State of North Carolina

Office of the State Auditor

Beth A. Wood, CPA

Department of Information Technology

Executive Branch Security Governance and Management

Information Systems Audit

May 2016

NC OSA
The Taxpayers' Watchdog

EXECUTIVE SUMMARY

PURPOSE

This audit was conducted to assess information technology (IT) security governance and management practices by the Department of Information Technology (Department) over the Executive Branch. This audit covered many key areas that are essential to ensuring proper IT security.

BACKGROUND

The services the State provides to its 10 million citizens are highly dependent upon IT systems. The State spends approximately $3 billion every two years on IT needs. The State Chief Information Officer (State CIO), the Department's Enterprise Security and Risk Management Office (ESRMO), and state agencies play a role in protecting the state's systems and data. The increasing dependency upon IT systems increases the need to protect government systems and information from continuously evolving security threats.

KEY FINDINGS

- The Department does not have all governance and management activities in place to ensure effective oversight of Executive Branch IT security
- The Department has deficiencies in its prevention, detection, and response processes to effectively protect government systems and data

KEY RECOMMENDATIONS

- The State CIO should direct ESRMO to implement in the next biennium a comprehensive and well-documented risk management framework
- The State CIO should direct ESRMO to immediately establish and post performance measures on the Department's website as required by law. The State CIO should ensure these performance measures do not jeopardize the state's security
- The State CIO should direct ESRMO to commence annual assessments, as required by law and in the next biennium, of each agency and each vendor to determine compliance with state security standards
- The State CIO should direct ESRMO to complete, and communicate to agencies, in the next biennium the Department's comprehensive strategy for agencies to conduct security assessments
- The State CIO should direct personnel to immediately address and resolve vulnerabilities detected during scans of systems within established target deadlines

MATTER FOR FURTHER CONSIDERATION

- IT security law should be modernized

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 23, 2016

The Honorable Pat McCrory, Governor
Members of the North Carolina General Assembly
Mr. Keith Werner, State Chief Information Officer
Ms. Maria Thompson, State Chief Risk Officer

Ladies and Gentlemen:

We are pleased to submit the results of our information systems audit titled *Executive Branch Security Governance and Management.*

This audit was initiated to assess information technology (IT) security governance and management practices by the Department of Information Technology (Department) over the Executive Branch.

The audit objectives were to determine: 1) whether the Department has governance and management activities in place to ensure effective oversight of Executive Branch IT security; and 2) whether the Department has effective prevention, detection, and response activities in place to protect government systems and data.

To facilitate the implementation of the recommendations made in this audit report, the State should consider an IT security "sprint." Stakeholders would come together and focus the efforts of state government with the goal of expediting the protection of state IT systems and data in 30 days.

The Department was presented the findings and recommendations of this audit in advance, and its written comments are included in *Appendix A*.

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

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

Department of Information Technology

In September 2015, the Department of Information Technology (Department) was established to consolidate the state's information technology (IT) functions, powers, duties, obligations, and services within a single cabinet-level department.[1] The Department operates under the leadership of the State Chief Information Officer (State CIO), who is appointed by the Governor.

Except as otherwise provided by law, the General Assembly, the Judicial Department, and the University of North Carolina and its constituent institutions are exempt from Article 15 of Chapter 143B of the North Carolina General Statutes that established the Department and defined the duties of the State CIO.

State CIO and ESRMO – Responsibility

By state law, the State Chief Information Officer (State CIO) is responsible for ensuring the security of all state IT systems and protecting the associated data. The State CIO is also tasked with establishing statewide security standards and monitoring state agency compliance.[2]

The Enterprise Security and Risk Management Office (ESRMO) assists the State CIO in providing oversight of IT security statewide.

According to the ESRMO website:

> "ESRMO supports the State CIO by providing leadership in the development, delivery and maintenance of a cybersecurity program that safeguards the state's IT assets against unauthorized use, disclosure, modification, damage or loss. This comprehensive statewide program encompasses information security implementation, monitoring, threat and vulnerability management, cyber incident management, and enterprise business continuity management.
>
> The ESRMO works with executive branch agencies to help them comply with legal and regulatory requirements, the statewide technical architecture, policies, industry best practices, and other requirements. We also work with state agencies, federal and local governments, citizens and private sector businesses to manage risk to support secure and sustainable information technology services to meet the needs of our citizens."

State CIO and ESRMO – Over the Years

In 2001, the General Assembly passed legislation giving the State CIO the responsibility to set enterprise-wide information security policies and standards to be followed by State agencies. ESRMO was established in 2004.

In January 2015, the State appointed its first ever State Chief Risk Officer to lead the statewide security efforts of ESRMO.

Number of ESRMO Personnel				
2011	**2012**	**2013**	**2014**	**2015**
6	5	5	5	6
Source: Department of Information Technology				

[1] North Carolina General Statute 143B - Article 15, Department of Information Technology
[2] North Carolina General Statute 143B-1376, Statewide Security Standards

Importance of Information Technology (IT) and Information Security

Each year the National Association of State Chief Information Officers (NASCIO) conducts a survey of state CIOs around the country to identify and prioritize the top policy and technology issues facing state government. According to the most recent survey, 'security & risk management' tops the list of state CIO priorities for 2016.[3]

To protect citizen information and state business data and technology systems, and to provide the public with confidence in state services, the State must maintain IT security and risk management as a priority. Adequate security is about managing risk. Security threats are becoming more sophisticated.

Modern citizen interactions are more automated and digital, with a heavy reliance on technology. The way citizens interact with government has changed. Historically, transactions were handled primarily face-to-face or over the phone.

Examples of IT Security Breaches Reported by Other States

- **Georgia** (2015) **–** The Georgia Department of Community Health reported two separate network server hacking incidents in which over 900,000 health records were exposed.
- **Virginia** (2015) – The Department of Medical Assistance Services reported a network server hacking incident in which 697,586 plan member records were exposed.
- **Oregon** (2014) – Names, birth dates, Social Security numbers, and other personally identifiable information belonging to about 1.3 million job seekers in Oregon was exposed after hackers gained access to a database containing the information at the State Employment Department.
- **Montana** (2014) – the Department of Public Health and Human Services had to notify 1.3 million current and former medical patients after a computer server was hacked.
- **Maryland** (2014) – The University of Maryland reported hackers stole records of more than 300,000 faculty, staff, and students. The information stolen included names, social security numbers, and date of birth.
- **North Dakota** (2014) – The North Dakota University System acknowledged that hackers gained access to servers and records for over 290,000 students and staffers in the state.

North Carolina Agencies – Overview

The services the State of North Carolina provides to its 10 million citizens are highly dependent upon state agency IT systems which maintain sensitive and personally identifiable information. Below is a representation of select State agencies and a brief overview of services provided and information processed.

- **NC Department of Health and Human Services:** Operates IT systems that support the delivery of health and human-related services to all North Carolinians, especially the most vulnerable citizens – children, elderly, disabled and low-income families. These IT systems maintain and process personal and sensitive data such as medical, health, and financial information for state assistance recipients and applicants.
- **NC Department of Public Instruction:** Operates IT systems that serve 115+ local public school districts, 2,500+ traditional public schools, and 148+ charter schools. These IT systems maintain and process personal and sensitive data such as

[3] NASCIO – 2016 State CIO Priorities, November 2015.

educational, transcript, and family records for Pre-K-12 students, teachers, parents, administrators, and volunteers that serve public schools.

- **NC Department of Public Safety:** Operates IT systems that support various public safety initiatives such as adult correction, juvenile justice, emergency management, and National Guard, State Highway Patrol, State Bureau of Investigation, and victim services. These IT systems maintain and process personal and sensitive data such as background investigation records of current, former, and prospective employees and contractors. These systems also maintain and process information for citizens and prisoners.

- **NC Department of Revenue:** Operates IT systems that collect revenue for the State and process over 11,000,000 tax returns a year. These IT systems maintain and process personal and sensitive data such as financial and tax information of North Carolina taxpayers and businesses.

- **NC Department of State Treasurer:** Operates IT systems that run the State Bank and administer the retirement, benefit, and health plans that serve all state employees, teachers, retirees, current and former lawmakers, university and community college personnel, and their dependents. These IT systems maintain and process personal and sensitive data such as health, retiree, beneficiary, and state investment information.

- **NC Department of Transportation:** Operates IT systems that support one of the largest highway systems in the nation, the nation's second largest state-owned ferry system, 350+ public and private airports, and serve the state's 7.3 million licensed drivers and owners of the 9 million vehicles registered in the State. These IT systems maintain and process sensitive and personal data such as financial, driver's license, permits and personal identification card information.

- **NC Office of State Human Resources:** Operates IT systems that support attracting, retaining, and developing the State government workforce. These IT systems maintain and process personal and sensitive data for 130,000 current state government employees, as well as contractors, former, and prospective state government employees.

The audit objectives were to determine: 1) whether the Department of Information Technology (Department) has governance and management processes in place to ensure effective oversight of Executive Branch information technology security; and 2) whether the Department has effective prevention, detection, and response processes in place to protect government systems and data.

The audit scope included the following areas and time periods:

- Strategic goals and performance measures (2010 to present)
- Security liaisons (2012 to present)
- Security expenditures (2000 to present)
- Agencies' compliance with security standards (2010 to present)
- Risk management (2012 to present)
- Incident management (2005 to present)
- Vulnerability management (2014 to present)
- Security assessments (2005 to present)
- Business continuity planning and disaster recovery (2011 to present)

The audit scope did not include the General Assembly, the Judicial Department, or The University of North Carolina System and its 17 campuses, as they are exempt from Article 15 of Chapter 143B of the North Carolina General Statutes that established the Department and defined the duties of the State Chief Information Officer.

The audit fieldwork was conducted from August 2015 to February 2016.

To accomplish the first audit objective, auditors interviewed the state's Chief Risk Officer and administrators from the Enterprise Security and Risk Management Office (ESRMO) and the Department. Auditors reviewed statewide IT investment and expenditure reports as well as the statewide chart of accounts. Additionally, auditors reviewed the job descriptions of select security personnel in the State to gain an understanding of their roles and responsibilities and attended relevant meetings.

To accomplish the second audit objective, auditors conducted interviews with ESRMO personnel, obtained access to technical systems, and analyzed IT security vulnerabilities and incident data. Auditors analyzed IT security reports, appropriate technical literature, and third-party reports. Auditors reviewed IT security related policies, plans in the State and existing IT security memorandums of understanding. Auditors interviewed personnel from the NC National Guard and the NC Division of Emergency Management to obtain an understanding of their role in cybersecurity in the State. Additionally, auditors interacted with the U.S. Government Accountability Office (GAO) regarding the reporting of IT security topics in government.

To obtain a complete view of select security processes and an understanding of ESRMO's oversight, auditors also engaged four major State agencies.

As a basis for evaluating the areas in scope we applied applicable North Carolina General Statutes, Executive Orders, the North Carolina Statewide Information Security Manual (2015), guidance from the Government Accountability Office (GAO), and the Control

Objectives for Information Technology (COBIT 5) framework issued by ISACA.[4] COBIT 5 is a comprehensive framework that helps enterprises achieve their objectives for the governance and management of enterprise information and technology assets. Auditors also applied guidance from the National Institute of Standards and Technology (NIST), Special Publication (SP) 800-53 Rev.4: *Security and Privacy Controls for Federal Information Systems and Organizations*, based on ESRMO's intent to transition the State's existing security standards framework to NIST. We applied NIST guidance with the understanding that compliance to SP 800-53 is not required at this time but will be after the transition.

