Okaloosa County
Clerk Of Circuit Court

Department of Inspector General

Information Technology Cybersecurity Audit

REPORT NO. COC 25-01

REPORT ISSUED OCTOBER 21, 2025

ISSUED BY: RENEE FENNELL LARKEY, INSPECTOR GENERAL

DEPARTMENT OF INSPECTOR GENERAL

OKALOOSA COUNTY, FLORIDA

BRAD EMBRY, CLERK OF CIRCUIT COURT AND COMPTROLLER

October 21, 2025

Brad Embry
Clerk of Circuit Court & Comptroller
Okaloosa County Administration Building
101 E. James Lee Blvd
Crestview, FL 32536

Clerk Embry,

Please find attached the final report on our compliance review of the Local Government Cybersecurity Act as delineated in Florida Statute 282.3185.

Our office would like to thank Byran Follmar and his staff for the cooperation and accommodation afforded us. Should you have any questions please do not hesitate to call me at (850) 689-5000 Ext. 3432.

Respectfully,

Renee F. Larkey

Renee F. Larkey, Inspector General

CC: John Anderson, Chief Deputy of Operations
Bryan Follmar, IT Director

Contents

Introduction

Based on the 2024 County-wide Risk Assessment, the Department of Inspector General 2025 Audit Plan included an examination of the Okaloosa County Clerk of the Court and Comptroller's (Clerk) compliance with Florida Statute 282.3185. Public awareness of the Clerk's office is elevated because of its work which involves recording public records and receiving filings for court cases. Compliance with 282.3185 is required by Florida Law and reflects the Clerk's commitment to the protection of computer resources and information on file with the Clerk's office.

Objective

The objective of this audit is to assess the Okaloosa Clerk of the Circuit Court and Comptroller's compliance with the Local Government Cybersecurity Act (ACT) requirements as delineated in Florida Statute 282.3185.

Scope and Methodology

The scope of our audit includes cybersecurity awareness and training activities as well as any incident notifications made during the period 10-1-24 through 9-30-25. The scope includes notification made to Florida Digital Services of the adoption of cybersecurity standards made by the Clerk as of the date of notification. Our audit methodology included interviews with the Clerk Information Technology (IT) staff, contact and verification with Florida Digital Services, obtaining pertinent training reports from Clerk IT and Human Resources (HR) departments.

Note: The Clerks' former IT Director left employment on May 1, 2025, and the new IT Director commenced employment May 19, 2025. This management change occurred during the audit scope timeframe.

Management is responsible for ensuring compliance and adequate safeguarding of public resources from fraud, waste, or abuse. This includes the design, implementation, and maintenance of internal controls relevant to the objectives. This review was conducted in compliance with Standards for Offices of Inspector General issued by the Association of Inspectors General and the International Professional Practice Framework issued by the Institute of Internal Auditors.

Background

The Florida Cybersecurity Act establishes cybersecurity requirements for state agencies. The Local Government Cybersecurity Act extends similar obligations to counties and municipalities and became effective July 1, 2022. The **relevant portions** of the ACT are shown below:

Section 282.3185 Local government cybersecurity—

(1) SHORT TITLE. - This section may be cited as the "Local Government Cybersecurity Act."

(2) DEFINITION. – As used in this section, the term "local government" means any **county** or municipality.

(3) CYBERSECURITY TRAINING. –

(a) The Florida Digital Service shall:

1. Develop a basic cybersecurity training curriculum for local government employees. **All local government employees with access to the local government's network must complete the basic cybersecurity training within 30 days after commencing employment and annually thereafter.**

2. Develop an advanced cybersecurity training curriculum for local governments which is consistent with the cybersecurity training required under s. 282.318(3)(g). **All local government technology professionals and employees with access to highly sensitive information must complete the advanced cybersecurity training within 30 days after commencing employment and annually thereafter.**

(4) CYBERSECURITY STANDARDS. –

(a) **Each local government shall adopt cybersecurity standards that safeguard its data, information technology, and information technology resources to ensure availability, confidentiality, and integrity. The cybersecurity standards must be consistent with generally accepted best practices for cybersecurity, including the National Institute of Standards and Technology Cybersecurity Framework.**

(b) **Each county with a population of 75,000 or more must adopt the cybersecurity standards required by this subsection by January 1, 2024**. Each county with a population of less than 75,000 must adopt the cybersecurity standards required by this subsection by January 1, 2025.

