STATE OF NORTH CAROLINA

INFORMATION SYSTEMS AUDIT

OFFICE OF INFORMATION TECHNOLOGY SERVICES
INFORMATION TECHNOLOGY GENERAL CONTROLS

OCTOBER 2014

OFFICE OF THE STATE AUDITOR

BETH A. WOOD, CPA

STATE AUDITOR

EXECUTIVE SUMMARY

PURPOSE

This audit was conducted to determine the effectiveness of information technology general controls in the Office of Information Technology Services (ITS). The audit specifically focused on controls for the virtual server environment managed by ITS and the North Carolina Identity Management Service (NCID) system.

BACKGROUND

ITS implemented its virtual environment in 2007. The virtual environment enables ITS to save money by reducing the number of physical servers needed to support operations. ITS is responsible for managing the security, configurations, and resources (capacity, processing speed, etc.) for the virtual environment.

ITS began using NCID in 2001 to provide state agency, local government, business, and individual users access to many state information resources through just one account. ITS supports the NCID application and establishes the initial organization, agency, and NCID administrator accounts. The individual agencies and organizations manage NCID user administration.

KEY FINDINGS

- There is a lack of documented procedures for managing the ITS virtual environment.
- Service level agreements between ITS and clients are not reviewed regularly.
- Changes are made to the ITS virtual environment without documented authorization.
- Required information is not included in documentation for changes to key systems.
- Prior year audit issues have not been resolved which increases risks to ITS operations.

KEY RECOMMENDATIONS

- ITS should develop, implement, and maintain updated standard operating procedure documentation to manage the virtualization platforms.
- ITS should conduct and document periodic service level reviews with customers.
- ITS should ensure that only system updates authorized through the change control process are applied.
- ITS should create a quality review process to ensure change requests have all required attributes and comply with standards.
- ITS should implement recommendations from the July 2013 Information Technology General Controls audit. ITS should develop a formal process for addressing external audit findings.

OTHER INFORMATION

Items regarding security controls, due to their sensitivity, were reported to the agency by separate letter and should be kept confidential as provided in *North Carolina General Statute 132.6.1(c).*

Key findings and recommendations may not be inclusive of all findings and recommendations in the 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

October 21, 2014

The Honorable Pat McCrory, Governor
Members of the North Carolina General Assembly
Mr. Chris Estes, State Chief Information Officer

Ladies and Gentlemen:

We are pleased to submit the results of our information systems audit of the Office of Information Technology Services (ITS) information technology general controls.

The audit objectives were to determine if: 1) information technology general controls exist for the virtual server environments and for the North Carolina Identity Management (NCID) system managed by ITS; 2) security controls exist for the virtual server environments managed by ITS; 3) prior year audit issues have been successfully resolved; and 4) NCID system security configuration controls are in place.

The results of our audit disclosed deficiencies that are reportable under Government Auditing Standards. The items regarding server security, due to their sensitivity, are reported by separate letter and should be kept confidential as provided *in North Carolina General Statute132-6.1(c).* The Office of the State Auditor initiated this audit as authorized by *North Carolina General Statute 147-5A.*

The Office of Information Technology Services was presented in advance with the findings and recommendations on April 28, 2014. ITS' written comments to this report are included after each recommendation section and in Appendix A.

We wish to express our appreciation to ITS for the courtesy, cooperation, and assistance provided us during the audit.

Respectfully submitted,

Beth A. Wood

Beth A. Wood, CPA
State Auditor

TABLE OF CONTENTS

PAGE

INTRODUCTION

AUDIT FINDINGS, RECOMMENDATIONS, AND RESPONSES

APPENDICES

BACKGROUND

The General Assembly, in recognition of the need to better manage the acquisition and use of information technology in general state government, created the Office of Information Technology Services (ITS) in 1983 (at the time called State Information Processing Services).

ITS is the leading provider of information technology services such as hosting, network, video, telecommunications, and enterprise services (e.g. e-mail) to state agencies, local governments, and educational institutions. *North Carolina General Statute 147-33.83* stipulates, among other things, that ITS shall provide cities, counties, and other local governmental units with access to ITS information resource centers and services. ITS uses mainframe computers, distributed computing servers, and statewide voice, data, and video networks to provide these services. ITS operates as an internal service fund and recovers the cost of providing these services through direct billings to clients.

ITS implemented its virtual environment in 2007. In the virtual environment, multiple operating systems and applications run concurrently on a single server platform in isolated environments called virtual machines. ITS creates and runs the virtual machines using VMWare or the Hardware Management Console (HMC)**.**[1] ITS controls security, configurations, and resources (capacity, processing speed, etc.) for the virtual environment. Agencies are responsible for their applications and data residing on these virtual machines. There were 709 virtual machines deployed across 12 agencies at the time this audit was conducted.

ITS implemented the North Carolina Identity Management (NCID) in 2001 to give state, local, business and citizen groups access to many state information resources through just one account. NCID was also supposed to help decrease the time users needed to complete a request for information. ITS supports the NCID application, and sets up initial organization, agency, and NCID administrator accounts. The organizations and agencies using NCID are responsible for user administration.