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 Article 5A of Chapter 147 of the North Carolina General Statutes.

[4] 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

OBJECTIVE 1
CONCLUSION AND FINDINGS

Audit Objective #1

Determine whether the Department of Information Technology has governance and management activities in place to ensure effective oversight of Executive Branch information technology security.

Types of Governance and Management Activities[5]

Governance	Management
Evaluate risk management Direct risk management Monitor risk management	1. Collection of data 2. Analyzing risk 3. Maintaining a risk profile 4. Articulating risk 5. Defining a risk management action portfolio 6. Responding to risk

Audit Conclusion for Objective #1

The Department of Information Technology does not have all governance and management activities in place to ensure effective oversight of Executive Branch IT security.

Audit Findings for Objective #1

1) No Comprehensive Risk Management Framework Compromises Secure and Sustainable IT Services

2) No Performance Measures Prevent Assessment of Security Efforts

3) Inadequate IT Security Financial Reporting Limits Assessment of Investments to Security Risks

4) Undefined Roles and Responsibilities Reduce Effectiveness of Agency Security Liaisons

[5] Source: ISACA, COBIT 5 Framework.

FINDING 1: NO COMPREHENSIVE *RISK MANAGEMENT FRAMEWORK* COMPROMISES SECURE AND SUSTAINABLE IT SERVICES

The state's Enterprise Security and Risk Management Office (ESRMO) has some risk management activities in place. The implementation of a comprehensive risk management framework would enable ESRMO to prevent, detect and respond to information (IT) security risks in the State.

Governance Activities Not Comprehensively Implemented

Auditors found the State Chief Information Officer (State CIO) has not implemented key governance activities to evaluate and monitor risk management. For example, the following risk governance activities are not formally performed by executive management:

- Determining the level of IT-related risk that the State is willing to take to meet its objectives (risk appetite)
- Evaluating risk management activities to provide reasonable assurance that IT risk management practices are appropriate
- Monitoring the extent to which the risk profile is managed within the risk appetite thresholds and does not exceed it
- Monitoring key goals and metrics of risk governance and management processes against targets, analyzing the cause of any deviations, and initiating remedial actions to address the underlying causes

Risk Management Activities Not Comprehensively Implemented

Collection of Data (Risk Information)

ESRMO receives information to enable IT-related risk identification and shares relevant risk data with key security stakeholders across state agencies. However:

- ESRMO's data collection strategy is primarily from sources external to the State and does not emphasize collection from internal tools and state agencies
- Internal data that is available and collected is not fully integrated with external data

Analyzing Risk

ESRMO has not implemented key activities to consistently develop and analyze useful risk information to support risk decisions in the State. For example:

- Building and regularly updating risk scenarios
- Estimating the frequency and magnitude of loss associated with risk scenarios
- Identifying exposures that may require a risk response
- Analyzing cost-benefit of potential risk response options

Maintaining a Risk Profile

ESRMO has not implemented key activities to maintain a risk profile for the State that includes an inventory of known risk and risk attributes. For example:

- Collaborating with state agencies to identify which IT services and IT infrastructure resources are essential to the state
- Capturing all risk profile information and consolidating it into an aggregated risk profile
- Defining a set of risk indicators that allow the quick identification and monitoring of risk
- Capturing information on IT risk events for inclusion in the IT risk profile

Articulating Risk

ESRMO has not implemented key activities to consistently provide information on the current state of IT-related exposures to key stakeholders. For example:

- Providing decision makers with an understanding of worst-case and most-probable scenarios
- Reporting the current risk profile to key stakeholders
- Reviewing and mapping the results of objective third-party assessments into the State's risk profile

Defining a Risk Management Action Portfolio

ESRMO has not implemented key activities to consistently manage opportunities to reduce risk to an acceptable level as a portfolio. For example:

- Maintaining an inventory of control activities that are in place to manage risk
- Determining whether each State entity monitors risk and operates within its tolerance levels

Responding to Risk

ESRMO has implemented processes to assist State entities in responding to IT security risks and incidents. However, ESRMO has not implemented key response activities. For example:

- Categorize incidents and compare actual exposures against risk tolerance thresholds
- Examine past adverse events and communicate process improvements to appropriate decision makers

Risk Identification and Assessment Compromised

As a result of not having a comprehensive risk management framework that includes both governance and management activities, ESRMO cannot effectively manage risk to support secure and sustainable IT services to citizens and other stakeholders.

Lacking management activities to consistently identify, assess, and reduce IT security risks, it is difficult to manage the state's IT systems and data against unauthorized use, disclosure,

modification, damage or loss. ESRMO is not able to consistently provide adequate and sufficient risk management guidance to other state agencies.

Risk Management Activities Not Evaluated

ESRMO's primary focus over the years has been on responding to risks and incidents, and the State CIO has not ensured that ESRMO's risk management program is comprehensive.

Prior to 2015, ESRMO was structured in a way in which it had dual roles and limited resources. Specifically, ESRMO personnel were responsible for security in the State as well as within the Office of Information Technology Services (OITS).[6] As a result, the priorities of ESRMO personnel tended to align more with OITS. Only two out five ESRMO employees were assigned to work on state agency risk management activities.

In January 2015, the State CIO's office hired its first Chief Risk Officer to oversee ESRMO. During the audit, the organizational structure of ESRMO was changed to eliminate its dual role and focus solely on statewide issues.

Best Practices Suggest an Integrated Governance and Risk Management Framework

Information technology governance and management best practices from ISACA and the National Institute of Standards and Technology (NIST) state that a comprehensive risk management strategy consists of key activities that are integrated with one another. At a high-level, a risk management program should contain the following types of governance and management activities:

Governance Activities
Evaluate risk management
Direct risk management
Monitor risk management

Management Activities
Collection of data
Analyzing risk
Maintaining a risk profile
Articulating risk
Defining a risk management action portfolio
Responding to risk

The *ISACA COBIT 5 Framework* provides that organizations should establish governance processes to direct, evaluate, and monitor risk management activities to ensure risk to the enterprise is identified and managed.[7] The *Framework* states that organizations should establish management processes around six key risk management activities to continually identify, assess and reduce IT-related risk within levels of tolerance set by enterprise executive management.[8]

The *NIST Security and Privacy Controls Framework* states:

> "An organization-wide risk management strategy includes, for example, an unambiguous expression of the risk tolerance for the organization, acceptable risk assessment methodologies, risk mitigation strategies, a process for consistently evaluating risk across the organization with respect to the organization's risk tolerance, and approaches for monitoring risk over time."[9]

[6] In September 2015, the Office of the State CIO and the Office of Information Technology Services were combined to form the Department of Information Technology.
[7] Governance Practice EDM03, Ensure Risk Optimization.
[8] Management Practice APO12, Manage Risk.
[9] NIST Special Publication 800-53r4, PM-9 Risk Management Strategy.

RECOMMENDATIONS

The State CIO should direct ESRMO to implement in the next biennium a comprehensive and well-documented risk management framework.

The State CIO should periodically evaluate the risk management framework to ensure its design is effective and efficient to achieve its purpose, including the positioning of ESRMO in the Department of Information Technology's organizational structure.

The State CIO should regularly monitor key risk management activities to determine that they are functioning as designed, including the assignment of ESRMO resources to effectively carry out key statewide risk management activities.

FINDING 2: NO *PERFORMANCE MEASURES* PREVENT ASSESSMENT OF SECURITY EFFORTS

Performance Measures a Work-In-Progress

During the audit, the State's Chief Risk Officer stated that development of key performance indicators (KPIs) had begun and on September 1, 2015, provided a draft document of these KPIs. These include:

- Percentage of incidents detected by internal controls
- Percentage of annual policy reviews accomplished
- Mean-Time to incident recovery
- Mean-Time to mitigate vulnerabilities
- Number of end users receiving appropriate training
- Number of security personnel achieving certification

As of February 29, 2016, the Department of Information Technology (Department) had not posted performance measures on its website for each function performed by the Department and the State Chief Information Officer (State CIO) as required by law.

Performance Measures Critical

Without performance measures, ESRMO cannot consistently measure and report whether it is effectively achieving its mission to support secure and sustainable IT services.

Particularly, the Enterprise Security and Risk Management Office (ESRMO) does not have performance measures to assess its security activities. There is no evidence-based way to know whether ESRMO is exceeding expectations, meeting expectations, or falling short of expectations for the services it provides, such as:

- Security Consulting
- Threat Management
- Incident Response
- Business Continuity and Disaster Recovery
- Cybersecurity Training and Awareness

Without ESRMO performance measures that align to the Biennial State IT Plan for 2015-2017, it is difficult for the State CIO to effectively monitor key plan goals and objectives particularly "'modernizing and securing IT systems."[10]

Performance Measures Not a High Priority

When asked why ESRMO had not established performance measures since 2010, the State's Chief Risk Officer stated that these had not been set because this was not a high priority compared to other initiatives given their environment of limited resources.

Legislation and Best Practices Require Performance Measures

Legislation that created the Department in 2015 mandated the State CIO establish and post on its website specific, quantifiable performance measures on or before January 1, 2016.

> "On or before January 1, 2016, the State Chief Information Officer shall establish specific, quantifiable performance measures for each function performed by the Department of Information Technology and the State Chief Information Officer. These performance measures shall be posted on the Department of Information Technology Web site and, at a minimum, shall be updated on a monthly basis. Any plans shall include mitigation strategies to resolve any failure to meet established performance measures." [11]

Best practices require management to establish goals and measurable objectives for government programs.

The Government Accountability Office (GAO) states:[12]

> "Management defines objectives in measureable terms so that performance toward achieving those objectives can be assessed."

ISACA recommends that organizations define performance targets.[13]

The National Institute of Standards and Technology (NIST) in its *Security and Privacy Controls* framework that ESRMO intends to transition to states that organizations should:

> "... develop, monitor, and report on the results of information security measures of performance"[14]

RECOMMENDATIONS

The State CIO should direct ESRMO to immediately establish and post performance measures on the Department of Information Technology's website as required by law. The State CIO should ensure these performance measures do not jeopardize the state's security.

The State CIO should now and periodically evaluate the performance measures to ensure that they are linked to Department strategic goals, key initiatives, and core services pertaining to security and are outcome based.

The State CIO should now and periodically monitor performance measures to determine that they are up-to-date and are used by ESRMO in decision making.

[10] NC Biennial State IT Plan (2015-2017).
[11] Session Law 2015-241, Section 7.11.(A), Information Technology Performance Measures.
[12] GAO, Standards for Internal Control, September 2014.
[13] Management Practice, MEA01.02, Set Performance and Conformance Targets.
[14] NIST Special Publication 800-53r4, PM-6 Information Security Measures Of Performance.

