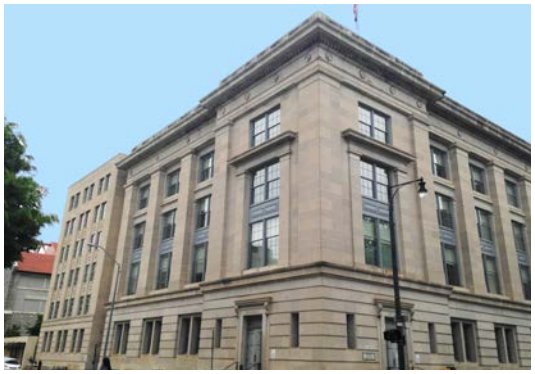
State of North Carolina

Office of the State Auditor

Beth A. Wood, CPA



Department of Information Technology

Information Technology General Controls

Information Systems Audit

July 2016

NC OSA
The Taxpayers' Watchdog

EXECUTIVE SUMMARY

PURPOSE

The objective of this information systems audit at the Department of Information Technology (DIT) was to assess the general and business process application controls that DIT maintained as an organization providing services to state agencies.

BACKGROUND

DIT operated as a single source for information technology (IT) services for executive branch agencies across the state. The department operated under the leadership of the State Chief Information Officer.

DIT's services included hosting, network, telecommunications, desktop computing, project management services, and unified communications such as email and calendaring. DIT used mainframe computers, distributed computing servers, and statewide voice, data, and video networks to provide these services.

DIT operated as an internal service fund and recovered the cost of providing these services through direct billings to state agencies.

KEY FINDINGS

- Not performing the required annual review of the standard pre-approved changes (SPACs) inventory could compromise the reliability and availability of systems.
- Not retaining testing documentation increased the risk that systems may not operate as intended.

KEY RECOMMENDATIONS

- The State CIO should immediately direct the Change Management Process Owner to initiate annual reviews of SPACs pursuant to DIT policy.
- The State CIO should evaluate policies and procedures as soon as possible, and periodically thereafter, to ensure the testing of changes is documented effectively and efficiently consistent with best practices.

SECURITY FINDINGS AND RECOMMENDATIONS

Findings regarding security, due to their sensitivity, were reported to DIT 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 27699-0600
Telephone: (919) 807-7500
Fax: (919) 807-7647
http://www.ncauditor.net

AUDITOR'S TRANSMITTAL

The Honorable Pat McCrory, Governor
Members of the North Carolina General Assembly
Keith Werner, State Chief Information Officer

Ladies and Gentlemen:

This report presents the results of our information technology controls audit at the Department of Information Technology (DIT).

We performed the audit by authority of *North Carolina General Statute 147-5A* and conducted it in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States.

The objective was to assess the general and business process application controls that DIT maintained as an organization providing services to state agencies.

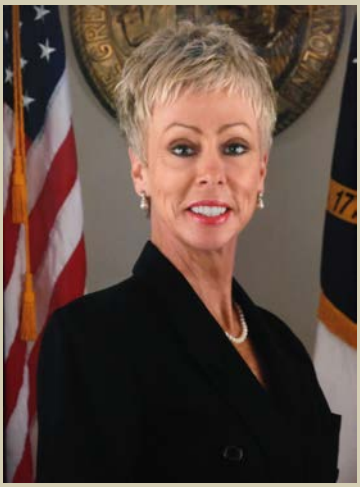
The results of our audit disclosed findings considered reportable under generally accepted government auditing standards. Findings which regard security, due to their sensitivity, were reported to DIT by separate letter in accordance with these standards and should be kept confidential as provided in *North Carolina General Statute 132-6.1(c).*

We wish to express our appreciation to the management and staff of the Department of Information Technology for the courtesy, cooperation, and assistance provided us during the audit.

