State of North Carolina

Office of The State Auditor

Beth A. Wood, CPA

Department of State Treasurer

Core Banking System Pre-Implementation

Information Systems Audit

May 2015

NC OSA
The Taxpayers' Watchdog

EXECUTIVE SUMMARY

PURPOSE

This pre-implementation audit was conducted to determine if the State's Core Banking system upgrade project has significant risks that could jeopardize a successful go-live. Any major system interruption could cause a significant loss of financial services to state agencies, universities, and other government institutions.

BACKGROUND

On July 20, 2015, the North Carolina Department of State Treasurer (Department) is scheduled to go-live with an upgraded Core Banking system. The State's Core Banking system manages the flow of moneys collected and disbursed by all State agencies, institutions, universities, and community colleges. Federal funds and taxes paid to the State flow through this system.

There are over 5,000 Core Banking system users throughout the State. During fiscal year 2012-2013, the system processed more than 5.5 million warrants (State checks), representing approximately $20 billion in payments, and executed approximately 21,600 wire transactions in the amount of $153.6 billion. The audit fieldwork was conducted from January 20, 2015, to February 27, 2015.

KEY FINDINGS

The State's Core Banking system upgrade project has significant risks that could jeopardize a successful go-live if not addressed by the Department.

- Insufficient oversight from independent entities and lack of documentation to facilitate the oversight puts successful completion of the project plan at risk.
- Struggle to execute tests and track results risks system readiness.
- Ineffective risk and issue management jeopardize identification and resolution of system development issues.
- Incomplete and undocumented data verification plan and go-live implementation plan increase risk of data integrity issues and a justifiable go-live decision.

KEY RECOMMENDATIONS

- The State Chief Information Officer's Enterprise Project Management Office should increase its involvement with the project, ensure Department status reports are completed as required, and work with the Department's Project Steering Committee to mitigate project risks.
- The Department should refine the project test execution and tracking procedures to include clear roles and responsibilities, a clear and structured approach for conducting user acceptance testing, and well-defined guidance for tracking the execution of test cases that provides an effective monitoring trail.
- The Department should ensure that project risks and issues are regularly reviewed, discussed, and updated to reflect their current status.
- The Department should develop a comprehensive plan for data validation to guide the review of data post-migration prior to go-live.
- The Department should create a formal, comprehensive, and detailed implementation plan that includes the criteria that will be used to determine the readiness of the system to go-live.

Key findings and recommendations are not 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
http://www.ncauditor.net

AUDITOR'S TRANSMITTAL

May 12, 2015

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

Ladies and Gentlemen:

We are pleased to submit the results of our information systems audit titled *Department of State Treasurer, Core Banking System Pre-Implementation.*

The audit objective was to determine if the State's Core Banking system upgrade project has significant risks that could jeopardize a successful go-live. The Department is scheduled to transition and go-live with the upgraded system on July 20, 2015.

The Office of the State Auditor initiated this audit to identify improvement opportunities prior to go-live as the risk of any major system interruption could cause a significant loss of financial services to state agencies, universities, and other government institutions.

The Department was presented in advance with the findings and recommendations. The Department reviewed a draft copy of this report, and its written comments are included in *Appendix C*.

We wish to express our appreciation to the staff of the Department 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

Article V, 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.

BACKGROUND, OBJECTIVES, SCOPE, AND METHODOLOGY

On July 20, 2015, the North Carolina Department of State Treasurer (Department) is scheduled to go-live with an upgraded Core Banking system. The State's current Core Banking system was installed in 2003.

Per *North Carolina General Statute 147 Article 6*, the Department is responsible for performing the banking operations of the State. Pursuant to that, the Department operates the State's Core Banking system. The State's Core Banking system operates as an online banking system for use by state agencies and universities to monitor their disbursements and issued warrants[1] (State checks).

The Department utilizes the Core Banking system for managing the flow of moneys collected and disbursed by all State agencies, institutions, universities, and community colleges. Additionally, local school systems disburse moneys through the system as allocated by the North Carolina Department of Public Instruction. In the course of conducting State business, the Core Banking system ensures that the State remains the beneficiary of the flow of funds through the system. An overview of the flow of state funds is provided in *Appendix A*.

There are over 5,000 users of the Core Banking system throughout the State. During fiscal year 2012-2013, more than 5.5 million warrants were processed through the Core Banking system, representing approximately $20 billion in payments. In addition, Banking Operations executed approximately 21,600 wire transactions in the amount of $153.6 billion.[2]

In January 2014, the Department entered into a contract with Mythics Consulting to perform an upgrade of the State's Core Banking system. Mythics contracted with Oracle (vendor) to provide services and continued support to the Department. The Department estimated the cost for the upgrade to be approximately $5 million.

To conduct this project no additional staff was hired by the Department. The Department's core IT upgrade project team consists of a project manager and three staff. During the project sixteen people from the banking operations division have assisted in conducting testing, however, they are not dedicated to the upgrade project 100% of the time. The vendor's upgrade project team consists of a project manager and three technical analysts.

The Department plans to go live with the Core Banking system in a new facility. The Department is scheduled to move out of their current location throughout the spring and summer. The move will consolidate Department operations into one central location.

Once the Core Banking system goes live, the State's Cash Management Control System (CMCS)[3] is scheduled to be replaced using the same vendor. The CMCS project is expected to last 11 months and cost approximately $1.7 million.[4] The go-live date of the new CMCS is dependent upon the full implementation of the Core Banking system upgrade.

---

[1] Warrant: Similar to a "check," drawn against the State Treasurer instead of against a commercial bank. Warrants are issued either by the State Controller or by a State agency under the State Controller's authority, and are presented to the State Treasurer for payment by financial institutions through the Federal Reserve System.