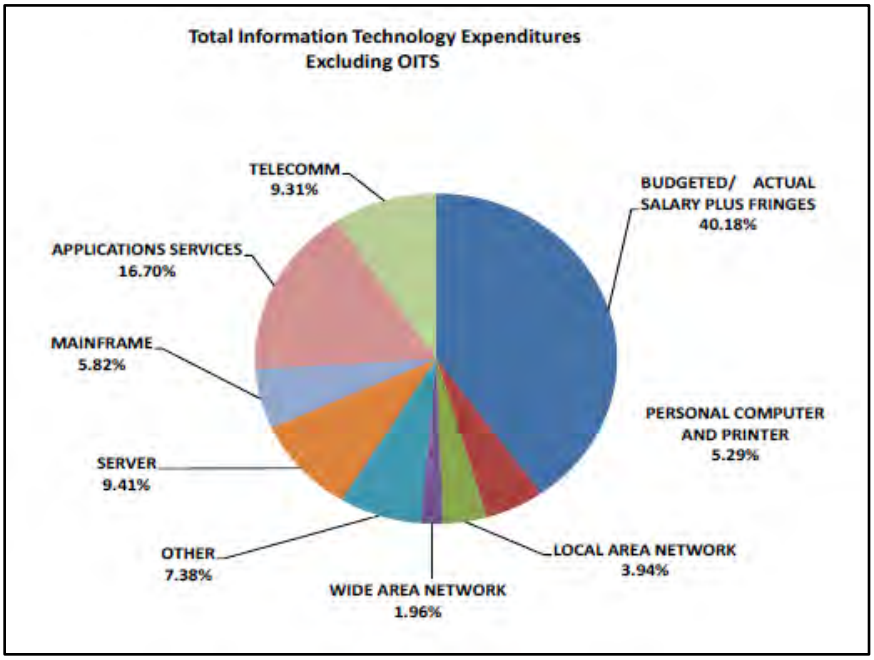
FINDING 3: INADEQUATE IT SECURITY *FINANCIAL REPORTING* LIMITS ASSESSMENT OF INVESTMENTS TO SECURITY RISKS

No Discrete View of Security Expenditure

The State's IT Expenditure Report (State IT Report) does not include a discrete view of information technology (IT) security investments and expenditures. Since 1999, law has required financial reporting and accountability to the Governor and the General Assembly coordinated by the Department of Information Technology with the Office of State Budget and Management (OSBM) and the Office of the State Controller (OSC).[15]

The State IT Report includes an overview of nine different IT categories and describes that IT security is grouped into a category called 'Other'. Four of the nine IT categories (44%) represent a lower percentage of IT expenditures than the 'Other' category.

The State's 2015 IT Expenditure Report includes the chart below that shows how the total IT expenditures ($1.325 billion) for fiscal year 2015 were distributed across the nine categories.[16]



Source: NC IT Expenditures Report for the Period Ended June 30, 2015
Note: The report's chart does not include the IT expenditures for the Department of IT totaling nearly $204 million during the same period.

In 2013, the Department of Information Technology created and set up separate accounts in the statewide chart of accounts to capture two types of IT security expenditures statewide:[17]

- IT security software
- IT security equipment

[15] NC General Statute § 143B-1335, *Financial reporting and accountability for information technology investments and expenditures.*
[16] http://www.ncosc.net/financial/ITReport_06302015.pdf.
[17] The accounts were created through the Office of the State Controller.

Since the creation of these accounts, security expenditures continue to be presented in the Other' category, rather than separately, in the State IT Report.

Statewide Assessment of Security Investment to Security Threat Limited

Without the separate presentation of IT security expenditures, State decision makers do not know the actual amount of IT security investment and expenditures throughout state government and may lack information to make well informed budget and funding decisions for IT security.

A lack of transparency and attention to IT security expenditures increases the risk of insufficient funding to operations that help protect State government systems and data.

In 2014, the National Association of State Chief Information Officers (NASCIO) and Deloitte conducted a national cybersecurity study that asked state Chief Information Security Officers about their cybersecurity concerns.[18]

Their study found "… insufficient funding, sophisticated threats, and shortage of skilled talent threaten security and put state governments at risk."[19] Survey results showed lack of sufficient funding continues to be the #1 barrier to effective cybersecurity since 2010. Survey participants indicated that senior executive commitment is there, but funding is still insufficient.

Evaluation of State IT Report Not Made

The State CIO with OSC and OSBM has not continuously evaluated the State IT Report to determine whether there is a need or opportunity to improve its structure and presentation.

Law that mandates annual financial reporting and accountability for IT investments and expenditures states:

> **"The Department, along with the Office of State Budget and Management and the Office of the State Controller, shall develop** processes for budgeting and accounting of expenditures for information technology operations, services, projects, infrastructure, and assets for State agencies... Annual reports regarding information technology shall be **coordinated by the Department with the Office of State Budget and Management and the Office of the State Controller …**"[20] (Emphasis added)

Best practices recommend continuous review of communication and reporting. Specifically, the *ISACA COBIT 5 Framework* states that organizations should:

> "Continually examine and make judgement on the current and future requirements for stakeholder communication and reporting. Identify requirements for reporting on information security to stakeholders (e.g., what information is required, when it is required, how it is presented)...**Prioritize reporting on information security issues to stakeholders**."[21] (Emphasis added)

[18] Since 2010, Deloitte and NASCIO have conducted biennial surveys of the state government enterprise CISOs to take a pulse of cybersecurity issues.
[19] http://www.nascio.org/Publications/ArtMID/485/ArticleID/85/2014-Deloitte-NASCIO-Cybersecurity-Study-State-governments-at-risk-Time-to-Move-Forward.
[20] NC General Statute § 143B-1335, Financial reporting and accountability for information technology investments and expenditures.
[21] Governance Practice EDM05, Ensure Stakeholder Transparency.

Law and Best Practices Target Reporting on Security

Prior to 2015, state law defined IT as including "security goods and services". Specifically, general statutes described:

> "Information technology" means electronic data processing goods and services, telecommunications goods and services, **security goods and services**, microprocessors, software, information processing, office systems, any services related to the foregoing, and consulting or other services for design or redesign of information technology supporting business processes."[22] (Emphasis added)

Best practices recommend accountability by reporting all IT-related costs and investments, and prioritizing reporting on IT security. Specifically, the *ISACA COBIT 5 Framework* states:

> "Establish and maintain a method to account for all IT-related costs, investments *and depreciation as an integral part of the enterprise financial systems and chart of accounts to manage the investments and costs of IT."*[23] (Emphasis added)

> "Prioritize reporting on information security issues to stakeholders*."*[24]

RECOMMENDATIONS

The State CIO should direct ESRMO to develop processes with the Office of State Controller and the Office of State Budget and Management to discretely present IT security investments and expenditures in the 2016 State IT Expenditures Report.

The State CIO should periodically evaluate the effectiveness of the State IT Expenditure Report by consultation with the Governor and General Assembly members.

The State CIO should monitor the process to prepare the State IT Expenditure Report to ensure process is functioning as designed.

FINDING 4: UNDEFINED *ROLES AND RESPONSIBILITIES* REDUCE EFFECTIVENESS OF AGENCY SECURITY LIAISONS

Roles and Responsibilities Not Established

Pursuant to State law, agencies have designated a security liaison to coordinate with the State Chief Information Officer (State CIO).[25] However, roles and responsibilities for liaisons have not been established, agreed upon, and communicated to agencies.

There is a lack of consistency in the job descriptions for liaisons at the five different agencies that were reviewed as part of this audit.[26]

[22] NC General Statute 147-33.81, Definitions. [Note: This general statute was repealed by Session Law 2015-241]
[23] Management Practice APO06, Manage Budget and Costs.
[24] Governance Practice EDM05, Ensure Stakeholder Transparency.
[25] NC General Statute § 143B-1379(a)(4) State agency cooperation; liaisons.
[26] ESRMO is not responsible for writing or maintaining agency job descriptions.

- One agency had a job description that included a specific security liaison responsibility. This responsibility stated: “As the security liaison to the Office of the State CIO, this position is responsible for the timely reporting of security breaches.”
- Two agencies had job descriptions that simply stated: “serves as the Security Liaison.” No further or specific security liaison tasks or responsibilities were given.
- Two other agencies had job descriptions that did not mention a security liaison role or function at all.

After being presented this issue during the audit, the Enterprise Security and Risk Management Office (ESRMO) provided a template of a security liaison assignment memo that is addressed to agency heads. This memo has not been distributed to all agencies. The memo informs agency heads of the need to designate a security liaison and lists some of the liaison responsibilities.

Effectiveness of Liaisons Reduced

Without a well-defined, clear, and communicated set of responsibilities, security liaisons throughout the State are unable to serve effectively and consistently in the role intended by law or desired by the State CIO.

Additionally, state agency ability to evaluate the job performance of liaisons is reduced when liaison responsibilities are not defined.

Oversight by State CIO Lacking

The State CIO has not evaluated and monitored ESRMO processes to define and communicate the roles and responsibilities of liaisons.

- ESRMO personnel stated the roles and responsibilities of security liaisons were "left up to the agencies.” The head of ESRMO stated that security liaisons have roles and responsibilities identified in general statutes. However, the tasks listed in general statutes are specifically directed to the agency heads and not liaisons.
- The packet of information ESRMO sends to agency liaisons has not included guidance on roles and responsibilities. The packet of information provided forms required to complete a background check.
- The Department of Information Technology has internal policy manuals and plans that reference, even though not cohesively, security liaisons and some related tasks in-depth. These documents are not available to the agencies. The Statewide Information Security Manual, available to all agencies, does not reference security liaisons and related tasks in-depth.

Best Practices Recommend Clear Roles and Responsibilities

Information technology management best practices recommend that organizations establish an organizational structure that contains clear roles and responsibilities for security personnel. Specifically, the ISACA COBIT 5 Framework states that organizations should:

> “Establish, agree on and communicate IT-related roles and responsibilities for all personnel in the enterprise, in alignment with business needs and objectives. Implement adequate supervisory practices to ensure that roles and responsibilities are properly exercised, to assess whether all personnel have sufficient authority and resources to execute their roles and responsibilities,

and to generally review performance. Ensure that accountability is defined through roles and responsibilities."[27]

RECOMMENDATIONS

The State CIO should direct ESRMO to immediately define and communicate the roles and responsibilities of security liaisons to fulfill legislative intent.

The State CIO should periodically evaluate ESRMO's processes to define and communicate liaison roles and responsibilities and particularly that roles and responsibilities are consistent with current security needs and best practices.

The State CIO should periodically monitor the effectiveness and efficiency of security liaisons in carrying out their roles and responsibilities.

[27] Management Practice APO01.02, Establish Roles and Responsibilities.

OBJECTIVE 2
CONCLUSION AND FINDINGS

Audit Objective #2

Determine whether the Department of Information Technology has effective prevention, detection, and response processes in place to protect government systems and data.

From a formula standpoint, in its most basic form:

IT Security **=** *Prevention* + *Detection* + *Response*

Audit Conclusion for Objective #2

The Department of Information Technology has deficiencies in its prevention, detection, and response processes to protect government systems and data.

Audit Findings for Objective #2

Prevention

5) Lack of Compliance Assessments Jeopardizes Agency Effectiveness to Manage Security

Detection

6) Lack of Security Assessments Risks Unauthorized Access to Systems and Data

7) Unmet Targets to Address Identified Vulnerabilities Increase Likelihood of Unauthorized Access

Response

8) Failures in Incident Reporting Jeopardize the Response to Security Breach or Threat

9) Gaps in State Oversight Jeopardize Agency Business Continuity and Disaster Recovery

FINDING 5: LACK OF *COMPLIANCE ASSESSMENTS* JEOPARDIZES AGENCY EFFECTIVENESS TO MANAGE SECURITY

Last Assessment in 2004

Even though required by law and Executive Order, the State Chief Information Officer (State CIO) did not conduct periodic assessments of agency compliance, or their contracted vendors' compliance, with state security standards. These standards are manifested in the Statewide Information Security Manual maintained by the state's Enterprise Security and Risk Management Office (ESRMO).