Respectfully submitted,

Beth A. Wood

Beth A. Wood, CPA
State Auditor



Beth A. Wood, CPA
State Auditor

TABLE OF CONTENTS

PAGE

BACKGROUND 1

OBJECTIVE, SCOPE, AND METHODOLOGY 2

FINDINGS, RECOMMENDATIONS, AND RESPONSE

1) NOT PERFORMING THE REQUIRED ANNUAL REVIEW OF THE STANDARD PRE-APPROVED CHANGES INVENTORY COULD COMPROMISE THE RELIABILITY AND AVAILABILITY OF SYSTEMS 3
2) NOT RETAINING TESTING DOCUMENTATION INCREASED THE RISK THAT SYSTEMS MAY NOT OPERATE AS INTENDED 5

RESPONSE FROM THE DEPARTMENT OF INFORMATION TECHNOLOGY 6

ORDERING INFORMATION 8

Article 5A, Chapter 147 of the North Carolina General Statutes, gives the Auditor broad powers to examine all books, records, files, papers, documents, and financial affairs of every state agency and any organization that receives public funding. The Auditor also has the power to summon people to produce records and to answer questions under oath.


THE GREAT SEAL OF THE STATE OF NORTH CAROLINA
MAY 20. 1775
APRIL 12. 1776
ESSE QUAM VIDERI

BACKGROUND

Department of Information Technology

The Department of Information Technology (DIT) operated as a single source for information technology (IT) services for executive branch agencies across the state. The department operated under the leadership of the State Chief Information Officer. The *Current Operations and Capital Improvements Appropriations Act of 2015* (Session Law 2015-241 House Bill 97) established DIT.

DIT's services included hosting, network, telecommunications, desktop computing, project management services, and unified communications such as email and calendaring. DIT used mainframe computers, distributed computing servers, and statewide voice, data, and video networks to provide these services.

DIT operated as an internal service fund and recovered the cost of providing these services through direct billings to state agencies.

OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of this audit was to assess the general and business process application controls maintained by the Department of Information Technology (DIT) as an organization providing services to state agencies. The general control objectives were: security management, access controls, configuration management, segregation of duties, and contingency planning. The business process application control objectives were application level general controls, business process controls, and data management system controls. Examples of business processes (applications) potentially affected by DIT controls are:

- Department of Revenue – Collection of tax revenue.
- Office of the State Controller:
  - North Carolina Accounting System that supports the State's and State Agencies' financial statements and federal financial reporting.
  - BEACON payroll system for state employees.
- Department of Transportation – Vehicle Title, Driver License, and Vehicle Registration.
- Department of Health and Human Services – Eligibility determination and managing payments for programs such as Medicaid and Food Stamps.

The audit scope focused on information processing services at DIT that supported business processes at other state agencies which significantly impacted disclosures in their financial statements and their expenditure of federal financial assistance.

To accomplish our audit objectives, we gained an understanding of DIT's policies and procedures, interviewed key DIT administrators and other personnel, examined system configurations, examined system controls, reviewed appropriate technical literature, and reviewed computer-generated reports. The audit was conducted between October 2015 and February 2016.

As a basis for evaluating controls, auditors applied the guidance contained in the North Carolina Statewide Information Security Manual issued by DIT. The manual is based on industry best practices and follows the International Organization for Standardization Standard 27002 (ISO 27002) for information technology security framework. The manual also incorporates references to the National Institute of Standards and Technology (NIST) and other relevant standards. The manual sets forth the basic information technology security requirements for state government.

Additionally, auditors applied the guidance contained in the COBIT framework issued by ISACA. COBIT is a comprehensive framework that helps enterprises in achieving their objectives for the governance and management of enterprise information and technology assets.

We conducted this information systems audit in accordance with generally accepted government auditing standards (GAGAS). Those performance audit standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings 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.

FINDINGS, RECOMMENDATIONS, AND RESPONSE

1. NOT PERFORMING THE REQUIRED ANNUAL REVIEW OF THE STANDARD PRE-APPROVED CHANGES INVENTORY COULD COMPROMISE THE RELIABILITY AND AVAILABILITY OF SYSTEMS

The required annual review of the standard pre-approved changes (SPACs) inventory was not performed which increased the risk that the reliability and availability of systems could be compromised. DIT management stated that this review was not performed because the Change Management Process Owner did not have time to initiate the review. The Department of Information Technology (DIT) Change Management Policy requires that this review be performed annually.