[2] NC Department of State Treasurer - Annual Report FY 2012-2013

[3] CMCS is an online system used for recording daily transactions that affect the budgetary accounts of the State. State appropriated funds are recorded in CMCS upon certification of the State budget and are allotted to State agencies. The system also provides for the automated transfer of funds from one State agency to another. Daily transactions are electronically transferred to the Department of State Treasurer for posting to the State Treasurer's accounts within the Core Banking system.

[4] The contract value is allocated as follows: $1.1 million for customization and implementation; and approximately $200,000 for the first three years of support and maintenance. (Source: Office of the State Controller)

The audit objective was to conduct a pre-implementation audit of the State's Core Banking system upgrade project and determine if there are significant risks that could jeopardize a successful go-live. Any major system interruption could cause a significant loss of financial services to state agencies, universities, and other government institutions.

The audit scope included project management and oversight, project documentation, integration testing, critical risk and issue management, and go-live planning. The audit scope did not include system security and user acceptance testing as this testing phase was not started during the audit.

The audit period covered January 2014 through February 2015. The audit fieldwork was conducted from January 20, 2015, to February 27, 2015.

To accomplish the audit objective, auditors reviewed the executed contract with the vendor, gained an understanding of key project processes, reviewed appropriate technical literature, and analyzed project documents such as test status reports, test cases, test results, and risk and issue logs. Auditors also interviewed Department administrators, information technology (IT) program and project managers, vendor personnel, and system testing leads. Additionally, auditors observed the project's weekly status meetings, bi-weekly steering committee meetings, and testing operations. Furthermore, auditors analyzed project records within the State's IT project management tool which keeps a record of data for all approved State IT projects. Auditors also interviewed the project management advisor assigned by the State's Enterprise Project Management Office.

The Department and the vendor developed a *Project Management Framework*[5] for the execution of the Core Banking system upgrade project which defines the high-level approach that is to be used to manage the project. The *Project Management Framework* contains plans pertaining to various topics, including: issue and risk management; communications management; and quality management. It is applicable to the responsibilities of the Department and the vendor. As a basis for evaluating the areas in the audit scope, guidance contained in the *Project Management Framework* was applied.

Additionally, guidance contained in the Control Objectives for Information Technology (COBIT 5) framework issued by ISACA[6] was also applied. COBIT 5 is a comprehensive framework that helps enterprises achieve their objectives for the governance and management of enterprise information and technology assets. As a comprehensive framework, COBIT 5 encompasses IT guidance from other standards and frameworks such as the Information Technology Infrastructure Library (ITIL), the Project Management Body of Knowledge (PMBOK), and the International Organization for Standardization (ISO).

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 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.

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

[5] BT.070 Project Management Framework – NC Department of State Treasurer Banking Upgrade Project – Version 1.1, Last Updated: May 27, 2014

[6] ISACA is a non-profit and independent global provider of knowledge, certifications, community, advocacy and education on information systems assurance and security, enterprise governance and management of IT, and objectives for the governance and management of enterprise information and technology assets.

FINDINGS AND RECOMMENDATIONS

FINDING 1: Insufficient Oversight from Independent Entities and Lack of Documentation to Facilitate the Oversight Puts Successful Completion of the Project Plan at Risk

The Core Banking system upgrade project has not received adequate oversight from independent entities since the project began, such as the State's Enterprise Project Management Office (EPMO),[7] a third-party vendor, or the Department's internal audit division.

As a result, the project has not benefited from independent, objective viewpoints to ensure it achieves its established goals and requirements, and has a successful go-live.[8]

Also, the Department lacks documentation to facilitate project oversight such as a comprehensive project quality management plan, meeting minutes, and lessons learned.

Lacking this documentation risks effective project oversight processes, clear roles and responsibilities, and effective execution of quality assurance activities.

Lack of Involvement from Independent Entities

First, the State's Enterprise Project Management Office (EPMO) has had limited involvement throughout the project because:

- The Department did not submit consistently the required monthly project reports into EPMO's project management tool.[9] During the project, EPMO allowed the Department to make a consolidated report to address missed monthly reports. As of February 27, 2015, the last project status update was done in December 2014. The Department indicated it was unable to submit monthly reports due to limitations within EPMO's project management tool (PPM).
- EPMO personnel have not attended weekly or bi-weekly project status meetings, or had any other form of involvement with project personnel.
- The EPMO project management advisor assigned to the project was hired during the project.

Second, the Department did not contract with a vendor to provide independent verification and validation services (IV&V) related to project oversight, risk management, training, or system testing. According to the Department, they did not hire an IV&V vendor as this would have exceeded the project's budget.

Third, the Department's internal audit division has not had any formal involvement with the Core Banking system upgrade project.

- The Department's internal audit could have mitigated some risk of not having sufficient involvement from EPMO or an IV&V vendor.

[7] The Enterprise Project Management Office was established within the State Chief Information Officer's office in 2004 to help improve the management of major information technology (IT) projects.

[8] When the audit began the scheduled go-live date was April 24, 2015. During the audit, the Department and the vendor agreed to extend the system's go-live date approximately two weeks and set it to May 11, 2015. By the end of audit fieldwork, the Department stated that it planned to postpone the go-live date until after July 2015.

[9] Office of Information Technology Services - Project Portfolio Management Tool, Roles and Responsibilities

- The Department indicated the lack of involvement was due to staffing resources. The Department's internal audit office has been without a director for over a year and is comprised of two auditors. According to the Department any contractual staff augmentation would have increased the cost of the project beyond the budgeted funds.
- The internal auditors noted that they did not possess the necessary skill set to perform assessments of the Core Banking system upgrade project.

