2020 NSAA INORMATION TECHNOLOGY CONFERENCE

Office of the State Auditor

IT Governance & Security Auditing in North Carolina

September 29, 2020

NC OSA
The Taxpayers' Watchdog

Introduction

Speaker Bio –

DWAYNE T. MCKINLEY, CPA, CGFM, CISA

North Carolina Office of the State Auditor- Information Systems Audit Supervisor

Dwayne is an Information Systems Audit Supervisor with the North Carolina Office of the State Auditor. He has over 30 years of experience in information systems implementation and IT auditing. Prior to joining the State of North Carolina in 2011, Mr. McKinley was a senior executive with a start-up consulting firm and a senior manager for Bearing Point/KPMG.

Dwayne is a graduate of Point Park University in Pittsburgh, Pennsylvania with a BS in Accounting, cum laude, and is a licensed CPA in the states of Maryland and North Carolina.

Dwayne spends his non-auditing hours either relaxing on the beach or fishing on a boat with his wife, Teresa, and their two grand-daughters, Ellie, age 7 and Paisley, age 3.

NC OSA
The Taxpayers' Watchdog

Presentation Outline

- Overview of the North Carolina Office of the State Auditor
- History of IT Governance & Security Auditing @ NCOSA
- Recent IT Governance & Security Audit - DIT
- Audit Lessons Learned
- Future of IT Governance & Security Auditing @ NCOSA
- Recap and Questions

NC$OSA
The Taxpayers' Watchdog

OVERVIEW OF THE NORTH CAROLINA OFFICE OF THE STATE AUDITOR

- Elected State Auditor
- 4 divisions with 120 audit staff
  - Financial Audit
  - Performance Audit
  - Special Investigations
  - Information System Audit

NC OSA
The Taxpayers' Watchdog

INFORMATION SYSTEMS AUDIT

- ISA Division with 21 full-time staff
  - 1 Director
  - 4 Supervisors
  - 16 full-time staff
- IT Performance Audits (State Agencies, Universities, & Community Colleges)
    - ITGC
    - Pre/Post Implementation
    - Security
- Integrated Financial Audits with the Financial Audit Division

NC OSA
The Taxpayers' Watchdog

INFORMATION SYSTEMS AUDIT – DATA

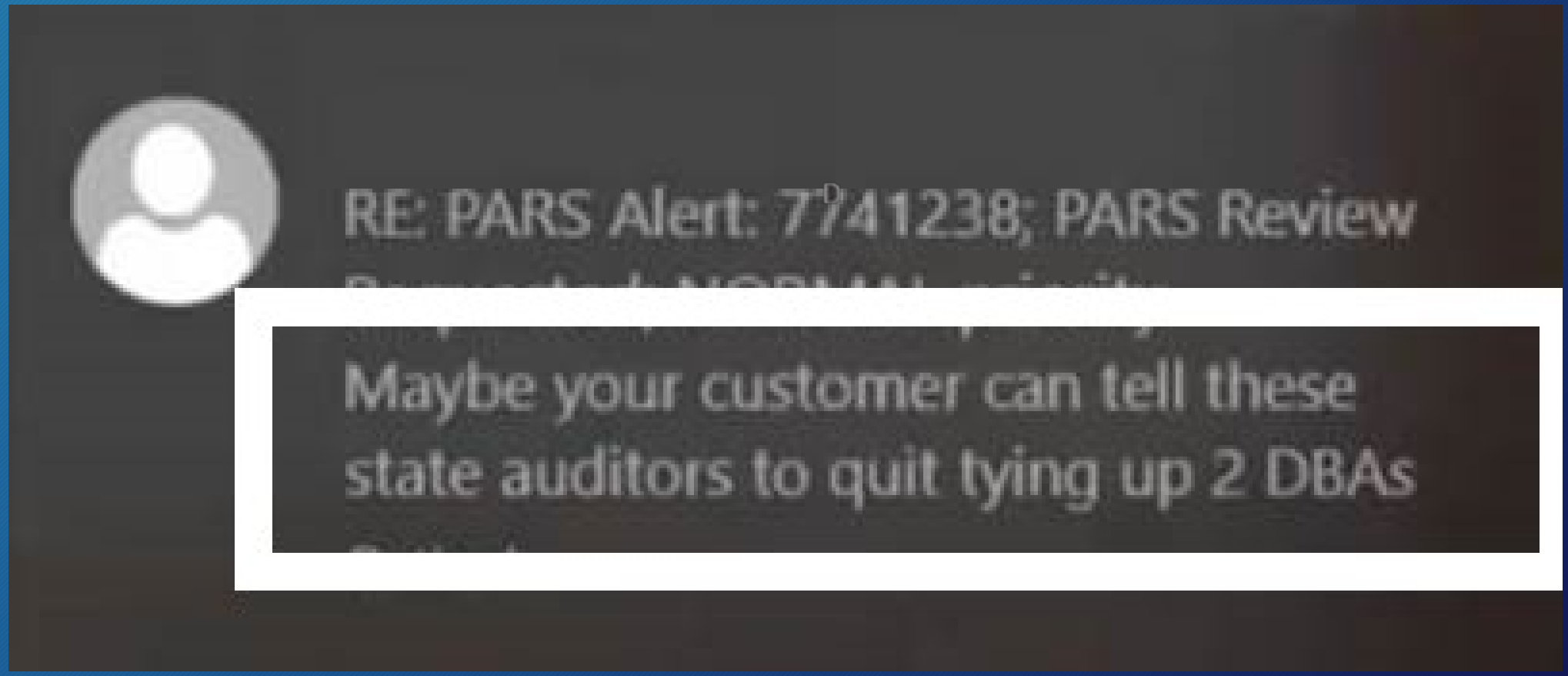
- Data Team
  - 1 supervisor & 6 staff
- Data Retrieval
- CAATs
- Data Analytics
  - Examining data relationships beyond typical audit
  - Identifying potential audit areas
  - AI & machine learning to identify risks & trends
- Robotics
  - Automating manual, redundant processes
  - Automating processes for efficiency