North Carolina General Statute 147-33.76, State Information Technology Management, stipulates the State Chief Information Officer (CIO) shall be responsible for developing and administering a comprehensive long-range plan to ensure the proper management of the State’s information technology resources. The State CIO shall set technical standards for information technology, review and approve major information technology projects, review and approve State agency information technology budget requests, establish information technology security standards, provide for the procurement of information technology resources, and develop a schedule for the replacement or modification of major systems. The State CIO is authorized to adopt rules to implement this Article.

[1] **VMWare** is an enterprise software hypervisor for servers that runs directly on the server hardware. Each virtual machine is called a guest machine. The hypervisor presents the guest operating system with a virtual operating platform and manages execution of the guest operating system.

HMC allows the system administrator to manage the software configuration and operation of partitions in a server system, and also to monitor and identify hardware problems.

The audit objectives were to determine whether: 1) information technology general controls exist for the virtual server environments and for the North Carolina Identity Management (NCID) system managed by Information Technology Services (ITS); 2) security controls exist for the virtual server environments managed by ITS; 3) prior year audit issues have been successfully resolved; and 4) NCID security configuration controls are in place.

To accomplish the audit objectives, the auditors gained an understanding of ITS' policies and procedures, interviewed key ITS administrators and other personnel, examined system configurations, tested on-line system controls, reviewed appropriate technical literature, and reviewed computer-generated reports.

The audit scope included: 1) a review of security controls for the ITS virtual server environments;
2) problem, incident and change management for NCID and virtualization; 3) ITS' responses for prior year audit findings; and 4) NCID security configuration controls. The audit fieldwork was conducted from December 10, 2013, to May 1, 2014.

As a basis for evaluating general controls, the auditors applied the guidance contained in the *North Carolina Statewide Information Security Manual* (*Statewide Security Manual*). It sets out the standards required by *North Carolina General Statute147-33.110*, which directs the State Chief Information Officer (State CIO) to establish a statewide set of standards for information technology security to maximize the functionality, security, and interoperability of the State's distributed information technology assets. The security manual sets forth the State government's basic information technology and security requirements.

Additionally, the auditors applied guidance contained in the Control Objectives for Information Technology (COBIT 5) framework issued by the Information Systems and Control Association (ISACA).[2] Per *North Carolina General Statute 143D-6*, the State Controller has directed State agencies to adopt COBIT as the information technology internal control standards for the State. COBIT is a comprehensive framework that assists enterprises in achieving their objectives for the governance and management of enterprise information and technology assets. This framework helps enterprises create optimal value from IT by maintaining a balance between realizing benefits and optimizing risk levels and resource use. COBIT enables IT to be governed and managed in a holistic manner for the entire enterprise, taking in the full end-to-end business and IT functional areas of responsibility, considering the IT-related interests of internal and external stakeholders.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate, evidence to provide a reasonable basis for our finding and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our 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] ISACA is a non-profit and independent leading global provider of knowledge, certifications, community, advocacy and education on information systems assurance and security, enterprise governance and management of IT, and IT-related risk and compliance.

FINDING #1: MANAGEMENT PROCESSES ARE INADEQUATE FOR MANAGING ITS' VIRTUAL ENVIRONMENTS AND THE NCID SYSTEM

Information Technology Services (ITS) management processes for the virtual environment and the North Carolina Identity Management Service (NCID) system are not fully developed or implemented. Improvement of management controls is needed to ensure adequate governance over the ITS managed virtual environments and the NCID system. Auditors found:

1) Lack of documentation for the virtual environments could harm operations
2) Service Level Reviews are not conducted consistently with clients
3) Changes are made to the virtual environment without documented authorization
4) Required information is not included in documentation requesting changes to systems

Lack of Documentation for the Virtual Environments Could Harm Operations

ITS has not established documented procedures to consistently perform various operations[3] for its VMWare and Advanced Interactive Executive (AIX) virtual platforms. When auditors asked for documented procedures applicable to the management of the VMWare and AIX virtual platforms, ITS indicated they did not exist. Rather, ITS relies on internal subject matter experts to determine how to perform various operations.

Failure to establish documented procedures could result in inconsistencies in the way staff apply system settings and monitor virtual operations. For example, lack of documentation could lead to inconsistent server configurations, which could potentially result in longer data processing times and a reduction in service quality. Additionally, lack of documentation could lead to inconsistent and limited monitoring which increases the risk of not detecting intrusions, which could compromise critical system data.

Three examples include:

First, ITS did not have documented procedures to create standard server baseline configurations for the AIX virtual platform. As a result, no standard configuration template exists. Therefore, baseline configurations may differ, introducing unwanted variance to operations and adversely affecting ITS' service delivery.

Second, ITS did not have documentation to show that the routine monitoring of security logs is performed. Not recording monitoring results limits the information available for ITS management to make sound decisions regarding security.