- The last statewide assessment was initiated by the State CIO in 2003 and completed in 2004. The assessment report provided a global view of the security of 25 agencies along with their rate of compliance with state security standards
- The State CIO has not assessed the ability of each agency's contracted vendors to comply with the state security standards

There have been no comprehensive statewide assessments of agency compliance against revised security standards. Since the last assessment in 2004, ESRMO has annually revised the Statewide Information Security Manual.

Assessment Are Critical to Prevent Security Failures

Without statewide assessments, the General Assembly, agency heads, and the State CIO do not have the data to identify and remediate security risks caused by agencies and vendors noncompliant with state standards. Security assessment results are required by law to be included in the Biennial State Information Technology Plan.

Executive Order No. 30[28], issued in November 2013, required annual assessments across cabinet agencies to ensure "full compliance with statutes, regulation, policies, standards and contractual obligations related to information security and information technology."

Without periodic assessments, a consistent mechanism is not in place to ensure that agencies and vendors are securing systems and data in compliance with over 130 security standards.

The Statewide Information Security Manual is the foundation for information technology security in the State. The manual establishes a statewide set of standards to maximize the functionality, **security**, and interoperability of the State's distributed information technology assets.[29] (Emphasis added)

The 2016 version contains seven chapters that cover the following areas:

1. Classifying Data and Legal Requirements
2. Securing the End User
3. Securing the Network
4. Securing Systems

[28] Executive Order 30 from the Office of Governor Pat McCrory was titled "*Fix and Modernize Information Technology Governance in Cabinet Agencies by Collaborating as One IT."*

[29] NC Statewide Information Security Manual (2015).

5. Physical Security
6. Cyber Security Incident Response
7. Business Continuity and Risk Management

Processes Not in Place to Determine Compliance

ESRMO does not have processes and methodologies in place to facilitate consistent assessments and reporting of agency compliance with statewide security standards.

- Department of Information Technology and the State Chief Risk Officer stated that insufficient staff and funding did not allow for periodic assessments. Management stated that the 2004 assessment was made possible due to a non-recurring state appropriation to ESRMO
- Since 2013, the State CIO and ESRMO have not tracked its compliance with law and Executive Orders. On September 18, 2015, ESRMO provided a document developed during the audit to begin tracking compliance
- When final reports or documentation required by Executive Order No. 30 was requested, ESRMO stated that no documentation was available to support briefings that may have occurred
- Guidance or templates have not been provided to agencies to enable consistent self-assessment of compliance
- The State Chief Risk Officer stated that work was underway to address gaps in assessment processes through the creation and future implementation of policies and security assessment tools as well as directives and communications to agencies

Law and Executive Orders Require Periodic Assessments

In 2003, law was made that required the State CIO to conduct assessments of each agency, and each agency's contracted vendors, ability and rate of compliance with security standards and report results in the State IT Plan. Specifically, it stated:

> "The State Chief Information Officer shall assess **periodically** the ability of each agency and each agency's contracted vendors to comply with the current security enterprise-wide set of standards established pursuant to this section. The assessment shall include, at a minimum, the rate of compliance with the enterprise-wide security standards and an assessment of security organization, security practices, security industry standards, network security architecture, and current expenditures of State funds for information technology security. The assessment of an agency shall also estimate the cost to implement the security measures needed for agencies to fully comply with the standards. Each agency subject to the standards shall submit information required by the State Chief Information Officer for purposes of this assessment. The State Chief Information Officer shall include the information obtained from the assessment in the State Information Technology Plan required under G.S. 147-33.72B."[30] (Emphasis added)

[30] NC General Statute 147-33.112. Assessment of agency compliance with security standards. [Note: This general statute was repealed by Session Law 2015-241]

On November 7, 2013, Executive Order No. 30 was issued by the Governor to require the State CIO to conduct annual compliance reviews across cabinet agencies and report to Cabinet Secretaries/Directors and the Governor.[31]

> "**Annually, beginning in March 2014**, the SCIO and CCIO's shall, for the purpose of protecting programs, data and information technology, conduct compliance reviews across the cabinet agencies to ensure full compliance with statutes, regulation, policies, standards and contractual obligations related to information security and information technology and report annually on the results of such reviews to Cabinet Secretaries/Directors and the Governor by the SCIO." (Emphasis added)

In September 2015, law was made that created the Department of Information Technology and in doing so replaced the requirement for periodic assessments with annual assessments.

> "At a minimum, the State CIO shall **annually** assess the ability of each State agency, and each agency's contracted vendors, to comply with the current security enterprise-wide set of standards established pursuant to this section. The assessment shall include, at a minimum, the rate of compliance with the enterprise-wide security standards and an assessment of security organization, security practices, security information standards, network security architecture, and current expenditures of State funds for information technology security. The assessment of a State agency shall also estimate the cost to implement the security measures needed for agencies to fully comply with the standards."[32] (Emphasis added)

On September 30, 2015, Executive Order No. 30 was terminated by Executive Order No. 79 after passage of law that created the Department of Information Technology.

RECOMMENDATIONS

The State CIO should direct ESRMO to commence, as required by law and in the next biennium, annual assessments of each agency and each vendor to determine compliance with state security standards.

The State CIO should periodically evaluate ESRMO's processes to conduct security assessments consistent with law, current security needs, and best practices.

The State CIO should periodically monitor the effectiveness and efficiency of ESRMO efforts to conduct security assessments.

[31] NC Executive Order No. 30, *Fix and Modernize Information Technology Governance in Cabinet Agencies by Collaborating as One IT.*

[32] NC General Statute § 143B-1378. Assessment of agency compliance with security standards.

FINDING 6: LACK OF *SECURITY ASSESSMENTS* RISKS UNAUTHORIZED ACCESS TO SYSTEMS AND DATA

Infrequent Assessments

The table below shows a breakdown of the 17 security assessments performed at 15 different agencies from 2011 to 2015, by external third-parties.

Number of Security Assessments Performed by Year				
2011	**2012**	**2013**	**2014**	**2015**
1	2	0	3	11
Note: Nine of the 11 (82%) security assessments performed in 2015 were conducted by the NC National Guard.				

Before a state agency may enter into any contract with another party for an assessment of network vulnerability, including network penetration or any similar procedure, the law[33] requires the agency to notify the State Chief Information Officer (State CIO) and obtain approval of the request. For the convenience of state agencies, the State CIO has contracted with vendors for agencies to use to conduct these assessments.

Risk of Unauthorized Access Increases

Without security assessments, the risk of unauthorized access to systems and data increases.

The 17 security assessments that have been conducted identified 27 critical and 188 high severity findings. A contractor conducting security assessments defined critical and high issues:

> Critical – "The vulnerability is known to be exploitable and discoverable with well-known methods and the tools to do so are free and easy to obtain. Evidence discovered during testing indicates that **exploitation of the vulnerability may have already occurred**." (Emphasis added)
>
> High severity – "Exploitation of the technical or procedural **vulnerability will cause substantial harm** to an agency. Significant political, financial, and/or legal damage is likely to result. The threat exposure is high, thereby increasing the likelihood of occurrence. Security **controls are not effectively implemented** to reduce the severity of impact if the vulnerability was exploited." (Emphasis added)

Oversight of Agency Security Assessments Lacking

Oversight by the state's Enterprise Security and Risk Management Office (ESRMO) lacks:

- A comprehensive strategy for conducting security assessments
- Tracking to ensure corrective actions are taken for assessment findings
- Analysis of agency security assessments findings to identify and share trends

[33] NC General Statute §143B-1377 - State CIO approval of security standards and risk assessments.

No Comprehensive Strategy for Conducting Security Assessments

Between 2011 and 2014, plans were developed that promoted processes for third-party vendors and the NC National Guard to assist the state agencies in conducting security assessments. However, these plans did not contain the contents of a comprehensive strategy.

The developed plans did not contain:

- A strategic and continuing agency schedule
- Resource requirements
- Roles and responsibilities between the Enterprise Security Risk Management Office (ESRMO) and the agencies
- A roadmap indicating the relative scheduling and interdependencies of the security assessments

Without a comprehensive strategy, the State had an elevated risk of not conducting security assessments consistently and across all agencies. For example, the number of security assessments conducted in previous years were few or none.

When asked why there had been no comprehensive plan, Department of Information Technology and ESRMO management indicated that their focus was on the day to day security operations given their environment of limited resources.

In 2015, the State CIO appointed a new State Chief Risk Officer who began the process of developing a comprehensive strategy.[34] This strategy includes a roadmap (schedule) for agencies to have annual security assessments. In 2015, assessments increased significantly.

IT governance and management best practices recommend that organizations create a strategic plan that defines the required initiatives, the sourcing strategy, and the measurements to be used to monitor achievement of goals, then prioritize the initiatives and develop a high-level road map. Specifically, the ISACA COBIT 5 Framework states that organizations should:

> "Determine dependencies, overlaps, synergies and impacts amongst initiatives, and prioritize the initiatives. Identify resource requirements, **schedule** and investment/operational budgets for each of the initiatives. **Create a road map** indicating the relative scheduling and interdependencies of the initiatives. Translate the objectives into outcome measures represented by metrics (what) and targets (how much) that can be related to enterprise benefits."[35] (Emphasis added)

No Tracking to Ensure Corrective Actions are Taken for Assessment Findings

ESRMO does not track and follow-up with agencies to determine if critical or high severity findings identified in security assessments were resolved or mitigated.

Security assessment findings that are known to be exploitable, and that if not addressed, could cause substantial harm to an agency. The State Chief Risk Officer stated that insufficient staff and lack of tools did not allow for tracking. Management also stated that they had started the process of obtaining a tool that would allow them to perform this function.

[34] The State Chief Risk Officer took over ESRMO in January 2015.
[35] Management Practice APO02.05, Define the strategic plan and road map.

IT governance and management best practices recommend tracking corrective actions to address issues. Specifically, the ISACA COBIT 5 Framework states that organizations should:

> "Review management responses, options and recommendations to address issues and major deviations, ensure that the assignment of responsibility for corrective action is maintained, and **track the results** of actions committed."[36] (Emphasis added)

No Analysis of Agency Security Assessment Findings to Identify and Share Trends

ESRMO also does not analyze security assessment findings to identify trends or lessons learned that can be shared with other agencies to prevent or address similar issues. Of the 17 security assessment reports that have been issued, none were analyzed for this purpose.

As a result, ESRMO is not ensuring that optimal value is derived across the State from the security assessments that have been conducted. Specifically, other agencies are not receiving valuable information that could help improve their security.

The State Chief Risk Officer stated that a lack of tools did not allow ESRMO to identify and share trends. Management stated that they had started the process of obtaining a tool that would allow them to perform this function.

