

STATE OF NORTH CAROLINA

OFFICE OF THE STATE AUDITOR

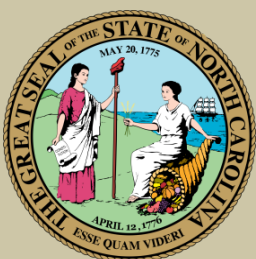
BETH A. WOOD, CPA



DEPARTMENT OF INFORMATION TECHNOLOGY

INFORMATION TECHNOLOGY GOVERNANCE AND SECURITY MANAGEMENT

INFORMATION SYSTEMS AUDIT
MARCH 2020



NCOSA
The Taxpayers' Watchdog

EXECUTIVE SUMMARY

PURPOSE

The purpose of this audit was to determine whether the Department of Information Technology (DIT) has established and implemented key objectives of information technology (IT) governance and security management in accordance with state policies and best practices.

BACKGROUND

DIT provides IT services for executive branch agencies and other government customers across North Carolina. DIT operates under the leadership of the State Chief Information Officer (State CIO), as appointed by the Governor.

By state law¹, the State CIO is responsible for ensuring that the State's IT resources are properly managed and all state IT systems and associated data are properly secured. The State CIO is also tasked with establishing statewide security standards and monitoring state agency compliance. Statewide security standards require agencies to conduct security and risk assessments to evaluate the level of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits.

KEY FINDINGS

- DIT's risk assessment process did not consider risks, other than security and availability, to ensure that risks posed to the State's IT operations and assets, and from third party service providers were identified, evaluated, mitigated, and monitored.
- DIT did not monitor contracts with third parties hosting data outside of the State's data center to ensure vendors' performance was sufficient and in compliance with contract requirements.

KEY RECOMMENDATIONS

- The State CIO should conduct a thorough risk assessment to consider risks, other than security and availability, in accordance with state policy.
- The State CIO should ensure that risks posed to the State's IT operations and assets and from service providers are identified, evaluated, mitigated, and monitored in accordance with state policy.
- The State CIO should ensure that monitoring of vendor performance and compliance with contract requirements is in accordance with state policy.
- The State CIO should ensure that vendor contract monitoring is a continuous process performed throughout the lifecycle of the contract.
- The State CIO should ensure that vendor contract renewal notifications are performed timely so that vendor performance analyses can be completed during the contract renewal process.

¹ North Carolina General Statute 143B-1322, State CIO Duties; Departmental Personnel and Administration

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
<https://www.auditor.nc.gov>

AUDITOR'S TRANSMITTAL

The Honorable Roy Cooper, Governor
Members of the North Carolina General Assembly
Tracy S. Doaks, Secretary and State Chief Information Officer

Ladies and Gentlemen:

We are pleased to submit this information systems audit report titled *Information Technology Governance and Security Management*.

The purpose of this audit was to determine whether the Department of Information Technology (DIT) has established and implemented key objectives of information technology governance and security management in accordance with state policies and best practices.

The DIT's Secretary and State Chief Information Officer reviewed a draft copy of this report. Her written comments are included starting on page 9.

This audit was conducted in accordance with Article 5A of Chapter 147 of the *North Carolina General Statutes*.

We appreciate the courtesy and cooperation received from management and the employees of the Department of Information Technology during our audit.

Respectfully submitted,

A handwritten signature in black ink that reads "Beth A. Wood".

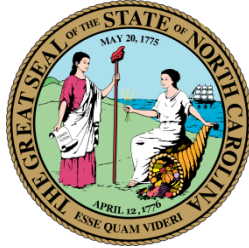
Beth A. Wood, CPA
State Auditor



Beth A. Wood, CPA
State Auditor

TABLE OF CONTENTS

	PAGE
BACKGROUND	1
OBJECTIVE, SCOPE, AND METHODOLOGY	3
RESULTS AND CONCLUSIONS	5
FINDINGS AND RECOMMENDATIONS	6
RESPONSE FROM DEPARTMENT OF INFORMATION TECHNOLOGY	9
ORDERING INFORMATION	14



BACKGROUND

Department of Information Technology

The Department of Information Technology (DIT) operates under the leadership of the Secretary and State Chief Information Officer (State CIO), as appointed by the Governor. The State CIO provides direct management over information technology (IT) operations and has statewide IT responsibilities, including technical architecture, procurement, project management, and security. A full list of the powers and duties of the department can be found in *North Carolina General Statutes Chapter 143B, Article 15*, which established DIT and directed the department to consolidate enterprise IT functions within the executive branch.