Third, ITS did not have up-to-date documentation for its "Change, Problem and Incident Management" process. ITS has not updated this documentation even though a major system upgrade occurred in November 2013 that affected how changes, problems and incidents are

[3] In the ITS virtual environment operations include the creation, modification, and removal of virtual platforms. This work includes building and securing the virtual platforms, making changes such as increasing network speed and memory, monitoring platforms and ensuring unwanted changes are identified and addressed, and removing platforms when they are no longer needed.

tracked. Failure to update key process documentation increases the risk that staff might make decisions based on outdated or incomplete information, which could lead to unstable operations.

Statewide security practices require ITS to maintain adequate documentation. The *Statewide Security Manual* requires state agencies to ensure that control system documentation is current and available for purposes such as auditing, troubleshooting and staff turnover.[4]

Service Level Reviews Are Not Conducted Consistently With Clients

ITS does not consistently hold periodic reviews of existing service level agreements with its customers. ITS was unable to provide documentation showing reviews occurred.

As a result of not holding periodic service level reviews, ITS may not receive critical feedback from customers that could be used to help improve its service. Consequently, there is increased risk that service delivery and operations could be adversely affected.

Furthermore, misunderstandings regarding expectations could occur. For example, auditors found that there are agency employees who believe ITS is responsible for the backup of their data. However, when auditors informed ITS about this, ITS indicated that its global SLA states: "Customers should ensure their backup, retention and business continuity requirements for customer owned data are clearly identified in the SLA."

ITS's global Service Level Agreement (SLA)[5] requires periodic reviews. The SLA states that periodic reviews should be held "**at a minimum on a quarterly basis** or as needed." (*Emphasis added*)

Changes Are Made To the Virtual Environment Without Documented Authorization

ITS has applied updates to Windows servers in the VMWare virtual environment without first ensuring a change request exists and the change has been authorized. When auditors asked ITS for a list of updates it had applied to the Windows servers and the associated authorizations for change, ITS could not provide this information. Furthermore, ITS staff informed the auditors that they routinely implement updates to Windows servers without first verifying management has authorized the updates.

As a result, there is an increased risk that unwanted updates could be implemented, which could lead to an unstable and unsecured operating environment. For example, by not having adequate change request documentation and formal approvals, an unauthorized change could be made in the virtual environment that could expose it to new vulnerabilities. Additionally, by lacking documentation that changes have been authorized ITS is not ensuring accountability and adequate historical logging of system changes for future troubleshooting.

Statewide security practices require proper authorizations for changes to networks and servers. The *Statewide Security Manual* requires that all changes to the Windows servers in the VMWare environment have a documented change request and are properly approved.[6]

[4] The *Statewide Security Manual*, Section 030207: Managing System Documentation

[5] The ITS Service Level Agreement includes 'Global Service Levels' which cover general areas of support and targets that are applicable to every ITS service. The SLA also provides levels of support and targets applicable to a specific service to include responsibilities of ITS and the customer.

Required Information Is Not Included In Documentation Requesting Changes to Systems

ITS documentation of completed changes to the virtual environment and to the NCID system is missing required information. Auditors reviewed a random sample of 61 out of 320 change requests completed in 2013 for the virtual environment and the NCID system and found 49% of the change requests were missing at least one of five required attributes (i.e., business justification, impact assessment, installation plan, test plan, and back out plan).

Failure to include the five required information attributes for all change requests increases the risk that ITS staff could make changes to the production environment that are not fully evaluated and could negatively affect service delivery and operations.

For example, a server configuration change that is not tested could result in a decline in performance such as processing speed, potentially adversely affecting service delivery. Without a back out plan for quickly recovering from this, service delivery could be affected for an extended period.

ITS procedures, as established in the *ITS User Guide to IT Service Management,*[7] require all five of the attributes (business justification, impact assessment, installation plan, test plan, and back out plan) to be documented in change requests.

Recommendations:

1) ITS should develop, implement, and maintain updated standard operating procedure documentation to manage the virtualization platforms.
2) ITS should conduct and document periodic service level reviews with customers.
3) ITS should ensure only system updates authorized through the change control process are applied.
4) ITS should create a quality review process to ensure change requests have all required attributes and comply with standards.

Agency Response: [*The responses below are a portion of the agency's full response which can be found in Appendix A*]

[Recommendation #1] ITS agrees. ITS is working towards introducing standard templates for policy and procedures to ensure uniformity. Once the template is approved the Virtualization platform documentation will be completed as outlined below, and ITS Internal Audit will conduct ongoing monitoring to ensure that required policies and procedures are in place and operating effectively. Responsible Person: Director, Information Technology Hosting Service, and Expected Completion Date: March 31, 2015.

[Recommendation #2] Review plans are being developed to institute regular Service Level Agreements (SLA) reviews in addition to recurring customer service reviews. Responsible

[6] The *Statewide Security Manual*, Section 030101: Configuring Networks and Configuring Domain Name Servers

[7] The *ITS User Guide to IT Service Mangement* includes guidance for active Operational Excellence Program ITIL processes within ITS Service Management, including Remedy, Incident, Problem, Change, and Release management.

Person: Director, Information Technology Support Services, and Expected Completion Date: January 31, 2015.