IT governance and management best practices recommend that organizations continuously evaluate issues and share improvement opportunities. Specifically, the ISACA COBIT 5 Framework states that organizations should:

> "Establish a platform to **share good practices** and to capture information on defects and mistakes to enable learning from them, identify recurring examples of quality defects, determine their root cause, evaluate their impact and result, and agree on improvement actions, and promote a culture of quality and continual improvement."[37] (Emphasis added)

RECOMMENDATIONS

The State CIO should direct ESRMO to complete, and communicate to agencies, in the next biennium its comprehensive strategy for agencies to conduct security (vulnerability) assessments.

The State CIO should direct ESRMO to immediately track assessment findings to ensure corrective actions are taken.

The State CIO should direct ESRMO to immediately analyze security assessment findings and share results in a secure manner with agencies.

The State CIO should periodically evaluate ESRMO's processes to enable security assessments consistent with law, current security needs, and best practices.

The State CIO should periodically monitor the effectiveness and efficiency of ESRMO efforts to enable agency security assessments.

[36] Management Practice MEA01.05, Ensure the implementation of corrective actions.
[37] Management Practice APO11.06, Maintain continuous improvement.

FINDING 7: UNMET TARGETS TO ADDRESS *IDENTIFIED VULNERABILITIES* INCREASE LIKELIHOOD OF UNAUTHORIZED ACCESS

Remediation Targets Not Met

Security vulnerabilities identified by the Department of Information Technology (Department) are not being addressed within the target deadlines set in the Statewide Information Security Manual.[38]

The Department performs monthly scans of its several operating servers (systems) and when vulnerabilities are found those responsible are notified of the need to take action within target.

The resolution of detected vulnerabilities was an issue across operating servers. For one of the several platforms scanned, 3,153 out of 8,380 (38%) detected vulnerabilities had not been addressed within the target deadline:[39]

- 906 'High' risk vulnerabilities (target is mitigation within seven days and remediation (resolution) within 21 days)
    - 55 high risk vulnerabilities were over one year old
    - 130 were at least 90 days old and less than one year
    - 721 were at least 30 days old but less than 90
- 2247 'Medium' risk vulnerabilities (target is mitigation within 30 days)
    - 14 medium risk vulnerabilities were over two years old
    - 106 were over one year old
    - 1246 were at least 90 days old and less than one year
    - 881 were at least 30 days old and less than 90

Risk of Data Breaches Increased

Without timely action to address high and medium risk vulnerabilities, the likelihood of a data breach occurring to a State system is increased.

The Statewide Information Security Manual defines high and medium risk vulnerabilities as:

> High-level Risk: A vulnerability that could cause grave consequences if not addressed and remediated immediately. This type of vulnerability is present within the most sensitive portions of the network or IT asset, as identified by the data owner. **This vulnerability could cause functionality to cease or control of the network or IT asset to be gained by an intruder.** (Emphasis added).
>
> Medium-level Risk: A vulnerability that should be addressed within the near future. Urgency in correcting this type of vulnerability still exists; however, the vulnerability may be either a more difficult exploit to perform or of lesser concern to the data owner.

[38] NC Statewide Information Security Manual (2015).
[39] Vulnerability data as of October 8, 2015. Per North Carolina General Statute 132-6.1(c), sensitive information is not included in this report.

Oversight of Vulnerability Remediation Lacking

Department personnel stated that information pertaining to security vulnerabilities was not shared with the appropriate leadership tasked with enforcing the timely remediation of vulnerabilities.

The Department had not designated someone to oversee the timely remediation of vulnerabilities.

Best Practices Recommends Remediation As Soon As Possible

IT governance and management best practices recommend that organizations remediate vulnerabilities within defined response times in accordance with an organizational assessment of risk.[40]

RECOMMENDATIONS

The State CIO should direct responsible Department of Information personnel to immediately address and resolve vulnerabilities detected during scans of Department systems within established target deadlines.

The State CIO should periodically evaluate Department processes to address and resolve vulnerabilities consistent with law, Department policy, and best practices.

The State CIO should periodically monitor the effectiveness and efficiency of Department efforts to address and resolve vulnerabilities detected during scan of Department systems.

FINDING 8: FAILURES IN INCIDENT *REPORTING* JEOPARDIZE THE RESPONSE TO SECURITY BREACH OR THREAT

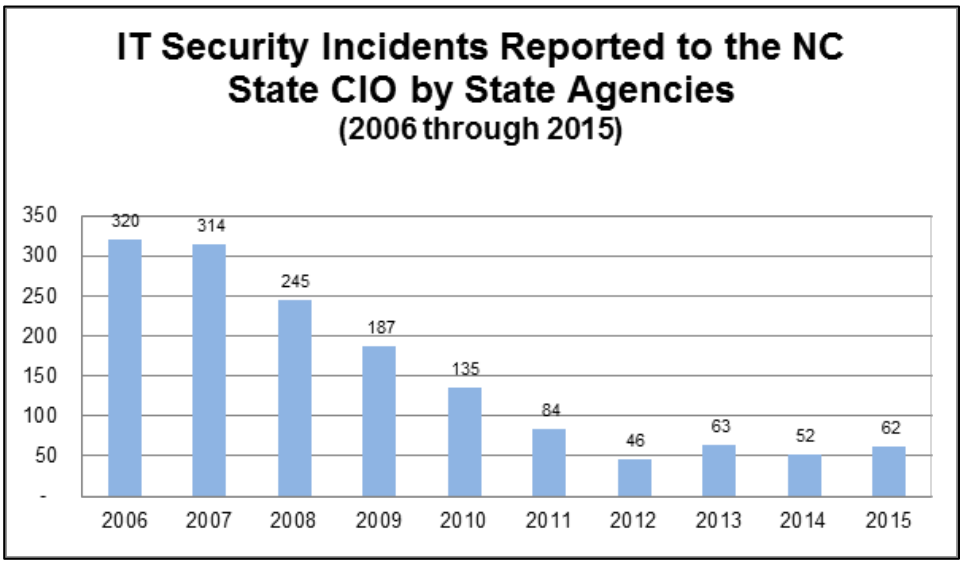
Data indicates that state agencies are not reporting all information technology (IT) security incidents to the State Chief Information Officer (State CIO). Incidents that are reported are often misclassified, incorrectly prioritized by the reporting agency, and may not be reported timely. The state Enterprise Security and Risk Management Office (ESRMO) has an inadequate process for ensuring the completeness, accuracy and timeliness of IT security incident data.

Effectively reporting all IT security incidents is essential to responding adequately to minimize any negative impact to state systems and information.

Significant Decrease in IT Security Incidents Reported

Over the past 10 years there has been a significant decrease in ITsecurity incidents reported by state agencies to the State Chief Information Officer (State CIO). The number of reported incidents has decreased by 81% in the past 10 years. Specifically, the number of reported incidents has decreased from 320 in 2006 to less than 62 in 2015.

[40] NIST Special Publication 800-53r4, RA-5 Vulnerability Scanning.

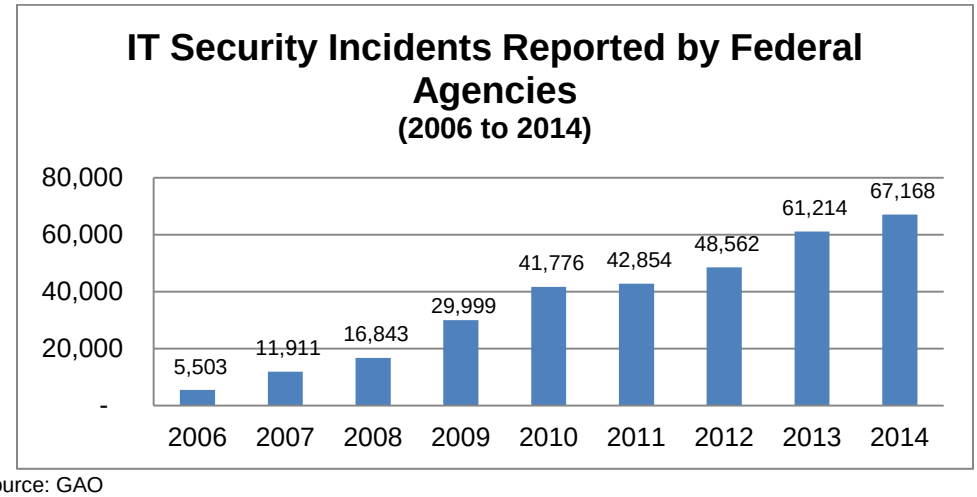


Source: NC IT Security Incident Database

The State's declining trend conflicts with the analyses of many well-known organizations that have highlighted increasing IT security incidents trends and statistics worldwide, affecting both private and public organizations. For example:

- ISACA has reported that the number of cybersecurity attacks and incidents have risen exponentially in the past several years.[41]

- The United States Government Accountability Office (GAO) has reported the number of information security incidents affecting systems supporting the federal government has steadily increased each year: rising from 5,503 in fiscal year 2006 to 67,168 in fiscal year 2014, an increase of 1,121 percent.[42]



Source: GAO

[41] ISACA publication, *Transforming Cybersecurity* (2013).
[42] GAO, *Cybersecurity Recent Data Breaches Illustrate Need for Strong Controls across Federal Agencies*, June 2015, GAO-15-725T.

Agencies Not Reporting All IT Security Incidents

State agencies did not report all IT security incidents to the State CIO and that agencies that previously reported incidents no longer report incidents.

- 16 agencies have not reported any IT security incidents for five years or more over the last decade
- In 2015, one agency tracked 109 incidents and only reported 7 (6%) to the State CIO. At least 10 of the 102 unreported incidents should have been reported per ESRMO guidelines
- Another agency did not have any tools or mechanism in place to track IT security incidents[43]
- Another agency had a tracking tool that had incomplete and missing information. The agency stated their tool failed in 2014 and all historical IT security incident data was lost

Difficult to Determine Whether Incidents Are Reported within Legal Requirements

It was difficult to determine whether security incidents were reported within 24 hours of confirmation as mandated by state law.

- ESRMO does not track whether agencies report incidents within 24 hours of confirmation
- The state's incident reporting form used by agencies does not capture the date/time an incident was confirmed by the agency
- The incident reporting form set "January 1, 2011" as the default for the date of incident. Various instances in 2012 (5), 2013 (10), 2014 (6), and 2015 (5) were reported as occurred on "January 1, 2011"

Agency Classification and Prioritization of Incidents Is Ineffective

Without proper classification and prioritization, it is difficult to analyze incident data, assess the significance of the incident, and identify areas that require further attention and improvement.

Classification

For the past ten years, a high percentage of reported IT security incidents were not classified effectively. The nature of the incident was not explicitly identified. Specifically, a high percentage of incidents reported were classified as 'unknown' or 'other' rather than to one or more of the 13 specific categories available (for example, intrusion, theft, privacy, website defacement, information disclosure, etc.).

- In 2006, 47% of all incidents reported by agencies were classified as 'Unknown' and 'Other'
- In 2010, 88% of all incidents reported by agencies were classified as 'Unknown' and 'Other'
- In 2015, 63% of all incidents reported by agencies were classified as 'Unknown' and 'Other'

[43] Following good management practices, each agency is able to maintain tools, applications, or processes for tracking incidents. ESRMO has indicated that it maintains the authoritative database in the State for reported incidents.