Services Provided by the Department of Information Technology

DIT is the primary IT service provider for North Carolina state government. Providing shared services across agencies allows the State to realize efficiencies and cost savings through economies of scale. DIT provides a wide range of IT services to state agencies, local governments, and educational institutions across North Carolina, including hosting, network, telecommunications, desktop computing, project management services, identity and access management, and other platforms. Public programs, such as Food and Nutrition Services, Medicaid, Work First, and Child Care are dependent on DIT services to deliver public assistance services and keep data protected.

DIT has a variety of responsibilities in addition to providing these services, ranging from procuring IT assets and services, to implementing the State's Health Information Exchange, promoting broadband infrastructure expansion across the State, and housing the State's 911 Board for emergency response.

Importance of Information Technology Governance and Security Management

By state law², the State CIO is responsible for ensuring that the State's IT resources are properly managed and all state IT systems and associated data are properly secured. The State CIO is also tasked with establishing statewide security standards and monitoring agency compliance.

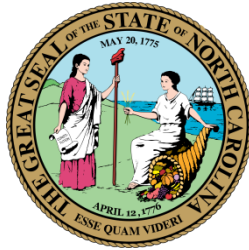
To ensure that the State's IT resources are properly managed, the State CIO must maintain IT governance consisting of leadership, organizational structures, and processes to ensure that enterprise IT supports each organization's strategies and objectives. Enterprise IT governance involves managing IT operations and IT projects to ensure alignment between these activities and the needs of the agencies within the executive branch. Proper alignment between enterprise IT and the agencies within the executive branch means:

- Agency management understands the potential and limitations of IT.
- The consolidated enterprise IT function understands the objectives and corresponding needs of the agencies within the executive branch.
- This understanding is applied and monitored throughout the executive branch via an appropriate governance structure and accountability.

To protect citizen information and state business data, IT systems, and to provide the public with confidence in state services, the State must maintain IT security and risk management as

² North Carolina General Statute 143B-1322, State CIO Duties; Departmental Personnel and Administration

a priority. Adequate security is about managing risk. Effective risk management involves conducting annual risk and security assessments to help identify, analyze, mitigate, and monitor risks associated with an agency's business, IT infrastructure, data, and physical security. Statewide security standards require agencies to conduct security and risk assessments to evaluate the level of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits.



OBJECTIVE, SCOPE, AND METHODOLOGY

We conducted this information systems 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.

The purpose of this audit was to determine whether the Department of Information Technology (DIT) has established and implemented key objectives of information technology (IT) governance and security management in accordance with state policies and best practices. In planning the audit, we considered IT control objectives as follows:

1) Governance

- Assess the use of IT in enabling the achievement of DIT's goals and objectives.
- Ensure controls are in place to identify and manage enterprise IT risk.
- Assess the value measurement process to ensure that IT costs align with business goals.
- Assess the IT strategy to ensure that IT aligns with business direction.
- Assess knowledge management to ensure proper alignment of IT knowledge and experience with governance decision making.

2) Security Management

- Assess the security governance program to ensure that IT systems are protected.
- Assess the security awareness process to ensure that resource owners, system administrators, and users are aware of security policies.
- Ensure controls are in place to periodically monitor and assess the effectiveness of security over IT systems and data.
- Ensure controls are in place to identify vulnerabilities and effectively remediate IT security weaknesses.
- Assess vendor management process to ensure that third party activities are secured, documented, and monitored.

