OFFICE OF INDEPENDENT INTERNAL AUDIT

DeKalb County
GEORGIA

Office of Independent Internal Audit
Excellence. Integrity. Objectivity. Respect

July 2024

DeKalb County Government
County-wide

CYBERSECURITY GOVERNANCE AUDIT
FINAL REPORT

Lavois Campbell, CIA, CISA, CFE, CGA
Chief Audit Executive

Audit Report No. IA-2022-120-IT

REDACTION NOTICE

Sections of this audit report have been redacted to protect information, "which if made public could compromise security against sabotage, criminal or terroristic acts."
O.C.G.A § 50-18-72(25)(A).

OFFICE OF INDEPENDENT INTERNAL AUDIT

DeKalb County
GEORGIA

Office of Independent Internal Audit
Excellence. Integrity. Objectivity. Respect.

Lavois Campbell
Chief Audit Executive

CYBERSECURITY GOVERNANCE AUDIT REPORT NO. Audit Report No. IA-2022-120-IT

HIGHLIGHT SUMMARY

Why We Performed the Audit

In accordance with the Office of Independent Internal Audit (OIIA) annual audit plan, we conducted a Cybersecurity Governance Audit. The purpose of the audit was to evaluate and assess the County's Cyber Security framework, policies, controls, and procedures developed to safeguard the County's cyber activities from cyber-attacks and their crippling effects.

In today's interconnected world, where technology is deeply integrated, ensuring the security of information systems has become critical. Like most organizations, DeKalb County depends on digital systems to conduct business and collects, stores, and transmits sensitive and personally identifiable information and other information electronically. In the face of developing and increasing threats to and attacks on both the information stored and the computer systems that store such information, organizations are considering how to best protect their Information systems by developing effective policies, procedures, and controls to identify, protect, detect, respond and to recover from cybersecurity attacks. Cyber-attacks can have some crippling effects on organizations, such as destroying their reputations, disrupting their businesses, and causing huge financial losses.

According to a recent threat landscape survey published by the Information Systems Audit and Control Association (ISACA) in the State of Cybersecurity 2023 (Global Update on Workforce Efforts, Resources, and Cyber Operations), thirty-eight percent of respondents indicated that their organization is experiencing more cyber attacks than a year ago, thirty-one percent responded same, twenty percent preferred not to answer, and eleven percent responded fewer attacks.

How We Performed the Audit

The audit focused on the Department of Information Technology's (DoIT) current Cyber Security Governance processes. Our methodology included, but was not limited to, the following:

- Reviewed the policies and procedures relating to the Information Technology Department and related best practices.
- Selected and tested a sample of controls.
- Interviewed the concerned stakeholders.

Background

DeKalb County and its various departments and agencies provide essential services to its citizens. To provide these services, the departments utilize various applications to collect, record, and process the County resident's sensitive data and personally identifiable information (PII) to provide these services. Therefore, information systems governance is highly relevant in today's digital landscape.

Cyber Security governance is critical for Dekalb County to help identify and protect against potential vulnerabilities, respond to incidents promptly. The Department of Information Technology (DoIT) has the responsibility to set policy and provide guidance and oversight for the security and privacy of all the IT systems

What We Found

[redacted]

	Audit Findings	[redacted]
[redacted]	[redacted]	
[redacted]	[redacted]	
[redacted]	[redacted]	
[redacted]	[redacted]	
[redacted]	[redacted]	
[redacted]	[redacted]	
[redacted]	[redacted]	
[redacted]	[redacted]	
[redacted]	[redacted]	
[redacted]		

🟩	Low risk
🟨	Medium Risk
🟥	High Risk

What We Recommend

We recommend that DoIT management take steps to address the control process deficiencies identified in this report.

How Management Responded

A total of 10 exceptions were noted and Management agreed to 6 in their entirety. Management partially agreed to the remaining 4.