Annual Review Not Performed

The DIT did not perform in calendar year 2015 the required annual review of the SPAC inventory.

A SPAC is a change that has been reviewed by DIT's Business Change Advisory Board to ensure it meets predefined characteristics for determining that it is a low-risk, low impact change. Examples of a SPAC include:

- Allocating additional storage space
- Planned replacement of computer workstations
- Database maintenance tasks

The DIT Change Management Policy[1] identifies the requirements for a change to be considered a SPAC include:

- Procedure has been executed many times and has not failed
- Activities (tasks) required must be well known, documented and follow a predefined path
- Required resources (staff and material) and duration must be known in advance by all affected groups
- Impact to the DIT infrastructure must be known in advance by all affected groups
- Procedure is fully documented
- Test plans and, if unsuccessful, plans for reversing the change to the previous version have been documented and tested

By pre-approving the change and allowing it to bypass the standard approval process each time it is executed, the change management team, including the Business Change Advisory Board, are able to focus on higher risk, higher impact changes that require more analysis to determine the risks associated with making the change.

[1] Change Management Policy Document OEP-20-11

Increased the Risk that the Reliability and Availability of Systems Could be Compromised

Without the annual review, SPACs which are no longer low risk, low impact, would not be identified. In fact, the last review occurred in calendar year 2014 and 23 percent of the SPACs reviewed no longer met requirements.

Furthermore, 14 additional SPACs were added since 2014, increasing the number of pre-approved change requests in 2015 to 51.

Not identifying SPACs that are no longer low-risk, low impact, increased the likelihood that DIT information processing services that supported business processes at other state agencies could be interrupted and lead to monetary losses. Systems hardware and related programs may not operate as intended and unauthorized changes may be introduced. This could impact agency financial statement disclosures and agency expenditure of federal financial assistance.

No Time to Initiate Annual Review

The Change Management Process Owner stated that she did not initiate the 2015 SPAC review because her "responsibility is providing support for daily change management, leaving little or no time to manage the review processes."

The Change Management Process Owner further stated that she does "not have authority to ensure timely response from the SPAC owners who are in various organizations throughout DIT."

Policy Requires Annual Review

The DIT Change Management Policy designates the Change Management Process Owner to oversee the change management process including the change management policy and ensuring that the policy is being followed.

The DIT Change Management Policy provides:

> "The Change Management Process Owner will initiate annual reviews of the Standard Pre-Approved Change Applications."

RECOMMENDATIONS

- The State CIO should immediately direct the Change Management Process Owner to initiate annual reviews of SPACs pursuant to DIT policy.
- The State CIO should evaluate processes as soon as possible, and periodically thereafter, to ensure that SPACs are reviewed effectively and efficiently.
- The State CIO should monitor processes at least yearly to ensure that SPACs are reviewed pursuant to DIT policy.

2. NOT RETAINING TESTING DOCUMENTATION INCREASED THE RISK THAT SYSTEMS MAY NOT OPERATE AS INTENDED

The Department of Information Technology (DIT) did not retain the results and approval of testing for changes made to systems hardware or software programs.

There were 2,031 change requests during the period of which auditors took a random sample of 60 change requests. Of those 60 changes, only 10 change requests required testing. DIT was not able to produce evidence of testing for eight (80%) of those changes.

A disciplined process for testing changes before implementation is necessary to ensure that systems operate as intended and that unauthorized changes are not introduced.

A disciplined process includes:

- retaining documentation and approval of test results,
- supervisory review and documented approvals by appropriate personnel before and after testing, and
- obtaining final user acceptance only after testing is successfully completed and reviewed by the user.

Because DIT did not retain testing documentation, there is no evidence to provide reasonable assurance that DIT followed a disciplined testing process before implementing changes.

The DIT Change Policy requires testing of changes, but does not require retention of a formal record of the test results and approval showing the test was successful. Therefore, DIT did not retain documentation of testing results in its change management process.