IT Security Incidents Reported by Classification Category				
Year	**'Unknown' Category**	**'Other' Category**	**Specific category**	**Total Incidents**
2006	78 (25%)	71 (22%)	171 (54%)	320
2010	90 (67%)	29 (21%)	16 (12%)	135
2015	10 (16%)	29 (47%)	23 (37%)	62

Source: ESRMO Incident Tracking Database (2006-2015)
Note: Auditors reviewed incident information between 2006 to 2015, and selected three years (2006, 2010, 2015) to provide a representation of the data for the beginning, middle and end points of the last decade.

Prioritization

For the past ten years a high percentage of incidents reported were of a 'low' priority. The 'incident priority' question in the incident reporting form was set to a default answer of "low". It is difficult to determine if the reported prioritization is accurate.

IT Security Incidents Reported by Priority						
Year	**Low Priority**	**Minimal Priority**	**Medium Priority**	**High Priority**	**Severe Priority**	**Total Incidents**
2006	**244 (76%)**	23 (7%)	36(11%)	14(4%)	3(<1%)	320
2010	**108 (80%)**	11(8%)	14(10%)	1(<1%)	1(<1%)	135
2015	**34 (55%)**	9(15%)	10(16%)	7(11%)	2(3%)	62

Source: ESRMO Incident Tracking Database (2006-2015)
Note: Auditors reviewed incident information between 2006 to 2015, and selected three years (2006, 2010, 2015) to provide a representation of the data for the beginning, middle and end points of the last decade.

Process for Reporting IT Security Incidents Is inadequate

There has been a lack of oversight and periodic assessment by ESRMO to ensure the State's incident reporting governance mechanism is operating effectively.

Across agencies there were different views as to when and what incidents to report. ESRMO has given agencies discretion to report what they consider to be security incidents.

Prior to 2015, state law did not define an 'IT security incident' and the Incident Management Plan developed by the State CIO's office, which contained guidance and key definitions, was not made widely available to agencies.

The incident reporting form is not practical. The form has many key questions that agencies are not required to complete and many key fields contain default answers.

- Only 2 out of 23 (13%) questions are required to be completed by agencies, including key information such as the date/time of incident and whether personally identifiable information was involvedThe incident classification category question is set to a default answer of "Unknown"

- The incident priority question is set to a default answer of "low"

State Law and Best Practices Target Incident Reporting

State law mandates agencies to report all IT security incidents to the State CIO:

> "The head of each State agency shall cooperate with the State Chief Information Officer in the discharge of his or her duties by: (1) Providing the full details of the agency's information technology and operational requirements and of all the agency's information technology security incidents within 24 hours of confirmation."[44]

The *ISACA COBIT 5 Framework* recommends that organizations effectively classify and prioritize IT security incidents.[45]

IT best practices recommend that organizations periodically assess the effectiveness of mandatory reporting mechanisms to ensure information is accurate and reliable.

Specifically, the *ISACA COBIT 5 Framework* states that organizations should:

> "Continually examine and make judgement on the current and future requirements for stakeholder reporting, including mandatory reporting requirements. Ensure the establishment of effective stakeholder communication and reporting, including mechanisms for ensuring the quality and completeness of information, and oversight of mandatory reporting. Periodically assess the effectiveness of the mechanisms for ensuring the accuracy and reliability of mandatory reporting. Determine whether the requirements of different stakeholders are met."[46]

RECOMMENDATIONS

The State CIO should direct state agencies to report immediately security incidents compliant with law and ESRMO instruction.

The State CIO should now and periodically evaluate ESRMO's processes for agencies to report security incidents compliant with law, ESRMO instruction, and best practices to ensure agencies effectively classify, prioritize, and report timely all IT security incidents.

The State CIO should now and periodically monitor the effectiveness and efficiency of agency efforts to report security incidents.

FINDING 9: GAPS IN STATE OVERSIGHT JEOPARDIZE AGENCY BUSINESS CONTINUITY AND DISASTER RECOVERY

While the state's Enterprise Security and Risk Management Office (ESRMO) annually reviews the business continuity and disaster recovery plans (BCP)[47] of state agencies,[48] it has not ensured that agencies perform required testing of their plans for all critical applications.[49]

[44] NC General Statute § 143B-1379, (a)(1), State agency cooperation; liaisons.
[45] Management Practice DSS02, Manage Service Requests and Incidents.
[46] Governance Practice EDM05, Ensure Stakeholder Transparency.
[47] Covers all of an agency's essential and critical business activities and includes references to procedures to be used for the recovery of systems that perform the agency's essential and critical business activities.
[48] All executive branch agencies subject to Article 15 of N.C.G.S. §143B.
[49] NC Statewide Information Security Manual (2015) Section 070103, Developing the BCP states: "The agency business continuity plan shall be tested annually, at a minimum. All critical applications shall be tested annually."

Furthermore, ERSMO has not assessed the adequacy of agency plans after their activation during an agency business interruption or disaster. ESRMO has not assessed the completeness and operating effectiveness of their current processes for oversight of BCP's.

In 2014, the Disaster Recovery Preparedness Council[50] released a report titled '*The State of Global Disaster Recovery Preparedness'*[51]*,* which found gaps in preparedness for organizations worldwide. Specifically, the survey found:

- 73% of organizations worldwide are unprepared for IT business continuity and disaster recovery.
- 23% of organizations never test their DR plans and when organizations do test their DR plans, more than 65% do not pass their own tests.
- More than half of the organizations that actually test DR plans don't document the results of their tests.
- Only one in four organizations who fail the first round of DR testing, ever actually re-test as part of their follow up.

No Tracking and Assessment of Plan Testing by Agencies

ESRMO has not maintained, since at least 2011, comprehensive documentation to track agency compliance with state security standards. It does not track agency adherence to scheduled plans to test business continuity and disaster recovery plans for all critical applications. ESRMO only tracks whether agencies have scheduled testing.

By not tracking, it is difficult for ESRMO to know whether state agencies are adequately prepared to continue critical government operations (e.g., health and human services, public safety, transportation services, etc.), and to maintain the availability of essential systems, in the event of a disruption or disaster (e.g., hurricanes, tornadoes, fire, floods, etc.).

Furthermore, ESRMO does not regularly review BCP test results and verify that the BCP works.

The State Chief Risk Officer stated that tracking test completion and reviewing test results has not been required.

IT governance and management best practices recommend assessing the effectiveness and performance of agencies given responsibility and authority. Specifically, the *ISACA COBIT 5 Framework* states that organizations should:

> "Assess the effectiveness and performance of those stakeholders given delegated responsibility and authority for governance of enterprise IT.[52]

No Tracking and Assessment of Plan Activation by Agencies

ESRMO does not track plan activation. It does not know which agencies have activated their BCP plan. It could not provide the number of times or list state agencies that have activated their plan since 2011.

[50] An independent research organization engaged in IT disaster recovery management, research, and benchmarking.
[51] http://drbenchmark.org/wp-content/uploads/2014/02/ANNUAL_REPORT-DRPBenchmark_Survey_Results_2014_report.pdf.
[52] Governance Practice EDM01.03, *Monitor the Governance System.*

Without oversight of plans when activated, ESRMO is unable to fully assess the adequacy of agency BCP plans, adherence to plans in the event they are activated, and that agencies carry-out their own post-activation review activities. Examples of areas that should be assessed after plan activation include: agency continuity capabilities, roles and responsibilities, skills and competencies, resilience to the incident, and technical infrastructure.

The State Chief Risk Officer stated that state agencies have not been required to report to ESRMO activation of BCP plans. The Statewide Information Security Manual does not contain clear guidance for agencies to follow regarding post-activation reviews.

IT governance and management best practices recommend that enterprises assess BCP plans following the resumption of business processes and services after a disruption. Specifically, the *ISACA COBIT 5 Framework* states that organizations should:

> "Assess adherence to the documented BCP. Determine the effectiveness of the plan, continuity capabilities, roles and responsibilities, skills and competencies, resilience to the incident, technical infrastructure, and organizational structures and relationships. Identify weaknesses or omissions in the plan and capabilities and make recommendations for improvement."[53]

RECOMMENDATIONS

The State CIO should direct ESRMO to immediately track and assess agency business continuity and disaster recovery plans.

The State CIO should direct ESRMO to track and assess agency activation of business continuity and disaster recovery plans.

The State CIO should now and periodically evaluate ESRMO's processes to oversee the adequacy and activation of business continuity and disaster recovery plans consistent with law, current security needs, and best practices.

[53] Management Practice DSS04.08, *Conduct Post-Resumption Review.*

MATTER FOR FURTHER CONSIDERATION

***During the course of an audit**, Office of the State Auditor staff may uncover potential issues that are outside of the audit objectives. Although the issues may not have been part of the planned objectives, the issues need to be presented to those charged with governance of the organization under audit. Below is such an issue.*

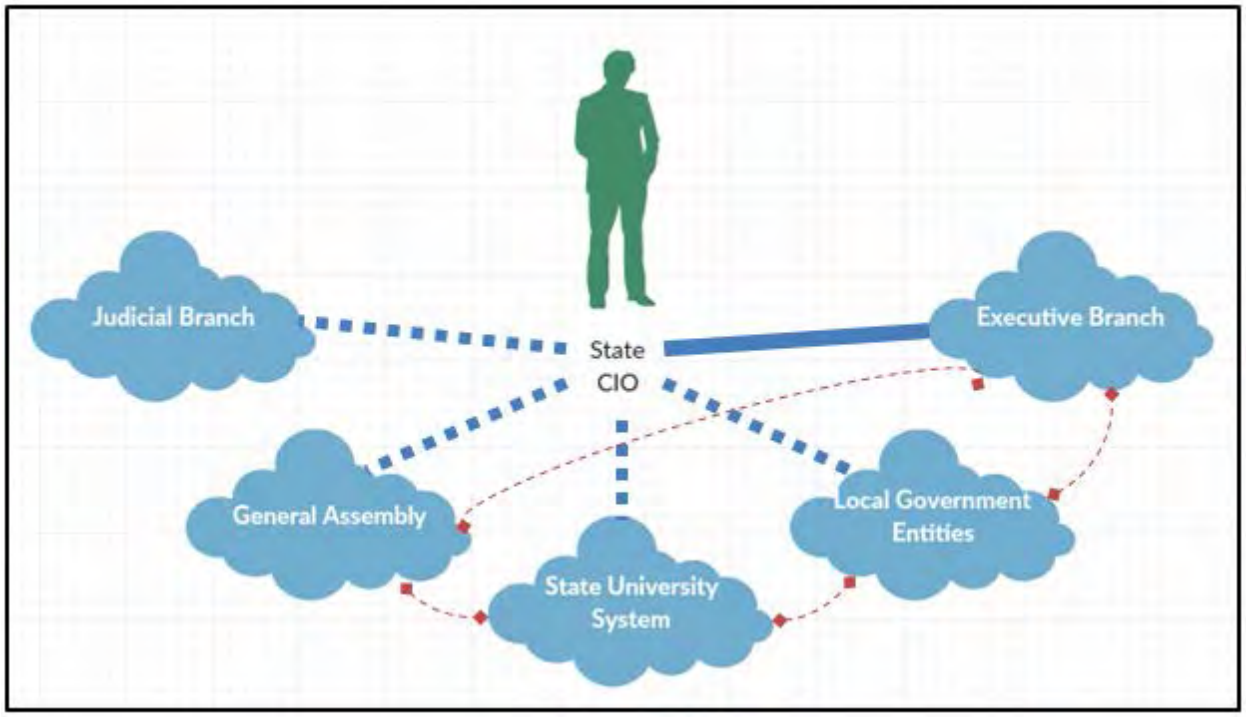
IT Security Law Should be Modernized

Current law pertaining to information technology (IT) security limits the oversight and enforcement capability of the State Chief Information Officer (State CIO) to ensure security of all state IT systems and associated data.[54]

IT security law should be reviewed to develop a modernized framework that is comprehensive and ensures effective governance and management to protect all state government systems and data.