After evaluating the IT control objectives, we identified risks in DIT's internal controls over enterprise governance and security management that expanded our audit scope related to two key objectives:

- 1) Determine whether DIT conducted a risk assessment of the State's IT operations and assets, and from third party service providers in accordance with the *North Carolina Statewide Information Security Manual*³.

³ Statewide Information Security Policies, Security Audit and Assessments, SCIO-SEC-314: Risk Assessment Policy (RA)

- 2) Determine whether DIT monitored contracts with third parties hosting data outside the State's data center in accordance with the State's *IT Procurement Policies and Procedures Manual*⁴ and state law.

We performed the following procedures to accomplish those audit objectives:

- Interviewed key DIT managers and staff.
- Reviewed policies and best practices.
- Reviewed state laws.
- Observed system and process controls related to the control objectives.
- Examined documentation supporting DIT's policies and procedures.
- Evaluated system processes and documentation against policy and state requirements.
- Identified and evaluated the risks and impacts of apparent weaknesses affecting the delivery of program services to state agencies and citizens.

Our audit scope covered the period between March 2019 through December 2019.

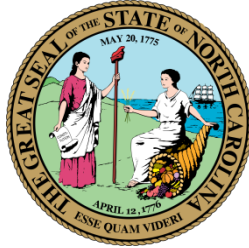
Because of the test nature and other inherent limitations of an audit, together with limitations of any system of internal and management controls, this audit would not necessarily disclose all performance weaknesses or lack of compliance.

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 the National Institute of Standards and Technology's (NIST) risk management framework for managing information security risk in state IT resources. The manual sets forth the basic IT security requirements for state government.

Additionally, auditors applied the guidance contained in the COBIT framework issued by ISACA⁵. COBIT is a comprehensive framework that helps enterprises in achieving their objectives for the governance and management of enterprise information and technology assets.

⁴ Department of Information Technology Statewide IT Procurement Office Manual, Revised July 2017, Chapter 17, Section 17.5.

⁵ 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.

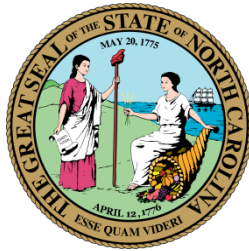


RESULTS AND CONCLUSIONS

Based on the results of audit procedures described in the *Objective, Scope, and Methodology* section of this report, we identified deficiencies in the Department of Information Technology's (DIT) controls over governance and security management that are considered reportable under *Government Auditing Standards* as follows:

- DIT's risk assessment process did not consider risks, other than security and availability, to ensure that risks posed to the State's information technology operations and assets, and from third party service providers were identified, evaluated, mitigated, and monitored.
- DIT did not monitor contracts with third parties hosting data outside of the State's data center to ensure vendors' performance was sufficient and in compliance with contract requirements.

These deficiencies are described in more detail in the *Audit and Recommendations* section of this report. Management's responses are presented in the *Response from Department of Information Technology* section of this report. We did not audit the responses, and accordingly, we express no opinion on them.



FINDINGS AND RECOMMENDATIONS

1. INADEQUATE RISK MANAGEMENT

The Department of Information Technology's (DIT) risk assessment⁶ process did not consider risks, other than security and availability, to ensure that risks posed to the State's information technology (IT) operations and assets, and from third party service providers were identified, evaluated, mitigated, and monitored.

Auditors reviewed DIT's risk assessment process related to its role as the primary service provider for North Carolina state government's IT assets and vital business functions. There was no evidence that DIT implemented activities to mitigate, manage, and monitor risks as required by State policy.