[Recommendation #3] ITS agrees. Recommendations for improvement were presented to the ITS Process Governance Board in December of 2013. One of those outcomes was an update to the change process so that all changes remain in a "open-completed" status until review by the process owner to determine if change process requirements were met, and if not, follow up with the requestor to ensure changes are compliant with process expectations. It is only after this review that changes will be marked as "closed." ITS will update ITSM process documentation with the migration to Remedy 8.1, or sooner, if the upgrade becomes delayed. Responsible Person: Director, Information Technology Support Services, and Expected Completion Date: March 31, 2015.

[Recommendation #4] ITS agrees. The North Carolina Identity Management follows the ITS Information Technology Infrastructure Library (ITIL) change management process, which includes the following approval steps: 1) Manager Approval, 2) Local Change manager Approval, 3) Change process owner Review, 4) ITS business customer advisory boards (BCAB), and ECAB (major change). The NCID team reviewed this process with the auditors extensively during multiple meetings and reiterated the need for completeness of the information with all team members. NCID leadership and ITS Internal Audit will ensure future compliance. Responsible Person: Manager, Information Technology Identity Management-Systems, and Expected Completion Date: Complete.

FINDING #2: SECURITY CONTROLS ARE INSUFFICIENT FOR MANAGING THE AIX VIRTUAL ENVIRONMENT

Details about security controls for the IBM Advanced Interactive Executive (AIX) virtual environment platform, due to their sensitive nature, were communicated to ITS management in a separate letter pursuant to *North Carolina General Statute 132-6.1(c).*

Agency Response: ITS response to this finding is captured in a sensitive letter pursuant to *North Carolina General Statute 132-6.1(c).*

FINDING #3: OFFICE OF THE STATE AUDITOR RECOMMENDATIONS WERE NOT FULLY IMPLEMENTED

Information Technology Services (ITS) did not fully implement recommendations to assist in managing risks to ITS operations as recommended in the July 2013 information systems audit report titled *Office of The Information Technology Services-Information Technology General Controls*. Specifically, ITS did not implement recommendations for three findings:

1) Policy requiring contractors to acknowledge understanding of the ITS policy is not enforced
2) ITS education and training policy is not adequate for key personnel
3) No monitoring of security baselines for UNIX servers

However, ITS did implement recommendations to remediate findings for programmers having the ability to make undocumented changes to the North Carolina Identity Management (NCID) application and for lack of management review of access rights for NCID administrator accounts.

Policy Requiring Contractors to Acknowledge Understanding of the ITS Policy is Not Enforced

ITS did not implement the Office of the State Auditor's recommendation to enforce ITS' policy to maintain on file a signed Office of Information Technology Service Policy Manual acknowledgement statement from all third-party contractors. Signed statements are not maintained for all contractors acknowledging that they have read and understand the policies.

The Office of the State Auditor's recommendation was based on "The Office of Information Technology Service Policy Manual," which states:

> "Managers shall give new employees and contractors adequate time to read the ITS Policy Manual and to ask any questions they might have during the employees' and contractors' first two weeks of work at ITS. At the end of the two week period, the employees and contractors will sign the ITS Policy Manual Acknowledgement Statement, acknowledging that they have been given the opportunity to read, understand and ask questions about the ITS Policy Manual."[8]

During the 2013 audit, the State Chief Security & Risk Officer indicated that ITS employees and third-party contractors have a continuing responsibility to stay current on "The Office of Information Technology Service Policy Manual," and that they are notified of revisions by the IT Policy and Programs Office or by their mangers.

In its written response to the 2013 audit, ITS responded that "an agency trainer who will begin work by mid-August will help managers consistently obtain and file signed statements of third party contractors acknowledging that they have read and understood *The Office of Information Technology Service Policy Manual*."

During the 2014 audit, ITS indicated that they had created a draft *Contractor Policy Manual* and were creating a separate policy for what contractors specifically need to know.

However, auditors were unable to obtain official copies of these documents or any signed statements of third party contractors acknowledging they have read and understood applicable ITS policies.

ITS Education and Training Policy Is Not Adequate For Key Personnel

ITS did not implement the Office of the State Auditor's recommendation to officially update the ITS Education and Training Policy to ensure system administrators and information security personnel obtain annual training pertinent to their roles and responsibilities.

The ITS Education and Training policy for employees is general in nature and does not require formal and regular training for the system administrators or the information security officer. The ITS policy states,

[8] The *Office of Information Technology Service Policy Manual*, Section 19.31: *ITS Policy Manual* Review

> "Ultimately, all ITS employees are responsible for their own development and education. Employees are expected to advance their own careers through appropriate self-education and self-improvement."[9]

This approach by ITS does not take reasonable actions to ensure the authorized and acceptable use of data, networks, and communications transiting the ITS systems or network. *The Statewide Security Manual* states agencies must clearly define security responsibilities for system administrators and "must also provide appropriate training for their system administrators."[10]

In its written response to the 2013 audit, ITS responded that "ITS has revised the ITS Education and Training Policy in order to confirm that system administrators and security personnel obtain annual training pertinent to their roles and responsibilities. The policy revision will be adopted after review and approved by senior management."

ITS provided auditors with a draft copy of the revised *ITS Education & Training Policy* during the 2014 audit. However, this policy is not official yet and no records were provided by ITS to show training had occurred.