IT governance and management best practices recommend appropriate involvement from independent third-parties if a project is considered critical. Specifically, the *ISACA COBIT 5 Framework* states that organizations should consider and clearly define the roles and responsibilities of other involved parties, including internal audit and compliance. Project teams should then review the results of objective third-party assessments, internal audit and quality assurance reviews. [10]

Lack of Documentation to Facilitate Oversight

The Department lacks documentation to facilitate adequate oversight of the upgrade project.

- Project quality management plan is not comprehensive.
- Meeting minutes are not consistently prepared.
- Lessons learned are not used to benefit upgrade project.

Lacking this documentation risks effective project oversight processes, clear roles and responsibilities, and effective execution of quality assurance activities. For example, without meeting minutes information pertaining to the project may not be shared timely and in a way that allows effective decision-making or review of assigned action items.

Project Quality Management Plan Is Not Comprehensive

Management of the project is not addressed in the quality management plan of the Core Banking system's *Project Management Framework*. The quality management plan focuses solely on the *product* of the project (i.e., software application) describing how it is to be monitored based on system testing.

The *Project Management Framework* indicates that a quality management plan which does not address *management* of the project risks the implementation process and work products meeting prescribed standards.

The *Project Management Framework* states that, "Project Quality Management should address **both** the **management** of the Project **and** the **product** of the Project". (Emphasis added).[11]

Meeting Minutes Are Not Consistently Prepared

Minutes were prepared for four of 68 (5%) project meetings held since the project began: 21 bi-weekly steering committee meetings and 47 weekly project status meetings. Minutes were

[10] Management Practice BAI01.12, Manage Project Resources and Work Packages; and Management Practice APO12.04, Articulate Risk

[11] Project Management Framework, Section 13: Quality Management

obtained for one steering committee meeting, one team status meeting, and two conference call meetings.

Even though the project's communications management plan indicates that meeting minutes are key outputs during the Core Banking upgrade project, the Department stated that meeting minutes are not necessary at the conclusion of each meeting.

The Department stated that conversation summaries and notes are circulated to meeting participants when necessary and that issues discussed in meetings primarily impact issues that are tracked in the Update Project Tracker Sheet. However, there is no assurance that this process is consistent or is as complete as keeping minutes after each meeting.

The Core Banking system *Project Management Framework* states that "project communications is a critical function in any project and a formal method must exist for effective communications with all project stakeholders." The framework states that of the six potential types of meetings that can occur during the project, five will have meeting minutes to serve as both a meeting input and output. Specifically, the framework states "the output from all these meetings is a set of minutes, distributed to all attendees."[12]

Lessons Learned Are Not Used to Benefit Upgrade Project

Lessons learned have not been documented during the project.

Not collecting and using lessons learned risks improvements to the current project.

The Department considers documentation of lessons learned a project closure activity and plans to document any lessons learned at the end of the project.

IT governance and management best practices recommend the gathering of lessons learned throughout a project. Specifically, the *ISACA COBIT 5 Framework* states that organizations **should regularly**, and upon completion of the project, **collect from the project participants the lessons learned and analyze the data and make recommendations for improving the current project** as well as project management method for future projects.[13] (Emphasis added)

RECOMMENDATIONS

- The State Chief Information Officer's Enterprise Project Management Office should increase its involvement with the project, ensure Department status reports are completed as required, and work with the Department's Project Steering Committee to mitigate project risks.
- The NC Council of Internal Auditing, along with the Office of State Budget and Management's Office of Internal Audit, should consider assessing the role of internal audit as it pertains to major information technology upgrade projects.
- The Department should designate someone to document meeting minutes to ensure effective communication and accurate recording of key decisions and actions items as the project gets closer to go-live.

[12] Project Management Framework, Section 12: Communications Management – Meeting Agendas, Attendees, Inputs, and Outputs

[13] Management Practice BAI01.13, Close a Project or Iteration (Phase)

- The Department should designate someone to collect and document lessons learned so improvements can be made for the current and future projects.

FINDING 2: Struggle to Execute Tests and Track Results Risks System Readiness

The Department struggled to execute planned tests and to track test results effectively.

Consequently, the progress of system testing was difficult for the Department and auditors to assess.

Struggle to Execute Planned Tests

Core Banking system integration testing was planned to begin on January 5, 2015, and last five weeks, however not all functionalities were available to be tested until January 26, 2015 (the 60% mark). The system integration testing phase was planned to be completed on February 6, 2015, however due to issues in executing planned tests it was extended an additional two weeks until February 20, 2015 (40% increase).

- System integration testing began while test cases and test procedures were still being developed. Test cases and test procedures were not finalized until the 4th week of the phase (the 80% mark).
- The direct banking function of the system was not available to be tested for the first three weeks out of the scheduled five weeks (the 60% mark) of system integration testing phase. Because the direct banking function was not available (and delays with completing testing) the system integration testing phase was extended an additional two weeks (40%). The direct banking function is what State agencies and universities access online.
- The vendor had to address unit testing[14] related issues that should have been completed prior to beginning the phase. These issues caused delays as testers would begin tests but would not be able to complete them due to flawed functionalities. During the system integration testing phase Department project personnel questioned the completeness of unit testing that was performed in 2014 by the vendor.
- Test defect documentation does not include an action plan field to contain detailed description of actions (including dates and owners) required to resolve the problem.

The contract to upgrade the system contains sections that collectively define the testing plan for the project and describe the various phases of testing to be performed.[15] However, the contract is high-level and does not provide the necessary guidance and sufficient details for an effective test tracking system. There were no details related to personnel assignments, time needed to execute system testing, and tracking of test completion.

[14] Unit testing: the software development process in which the smallest testable parts of an application, called units, are individually and independently scrutinized for proper operation.