In addition, DIT did not have evidence that its risk assessment process included risks, other than security and availability, such as:

- Business risk – The cost of and/or lost revenue associated with an interruption to normal business operations.
- Organizational risk – The direct or indirect loss resulting from one or more of the following:
 - Inadequate or failed internal processes
 - Human capital management, e.g. competency, retention, development, etc.
 - External events, e.g. natural disasters, terrorism, health crises, etc.
- IT risk – The loss of an automated system, network, or other critical information technology resource that would adversely affect business processes.
- Legal risk – Parameters established by legislative mandates, federal and state regulations, policy directives, and executive orders that impact delivery of program services.
- Reputational risk – General estimation, by the public, on how state services are delivered, such as integrity, credibility, trust, customer satisfaction, image, media relations, and political involvement.

Without performing a thorough risk assessment, DIT cannot ensure that risks affecting citizen information, state business data, and IT systems are effectively managed. IT operations could be negatively impacted from the absence of a thorough risk management process due to increased risk exposure. In addition, DIT may not be able to respond appropriately in the event of a threat affecting its IT environment. Failure to perform a thorough risk assessment can also hinder DIT's ability to have a realistic, overall understanding of IT risks in the State IT enterprise.

According to DIT, its risk assessment process focused on identifying and monitoring security and availability risks. Procedures were not in place to identify, evaluate, mitigate, and monitor other types of risks.

⁶ An IT risk assessment is used to determine the possible threats faced by an organization's IT environment and infrastructure.

The *North Carolina Statewide Information Security Manual*⁷ requires DIT and agencies to identify, evaluate, mitigate, and monitor risks impacting the State's IT assets and vital business functions. It also provides that the risk assessment must include risks posed to the State's operations and assets, and from third parties. Lastly, the policy requires that each risk must have a response that minimizes the effects of the risk to a point where the risk can be controlled and managed.

RECOMMENDATION

The State Chief Information Officer should conduct a thorough risk assessment to consider risks, other than security and availability, in accordance with state policy.

The State Chief Information Officer should ensure that risks posed to the State's IT operations and assets and from service providers are identified, evaluated, mitigated, and monitored in accordance with state policy.

2. INADEQUATE VENDOR MANAGEMENT

The Department of Information Technology (DIT) did not monitor contracts with third parties hosting data outside of the State's data center to ensure vendors' performance was sufficient and in compliance with contract requirements.

Specifically, DIT did not monitor to ensure the following:

- Vendors provided acceptable quality of service, met requirements, and adhered to contract conditions.
- Vendors delivered services efficiently, effectively, securely, confidentially, reliably, and continually.

Auditors reviewed the contract monitoring process for vendors hosting data outside of the State's data center. There was no evidence that DIT monitored vendor performance or compliance with contract requirements.

The lack of monitoring for vendor performance and compliance with contract requirements increases the risk that the State paid for services that were not provided or failed to meet state needs. It also increases the risk that poorly performing vendors could obtain additional contracts.

According to DIT, vendor performance and compliance with contract requirements was not monitored because internal notifications of contract renewals were often too late to do a complete vendor analysis.

Section 09 NCAC 06B.0501 of the *North Carolina Administrative Code* requires a purchasing agency to verify that services provided comply with terms of the contract. The State's *IT*

⁷ Statewide Information Security Policies, Security Audit and Assessments, SCIO-SEC-314: Risk Assessment Policy (RA)

*Procurement Policies and Procedures Manual*⁸ provides that a primary purpose of contract administration is to ensure that the vendor performs to the best degree possible. Satisfactory performance occurs when a vendor is providing the State timely delivery of the services specified in the contract, and the vendor is complying with all terms and conditions of the contract.

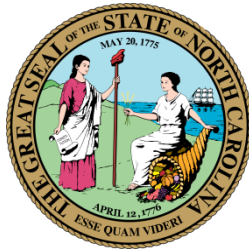
RECOMMENDATION

The State Chief Information Officer should ensure that monitoring of vendor performance and compliance with contract requirements is in accordance with state policy.

The State Chief Information Officer should ensure that vendor contract monitoring is a continuous process performed throughout the lifecycle of the contract.

The State Chief Information Officer should ensure that vendor contract renewal notifications are performed timely so that vendor performance analyses can be completed during the contract renewal process.

