dated in 2011, contained a significant gap because it did not consider Banner Hosted Services in its analysis. Without knowledge of specific risks associated with hosted services, campuses are not able to provide UNC-GA with feedback about additional areas related to integrity and confidentiality that should be more closely monitored.

Recommendations

The agreed upon metrics that drive the governance of Banner Hosted Services should be clearly defined in the Service Level Agreements between UNC-GA and each campus. To meet these goals effectively, UNC-GA should regularly review the performance of Banner Hosted Services against these metrics and actively communicate with the campuses areas of risk that could affect the performance of Banner Hosted Services:

- Implement a formal method to gather feedback from campuses on the performance of hosting services and risks they have identified in their own risk assessments. Incorporate this feedback in a periodic review process covering service level agreements, with the objective of ensuring written agreements are effective and adequately address risks related to availability, integrity, and confidentiality of UNC-GA Hosted Services.
- Perform an annual risk assessment that includes Banner Hosting Services and share information related to Banner Hosting Services with affected campuses. In cooperation with affected campuses, devise and implement plans to address risks on an agreed-upon timetable.

UNC-GA Response

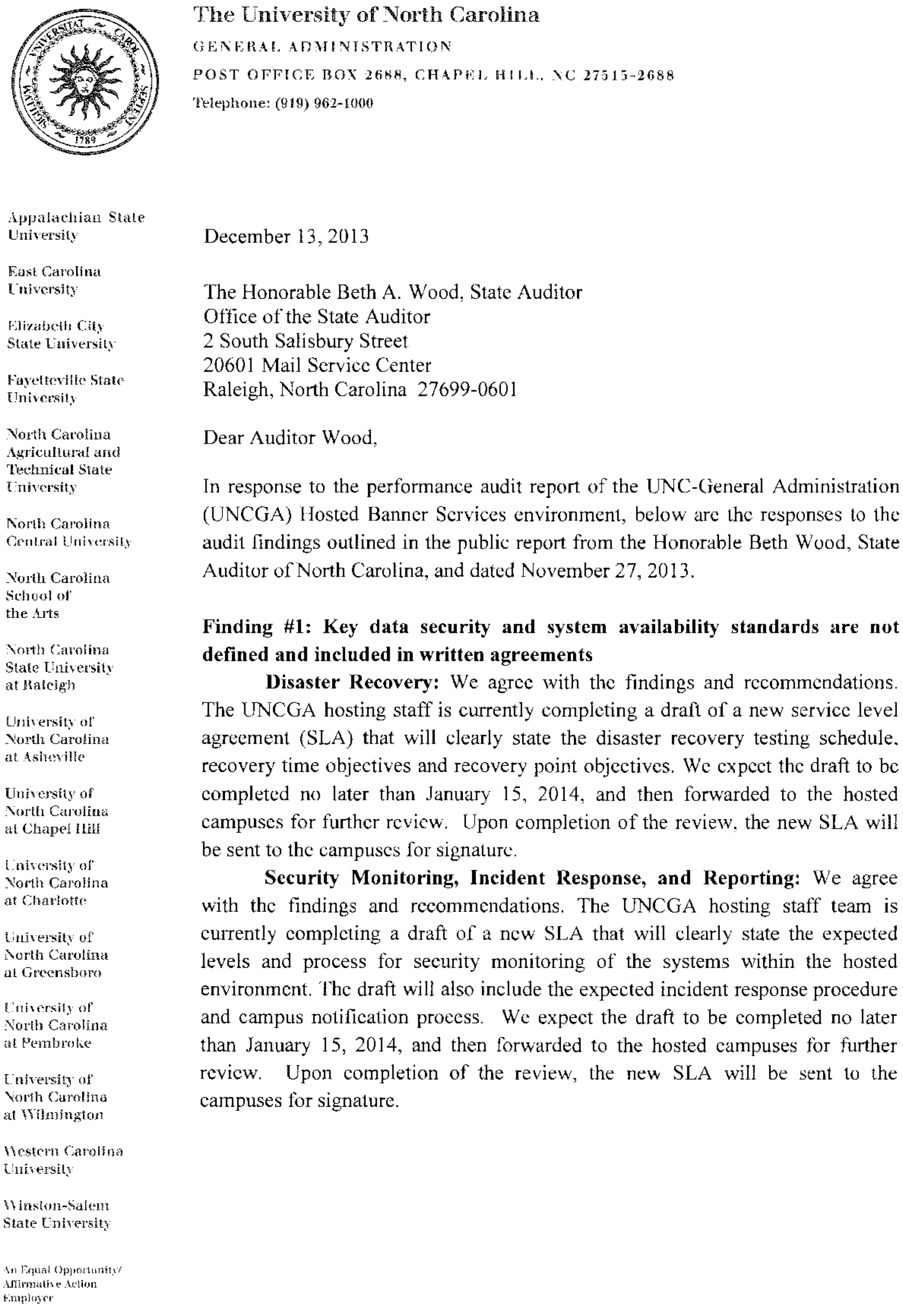
Policy Review and Campus Feedback:

- We agree with the findings and recommendations. The UNC-GA hosting staff will develop a formal mechanism to receive written campus feedback on an annual basis, and have this mechanism in place prior to March 1, 2014. For campuses subscribed to the hosted environment, we have implemented a new two-tiered governance structure that will help facilitate this process and provide multiple entry points to receive campus feedback. In the meantime, the campus representatives meet on a regular basis (at least quarterly) via in-person meetings or videoconferences. During those meetings, we provide the opportunity for the campus representatives to raise issues of concern and provide feedback. Additionally, UNC-GA hosting staff is also in constant contact — via email, text and phone — with campus representatives.

Risk Assessment:

- We agree with the findings and recommendations. The finding has been corrected and a new version of the UNC-GA Risk Assessment has been posted to the UNC-GA website. The updated version includes risk discussion for the hosted environment.

UNC-GA RESPONSE



The University of North Carolina
GENERAL ADMINISTRATION
POST OFFICE BOX 2688, CHAPEL HILL, NC 27515-2688
Telephone: (919) 962-1000

Appalachian State University

East Carolina University

Elizabeth City State University

Fayetteville State University

North Carolina Agricultural and Technical State University

North Carolina Central University

North Carolina School of the Arts

North Carolina State University at Raleigh

University of North Carolina at Asheville

University of North Carolina at Chapel Hill

University of North Carolina at Charlotte

University of North Carolina at Greensboro

University of North Carolina at Pembroke

University of North Carolina at Wilmington

Western Carolina University

Winston-Salem State University

An Equal Opportunity/ Affirmative Action Employer

December 13, 2013

The Honorable Beth A. Wood, State Auditor
Office of the State Auditor
2 South Salisbury Street
20601 Mail Service Center
Raleigh, North Carolina 27699-0601

Dear Auditor Wood,

In response to the performance audit report of the UNC-General Administration (UNCGA) Hosted Banner Services environment, below are the responses to the audit findings outlined in the public report from the Honorable Beth Wood, State Auditor of North Carolina, and dated November 27, 2013.

Finding #1: Key data security and system availability standards are not defined and included in written agreements

Disaster Recovery: We agree with the findings and recommendations. The UNCGA hosting staff is currently completing a draft of a new service level agreement (SLA) that will clearly state the disaster recovery testing schedule, recovery time objectives and recovery point objectives. We expect the draft to be completed no later than January 15, 2014, and then forwarded to the hosted campuses for further review. Upon completion of the review, the new SLA will be sent to the campuses for signature.

Security Monitoring, Incident Response, and Reporting: We agree with the findings and recommendations. The UNCGA hosting staff team is currently completing a draft of a new SLA that will clearly state the expected levels and process for security monitoring of the systems within the hosted environment. The draft will also include the expected incident response procedure and campus notification process. We expect the draft to be completed no later than January 15, 2014, and then forwarded to the hosted campuses for further review. Upon completion of the review, the new SLA will be sent to the campuses for signature.

The Honorable Beth A. Wood
December 13, 2013
Page 2

Dispute Resolution: We agree with the findings and recommendations. The UNCGA hosting staff is currently completing a draft of a new SLA that will clearly state the dispute resolution procedure. We expect the draft to be completed no later than January 15, 2014, and then forwarded to the hosted campuses for further review. Upon completion of the review, the new SLA will be sent to the campuses for signature.

Missing or ineffective Service Level Agreements:

Western Data Center: We agree with the finding and recommendation. The finding has been corrected; a Memorandum of Understanding has been signed with the Western Data Center.

Elizabeth City State University: We agree with the finding and recommendations. The finding has been corrected; the current SLA executed with Elizabeth City State University has been updated.