(d) **Each local government shall notify the Florida Digital Service of its compliance with this subsection as soon as possible.**

(5) INCIDENT NOTIFICATION. –

(a) **A local government shall provide notification of a cybersecurity incident or ransomware incident to the Cybersecurity Operations Center, Cybercrime Office of the Department of Law Enforcement, and sheriff who has jurisdiction over the local government in accordance with paragraph (b)…….**

(b)1. **A local government shall report all ransomware incidents and any cybersecurity incident determined by the local government to be of severity level 3, 4, or 5 as provided in s. 282.318 (3)(c) to the Cybersecurity Operations Center, the Cybercrime Office of the Department of Law Enforcement, and the sheriff who has jurisdiction over the local government as soon as possible but no later than 48 hours after discovery of the cybersecurity incident and no later than 12 hours after discovery of the ransomware incident…….**

The Legislature did not contemplate or provide for penalties to address non-compliance with the Act.

The Clerk IT Director provided the following framework(s) for definitions of basic and advanced cybersecurity and annual cybersecurity training:

Basic Cybersecurity Training:

- **Clerk Policy**
  - 7415 - Artificial Intelligence Usage Policy
  - 7617 - Computer System Acceptable Use Policy
  - 7619 - Agency Issued Technology
  - 8110 - Password Policy
  - 8115 - Email Encryption Policy
  - 8117 - Cyber Security Awareness and Training Policy
  - 8118 - Multifactor Authentication Policy
  - 8120 - Incident Response (this one is new and assigned to all new and current users to complete)
- **KnowBe4 Training** (Security awareness training and simulated phishing platform)
  - Initial Training for All Users - Links and Attachments: Think Before You Click
  - Initial Training for All Users - Using the Phish Alert Button: Report Suspicious Emails Using Microsoft Outlook
  - Initial/Annual Training for All Users - Security Awareness Training 2025
- **CJIS** (Criminal Justice Information Services)
  - CJIS Security and Privacy: Security Role training

Advanced Cybersecurity Training:

- **Clerk Policy**
  - 8108 - Clerk Help Desk Policy
  - 8109 - Elevated Privileges User Account Access Policy
  - 8112 - Change Management Policy
  - 8113 - Patch Management Policy
  - 8120 - Incident Response (the second part of this policy is for IT dept)
- **SOP** – Standard Operating Procedures

- Announcement on HelpDesk (Marquee)
- Benchmark - New Hire and Termination - Account Set up and disable
- CSI Redaction Service location for Benchmark
- Delete a User from the domain
- Switch IOS update
- Creating a user in Hybrid Exchange server
- Access Permissions for Each Department's New Hires

Annual Training:

- **Knowbe4 Training**:
  - Initial/Annual Training for All Users - Security Awareness Training 2025

- **CJIS Security and Privacy**:
  - Security Role training

The Clerk IT department monitors the applicable training provided via KnowBe4 and CJIS. The Clerk HR department monitors the Power DMS training provided initially and annually to Clerk staff.

Testing

Testing was conducted to determine if the requirements mandated in Florida Statute 282.3185 were met by the Clerk's office. Testing involved obtaining verification of the Clerks submission of an attestation reflecting adoption of cybersecurity standards, reviewing training documents to validate compliance with the training requirements, and ascertaining if the Clerk had incidents that required notification to appropriate authorities as shown in the ACT. Our testing included a review of all Clerk staff for annual training requirements, review of all new staff completing initial training and a review of all new IT staff completing initial advance IT training.

Conclusion

The Clerk submitted the Local Governance Cybersecurity Standards Attestation form to Florida Digital Service on May 14, 2024, indicating the Clerk had adopted Cybersecurity Standards as of January 1, 2024. This submission satisfied section (4) (d) of the Act as it indicates to submit the attestation as soon as possible without providing a hard compliance date.

As required by Section 282.3185(4)(d), Florida Statutes (F.S.), each local government shall notify the Florida Digital Service of its compliance with the subsection as soon as possible.	
Local Government Organizational Name: Please indicate the name of the local government which you are representing:	Okaloosa County Clerk of Circuit Court
Please indicate if your organization has adopted Cybersecurity Standards.	Yes
Adopted Cybersecurity Standards Please indicate which cybersecurity standards your organization has adopted:	"REDACTED"
Date of Adoption:	01/01/24
If you have not adopted cybersecurity standards, please indicate what cybersecurity standards you will be adopting:	
Date of when you plan to adopt:	