The State CIO has security oversight of Executive Branch agencies only. The State CIO does not have security oversight (dotted lines) of local government entities and other state government entities, even though these entities impact state government systems and data. As illustrated in the following diagram, IT security governance and management of state government systems and data operate in several silos.

State CIO Oversight



Notes: Solid blue line indicates direct oversight (dotted blue lines indicate no direct oversight). Red dotted lines indicate IT interconnectivity amongst entities.

[54] NC General Statute § 143B-1320, Definitions; scope; exemptions.

Law Limits State CIO IT Security Oversight

State law regarding security reads: "The State CIO shall be responsible for the security of all State information technology systems and associated data. The State CIO shall manage all **executive branch** information technology security and shall establish a **statewide** standard for information technology security…" [55] (Emphasis added)

The statewide security standards though are not applicable to all state government entities. State law reads: "Except as otherwise specifically provided by law, the provisions of this Chapter **do not apply** to the following entities: the General Assembly, the Judicial Department, and the University of North Carolina and its constituent institutions."[56] (Emphasis added)

The law does not otherwise provide direction to the exempted state agencies to govern and manage IT security even though they could impact state government systems and data.

The statewide security standards also do not apply to local governments. Law defines local government entities as: "A local political subdivision of the State, including a city, county, local school administrative units…or a community college." Law does not otherwise provide direction to local governments to govern and manage IT security even though they impact state government systems and data. State agencies operate systems that are interconnected with local government entities and share sensitive, financial, and personal citizen information. For example:

- The Department of Health and Human Services has new systems designed to improve the way the state and the 100 county departments of social services conduct business
- Department of Public Instruction systems provide teachers, students, parents and administrators with real-time access to student data, records, and teaching and learning resources
- Department of Public Safety systems establish links with the criminal justice community, receiving and supplying critical and timely information to the state's courts, law enforcement and crime victims
- Department of Transportation programs combine state vehicle registration fees and county property taxes into one renewal notice. Once citizens pay their invoice in one transaction the State transmits collected vehicle tax payments to the 100 counties.

While exempt state agencies and local government entities manage their own IT security, the State does not have an integrated structure to fully assess the risk exposure to the state's systems and data.

Exempt state agencies and local government entities have been affected by IT security incidents in the past, and at one point reported these incidents to the State CIO. For example, between 2006 and 2010, local government entities comprised an average of 74% of all IT security incident reporting entities. Between 2011 and 2015, local government entities decreased to an average of 29% of all reporting entities. Specifically, in 2006, 64 local government entities reported incidents to the State CIO, and in 2015, only 4 local government entities reported incidents.

The NC Statewide IT restructuring plan issued by the State CIO stated the State CIO "cannot effectively exercise statutory authority without a governance model built on central control of IT prioritization, budgeting, and oversight." (Emphasis added)

[55] NC General Statute § 143B-1376, Statewide security standards.
[56] NC General Statute § 143B-1320(b), Exemptions.

Law Limits State CIO Enforcement of Security Standards

For agencies subject to State CIO oversight, law does not contain sufficient and appropriate enforcement mechanisms to ensure adequate accountability of agency compliance with state IT security requirements.

Law provides that the State CIO may assume the direct responsibility of providing for the information technology security of any state agency that fails to adhere to state security standards."[57]

However, according to the NC Statewide IT restructuring plan, the "option of taking over inadequate security is not feasible in some cases." Additionally, there is no mechanism in which funds could potentially be withheld from agencies found to be non-compliant with security standards."

Comprehensive Framework is Ideal

The Federal Information Security Modernization Act of 2014 (FISMA) establishes a comprehensive framework that contains cohesive and detailed sections that cover various topics, such as: authority, oversight functions, agency responsibilities, and independent evaluations. Specifically, FISMA states that its purposes are to:

1) ''provide a comprehensive framework for ensuring the effectiveness of information security controls …" [Emphasis added]

2) recognize the highly networked nature of the current Federal computing environment and provide effective government-wide management and oversight of the related information security risks …" [Emphasis added]

Previous Matters for Further Consideration - On IT Legislation and Security Oversight

The Office of the State Auditor has released three other audit reports that include a Matter for Further Consideration (MFC) that also indicate the need for a modernized IT security and oversight framework.

On January 20, 2016, the Office of the State Auditor released two audit reports that included a MFC that indicated The University of North Carolina (UNC) Board of Governors should assess the authority given to UNC-General Administration (UNC-GA) for oversight of IT security at member institutions. Specifically, the MFC stated:

> *"Under State law, UNC-GA derives its authority over member campuses solely through direction from the UNC Board of Governors (Board). UNC-GA officials represent that the Board has not provided them authority to hold campuses accountable for complying with the IT security framework adopted by the member campuses."*[58]

On February 3, 2015, the Office of the State Auditor released an IT governance audit report that indicated the State had a conflict in the oversight of internal control standards for IT. Specifically, the MFC stated:

> *"The State Governmental Accountability and Internal Control Act and the general statute that lays out the responsibilities for the State Chief Information Officer (State CIO) have led to confusion about who is responsible for establishing and overseeing the effective implementation of internal controls over IT. The General Assembly should consider legislation to clarify and define the responsibilities of the State Controller and State CIO for internal control standards over IT to ensure complete oversight."*[59]

[57] NC General Statute § 143B-1376, Statewide security standards.
[58] http://www.ncauditor.net/EPSWeb/Reports/InfoSystems/ISA-2015-6088.pdf.
[59] http://www.ncauditor.net/EPSWeb/Reports/InfoSystems/ISA-2014-4660.pdf.


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

APPENDICES

Information Technology

PAT McCRORY

KEITH WERNER

May 16, 2016

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

Dear Ms. Wood:

We have reviewed the draft of the *Information Systems Audit for Executive Branch Security Governance and Management*. It is important to note that the issues identified primarily occurred during timelines when the State operated in a decentralized Information Technology (IT) operating model within state government. As noted within the *Restructuring Information Technology – To Improve Effectiveness, Efficiency and Citizen Satisfaction* document dated December 2014, "the core issues that have hindered success in the past are rooted in the way IT is governed and managed across the state." As identified in the document, "a key marker of success identified was Security and risk management: to protect citizen information and state business data and technology systems, and to provide the public with confidence in state services, the state must maintain IT security and risk management as a priority across the enterprise." The establishment of the consolidated and unified Department of Information Technology (DIT) is a major step in remediating the gaps with regard to security, privacy and risk management statewide. DIT and the Enterprise Security and Risk Management Office (ESRMO) have projects in flight to take corrective actions and address previously identified gaps in cybersecurity management. DIT has a Security Program in place that will modernized as required.

We respond to the Auditor's recommendations as follows:

FINDING 1: NO COMPREHENSIVE RISK MANAGEMENT FRAMEWORK COMPROMISES SECURE AND SUSTAINABLE IT SERVICES.

RECOMMENDATIONS:
The State CIO should direct ESRMO to implement in the next biennium a comprehensive and well-documented risk management framework.

The State CIO should periodically evaluate the risk management framework to ensure its design is effective and efficient to achieve its purpose, including the positioning of ESRMO in the Department of Information Technology's organizational structure.

The State CIO should regularly monitor key risk management activities to determine that they are functioning as designed, including the assignment of ESRMO resources to effectively carry out key statewide risk management activities.

DIT Response:
As stated earlier the past decentralized operation of State and supporting IT Security infrastructure has restricted the ability to effectively manage systems and personnel, and implement a holistic risk management framework (RMF). ESRMO has been using the ISO 27001 standard for RMF; however, DIT will be adopting a more comprehensive RMF that, coupled with the DIT consolidation effort, should allow for better governance. As a note, a major part of the DIT plan, as identified by the DIT Transition Program Office, is security and privacy. Security has been specifically identified as one of the ***critical*** swim lane projects to be consolidated as part of the DIT consolidation effort. It is through consolidation that the State can experience true economies of scale and significant improvement in Security and Risk Governance.

In the absence of a consolidated organization, ESRMO has developed and maintains a Strategic Plan which provides governance through establishment of goals and objectives specifically designed to reduce the risk to the citizens' data and establish a roadmap for compliance and incident response. ESRMO has also made significant movement in migrating from the ISO 27001 standard that was previously in use, to the adoption of the National Institute of Standards and Technology (NIST) Risk Management Framework. This framework is widely adopted by a majority of states and was identified by the U.S. Department of Defense, federal agencies and the National Association of State Chief Information Officers (NASCIO) as an industry best practice.

Prior to the OSA audit, DIT, through the Network Simplification Project, had begun the task of updating its security infrastructure to include replacing aging Security Information Event Management (SIEM) tools which will address the ability to comprehensively capture, correlate and report on anomalous activities within the network. In the past, this was a manually-intensive process, but the new technologies will increase the speed to detect, respond and report, shortening the life cycle for incident response.

Other notable improvements made or that are in progress include:

- Deployment of the State's first Enterprise Risk Governance and Compliance (EGRC) tool. This tool will aid in the identification and tracking of compliance throughout the State and provide dashboard reporting for compliance.
- Development of a Continuous Monitoring Plan to address the legislative requirement to not only meet the annual assessment schedule, but to regularly interrogate the network to identify unapproved changes.
- Data Mapping Inventory was conducted in 2015, in coordination with DIT and supported agencies, to identify and track the location of the confidential data stored within the State Data Centers
- Development of a Privacy Threshold Analysis (PTA) document to capture confidential data sets being stored by systems and determine the appropriate risk level and security controls that are needed.
- In 2016, ESRMO provided mandatory Cyber Awareness training that is funded by ESRMO and provided to the entire executive branch. Due to legislative restrictions, ESRMO cannot mandate cyber awareness training to legislative and judicial branches; however, this training is provided to them for their use.

- ESRMO provides monthly updates to all Agency CIOs and Security Liaisons on threats, risk and security posture as it relates to patch management, vulnerability management, end- of-lifecycle management, as well as other related topics.
- Development of an Enterprise Security Strategic Plan

Responsible Person: Maria Thompson, Chief Risk Officer, ESRMO
Expected Completion Date: First quarter of Calendar Year (CY) 2017.

FINDING 2: NO PERFORMANCE MEASURES PREVENT ASSESSMENT OF SECURITY EFFORTS

RECOMMENDATIONS:
The State CIO should direct ESRMO to immediately establish and post-performance measures on the Department of Information Technology's website as required by law. The State CIO should ensure these performance measures do not jeopardize the state's security.

The State CIO should now and periodically evaluate the performance measures to ensure that they are linked to Department strategic goals, key initiatives, and core services pertaining to security and are outcome based.

The State CIO should now and periodically monitor performance measures to determine that they are up-to-date and are used by ESRMO in decision making.

DIT Response: ESRMO has developed draft performance measures and will work to optimize performance metrics in line with industry standards and provide a dashboard reporting ability to deliver enterprise-wide visibility on key security projects and services. Additionally, ESRMO will monitor and align the performance measures against IT and security strategic missions.