[15] The contract mentions the timing, obligations of parties, acceptance criteria, training requirements, and the installation of the test environment, as well as the components of the testing process, such as test cases, error definition, and a traceability matrix of customizations to test cases and/or desktop guides. The contract includes the test phases of the project: Unit Testing, System Integration Testing, and User Acceptance Testing.

Project personnel indicated that there was a need to get testing more organized and have a better structure in place before beginning the next major phase of the project, user acceptance testing.

IT governance and management best practices recommend using clearly defined test instructions. Specifically, the *ISACA COBIT 5 Framework* states that organizations should create an integrated test plan, undertake all tests in accordance with the test plan, and record testing outcomes and communicate results of testing to stakeholders in accordance with the test plan.[16]

IT governance and management best practices support the Department's decision to extend system integration and user acceptance testing phases. Specifically, the *ISACA COBIT 5 Framework* states that organizations should "Undertake all tests in accordance with the test plan and practices … Repeat tests until all significant errors have been resolved."[17]

Struggle to Track Test Results

The Core Banking's system integration testing phase began before an effective test tracking system was put in place. The Department and the vendor tracked separately the progress of system integration testing using tables like the one on the next page.[18] During weekly project meetings, the Department and the vendor did not always agree with the information presented on the status of the completion of testing and re-testing. For example:

- On February 18, 2015, the Department disagreed with the vendor's test tracking which indicated that system integration testing was close to being done. Department project personnel stated there were "quite a few things to retest."
- On February 25, 2015, the Department disagreed with the vendor's test tracking analysis. Department project personnel stated "Cannot put a 'Yes' when [a test is] not done.", and "a big jump for vendor stating that testing is complete."

The table used during weekly project meetings to discuss the progress of testing did not include key performance indicators to adequately track and discuss test results such as:

- Total number of tests
- Number of executed tests
- Number of passed tests
- Number of issues (defects)
- Number of resolved issues (defects)
- Number of issues (defects) by severity level

Core Banking – Direct Banking Testing

Name of Functionality	Tested Once	Testing Completed	Issue Reported
CIT Manual Match	Y	Y	Y
CD Contract Booking	Y	Y	N
Collateral Booking	Y	N	Y
Standing Instruction Diary	Y	Y	Y
Security Management	Y	Y	Y

[16] Management Practice BAI03.08, Execute Solution Testing

[17] Management Practice BAI03.08, Execute Solution Testing

[18] *Appendix B* includes a full status report of system integration testing activity as of February 25, 2015.

Teller Entry	Y	Y	Y
Clearing exception	Y	Y	Y
BAI transaction upload	Y	Y	N
BAI recon upload	Y	Y	Y
FT Template	Y		Y
Agency Admin User Creation	Y		Y
Agency User creation	Y		N
User Account Mapping	Y		N
Rule Maintenance	Y		N
FT Initiation	Y		Y
Stop pay upload	Y		Y
Positive Pay upload	Y		Y
Image Retrieval	Y		Y
Single Positive Pay Input	Y		Y
Single Stop Pay Input	Y		Y

Source: Weekly Status Report, System Integration Testing Activity – February 25, 2015

By not being able to show and prove that all interface and functional requirements were tested, this leads to ineffective monitoring of the project's system integration testing phase risking whether the system will meet business needs. It was difficult to verify that all required tests were actually performed.

The Department acknowledged that progress tracking should be improved and indicated that it had begun taking steps to modify processes to improve the monitoring of the next testing phase, user acceptance testing.

IT governance and management best practices recommend maintaining an audit trail of test results and communicating adequately test results. Specifically, the *ISACA COBIT 5 Framework* states that organizations should "ensure that an audit trail of test results is maintained and that test results are communicated to stakeholders in accordance with the test plan."[19]

RECOMMENDATION

- The Department should refine the project test execution and tracking procedures to include clear roles and responsibilities, a clear and structured approach for conducting user acceptance testing, and well-defined guidance for tracking the execution of test cases that provides an effective monitoring trail.

[19] Management Practice BAI03.08, Execute Solution Testing

FINDING 3: Ineffective Risk and Issue Management Jeopardizes Identification and Resolution of System Development Issues

The Department and vendor have not executed effectively the project's risk and issue management strategy as project risks and issues are not identified, logged, and/or resolved effectively. Specifically, auditors found:

- The project's risk log was not used and updated.
- The project's issue list was not consistently used and updated.

Consequently, there is an increased risk of having unaddressed risks and issues that could adversely impact the quality, cost, and schedule of the system upgrade project.

The Project's Risk Log Was Not Used and Updated

> **Risk**: The possibility of an uncertain future outcome or condition that if it occurs has a positive or negative impact on a project's objectives. (Definition Source: Core Banking system project)

The risk log was initially created and reviewed when the project began but no follow-on reviews or updates were performed even though new risks to the project emerged during the year.

- As of February, 27, 2015, the last update to the risk log was on April 11, 2014.
- During weekly project status meetings, Department and vendor personnel did not open or discuss the project's risk log even though it was covered in the presentation slides and a website link to the risk log was provided for all to access.
- The Department stated that the project's issue log was used in some cases by project personnel to add risk items.

The Core Banking system *Project Management Framework* states that "risks should be entered on the risk log and categorized by type and priority, and an estimated closure date should be assigned."[20] The plan includes the following note, "a best practice is to discuss risks and the response plans in project status meetings, including executive steering committee meetings."