TABLE OF CONTENTS

BACKGROUND AND INTRODUCTION

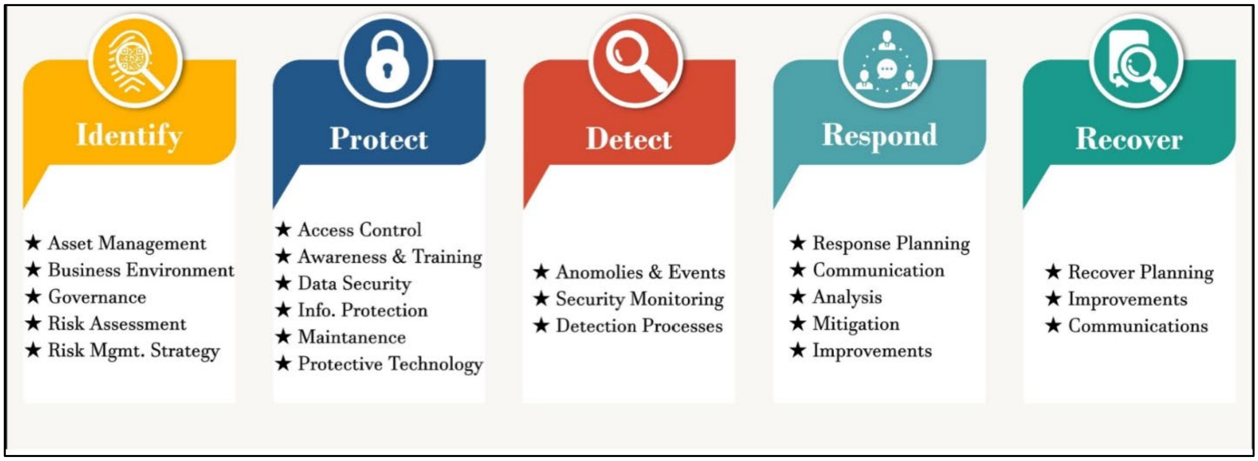
Cybersecurity is paramount in today's digital age, particularly for government entities entrusted with sensitive information. It is defined as protecting electronic information and communications systems to ensure confidentiality, integrity, and availability. In today's digital age, the protection of sensitive data stored by the government, military, corporate, financial, and medical organizations is of the utmost importance. With the increasing frequency and complexity of cyber-attacks, it is crucial for organizations to strengthen their information technology (IT) infrastructure through well-defined governance structures, policies, and controls.

Federal regulations, such as the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act (HIPAA), and the Federal Information Security Management Act (FISMA), mandate stringent cybersecurity measures. The consequences of cybersecurity breaches are severe, ranging from reputational damage to financial losses. Recent major data breaches in government agencies and private organizations underscore the urgent need for comprehensive cybersecurity measures.

Like many organizations, DeKalb County relies on information technology infrastructure to deliver programs and services, necessitating collecting, storing, and transmitting sensitive data. The Department of Innovation and Technology (DoIT) oversees the County's IT resources and cybersecurity efforts. It is responsible for establishing and enforcing technology and data security policies. User departments are also responsible for helping to mitigate the risk of data breaches.

Aligned with the National Institute of Standards and Technology (NIST) Framework, DeKalb County's cybersecurity measures encompass five components: Identify, Protect, Detect, Respond, and Recover. These measures include policy development, governance oversight, risk management, cybersecurity training, incident response and disaster recovery planning, and regular testing.

Five NIST Cybersecurity Framework Components



WHY WAS THIS AUDIT PERFORMED

Given the increasing sophistication of cyber threats and the critical role of IT systems in County operations, assessing the adequacy of cybersecurity measures is imperative to safeguard sensitive information and maintain operational resilience.

OUR SCOPE AND METHODOLOGY

The primary goal of this audit was to assess the adequacy and effectiveness of the County's cybersecurity governance processes, including the necessary structures, policies, procedures, and mechanisms to manage cybersecurity risks effectively. The main criterion was the NIST SP 800-53 cybersecurity framework. This audit did not test the operating effectiveness of the controls but focused on the implementation and design of the controls. Our methodology included but was not limited to the following: researched related best practices; reviewed current County cybersecurity-related policies and procedures; reviewed supporting documentation; interviewed appropriate County personnel; and reviewed other applicable documentation and information.

AUDIT RESULTS

[redacted] Detailed findings and recommendations for improvement are outlined in the report.

Finding 1: [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Recommendation:

[redacted]

[redacted]

Management Response (DoIT Management):

Management Agreement	*Description of Management's Action Plan to Address Finding*	*Estimated Timeline to Implement Action Plan*
☒ Agree ☐ Disagree	[redacted]	[redacted]
Reason For Disagreement:		

~~Finding 2:~~ [redacted]

[redacted]

Control Area	Control	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]		[redacted]
[redacted]		[redacted]

[redacted]

[redacted]

Recommendation:

We recommend that DoIT Management revise the ISP-[redacted]-
[redacted]

Management Response (DoIT Management):

Management Agreement	*Description of Management's Action Plan to Address Finding*	*Estimated Timeline to Implement Action Plan*
☒ Agree ☐ Disagree	[redacted]	[redacted]
***Reason For Disagreement*:**		

Finding 3: [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Recommendation:

We recommend that DoIT management should:

[redacted]

[redacted]

Management Response (DoIT Management):

Management Agreement	*Description of Management's Action Plan to Address Finding*	*Estimated Timeline to Implement Action Plan*
☒ **Agree** ☐ **Disagree**	[redacted]	[redacted]
Reason For Disagreement:		

Finding 4: [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Recommendation:

We recommend that DoIT management should:

[redacted]

Management Response (DoIT Management):