No Monitoring Of Security Baselines For UNIX Servers

ITS did not implement the Office of the State Auditor's recommendation for monitoring of security baselines for the UNIX servers.

Details for the security related issue, due to sensitive nature, have been communicated to management in a separate letter pursuant to *North Carolina General Statute 132-6.1(c).*

***Recommendations*:**

1) ITS should fully implement the recommendations from the July 2013 Information Technology General Controls audit.
2) ITS should develop a formal process for addressing external audit findings in a timely manner. This process should promote accountability and involve ITS management to ensure adequate oversight, enforcement, and compliance.

Agency Response: [*The responses below are a portion of the agency's full response which can be found in Appendix A*]

[Recommendation #1] ITS was in a state of transition and turnover of the Internal Audit team for a number of months, greatly impacting the 2013 audit actions and causing a delay in executing some of the 2013 action items. The present Internal Audit team will coordinate the remediation timeline outlined below.

ITS has developed and implemented a policy to obtain signatures from contractors attesting that they have read the policy manual given to them. Responsible Person: Director, Human Resources Managing Partner & Manager, Information Security, and Expected Completion Date: Recommendation met.

[9] The *Office of Information Technology Service Policy Manual*, Section 2.09: Education and Training
[10] The *Statewide Security Manual*, Section 030202: Administering Systems

Additionally, the Enterprise Security and Risk Management Office have acquired a targeted information security training solution from the organization known as SANS. Targeted modules, potentially including Payment Card Industry – Decision Support System (PCI-DSS), personally identifiable information (PII), and advanced persistent threats, will be delivered to all systems administrators and security professionals at ITS through the state's learning management system. Responsible Person: Manager, Information Security, and Expected Completion Date: Training in progress for 2014-2015.

The ITS response to the finding pertaining to no monitoring of security baselines for the UNIX servers is captured in a sensitive letter pursuant to *North Carolina General Statute 132-6.1(c).*

[Recommendation #2] ITS had updated its Policy to include a formal process to address external audit. It was approved by the State Chief Information Officer (SCIO) in March 2014.

FINDING #4: NORTH CAROLINA IDENTITY MANAGEMENT (NCID) SYSTEM SECURITY CONFIGURATION CONTROLS ARE IN PLACE

Note: No Corrective Actions Are Required for this Finding

ITS implemented the North Carolina Identity Management (NCID) system to give state, local, business and citizen groups access to many state information resources through just one account. Auditors found the NCID security configuration controls examined during the audit appeared to be effective at mitigating security risks.

Segregation of Duties Between ITS and Agencies

Roles and responsibilities for controlling access to NCID exist and are clearly defined between ITS and the agencies. ITS supports the NCID application and establishes initial organization, agency and NCID administrator accounts. The individual agencies and organizations use these administrators to issue an NCID to its users. They also control access to the resources these users use.

As a result of adequate segregation of duties, the risk of unauthorized access to data and misuse of agency resources is reduced.

This approach follows the requirements of the *Statewide Security Manual* that agencies must ensure there is proper segregation of duties to reduce the risk of agency system misuse and fraud.[11]

NCID Users' Authentication Controls to System and Sensitive Data

ITS and the agencies have implemented effective security controls such as having delegated NCID administrators, encrypting sensitive NCID data, and assigning a unique NCID user id and password. These controls help ensure user information remains protected from unwanted intruders.

As a result, NCID data remains protected from unwanted exposure.

[11] The *Statewide Security Manual*, Section 080206: Separating System Development and Operations

This approach follows the requirements of the *Statewide Security Manual* including employing measures to safeguard the confidentiality, integrity, and availability of data such as encryption in transit, and/or in storage and monitoring of user credentials.[12]