NC OSA
The Taxpayers' Watchdog

COVID-19 IMPACT

- **Adaptation of audit processes**
  - **Remote auditing**
  - **Technology focus**
    - Virtual conferencing (screen shots, recording, chat)
    - Secure file transfer (sFTP)
  - **Focused/refined audit scope**
    - Eliminated Physical Security
  - **Efficiencies realized**
    - Lower cost
    - Faster response

VIRTUAL FAUX PAS



HISTORY OF IT GOVERNANCE & SECURITY AUDITING

- Early 2000's
- Challenges of Financial vs Information Systems
  - Financial Controls Focused
  - Partnerships/Data retrieval
  - Performance Audits – COBIT deeper financial controls focused
  - Staff confusion on audit scope focus

NC OSA
The Taxpayers' Watchdog

HISTORY OF IT GOVERNANCE & SECURITY AUDITING

- 2010 and beyond
  - Re-engineering Partnership with Financial Audits
  - One Office/One Team
- 2011 Yellow Book
  - Re-engineering IT Performance Audits
- ITGC – State Information Security Manual & COBIT
- Pre/Post Implementation Audits
  - State's history of failed & over-budget IT projects
- FISCAM

NC OSA
The Taxpayers' Watchdog

HISTORY OF IT GOVERNANCE & SECURITY AUDITING

Recent History

- Governance
- Pre/Post Implementation Audits
  - Statewide Financial System
  - Statewide eCourt System
- Governance & Security – CIS Controls

NC OSA
The Taxpayers' Watchdog

ATTENDANCE CHECK

OVERVIEW OF DIT

NC Department of Information Technology

- Primary IT Service Provider for State Agencies
- Leadership of the Secretary & State CIO; Cabinet Level Agency
- Consolidation of Executive Branch IT Functions
- Wide Range of IT Operations
- Charged with Governance & Security
- NIST Security Standard

WHY WE DID THIS AUDIT

- **DIT central to CAFR & Single Audit**
- **Annual Integrated Financial Audit**
- **Bi-annually IT Performance Audit**
  - First re-engineered audit - 2012
- **Initial Risk Assessment**