IT governance and management best practices recommend monitoring and controlling IT project risks. Specifically, the *ISACA COBIT 5 Framework* states that organizations should "review a project risk register of all potential project risk … Analyze the log periodically for trends and recurring problems to ensure that root causes are corrected."[21]

[20] Project Management Framework, Section 9: Issue, Problem, and Risk Management

[21] Management Practice BAI01.10, Manage Program and Project Risk

The Project's Issue Log Was Not Consistently Used and Updated

> **Issue**: An open concern or matter that is under discussion and could adversely impact the success of a project. (Definition Source: Core Banking system project)

Some executive steering committee meetings had meeting slides which indicated "No Issues" even though open issues existed at the time.

The Department acknowledged delays in updating the project's issue log and indicated that it would review the log to ensure it was current and would add uncaptured items. The project's issue log showed:

- New issues discussed by the Department and the vendor during weekly project status meetings were not added in a timely manner or prior to the next weekly meeting (e.g., roadmap for patching) and in some cases were not added at all (e.g. system issue with internet browser).
- Nine of 11 (81%) open issues had not been updated in over 90 days, regardless of their priority. The priority of these nine open issues consisted of three high priority issues, two medium priority issues, and four low priority issues. Specifically:
    - Two of 11 (18%) open issues had not been updated in over 300 days
    - Four of 11 (36%) open issues had not been updated in over 200 days
    - Three of 11 (27%) open issues had not been updated in over 90 days
- As of January 2015, one medium priority issue had received its last update on March 7, 2014. Another medium priority issue had received its last update in September 2014.
- The "remarks" section for open issues lacked details and the intended "detailed description of actions (including dates and owners) required for resolving the issue" was not consistently captured.
- The "responsibility" field for each issue only identified a group (e.g., NC DST, OSC, or Vendor) and not specific individuals in those groups.

The Core Banking system *Project Management Framework* states that the Department and vendor review the issues list jointly "every week during weekly project status review meetings."[22] The plan includes the following note: "a best practice is to discuss open issues and action items in project status meetings, including executive steering committee meetings, and to make an effort to put a "hard closure" on lingering issues and action items."

The *ISACA COBIT 5 Framework* states that organizations should "maintain and review … a risk mitigation log of all project issues and their resolution. Analyze the log periodically for trends and recurring problems to ensure that root causes are corrected."[23]

RECOMMENDATIONS

- The Department should designate someone to formally maintain the project's risk and issue logs.

[22] Project Management Framework, Section 9: Issue, Problem, and Risk Management

[23] Management Practice BAI01.10, Manage Program and Project Risk

- The Department should ensure that project risks and issues are regularly reviewed, discussed, and updated to reflect their current status.

FINDING 4: Incomplete and Undocumented Data Verification Plan and Go-Live Implementation Plan Increase Risk of Data Integrity Issues and a Justifiable Go-Live Decision

The Department lacks complete documented plans to ensure effective execution of key pre-implementation activities and proper awareness of go-live procedures and criteria.

- A complete data verification plan does not exist.
- A complete implementation plan to include go-live criteria does not exist.
- For both plans, those portions that do exist have not been documented.

Without these documents there is an increased risk that project personnel will not have adequate and sufficient guidance to complete all required data verification tasks prior to go-live and will not be aware of the necessary steps and criteria to ensure a successful project go-live.

A Complete and Documented Data Verification Plan Does Not Exist

As the State's Core Banking system nears its scheduled go-live date there is no comprehensive plan covering the specific methods for the collection, conversion and verification of system data.

- During the audit the Department stated that data collection and conversion activities were being conducted by the vendor.
- The Department's involvement in data migration activities was confined to data verification.
- The Department acknowledged the need to improve documented plans for data verification and indicated that it had begun to document these steps.

Without a detailed plan to compare the original and converted data for completeness and integrity it is difficult to identify and effectively resolve any errors found during conversion.

IT governance and management best practices recommend the establishment of a comprehensive data conversion and verification plan. Specifically, the *ISACA COBIT 5 Framework* states that organizations should:

> "**Incorporate in the data conversion plan methods for collecting, converting and verifying data to be converted. Include comparing the original and converted data for completeness and integrity.** Rehearse and test the conversion before attempting a live conversion. Co-ordinate and verify the timing and completeness of the conversion cutover so there is a smooth, continuous transition with no loss of transaction data. Plan to back up all systems and data taken at the point prior to conversion. Maintain audit trails to enable the conversion to be retraced and ensure that there is a recovery plan covering rollback of migration and fallback to previous processing should the migration fail.

> Plan retention of backup and archived data to conform to business needs and regulatory or compliance requirements."[24] (Emphasis added)

A Complete and Documented Implementation Plan to Include Go-Live Criteria Does Not Exist

The Department does not have a comprehensive implementation plan that describes the steps required for moving from the current Core Banking system into the upgraded system.

- The Department has not established a documented set of predetermined critical success criteria to base a go-live decision.
- Some aspects of the system's implementation approach are included in the contract.[25]
- Beyond the elements covered in the contract, there is no additional guidance or detailed procedures.

An implementation plan started early allows enough time for proper planning as well as for the project team, internal users, and external system users to understand go-live expectations, roles and responsibilities, and to provide comments as needed to ensure a successful go-live.

The Department stated that a formal implementation plan does not exist, but there is enough time remaining in the project to create it.

The Department also stated that it has not received guidance from the Enterprise Project Management Office (EPMO) regarding go-live planning.

IT governance and management best practices recommend the establishment of a comprehensive implementation plan that is approved by technical and business stakeholders. Specifically, the *ISACA COBIT 5 Framework* states that organizations should:

> "Create an implementation plan that reflects the broad implementation strategy, **the sequence of implementation steps, resource requirements, inter-dependencies, criteria for management acceptance of the production implementation**, installation verification requirements, transition strategy for production support, and update of business continuity plans."[26] (Emphasis added)

RECOMMENDATIONS

- The Department should obtain, evaluate and monitor the vendor plan to collect and convert system data.
- The Department should develop a comprehensive plan for data validation to guide the verification of data post-migration prior to go-live.
- The Department should create a formal, comprehensive, and detailed implementation plan that also includes the criteria that will be used to determine the readiness of the system to go-live.