Finding #2: Long-term preservation of financial data

Long-Term Archival Storage of Data: We agree with the findings and recommendations. The UNCGA hosting staff is currently completing a draft of a new SLA that will clearly state the campus's responsibility for the long-term archiving and offsite storage of campus financial data. We expect the draft to be completed no later than January 15, 2014, and then forwarded to the hosted campuses for further review. Upon completion of the review, the new SLA will be sent to the campuses for signature.

The UNCGA hosting staff will conduct a survey and review process to identity campus processes, options, expectations and retention requirements in this area. This survey will be completed by January 31, 2014, and if it is determined this service needs to be offered within the hosted environment, the UNCGA hosting staff will develop a solution with an appropriate business model, and submit the proposal to the campuses for review. The solution will clearly state the performance goals related to frequency of archiving, the identification of any security measures required for the archived data, and the identification of responsible parties for the maintenance of off-site storage. Upon campus approval, the proposed solution will be implemented. A description of the service, along with its performance metrics and responsibilities, will be clearly stated as an addendum to the existing SLA, or, depending on the adopted business model, a separate SLA covering the archival storage of data will be developed.

Finding #3: No formal training process and confidentiality agreements

Formal Training and Security Awareness: We agree with the findings and recommendations. The UNCGA Division of Information Technology is currently developing a UNCGA program to cover general annual security awareness and sensitive data handling, and this program will include the personnel who support and use data from the hosted environment. We have procured training videos from the SANS "Securing the Human" program, as well as the "application developer" modules, and will deploy these videos as part of our training program.

The Honorable Beth A. Wood
December 13, 2013
Page 3

We will work with UNCGA Division of Human Resources to develop our enterprise plan, and if the rollout of the general plan is delayed beyond March 15, 2014, we will roll out a targeted effort to the technical staff within the hosted environment prior to that date. We will supplement the formal effort with occasional web ex presentations (or similar) from experts and vendors who operate in the data security awareness and policy space (FBI cyber security program, etc.).

Confidentiality Agreements: We agree with the findings and recommendations. As part of the general security awareness training outlined above, the UNCGA Division of Information Technology will develop a blanket confidentiality agreement for the employees at UNCGA, and if the rollout of the general confidentiality agreement is going to be delayed beyond March 15, 2014, we will roll out a specific confidentiality agreement to the technical staff within the hosted environment prior to that date.

Finding #4: Feedback from campuses needed to assess performance and minimize risks

Policy Review and Campus Feedback: We agree with the findings and recommendations. The UNCGA hosting staff will develop a formal mechanism to receive written campus feedback on an annual basis, and have this mechanism in place prior to March 1, 2014. For campuses subscribed to the hosted environment, we have implemented a new two-tiered governance structure that will help facilitate this process and provide multiple entry points to receive campus feedback. In the meantime, the campus representatives meet on a regular basis (at least quarterly) via in-person meetings or video-conferences. During those meetings, we provide the opportunity for the campus representatives to raise issues of concern and provide feedback. Additionally, UNCGA hosting staff is also in constant contact — via email, text and phone — with campus representatives.

Risk Assessment: We agree with the findings and recommendations. The finding has been corrected and a new version of the UNCGA Risk Assessment has been posted to the UNCGA website. The updated version includes risk discussion for the hosted environment.

Sincerely,

Thomas Ross
President

ORDERING INFORMATION

Copies of this report may be obtained by contacting the:

Office of the State Auditor
State of North Carolina
2 South Salisbury Street
20601 Mail Service Center
Raleigh, North Carolina 27699-0601

Telephone: 919-807-7500

Facsimile: 919-807-7647

Internet: http://www.ncauditor.net

To report alleged incidents of fraud, waste or abuse in state government contact the:

Office of the State Auditor Fraud Hotline: 1-800-730-8477

or download our free app

https://play.google.com/store/apps/details?id=net.ncauditor.ncauditor

https://itunes.apple.com/us/app/nc-state-auditor-hotline/id567315745

For additional information contact:
Bill Holmes
Director of External Affairs
919-807-7513

This audit, including sensitive matters reported by a separate letter, was conducted in 1077 hours at an approximate cost of $81,852. The total cost of the audit represents 0.4% of the total UNC-GA budget ($18,411,141) for the fiscal year ended June 30, 2013.