Management Agreement	*Description of Management's Action Plan to Address Finding*	*Estimated Timeline to Implement Action Plan*
☒ Partially Agree ☐ Disagree	[redacted]	[redacted]

	[redacted]	
Reason For Disagreement:		

Finding 5:-[redacted]

[redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Recommendation:

We recommend that the DoIT management do the following:

[redacted]

Management Response (DoIT Management):

Management Agreement	*Description of Management's Action Plan to Address Finding*	*Estimated Timeline to Implement Action Plan*
☒ Partially Agree ☐ Disagree	[redacted]	[redacted]
Reason For Disagreement:		

Finding 6:- [redacted]

[redacted]

[redacted]–

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]-

[redacted]

[redacted]

[redacted]

Recommendation:

Based on the findings, we recommend that DoIT Management should:

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

Management Response (DoIT Management):

Management Agreement	*Description of Management's Action Plan to Address Finding*	*Estimated Timeline to Implement Action Plan*
☒ Partially Agree ☐ Disagree	[redacted]	[redacted]

	[redacted]	
Reason For Disagreement:		

Finding 7: [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Recommendation:

We recommend that DoIT management should:

[redacted]

Management Response (DoIT Management):

Management Agreement	*Description of Management's Action Plan to Address Finding*	*Estimated Timeline to Implement Action Plan*
☒ **Agree** ☐ **Disagree**	[redacted]	[redacted]
Reason For Disagreement:		

Finding 8: [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted]

Recommendation:

We recommend that DoIT management should:

- [redacted]
- [redacted]
- [redacted]
- [redacted]

Management Response (DoIT Management):

Management Agreement	*Description of Management's Action Plan to Address Finding*	*Estimated Timeline to Implement Action Plan*
☒ **Agree** ☐ **Disagree**	[redacted]	[redacted]
***Reason For Disagreement**:*		

Finding 9: [redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

- [redacted]
- [redacted]

Recommendation:

Based on our findings, we recommend that DOIT do the following:

- [redacted]
- [redacted]

[redacted]

Management Response (DoIT Management):

Management Agreement	***Description of Management's Action Plan to Address Finding***	***Estimated Timeline to Implement Action Plan***
☒ **Partially Agree** ☐ **Disagree**	[redacted]	[redacted]
Reason For Disagreement:		

Finding 10: [redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted]

Recommendation:

To ensure compliance with NIST requirements, we recommend that DoIT Management should:

[redacted]

Management Response (DoIT Management):

Management Agreement	*Description of Management's Action Plan to Address Finding*	*Estimated Timeline to Implement Action Plan*
☒ **Agree** ☐ **Disagree**	[redacted]	[redacted]
Reason For Disagreement:		

APPENDICES

Appendix I – Purpose, Scope, and Methodology

Purpose

The objective was to assess the County's Cybersecurity governance processes. The current cybersecurity activities and procedures were evaluated against the Cybersecurity guidelines issued by the National Institute of Standards and Technology (NIST) and County policies to identify areas for improvement.

Scope and Methodology:

The scope of our audit focused on the current cybersecurity governance practices and processes.

Our methodology included evaluating the County's governance practices against the guidelines issued by NIST 800-53 and the five elements of the NIST Framework for cybersecurity (Identify, Protect, Detect, Respond, and Recover). It also included but was not limited to the following:

- Researched related best practices.
- Reviewed current County Information Security and cybersecurity-related policies and procedures.
- Interviewed appropriate County personnel and the Department of Innovation and Technology.
- Reviewed other applicable documentation and information.

Appendix II – Management Response

DEPARTMENT OF
INNOVATION & TECHNOLOGY

DeKalb County
GEORGIA

OFFICE OF CIO & DIRECTOR
JOHN A. MATELSKI

June 21, 2024

Lavois Campbell
Chief Audit Executive
Office of Independent Internal Audit
1300 Commerce Drive, Suite 300
Decatur, Georgia 30030

RE: **Management Response to "Cybersecurity Governance *Audit Report No. IA-2022-120-IT"***

Dear Mr. Campbell:

In accordance with DeKalb County, Georgia – Code of Ordinances / Organizational Act Section10A- Independent Internal Audit, this is our response to the audit named above provided in this document. As required by the ordinance, our response includes 1) a statement regarding our agreement or disagreement along with reasons for any disagreement, 2) our plans for implementing solutions to issues identified, and 3) the timetable to complete such plans.

If you have any questions about this response, please contact John Matelski, CIO, Department of Innovation & Technology (DoIT).

