Collier County Clerk of Courts
Office of Inspector General

Consulting Services Report 2023.17
Cybersecurity NIST Risk Assessment and GAP Analysis

Inspector General Insights

Background: In July of 2022, the State of Florida passed House Bill 7055 which established information security mandates to be in place by the end of 2023. The mandates included the need for all state agencies and local governments to implement a cybersecurity risk management framework like the National Institute of Standards and Technology (NIST) Cybersecurity Framework for enterprise risk and security. The NIST framework outlines processes and standards for governance and controls that will help mitigate potential threats and help safeguard the operations of all areas of the Clerk's Office.

Florida's Chief Inspector General has been encouraging other Inspector General offices to begin conducting enterprise audits of certain controls under the NIST Detect Domain and the Continuous Security Monitoring category. Her agency began these reviews in 22 state agencies to develop a baseline understanding of IT program readiness, maturity, and resiliency. This became a greater priority for State agencies when legislation was passed in 2021 that called for each State IGs' agency to have specific cyber audit plans based on the highest risks to be addressed with existing resources. The 2022 cybersecurity legislation above included local governments.

The proposed Institute of Internal Audit (IIA) Global Internal Audit Standards (effective January 2025) require a review of cybersecurity and information technology governance, including compliance with the "Topical Requirements" for these functions. The IIA Topical Requirements are supplements to the Global Internal Audit Standards, and these requirements serve as the authority for the mandatory audit practices required to be followed when that subject is the focus of an internal audit engagement. In addition to these requirements, the Topical Requirements also include "Considerations", which are "not mandatory but serve as best practices for evaluating the design and implementation." Conformance with Topical Requirements will be evaluated in peer reviews or quality assessments, and evidence of conformance will be demonstrated by completing the IIA's checklist, to demonstrate conformance with each requirement or to explain why conformance was not achieved.

To comply with the established timeline of the 2022 legislation, the Clerk's Office initiated an organization-wide risk assessment and gap analysis. A third-party vendor with information security expertise was utilized to conduct the reviews. The OIG used this opportunity to follow the Chief Inspector General's lead by conducting our review in tandem with the third-party vendor to develop a baseline understanding of the cybersecurity controls. This baseline will provide the basis for creation of the audit programs for the required IIA cybersecurity audits.

Objective: The NIST risk analysis allows management to identify and evaluate any risks associated with the use of information systems in all Clerk areas. The gap analysis is utilized to assess information security processes for control gaps or improvements.

Scope/Methodology: OIG staff worked with external security experts to review information security policies, procedures, and controls. The review included extensive interviews with the Clerk's Information Technology staff as well as various department staff and external service providers. All cybersecurity information shared during the interviews is exempt from public disclosure per House Bill 7057.

Observations: During our review, we noted the following:

What's Working:

- ✓ Information security policies and procedures are in place to provide reasonable protection against cybersecurity threats.
- ✓ Employees are required to complete cybersecurity training monthly.

Action Items:

- IT governance processes and controls could be enhanced by ensuring roles and responsibilities are clearly defined.
- We recommend a standardized method of oversight of external vendors providing information system services.

Recommendations & Actions: In addition to the two action items noted by the OIG, the third-party vendor furnished a prioritized list of additional enhancements, which focused on governance security measures and controls, and standardizing the processes across the organization.

Conclusion: According to the final summary report of the third-party vendor:

- "The **Risk Assessment** yielded a Low-Risk rating, which is an excellent result and mainly reflects that Collier County Clerk's (CCC's) information security controls are well implemented and working effectively.
- The NIST **Gap Assessment** … found that CCC's information security practices align adequately with the NIST framework. At the same time additional improvements are recommended with respect to security policies and procedures documentation…"

The OIG found the NIST risk assessment and gap analysis effective in providing management with insight into key areas of risk related to information security. The OIG will continue to monitor the status of the action items.

Total # Interviews	Amounts Audited or Reviewed	Questioned Costs	Taxpayer Savings	# Observations / Recommendations
20	$ 0.00	N/A	N/A	2