NCID Directory Back-ups

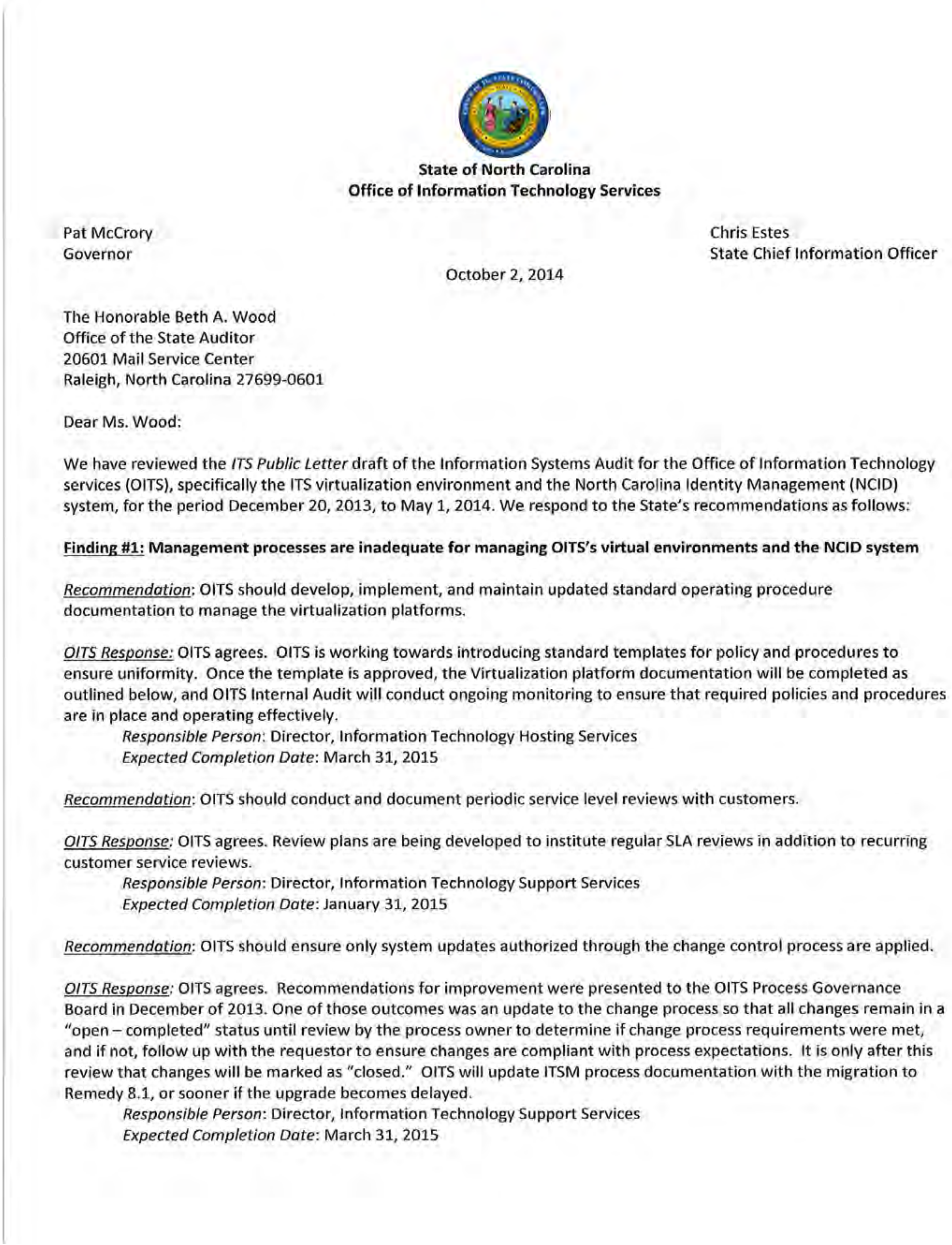
Auditors also found ITS routinely creates copies of NCID user information and properly retains it. As a result, if a disaster occurs, the integrity and availability of user information is maintained.

This approach follows the requirements of the *Statewide Security Manual* including critical data files shall be backed up, and if confidential data is backed up, the backup media shall receive appropriate security controls.[13]

[12] The *Statewide Security Manual*, Section 020101: Managing Access Control Standards

[13] The *Statewide Security Manual*, Section 030503: Managing Databases

APPENDIX A – AGENCY RESPONSE



State of North Carolina
Office of Information Technology Services

Pat McCrory
Governor

Chris Estes
State Chief Information Officer

October 2, 2014

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

Dear Ms. Wood:

We have reviewed the *ITS Public Letter* draft of the Information Systems Audit for the Office of Information Technology services (OITS), specifically the ITS virtualization environment and the North Carolina Identity Management (NCID) system, for the period December 20, 2013, to May 1, 2014. We respond to the State's recommendations as follows:

Finding #1: Management processes are inadequate for managing OITS's virtual environments and the NCID system

Recommendation: OITS should develop, implement, and maintain updated standard operating procedure documentation to manage the virtualization platforms.

OITS Response: OITS agrees. OITS is working towards introducing standard templates for policy and procedures to ensure uniformity. Once the template is approved, the Virtualization platform documentation will be completed as outlined below, and OITS Internal Audit will conduct ongoing monitoring to ensure that required policies and procedures are in place and operating effectively.

Responsible Person: Director, Information Technology Hosting Services
Expected Completion Date: March 31, 2015

Recommendation: OITS should conduct and document periodic service level reviews with customers.