Best practices require that test results be recorded and maintained. Specifically, the *ISACA COBIT 5 Framework* states:

> "Execute testing continually during development, including control testing, in accordance with the defined test plan … identify, **log** and prioritize errors and issues identified during testing … ensure that an **audit trail** of test results is maintained and **record** testing outcomes and **communicate** results of testing to stakeholders in accordance with the test plan."[2] (Emphasis added)

RECOMMENDATIONS

- The State CIO should evaluate policies and procedures as soon as possible, and periodically thereafter, to ensure the testing of changes is documented effectively and efficiently consistent with best practices.
- The State CIO should monitor processes at least yearly to ensure the testing of configuration changes is documented pursuant to DIT policy and procedure.

[2] Management Practice BAI03.08 Execute Solution Testing

Information Technology

PAT McCRORY
Governor

KEITH WERNER
State Chief Information Officer

July 5, 2016

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

Dear State Auditor Wood:

We have reviewed the *ITS Public Letter* results of our information technology controls audit at the Department of Information Technology (DIT) for the period December 2015, to February 2016. We respond to the State's recommendations as follows:

Finding #1: Not Performing the Required Annual Review of the Standard Pre-Approved Changes Inventory Could Compromise the Reliability and Availability of Systems

Recommendations:
- The State CIO should immediately direct the Change Management Process Owner to initiate annual reviews of SPACs pursuant to DIT policy.
- The State CIO should evaluate processes as soon as possible, and periodically thereafter, to ensure that SPACs are reviewed effectively and efficiently.
- The State CIO should monitor processes at least yearly to ensure that SPACs are reviewed pursuant to DIT policy

DIT's Response:
DIT resolved this finding in April 2016. The Service Excellence Director, Richard Kelso, implemented a Standard Pre-Approved Change (SPAC) review policy that specifically requires SPACs to be reviewed and documented annually. This change was in place in April 2016. The point of contact is Michael Ware.

Responsible Person: Service Excellence Director

Expected Completion Date: Completed April 2016

Finding #2: Not Retaining Testing Documentation Increased the Risk That Systems May Not Operate as Intended

Nothing Compares™
State of North Carolina | Department of Information Technology
4101 Mail Service Center | Raleigh, NC 27699-4101
919 754 6100 T

Recommendation:
- The State CIO should evaluate policies and procedures as soon as possible, and periodically thereafter, to ensure the testing of changes is documented effectively and efficiently consistent with best practices.
- The State CIO should monitor processes at least yearly to ensure the testing of configuration changes is documented pursuant to DIT policy and procedure.

DIT's Response:
DIT resolved this finding was resolved in April 2016. The Service Excellence Director, Richard Kelso, implemented a new Change Management process in April 2016. This new process includes several actions that addresses this finding. The new Change Approval Board will not approve changes that do not include a test plan. Additionally, the process requires generating a separate ticket for test (if available) and production environments and correlating these tickets. In the past, one change was made for all environments, this change will track failed tests more easily and failures in the testing environment will halt the change from moving to the production environment. This also allows a way to verify testing was accomplished.

Unsuccessful changes in the production environment require a Post-production Implementation Review (PIR) or will move directly into Problem Management process via a Problem Investigation. Unsuccessful changes and their corresponding PIR or Problem Investigation will be linked to the related change.

The Work Info record (Install Results – Detail) of a CRQ will annotate if the implementation of a Change was successful or unsuccessful, thereby validating that the Test Plan was successful or unsuccessful.

DIT feels these changes meet the security manual requirement for testing and documenting the results of testing changes. The point of contact is Michael Ware.

Responsible Person: Service Excellence Director

Expected Completion Date: Completed April 2016

Sincerely,

Keith Werner
Secretary and State CIO

Nothing Compares
State of North Carolina | Department of Information Technology
3101 Mail Service Center | Raleigh, NC 27699-3101
919.754.6000 | T

ORDERING INFORMATION

COPIES OF THIS REPORT MAY BE OBTAINED BY CONTACTING:

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

NC OSA
The Taxpayers' Watchdo

This audit was conducted in 1,693 hours at an approximate cost of $176,342.