[24] Management Practice BAI07.02, Plan Business Process, System and Data Conversion

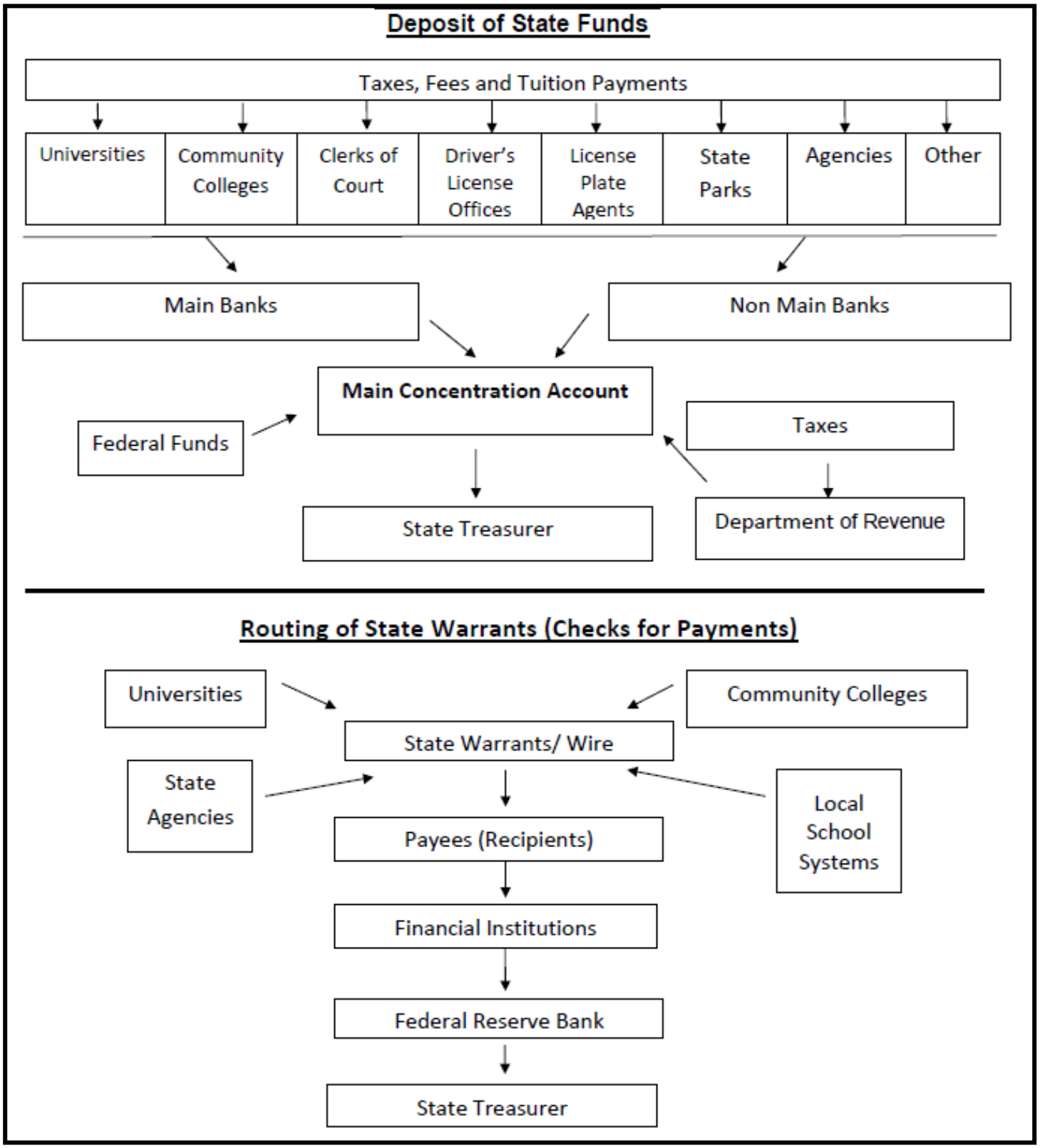
[25] The contract to replace the State's Core Banking system addresses at a high-level some elements of an implementation plan such as: data migration, training, and early vendor production support.

[26] Management Practice BAI07.01, Establish an Implementation Plan


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

APPENDICES

FLOW OF STATE FUNDS



Source: Department of State Treasurer – Banking Services Handbook

System Integration Testing Status Activity

(Source: Core Banking Weekly Project Status Report, February 25, 2015)

Core Banking – Interface Testing (testing exchanges between different computer systems)

Name of Interface	Tested Once	Testing Completed	Issue Reported
BAI File Upload	Y	Y	N
CMCS File Upload	Y	Y	N
MICR File Upload	Y	Y	N
Positive Pay	Y	Y	N
Stop Pay	Y	Y	Y
Monthly Outgoing Warrant File	Y	Y	N
Ad-hoc Warrant File	Y	Y	N
Daily warrant File	Y	Y	Y
Interest Handoff	Y	Y	N
FTP	Y	Y	N
FT – DOR	Y	Y	N

Core Banking - Functional Testing (testing system against business requirements)

Name of Functionality	Tested Once	Testing Completed	Issue Reported
FT Template	Y	Y	N
FT Bulk Authorization	Y	Y	N
FT Bulk Liquidation	Y	Y	N
FT contract Booking	Y	Y	N
Recon Capture (External entry and Internal entry)	Y	Y	N
Recon Auto Match	Y	Y	N
Recon Manual Match	Y	Y	Y
Recon statement excel upload	Y	Y	N