⁸ Department of Information Technology Statewide IT Procurement Office Manual, Revised July 2017, Chapter 17, Section 17.5.



RESPONSE FROM DEPARTMENT OF INFORMATION TECHNOLOGY



**NORTH CAROLINA DEPARTMENT OF
INFORMATION TECHNOLOGY**

Roy Cooper
Governor

Tracy S. Doaks
Secretary and State Chief Information Officer

The Honorable Beth A. Wood, CPA
State Auditor
2 S. Salisbury Street
20601 Mail Service Center
Raleigh, NC 27699-0600

Tuesday, March 10, 2020


Dear State Auditor Wood:

Thank you for the opportunity to review and comment on your draft report titled *Information Technology Governance and Security Management*.

As the primary IT service provider for North Carolina state government, we strive to ensure that the State's IT resources are properly managed in all areas including governance and security management.

Thank you very much for your time and attention to these important issues. Please do not hesitate to reach out if you have any further questions.

Sincerely,

DocuSigned by:

EEADAC04EB804A3...

Tracy S. Doaks
Secretary and State Chief Information Officer

**NORTH CAROLINA DEPARTMENT OF
INFORMATION TECHNOLOGY****Roy Cooper**
Governor**Tracy S. Doaks**
Secretary and State Chief Information Officer**N.C. Department of Information Technology response****Finding #1: Inadequate risk management**

The Department of Information Technology's (DIT) risk assessment process did not consider risks, other than security and availability, to ensure that risks posed to the State's information technology (IT) operations and assets, and from third party service providers were identified, evaluated, mitigated, and monitored.

Recommendations

The State Chief Information Officer should conduct a thorough risk assessment to consider risks, other than security and availability, in accordance with state policy.

The State Chief Information Officer should ensure that risks posed to the State's IT operations and assets and from service providers are identified, evaluated, mitigated, and monitored in accordance with state policy.

NCDIT Response

NCDIT agrees with this finding and recommendations.

As noted in the audit report, NCDIT IT risk assessment processes and activities focus on identifying and monitoring IT security and availability risks posed to the State's IT operations and assets.

While consideration of non-IT risks is not explicit in NCDIT IT risk assessment activities, the impact of a negative IT event to the State's business operations, legal mandates, reputation, and delivery of services to citizens is inherent to the IT risk management program.

To address this concern, the State Chief Risk Officer will develop a two-phased approach to remediation. Phase 1 will include conducting a review and documentation of all non-IT risk. Appropriate funding will be requested for the agency to have an independent assessment of these risks. This corrective action will be implemented by June 30, 2020. Phase 2 includes the third-

**NORTH CAROLINA DEPARTMENT OF
INFORMATION TECHNOLOGY****Roy Cooper**
Governor**Tracy S. Doaks**
Secretary and State Chief Information Officer

party assessment and development of the risk register. This corrective action will be implemented by September 1, 2020 and is dependent on budget allocations.

NCDIT also agrees that the department will optimize its processes for documenting its risk identification, evaluation, mitigation, and monitoring efforts in a more comprehensive manner. NCDIT plans to accomplish this through automation, utilizing a Governance Risk and Compliance (GRC) solution. The State Chief Risk Officer will be responsible for this action. A specific timeline for this improvement is unknown at this time due to competing priorities and funding deficiencies.

These initiatives will enhance NCDIT's current IT risk and continuous monitoring program that includes:

- A 24 hours per day, seven days per week, 365 days per year Security Operations Center (SOC) that monitors ongoing risks to State IT assets and resources. The SOC conducts continuous monitoring of that environment. All identified security risks are categorized and remediated or mitigated through various control methods.
- A Vulnerability Management Program that conducts credentialed vulnerability scans of every connected asset every seven days. The scans identify and detect any potential risks to State operations and assets. These scans are sent to the Security Incident Event Management (SIEM) tool for SOC monitoring.
- Active Threat Monitoring – a current project to deploy threat hunting agents to almost all executive branch agencies. These agents are fully deployed to all consolidated agencies and is now being deployed to optimized agencies.
- Vendor Risk Management – to comply with state statutes, DIT developed a vendor risk management program that requires all cloud hosted (service provider) procurement by state agencies to be managed through the DIT Exception Process. As part of the process, agencies must complete a Privacy Threshold Analysis (PTA) document that identifies the classification of the data to be hosted. Agencies are required¹ to have the vendor complete the following documents:
 - Vendor Readiness Assessment Report (VRAR):
<https://it.nc.gov/documents/vendor-readiness-assessment-report>

¹ <https://it.nc.gov/documents/request-proposal-rfp-form/>



**NORTH CAROLINA DEPARTMENT OF
INFORMATION TECHNOLOGY**

Roy Cooper
Governor

Tracy S. Doaks
Secretary and State Chief Information Officer

- Provide a SOC 2 Type 2 report² for the SaaS, IaaS, or PaaS³ to be used; or
- Provide an ISO 27001 certification;⁴ or;
- Provide a FedRAMP certification.⁵

If the vendors do not have a third-party attestation report, DIT will issue Conditional Authority to Operate requiring that the vendor:

- formally attest to obtaining a third-party attestation within 12 months (if the data is classified as restricted or highly restricted); and
- provide a credentialed scan of the environment; and
- provide a third-party penetration test; and
- complete the VRAR.

Finding #2: Inadequate vendor management

The Department of Information Technology (DIT) did not monitor contracts with third parties hosting data outside of the State's data center to ensure vendors' performance was sufficient and in compliance with contract requirements.

Recommendations

The State Chief Information Officer should ensure that monitoring of vendor performance and compliance with contract requirements is in accordance with state policy.

The State Chief Information Officer should ensure that vendor contract monitoring is a continuous process performed throughout the lifecycle of the contract.

² A SOC 2 Type 2 report is an internal control report from an independent third-party auditor capturing how a company safeguards customer data. Reports cover principles of security, availability, confidentiality, and privacy.

³ SaaS is software as a service. IaaS is infrastructure as a service. PaaS is platform as a service.

⁴ ISO 27001 is a specification for an information security management system (ISMS). An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organization's information risk management processes.

⁵ The Federal Risk and Authorization Management Program (FedRAMP) is a federal program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.



**NORTH CAROLINA DEPARTMENT OF
INFORMATION TECHNOLOGY**

Roy Cooper
Governor

Tracy S. Doaks
Secretary and State Chief Information Officer

The State Chief Information Officer should ensure that vendor contract renewal notifications are performed timely so that vendor performance analyses can be completed during the contract renewal process.

NCDIT Response

NCDIT agrees with the State Auditor's recommendations regarding vendor management.

Rigorous vendor management is essential to NCDIT's mission to deliver value to state agencies and safeguard taxpayer resources. NCDIT recently performed a contract life-cycle maturity assessment of its contract and vendor management functions and has taken a number of steps already to perform more proactive oversight and monitoring of vendor performance and compliance with contract requirements.

As a result of this audit, NCDIT is realigning responsibilities and broadening its vendor management functions to ensure that new requests for proposals include enforceable service level agreements and monitor contracts on a continuous basis to avoid mistakes and delays.

To accomplish this, NCDIT created a Contract and Vendor Management Director position, and implementation of the Contract Management module of the Information Technology Service Management (ITSM) tool is underway. This tool, in conjunction with the Ariba Contracts Module, will track contract start and end dates, active status, terms and conditions, related documents, renewal information and financial terms.

The Director of Contractor and Vendor Management will be responsible for this corrective action. The corrective action is expected to be completed by December 31, 2020.

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 27699-0600

Telephone: 919-807-7500
Facsimile: 919-807-7647
Internet: <https://www.auditor.nc.gov>

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.ncstateauditor.ncauditor&hl=en_US



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

For additional information contact
North Carolina Office of the State Auditor at **919-807-7666**