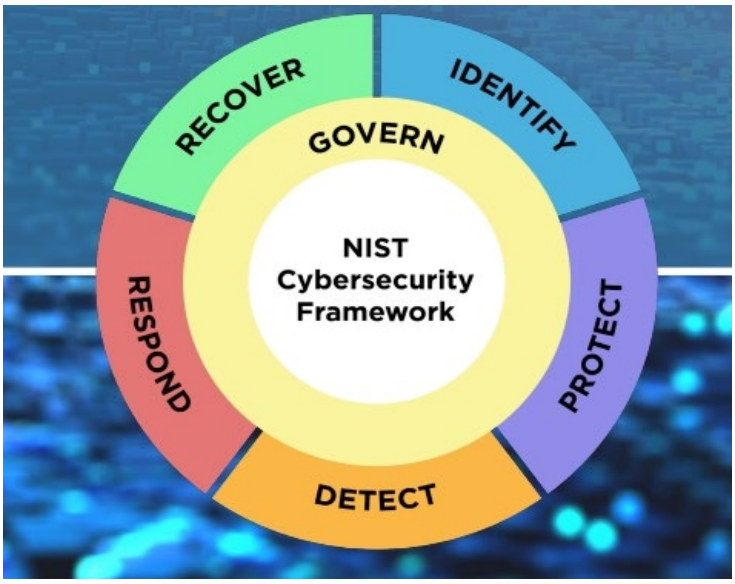
Our testing of the annual training required by the Act found that the Clerk staff had 99% training compliance. One employee failed to complete the training timely, but this was mitigated by the fact the employee left employment just outside the annual training campaign window.

Testing of new employees' initial training found the following:

Initial Power DMS policy training – * 91% on-time compliance.
Initial KnowBe4 cybersecurity training – * 82% on-time compliance.
Initial CJIS Security and Privacy Training – * 27% on-time compliance.
* The percentages include the new (non-management) IT employee hired in the timeframe of the audit.

Testing of the new (non-management) IT staff members' Advanced IT Training found that one of the Advanced IT Training policies was completed outside the 30-day initial training window. The IT Advanced SOP reviews completed by new IT staff are currently not tracked or logged so compliance of these were indeterminate for the audit.

Based on a cross walk of Clerk Policies and the National Institute of Standards and Technology Cybersecurity Framework (NIST) completed by this office, the Clerk Policies referencing cybersecurity are compliant with the NIST framework after the addition of Clerk policy 8120 - Incident Response on August 29, 2025. The framework references the following items:



This framework is designed to help organizations manage and reduce their cybersecurity risks.

We are pleased to report that as of the completion date of our audit, all training required (exclusive of Advanced IT SOP's which are not tracked) has been completed by staff currently employed by the Okaloosa Clerk of the Circuit Court and Comptroller.

The Clerks office had no reportable cybersecurity or ransomware incidents in the audit scope timeframe.

Recommendations:

Audit recommendations are provided to mitigate process risks and improve programs and operations.

Recommendation 1:

The Clerks' IT and Human Resources departments should consider a method to track training completion of Initial, CJIS and Advanced IT training to improve on-time training compliance. The Clerk IT Director indicated he is already working on a tracking mechanism for SOP completion in the department.

Recommendation 2:

Because the Clerks' office uses a combination of Clerk Policies, SOP's, CJIS, and KnowBe4 training as the basis of its' cybersecurity training, consideration should be given to making a formalized document or training plan that enumerates and defines what is inclusive of cybersecurity training for staff.

Audit Findings:

Audit findings are a summary of operational weakness, deficiencies, adverse conditions, or the need for process changes.

Finding 1:

Condition: A low on-time compliance rate was found for completion of CJIS and KnowBe4 initial training.

Criteria: The Local Government Cybersecurity Act requires completion of training within 30 days of employment and on an annual basis.

Cause: Review of training reports found that in some cases staff were not enrolled in the training by IT within the 30-day window, therefore there was not a mechanism for staff to be compliant within the training timeframe.

Effect: Staff were not compliant with the 30-day training window provided in the Local Government Cybersecurity Act.

Recommendation: CJIS and KnowBe4 training should be issued to newly employed staff within the 30-day window provided for cybersecurity training completion.

Management Response:

Management acknowledges the finding regarding the low on-time compliance rate for CJIS and KnowBe4 initial training.

The delay in training compliance was primarily due to a gap in the onboarding process, as well as the fact that CJIS training requirements vary by position. As a result, employees were not consistently enrolled in the required training modules within the 30-day window. This issue stemmed from a lack of automation and standardized procedures for triggering training assignments upon hire.

To address this issue and ensure compliance with the Local Government Cybersecurity Act, the following corrective actions have been implemented:

Standardized Onboarding Process: A consistent onboarding process has been developed to ensure all new hires are enrolled in CJIS and KnowBe4 training within their first week of employment, regardless of position or role responsibilities.

Ongoing Monitoring, Reporting and Corrective Actions: A monthly compliance report is now generated and reviewed by IT leadership to proactively monitor training completion rates and identify any gaps. Department supervisors are notified of training deadlines to ensure their staff complete the required training within the mandated timeframe. Failure to meet or maintain training requirements will result in the employee's user account being locked until compliance is achieved.

Continued HR Coordination: The IT Department will continue working closely with Human Resources to further integrate employee onboarding with required cybersecurity training assignments.

Management expects these corrective actions will ensure all new employees are enrolled in and complete CJIS and KnowBe4 training within the 30-day requirement, thereby improving compliance and strengthening the organization's overall cybersecurity posture.