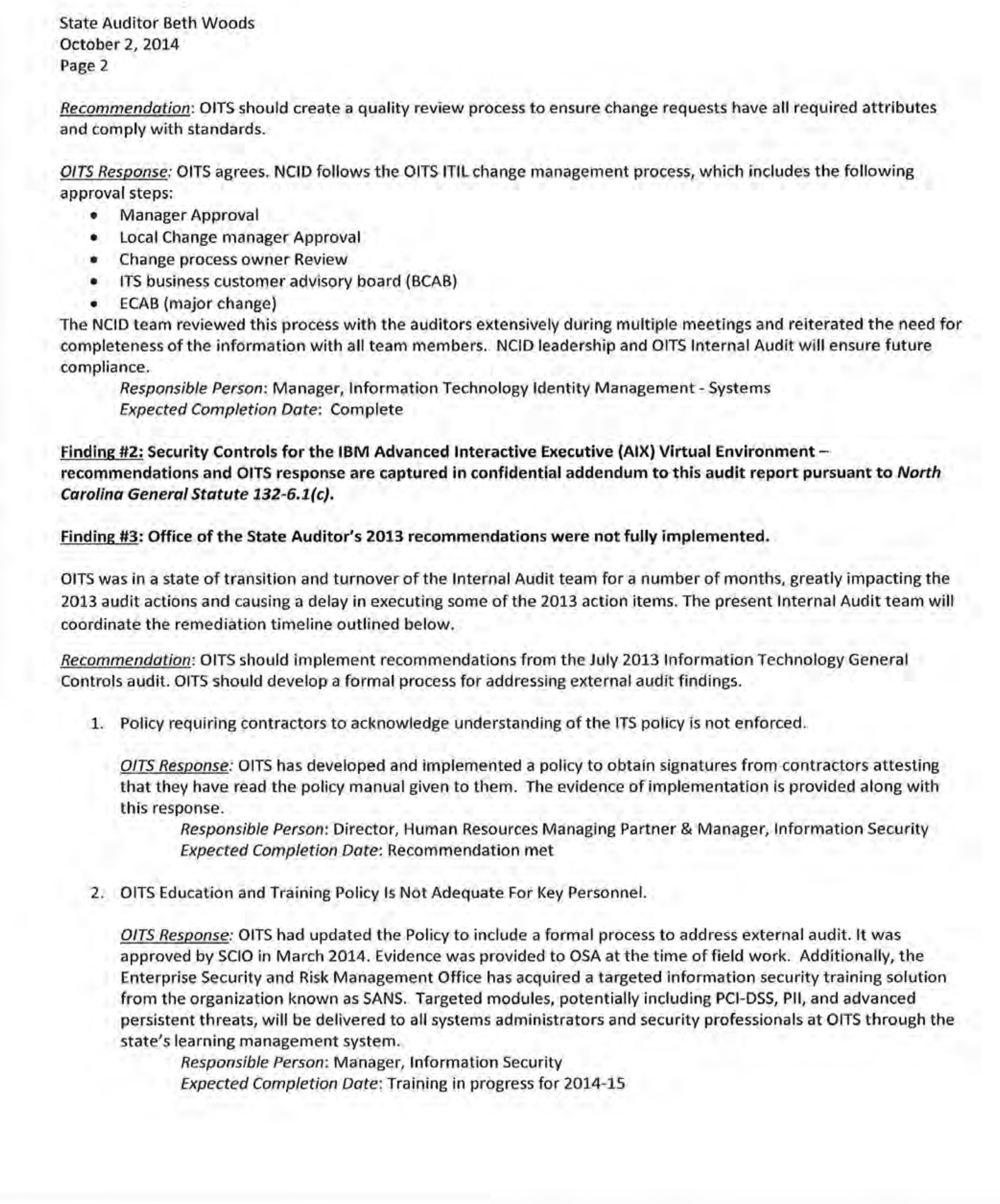
OITS Response: OITS agrees. Review plans are being developed to institute regular SLA reviews in addition to recurring customer service reviews.

Responsible Person: Director, Information Technology Support Services
Expected Completion Date: January 31, 2015

Recommendation: OITS should ensure only system updates authorized through the change control process are applied.

OITS Response: OITS agrees. Recommendations for improvement were presented to the OITS Process Governance Board in December of 2013. One of those outcomes was an update to the change process so that all changes remain in a "open – completed" status until review by the process owner to determine if change process requirements were met, and if not, follow up with the requestor to ensure changes are compliant with process expectations. It is only after this review that changes will be marked as "closed." OITS will update ITSM process documentation with the migration to Remedy 8.1, or sooner if the upgrade becomes delayed.

Responsible Person: Director, Information Technology Support Services
Expected Completion Date: March 31, 2015



State Auditor Beth Woods
October 2, 2014
Page 2

<u>Recommendation</u>: OITS should create a quality review process to ensure change requests have all required attributes and comply with standards.

<u>OITS Response</u>: OITS agrees. NCID follows the OITS ITIL change management process, which includes the following approval steps:

- Manager Approval
- Local Change manager Approval
- Change process owner Review
- ITS business customer advisory board (BCAB)
- ECAB (major change)

The NCID team reviewed this process with the auditors extensively during multiple meetings and reiterated the need for completeness of the information with all team members. NCID leadership and OITS Internal Audit will ensure future compliance.

Responsible Person: Manager, Information Technology Identity Management - Systems
Expected Completion Date: Complete

<u>Finding #2:</u> Security Controls for the IBM Advanced Interactive Executive (AIX) Virtual Environment – recommendations and OITS response are captured in confidential addendum to this audit report pursuant to *North Carolina General Statute 132-6.1(c).*

<u>Finding #3</u>: Office of the State Auditor's 2013 recommendations were not fully implemented.

OITS was in a state of transition and turnover of the Internal Audit team for a number of months, greatly impacting the 2013 audit actions and causing a delay in executing some of the 2013 action items. The present Internal Audit team will coordinate the remediation timeline outlined below.

<u>Recommendation</u>: OITS should implement recommendations from the July 2013 Information Technology General Controls audit. OITS should develop a formal process for addressing external audit findings.