NC OSA
The Taxpayers' Watchdog

WHAT TO AUDIT

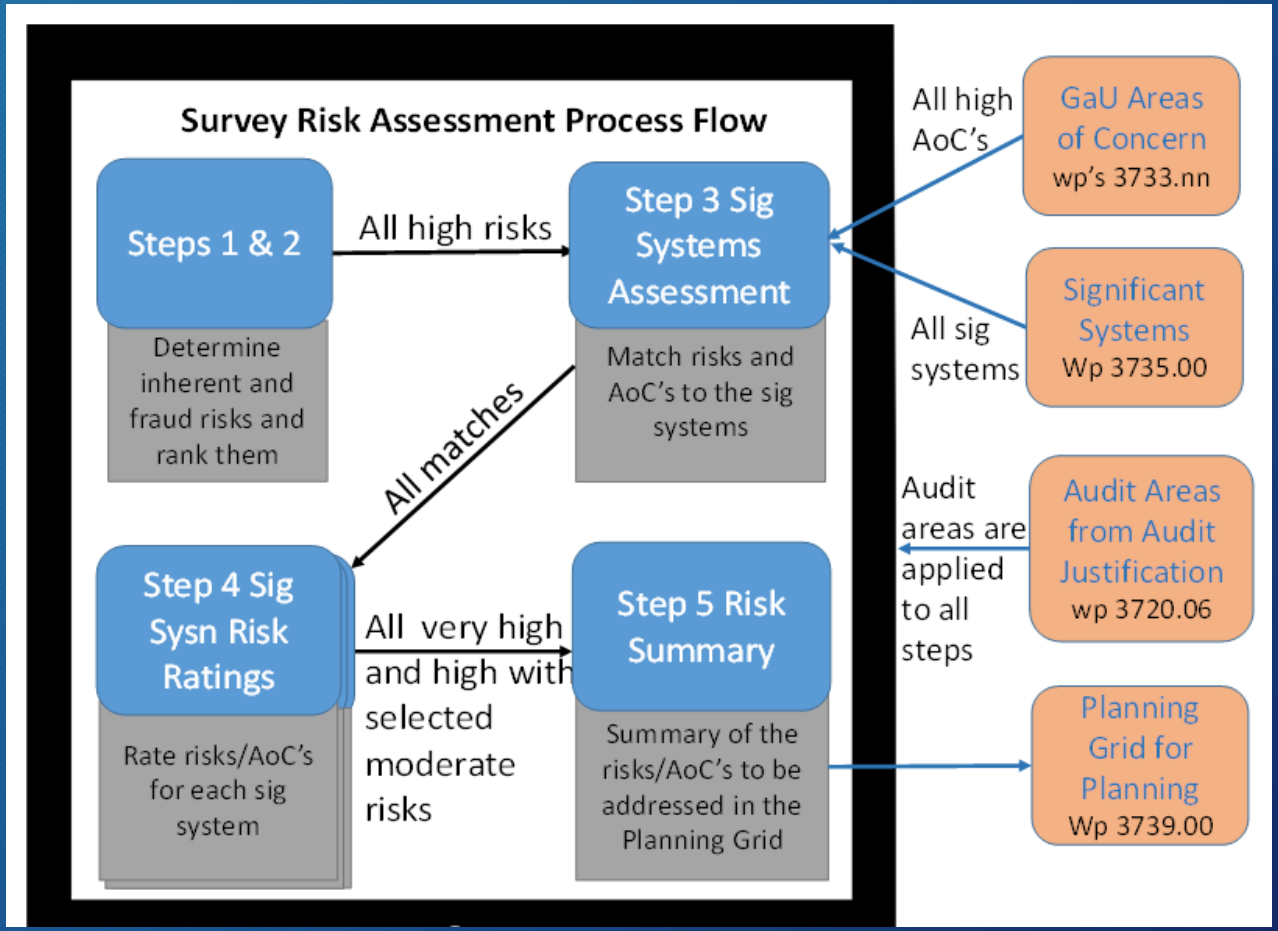
NC OSA
The Taxpayers' Watchdog

METHODOLOGY

- **Audit Period March – December 2019**
- **2011 Yellow Book**
- **COBIT & Statewide Information Security Manual (NIST)**
- **Risk based approach**
- **Procedures**
  - Key mangers
  - Policies, laws, best practices
  - Observation of process
  - Examination of audit evidence