Responsible Person: Maria Thompson, Chief Risk Officer, ESRMO
Expected Completion Date: First quarter of CY2017.

FINDING 3: INADEQUATE IT SECURITY FINANCIAL REPORTING LIMITS ASSESSMENT OF INVESTMENTS TO SECURITY RISKS

RECOMMENDATIONS:
The State CIO should direct ESRMO to develop processes with the Office of State Controller and the Office of State Budget and Management to discreetly present IT security investments and expenditures in the 2016 State IT Expenditures Report.

The State CIO should periodically evaluate the effectiveness of the State IT Expenditure Report by consultation with the Governor and General Assembly members.

The State CIO should monitor the process to prepare the State IT Expenditure Report to ensure process is functioning as designed.

DIT Response: This specific recommendation requires coordination outside of ESRMO. DIT will work with the Office of State Controller and the Office of State Budget and Management to establish a discreet line item for the tracking and reporting of IT Security investments. ESRMO will work with

the DIT Chief Financial Officer and the DIT Transition Program Office to identify the categories of security investments to be tracked within this line item number.

Responsible Person: Trevor Minor, Chief Financial Officer, Department of Information Technology
Expected Completion Date: TBD.

FINDING 4: UNDEFINED ROLES AND RESPONSIBILITIES REDUCE EFFECTIVENESS OF AGENCY SECURITY LIAISONS

RECOMMENDATIONS:
The State CIO should direct ESRMO to immediately define and communicate the roles and responsibilities of security liaisons to fulfill legislative intent.

The State CIO should periodically evaluate ESRMO's processes to define and communicate liaison roles and responsibilities and particularly that roles and responsibilities are consistent with current security needs and best practices.

The State CIO should periodically monitor the effectiveness and efficiency of security liaisons in carrying out their roles and responsibilities.

DIT Response: This finding has been remediated. ESRMO released a memo in March 2016 to State CIOs and Agency Security Liaisons, directing all Security Liaisons to acknowledge and sign an appointment letter that detailed the standard roles and responsibilities for their duties. This appointment letter has been included in the standard Security Liaison package for newly-appointed liaisons. All appointment letters will be audited annually.

Responsible Person: Maria Thompson, Chief Risk Officer, ESRMO
Expected Completion Date: Completed.

FINDING 5: LACK OF COMPLIANCE ASSESSMENTS JEOPARDIZES AGENCY EFFECTIVENESS TO MANAGE SECURITY

RECOMMENDATIONS:
The State CIO should direct ESRMO to commence, as required by law and in the next biennium, annual assessments of each agency and each vendor to determine compliance with State security standards.

The State CIO should periodically evaluate ESRMO's processes to conduct security assessments consistent with law, current security needs, and best practices.

The State CIO should periodically monitor the effectiveness and efficiency of ESRMO efforts to conduct security assessments.

DIT Response: ESRMO has adopted the Department of Homeland Security (DHS) mandatory program for Continuous Diagnostics and Mitigation (CDM). This program is being used within the

U.S. Department of Defense and all federal agencies, in order to [1] "fortify the cybersecurity of government networks and systems." ESRMO is also in the process of hiring an IT Security Specialist specifically to spearhead this task. Through CDM, ESRMO will be able to identify and prioritize risks based on potential impact, and allowing for better utilization of security personnel throughout the state.

ESRMO is finalizing the Continuous Monitoring Plan which will address the CDM program and Risk/Security assessment schedule for all agencies. The Plan utilizes a 3-year accreditation process which will allow agencies to budget for a mandatory full 3rd party assessment every three years. The subsequent year's assessments will be completed using a combination of the following:

- Cybersecurity Self-Assessment
- Vulnerability Assessment through network, server and desktop scans

The Continuous Monitoring Plan requires all agencies to provide to the State CIO, no later than 01 September of each year, an assessment report indicating their compliance levels as it relates to the Statewide Information Security Policy, and includes all cloud vendors. Each agency must also identify unfunded mandates, such as third party assessments and equipment and personnel shortages. ESRMO has been conducting vulnerability assessments to identify risks due to unpatched network devices and identify compliance with patch management policies. These assessments were conducted on a monthly schedule. ESRMO has since increased the frequency of scans to occur on a 7-day interval.

Lastly, as was previously mentioned, ESRMO is in the process of deploying the Enterprise Governance Risk and Compliance (EGRC) tool which will be used to track/monitor security assessments, provide compliance reports and manage remediation schedule for identified deficiencies.

Responsible Person: Maria Thompson, Chief Risk Officer, ESRMO
Expected Completion Date: First quarter of CY2017.

FINDING 6: LACK OF SECURITY ASSESSMENTS RISKS UNAUTHORIZED ACCESS TO SYSTEMS AND DATA

RECOMMENDATIONS:
The State CIO should direct ESRMO to complete, and communicate to agencies, in the next biennium its comprehensive strategy for agencies to conduct security (vulnerability) assessments.

The State CIO should direct ESRMO to immediately track assessment findings to ensure corrective actions are taken.

The State CIO should direct ESRMO to immediately analyze security assessment findings and share results in a secure manner with agencies.

The State CIO should periodically evaluate ESRMO's processes to enable security assessments consistent with law, current security needs, and best practices.

---

[1] Department of Homeland Security – Continuous Diagnostics and Mitigation (CDM)
https://www.dhs.gov/cdm

The State CIO should periodically monitor the effectiveness and efficiency of ESRMO efforts to enable agency security assessments.

DIT Response: ESRMO and State agencies have expressed difficulties in meeting this **unfunded mandate**, i.e. (G.S. § 143B-1342 - Assessment of agency compliance with security standards). Personnel and funding deficiencies preclude a 3rd Party Assessment every year. In order to meet this mandate, ESRMO has developed a 3-year assessment schedule as part of the Continuous Monitoring Plan.

Additionally, ESRMO has created a 918A convenience contract for risk and security assessments for all agencies to use. This contract has vetted private sector companies who have the required skillsets to conduct 3rd party assessments. Furthermore, the State CIO has established a Memorandum of Understanding with the National Guard's Cyber Division to provide security assessments at a greatly reduced rate. These assessments, however, are subject to the availability of the National Guard resources. All assessments are conducted using a template that ESRMO has established. This template provides a ***standard*** security assessment reporting mechanism to be used by all agencies to ensure that there is consistency in approach and methodology. Finally, ESRMO has begun the education process with all agencies to ensure they understand that all cloud vendors must be assessed to the same level of compliance as government bodies. See ESRMO response in #5 for additional details.

Responsible Person: Maria Thompson, Chief Risk Officer, ESRMO
Expected Completion Date: Second quarter of CY2017.

FINDING 7: UNMET TARGETS TO ADDRESS IDENTIFIED VULNERABILITIES INCREASE LIKELIHOOD OF UNAUTHORIZED ACCESS

RECOMMENDATIONS:
The State CIO should direct responsible Department of Information Technology personnel to immediately address and resolve vulnerabilities detected during scans of Department systems within established target deadlines.

The State CIO should periodically evaluate Department processes to address and resolve vulnerabilities consistent with law, Department policy, and best practices.

The State CIO should periodically monitor the effectiveness and efficiency of Department efforts to address and resolve vulnerabilities detected during scan of Department systems.

DIT Response: ESRMO has met on numerous occasions with the DIT Shared Delivery team(s) directly responsible for the patching and remediation of identified vulnerabilities. ESRMO has also briefed the Agency CIOs on their business owner roles and responsibilities as it pertains to application patch management. ESRMO continues to work diligently with Shared Delivery to escalate and reduce vulnerability count and document compensating controls in place in order to reduce the risks to a more desired state. Patch management is an integral part of maintaining an acceptable risk level. The latest version of the Statewide Information Security Manual has been updated to reflect a more widely accepted patch schedule based on risk to the network. This

change should allow for more bandwidth for System Administrators to test and deploy patches, while still giving preference to those critical and zero-day attack patches. DIT Shared Delivery is in the process of revamping their patch management methodologies to align with the Statewide Information Security Policy. ESRMO will continue to monitor for compliance.

Responsible Person: Maria Thompson, Chief Risk Officer, ESRMO
Expected Completion Date: First quarter of CY2017.

FINDING 8: FAILURES IN INCIDENT REPORTING JEOPARDIZE THE RESPONSE TO SECURITY BREACH OR THREAT

RECOMMENDATIONS:
The State CIO should direct state agencies to report immediately security incidents compliant with law and ESRMO instruction.

The State CIO should now and periodically evaluate ESRMO's processes for agencies to report security incidents compliant with law, ESRMO instruction, and best practices to ensure agencies effectively classify, prioritize, and report timely all IT security incidents.

The State CIO should now and periodically monitor the effectiveness and efficiency of agency efforts to report security incidents.

DIT Response: During the course of this audit, it became apparent that the definition of a reportable IT security incident, as written by law, is too broad. Based on the current law, all incidents, to include virus infections, may be included in the 24-hour reporting timeline. This type, and other lower risk security "events," are being captured within other tools within the organization, though not within the ESRMO Incident Reporting Tool. This issue requires a two-pronged approach.

1. ESRMO will work with the State Legislative Policy team to revamp the cybersecurity laws to more accurately reflect only those incidents that are defined as "major security incidents" for a 24-hour reporting requirement.
2. ESRMO will continue to educate State Agencies on their incident reporting requirements.

ESRMO is also revamping the Incident Reporting Tool to address all other deficiencies noted by the auditor team. ESRMO plans to consolidate this capability within the EGRC tool for State Agencies and maintain a forward-facing tool to support citizens and business reporting.

Responsible Person: Maria Thompson, Chief Risk Officer, ESRMO
Expected Completion Date: First quarter of CY2017.

FINDING 9: GAPS IN STATE OVERSIGHT JEOPARDIZE AGENCY BUSINESS CONTINUITY AND DISASTER RECOVERY

RECOMMENDATIONS:
The State CIO should direct ESRMO to immediately track and assess agency business continuity and disaster recovery plans.

The State CIO should direct ESRMO to track and assess agency activation of business continuity and disaster recovery plans.

The State CIO should now and periodically evaluate ESRMO's processes to oversee the adequacy and activation of business continuity and disaster recovery plans consistent with law, current security needs, and best practices.

DIT Response: ESRMO will work with the DIT Shared Delivery Disaster Recovery personnel to develop a process to track and monitor Business Continuity Plan (BCP) activations, effectiveness and lessons learned. ESRMO will also introduce to the agencies, via the annual business continuity training tentatively planned for July 2016, that more in-depth tracking and assessment of agency business continuity and disaster recovery plans will begin with the 2016 BCP submissions to the State CIO.

The ESRMO will update the Statewide Information Security Manual, Chapter 7 – Business Continuity and Risk Management to include additional language pertaining to BCP activation, tracking, assessment, and evaluation to determine the adequacy of business continuity and disaster recovery plans.

Responsible Person: Maria Thompson, Chief Risk Officer, ESRMO
Expected Completion Date: First quarter of CY2017.

Thank you again for the opportunity to respond to the draft audit. DIT looks forward to working with the Office of State Auditor, or any others, to improve the security posture of the State and overall protection of the citizen's data.

Sincerely,

Keith Werner, State CIO

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' Watchdog

This audit was conducted in 3959 hours at an approximate cost of $391,941.