Core Banking – Direct Banking Testing (system used by State agencies and universities)

Name of Functionality	Tested Once	Testing Completed	Issue Reported
CIT Manual Match	Y	Y	Y
CD Contract Booking	Y	Y	N
Collateral Booking	Y	N	Y
Standing Instruction Diary	Y	Y	Y
Security Management	Y	Y	Y
Teller Entry	Y	Y	Y
Clearing exception	Y	Y	Y
BAI transaction upload	Y	Y	N
BAI recon upload	Y	Y	Y
FT Template	Y		Y
Agency Admin User Creation	Y		Y
Agency User creation	Y		N
User Account Mapping	Y		N
Rule Maintenance	Y		N
FT Initiation	Y		Y
Stop pay upload	Y		Y
Positive Pay upload	Y		Y
Image Retrieval	Y		Y
Single Positive Pay Input	Y		Y
Single Stop Pay Input	Y		Y

A list of key terms used in these tables is provided on the next page.

KEY TERMS AND DEFINITIONS USED IN TESTING ACTIVITY REPORT

Bankers Administration Institute (BAI) File – An electronic file downloaded daily from each of the main depository banks; reflects the details of the prior day's agency deposits by agency location number, and is used for reconciliation purposes.

Cash Management Control System (CMCS) – Online system used by the Office of the State Controller for recording daily transactions that affect the budgetary account of the State.

Department of Revenue (DOR) File processing- All transactions initiated by agency for tax payment is handed off as DOR handoff file. This is for all transactions initiated from FCDB using specific fund transfer module products. User manually triggers the process to generate handoff file in FLEXCUBE. Users have an option to generate the file manually with a date range prompt.

Funds Transfers (FT) – Feature offered by the Department's Banking Operations Section, allowing State agencies to issue "warrants" electronically (online) against its disbursing or STIF account.

Magnetic Ink Recognition Character (MICR) – Refers to the data encoded with magnetic ink along the bottom of a check (including State warrants). The MICR fields include serial number, ABA transit routing number, account number, and amount; also used to describe the data file received from the FRB daily.

Positive Pay System – System operated by the Department's Banking Operations Section, providing agency disbursing and STIF accounts a service similar to one offered by certain commercial banks to detect counterfeit checks. The issuing State agency provides the Department with a file of its issued State warrants daily, allowing the Department to match presented warrants (serial number, account number, date amount) with the warrants presented for payment through the FRB.

Short-term Investment Fund (STIF) Account – An account an eligible entity may open with the Department pursuant to G.S. 147-69.3(b), G.S. 116-36.1, or G.S. 147-86.11(e) (1a). The account operates similar to an interest-bearing checking account. STIF accounts are maintained on the Department's Core Banking System. Some STIF accounts are mandatory, while others are voluntary.

Stop Payment – A request by an agency to the Department's Banking Operations Section to dishonor a warrant that the agency has issued should the warrant be presented for payment; can be submitted by agencies through the online Core Banking system.

AGENCY RESPONSE

NORTH CAROLINA

OFFICE OF THE TREASURER

JANET COWELL, TREASURER

May 8, 2015

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

Dear Auditor Wood,

I appreciate your efforts as we work together to make a better and more efficient state government. We value your observations and have already taken steps to improve the documentation and processes referenced in your recommendations. We additionally feel that these recommendations from the review and our swift integration of them into our key processes and framework have reinforced a positive environment for a successful go-live status for the Core Banking system upgrade. Our responses to each of your findings are below under "Agency Response".

Finding 1: Insufficient Oversight from Independent Entities and Lack of Documentation to Facilitate the Oversight Puts Successful Completion of the Project Plan at Risk.

Recommendations:

- The State Chief Information Officer's Enterprise Project Management Office should increase its involvement with the project, ensure Department status reports are completed as required, and work with the Department's Project Steering Committee to mitigate project risks.
- The NC Council of Internal Auditing, along with the Office of State Budget and Management's Office of Internal Audit, should consider assessing the role of internal audit as it pertains to major information technology upgrade projects.
- The Department should designate someone to document meeting minutes to ensure effective communication and accurate recording of key decisions and actions items as the project gets closer to go-live.
- The Department should designate someone to collect and document lessons learned so improvements can be made for the current and future projects.

Agency Response:

The Department of State Treasurer ("Department") acknowledges that independent oversight and improved documentation reduce risk. In past projects, the Department has utilized Independent Validation and Verification ("IV & V") services—most notably, for ORBIT, a four-year, multi-phase project involving a $17 million vendor contract to replace the State's Pension Management System. Although IV & V services can be expensive, we appreciate that such oversight is valuable and will consider it in the future. Likewise, the Department has begun examining whether developing our Internal Audit personnel to provide independent oversight for this type of IT project is possible. We will continue working with the State CIO's Enterprise Project Management Office ("EPMO") to provide information on project status and financial performance through the duration of the project and will work to ensure the timeliness of our reporting.

Regarding the documentation element of the finding, we agree that more formal minute-keeping on a consistent basis would help the project team mitigate risk. This process was noted in the overall project framework and since the review has been integrated into the formal project team meeting protocol.

In order to properly document overall "Lessons Learned" throughout the project, the suggested best practice of ongoing documentation around project lessons has been integrated into the project team processes. The Department originally had planned to formally document "Lessons Learned" at the conclusion of the project. However, to ensure complete inclusion of lessons learned, the Department agrees that work can begin now to collect information from project participants and stakeholders to improve the breadth and accuracy of the final, formal document. The Department will be providing documented Lessons Learned to the EPMO, as required for Project Closeout activities, and the project team at the Office of State Controller, as they initiate their project to replace the Cash Management Control System ("CMCS").