NC OSA
The Taxpayers' Watchdog

RISK ASSESSMENT BLACK BOX



NC OSA
The Taxpayers' Watchdog

OBJECTIVE POPULATION

- We applied guidance contained in COBIT to arrive at eight possible IT audit areas:
  1. IT Governance & Operations Management (GOV)
  2. Security Management (SM)
  3. Hardware and Software Infrastructure (HS)
  4. Logical Access (LA)
  5. Physical & Environmental Controls (PE)
  6. Network Perimeter Security (NP)
  7. Change Management (CM)
  8. Disaster Recovery and Contingency Plan (DR)

INITIAL OBJECTIVES

- IT Control Objectives
  - Governance
    - IT strategy
    - IT supporting business goals & objectives
    - Value measurement
    - Management of IT Risk
  - Security Management
    - Security governance program
    - Security Awareness
    - Monitoring & identification of risks & vulnerabilities
    - Vendor Management

NC OSA
The Taxpayers' Watchdog

SURVEY RESULTS

- No Governing or Oversight Board
  - August 2019
  - Legislature Enacted
  - IT Strategy Board
  - State Auditor
  - Initial Meeting: March 2020
- Several State CIO leadership changes

NC OSA
The Taxpayers' Watchdog

RISK BASED OBJECTIVES

- IT Risk Assessment
  - Risk Management policy is not being followed
  - All risks may not be identified
  - No analysis of impact and probability.
- 3rd Party Vendor Mgmt
  - No consistent monitoring of vendors' performance against contracts

NC OSA
The Taxpayers' Watchdog

FINDINGS & CONCLUSIONS

- IT Risk Assessment Not Comprehensive
  - Included only Security & Availability
  - Other risks omitted
  - No response to risks
    - Mitigate, Manage & Monitor
  - Effects
    - Risks not effectively managed
    - Increased risk exposure
    - Inappropriate or no response
    - Overall understanding of IT Risks
  - Recommendations
    - Thorough risk assessment
    - Implement activities to Mitigate, Manage & Monitor

NC OSA
The Taxpayers' Watchdog

FINDINGS & CONCLUSIONS

- No monitoring of 3rd parties
  - Acceptable quality
  - Efficiently, effectively, securely, reliably, etc.
  - Effects
    - Overpayment for services
    - Services not provided
    - Did not meet requirements
    - Additional contracts
  - Recommendations
    - Monitor vendors
    - Continuous process
    - Perform timely renewal analyses

NC OSA
The Taxpayers' Watchdog

MANAGEMENT'S REACTION/RESPONSE

- Agree, but we do it
- Pushback on criteria
- Realigned processes
- Created a new position
- Implement a Contract Mgmt tool

NC OSA
The Taxpayers' Watchdog

AUDIT LESSONS LEARNED

- Management's agreement on criteria
- Agreement on Issues with Management
- Timely communication with Audit Mgmt

NC OSA
The Taxpayers' Watchdog

AUDIT APPROACH PUNCHLIST

- COVID-19 impact
- Risk Assessment Refinement
- Adoption of 2019 Yellow Book
- Disclosure of internal control significant to audit objectives
- COBIT 2019 Alignment
- University Security Audits

NC OSA
The Taxpayers' Watchdog

UNIVERSITY SECURITY AUDITS

- Center for Internet Security (CIS ver 7.1) top 6 audit methodology
  - CIS1 - Inventory of Hardware Assets
  - CIS2 - Inventory of Software Assets
  - CIS3 - Continuous Vulnerability Management
  - CIS4 - Controlled use of Administrative Privileges
  - CIS5 - Secure configurations for Hardware and Software
  - CIS6 - Maintenance, Monitoring and Analysis of Audit Logs

Recap

- Overview of the North Carolina Office of the State Auditor
- History of IT Governance & Security Auditing @ NCOSA
- Recent IT Governance & Security Audit - DIT
- Audit Lessons Learned
- Future of IT Governance & Security Auditing @ NCOSA

NC$OSA
The Taxpayers' Watchdog

QUESTIONS

Dwayne T. McKinley, CPA, CISA, CGFM
Information Systems Audit Supervisor
(919) 807-7500
Dwayne_McKinley@NCAuditor.net

2 South Salisbury Street
20601 Mail Service Center
Raleigh, NC 27699-0600

https://www.auditor.nc.gov

NC OSA
The Taxpayers' Watchdog