Sincerely,

John Matelski, Chief Information Officer, Department of Innovation & Technology

Appendix III – Definitions and Abbreviations

Acronyms and Abbreviation

DoIT: Department of Innovation and Technology
HR: Human Resources
PII: Personally Identifiable Information
OIIA: Office of Independent Internal Audit
IT: Information Technology
HIPAA: Health Insurance Portability and Accountability Act
FISMA: Federal Information Security Management Act
NIST: National Institute of Standards and Technology
ISP: Information Security Policy
ISO: Information Security Officer
COO: Chief Operating Officer
CEO: Chief Executive Officer
DEMA: DeKalb County Emergency Management Agency
CM: Configuration management
CP: Contingency Planning
CIRT: Cyber Incident Response Team
CIO - Chief Innovation & Information Officer

Key Definitions

[redacted] This is a software-based solution designed to track and recover stolen or lost computers. It is used to track assets and protect sensitive information.

Governance Team – A Group of individuals responsible for overseeing and ensuring the effective management, control, and alignment of information technology within an organization.

Appendix IV

NIST Special Publication 800-53 - Recommended Security Controls.

	Controls	Policies (Y/N)	Procedures (Y/N)
[redacted]	[redacted] –	[redacted]	[redacted]
[redacted]	[redacted] –	[redacted]	[redacted]
[redacted]	[redacted] –	[redacted]	[redacted]
[redacted]	[redacted] –	[redacted]	[redacted]
[redacted]	[redacted] –	[redacted]	[redacted]
[redacted]	[redacted] –	[redacted]	[redacted]
[redacted]	[redacted] –	[redacted]	[redacted]
[redacted]	[redacted] –	[redacted]	[redacted]
[redacted]	[redacted] –	[redacted]	[redacted]
[redacted]	[redacted] –	[redacted]	[redacted]
[redacted]	[redacted] –	[redacted]	[redacted]
[redacted]	[redacted] –	[redacted]	[redacted]
[redacted]	[redacted] –	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted] –	[redacted]	[redacted]
[redacted]	[redacted] –	[redacted]	[redacted]
[redacted]	[redacted] –	[redacted]	[redacted]
[redacted]	[redacted] –	[redacted]	[redacted]

Appendix V - Cyber Security Awareness & Training

[redacted]

[redacted]

DISTRIBUTION

Action Official Distribution:

John Matelski, Chief Information Officer and Director of Innovation and Technology

Statutory Distribution:

Michael L. Thurmond, Chief Executive Officer

Robert Patrick, Board of Commissioners District 1

Michelle Long-Spears, Board of Commissioners District 2

Steve Bradshaw, Board of Commissioners District 4

Mereda Davis Johnson, Board of Commissioners District 5

Ted Terry, Board of Commissioners District 6

Gloria G. Gray, Chairperson, Audit Oversight Committee

Adrienne T. McMillion, Vice-Chairperson, Audit Oversight Committee

Tanja Christine Boyd-Witherspoon, Chairperson pro-tem

Lisa Earls, Audit Oversight Committee

Harold Smith, Audit Oversight Committee

Information Distribution:

Zachary L. Williams, Chief Operating Officer/ Executive Assistant

Vivian Ernstes, County Attorney

La'Keitha D. Carlos, CEO's Chief of Staff

Kwasi K. Obeng, Chief of Staff, Board of Commissioners

PROJECT TEAM

This report was submitted by:

Juile Ikioda

7.5.2024

Julie Ikioda, CISA, PMP
IT Internal Auditor, Senior
Office of Independent Internal Audit

Date

AND

7.5.2024

Toluwatope Ologbenla, MBA, CISA, CISM, PMP, CSM
IT Internal Auditor, Senior
Office of Independent Internal Audit

Date

This report was reviewed by:

maxwell Addico

7.5.2024

Maxwell Addico, CISA, ISO 27001 (LA)
IT Audit Manager
Office of Independent Internal Audit

Date

The report was approved by:

Lavois Campbell

7.5.2024

Lavois Campbell, CIA, CISA, CFE, CGA
Chief Audit Executive
Office of Independent Internal Audit

Date

STATEMENT OF ACCORDANCE

The mission of DeKalb County is to make the priorities of the citizens of DeKalb County; the priorities of County government - by achieving a safer DeKalb, building stronger neighborhoods, creating a fiscally accountable and more efficient county government, and uniting the citizens of DeKalb County.

The mission of the Office of Independent Internal Audit is to provide independent, objective, insightful, nonpartisan assessment of the stewardship or performance of policies, programs, and operations in promoting efficiency, effectiveness, and integrity in DeKalb County.

This performance audit was prepared pursuant to DeKalb County, Georgia – Code Ordinances/Organizational Act Section10A- Independent Internal Audit. 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 report is intended for the use of the agency to which it was disseminated and may contain information that is exempt from disclosure under applicable law. Do not release without prior coordination with the Office of Independent Internal Audit.

Please address inquiries regarding this report to the Office of Independent Internal Audit at 404-831-7946.