Finding 2: Struggle to Execute Tests and Track Results Risks System Readiness.

Recommendation:

- The Department should refine the project test execution and tracking procedures to include clear roles and responsibilities, a clear and structured approach for conducting user acceptance testing, and well-defined guidance for tracking the execution of test cases that provides an effective monitoring trail.

Agency Response:

The Department agrees with and has implemented the recommendation related to test execution and tracking. The Department acknowledges deficiencies in testing execution that, if left unaddressed, would have threatened system readiness. The Department began immediate work to address issues during the period of audit fieldwork.

During the period of audit fieldwork, the project was in the System Integration Testing ("SIT") phase of the project. As recommended in the audit report, the Department assigned specific personnel to the execution of test functions to improve testing accountability. The Department also improved test progress tracking to more accurately capture issues related to system functionality and provide reliable reports on testing progress to the Project Steering Committee. Issues identified in testing were assigned to individuals for retesting to validate issue resolution and promote accountability. As a result of this approach to testing, the project team was able to successfully complete the SIT phase of the project on March 20, 2015.

The organizational lessons of the SIT phase were applied to the User Acceptance Testing (UAT) phase of the project, currently in process and scheduled for completion on May 8, 2015. Individuals have been specifically assigned to perform testing functions, and a comprehensive schedule of testing activities to simulate daily processing activities and key monthly processes has been developed. As issues are identified, they are assigned to individuals for re-testing following resolution, and progress of testing and issue resolution is reported to the Project Steering Committee to ensure continued progress.

Finding 3: Ineffective Risk and Issue Management Jeopardizes Identification and Resolution of System Development Issues.

Recommendations:

- The Department should designate someone to formally maintain the project's risk and issue logs.
- The Department should ensure that project risks and issues are regularly reviewed, discussed, and updated to reflect their current status.

Agency Response:

The Department acknowledges the opportunity to improve the documentation of risks and issues and that improved documentation leads to stronger management and resolution of risk. Furthermore, we acknowledge that the Department has not formally maintained a project risk mitigation plan and is examining ways to improve the risk assessment process.

The Department does wish to clarify that software and system issues are reviewed and discussed as part of the project review process. We are examining ways to formalize and improve the documentation process.

The additional attention to tracking the issues and risk lists, as well as, formally reporting these as part of the project team processes will increase risk and issue awareness throughout the duration of the project.

In the current project framework, the responsibility to track risks and issues is directly assigned to the project manager. That assignment includes leading meetings to discuss the project's risks and issues. The project team recorded over 300 issues during the SIT phase of the project, prioritized the importance of all issues, and monitored resolution of the most critical. During the UAT phase, the team has recorded close to 200 issues, again, prioritizing and monitoring resolution. Issue management has occurred throughout this project, at various times using the project issue log, while at others, using test tracking logs. Based on the finding recommendations additional reporting and tracking processes are being integrated into the project management framework for additional risk mitigation and process consistency.

Finding 4: Incomplete and Undocumented Data Verification Plan and Go-Live Implementation Plan Increase Risk of Data Integrity Issues and a Justifiable Go-Live Decision

Recommendations:

- The Department should obtain, evaluate and monitor the vendor plan to collect and convert system data.
- The Department should develop a comprehensive plan for data validation to guide the verification of data post-migration prior to go-live.
- The Department should create a formal, comprehensive, and detailed implementation plan that also includes the criteria that will be used to determine the readiness of the system to go-live.

The Department agrees that a comprehensive implementation plan and a comprehensive plan for data verification are critical components for project success. Furthermore, we agree that advanced preparation of these plans best mitigates risk. We are assessing ways to improve our "go-live" planning in advance of implementation. Additionally, we agree that despite the possibility of a

changing go-live environment – the project team should have documented a scenario-based go-live plan that took those items into consideration. We recognize that a scenario-based go-live plan could have eliminated some of the undocumented risk.

As noted in the audit report, the Department plans to go-live with the Core Banking System in a new facility. We believe that a successful implementation plan must be oriented to the operating environment where go-live will take place. The operating environment of the new facility was not complete during the audit field-testing. Based on prior experience and consideration, the Department judged that the go-live documentation should be postponed until the new operating environment was complete.

During the first week of June, prior to production use, the new Core Banking System will be moved from the Department's current facility to the facility where go-live will occur. From early June through mid-July, the Department will test the Core Banking System in the new environment, as well as conduct migrations of data from the current system to the new system in preparation for final implementation activities on July 20, 2015. During these six weeks, the Department will thoroughly document the steps and processes necessary to activate the new Core Banking System in the new environment and verify the system's readiness for production use.

The Department will also fully document the validation tests necessary to assess the accuracy of data migration. The Project Sponsor and other senior Department officials will have an opportunity during this time to establish the go-live criteria that aligns to the system readiness and data migration tests.

In summary for overall risk assessment, the Department provided the audit team with the information related to overall go-live risk that the project plan has never been deemed at risk of non-completion or sub-standard completion. Independent of unrelated schedule changes made to accommodate the Department's move to a new building, the entire project schedule was extended for only two weeks, less than a 5% deviation from the original project plan produced in February 2014. The total change orders made to the project, independent of the move-related changes, encompassed charges of $125,714, about an 8% deviation of the original proposed implementation cost.

The Department appreciates your examination of our Core Banking Upgrade Project and the professionalism shown by your audit staff. We look forward to continuing to apply the recommendations made in the report and successfully deliver the State's Core Banking System Upgrade.

Sincerely,

Janet Cowell

Janet Cowell

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 1189 hours at an approximate cost of $156,203.