1. Policy requiring contractors to acknowledge understanding of the ITS policy is not enforced.

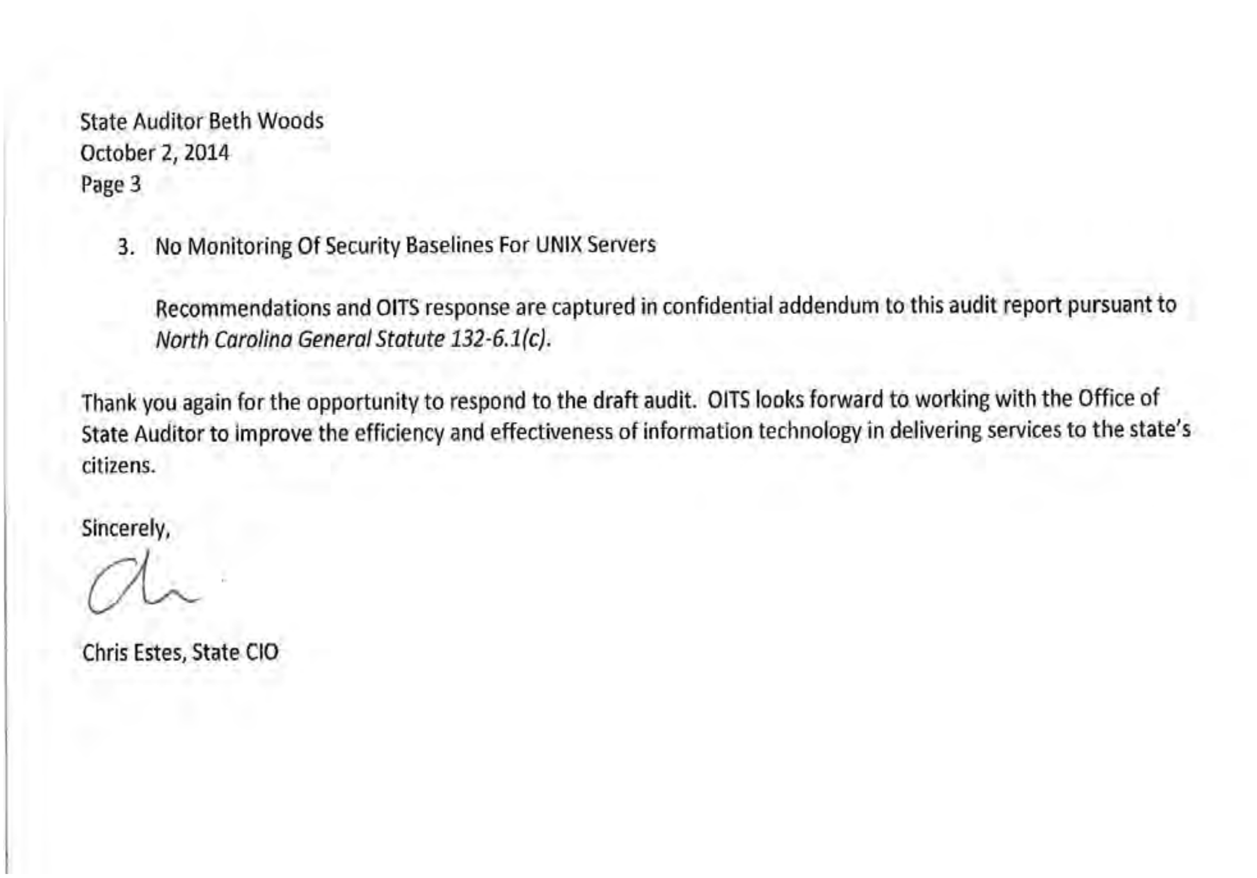
   <u>OITS Response</u>: OITS has developed and implemented a policy to obtain signatures from contractors attesting that they have read the policy manual given to them. The evidence of implementation is provided along with this response.

   Responsible Person: Director, Human Resources Managing Partner & Manager, Information Security
   Expected Completion Date: Recommendation met

2. OITS Education and Training Policy Is Not Adequate For Key Personnel.

   <u>OITS Response</u>: OITS had updated the Policy to include a formal process to address external audit. It was approved by SCIO in March 2014. Evidence was provided to OSA at the time of field work. Additionally, the Enterprise Security and Risk Management Office has acquired a targeted information security training solution from the organization known as SANS. Targeted modules, potentially including PCI-DSS, PII, and advanced persistent threats, will be delivered to all systems administrators and security professionals at OITS through the state's learning management system.

   Responsible Person: Manager, Information Security
   Expected Completion Date: Training in progress for 2014-15



State Auditor Beth Woods
October 2, 2014
Page 3

3. No Monitoring Of Security Baselines For UNIX Servers

   Recommendations and OITS response are captured in confidential addendum to this audit report pursuant to *North Carolina General Statute 132-6.1(c).*

Thank you again for the opportunity to respond to the draft audit. OITS looks forward to working with the Office of State Auditor to improve the efficiency and effectiveness of information technology in delivering services to the state's citizens.

Sincerely,

Chris Estes, State CIO

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 2100 hours at an approximate cost of $159,600.