

Office of the Internal Auditor

Advisory Memorandum

February 2023

Information System Technology
Policies Review





Advisory Memorandum

Background

Information Technology (IT) is critical in supporting Citizens' missions by providing applications, data, and tools that enable effective and efficient business processes. IT relies on governing documents (policies, procedures, standards, and guidelines) to a large extent to set requirements around the administration and utilization of applications and tools. IT governing documents are, therefore, key to maintaining the availability, confidentiality, and integrity of Citizens' applications, data, and tools.

Policies declare management's intentions through statements around principles. Standards delineate the requirements to be met (implemented) to meet management's stated principles. Procedures describe the steps by which processes will meet policies and standards. Guidelines provide additional guidance around policies, procedures, and standards.

Objectives and Scope

IT Senior Management requested the OIA to review the consistency, completeness, and relevance of current IT governing documents and the processes around IT governing document administration, conformance, implementation, and training. Only specific and current IT governing documents were in scope.

Results

Our review indicated that Citizens has IT governing documents for critical areas, including information security and privacy, acceptable use, software development, and enterprise resiliency. Our review also indicated that Citizens IT governing documents for critical areas align with the content present in leading practices.

We compared the Citizens IT governing documents in place with those expected to be in place based on leading practices. We found IT governing documents to provide coverage for most critical areas in line with leading practices. IT, including Information Security & Risk, is proactively updating/releasing additional IT governing documents.

The leading practices we included in our review were the following:

- Information Security:
 - CIS Critical Security Controls
 - NIST Cybersecurity Framework
 - CSA Cloud Controls Matrix
- IT Governance:
 - ISACA Control Objectives for Information Technology
 - ISACA Risk IT
 - COSO Enterprise Risk Management Framework
 - COSO Internal Control Framework
- IT Service Management:
 - Axelos Information Technology Infrastructure Library
- Change Management
 - ISACA Control Objectives for Information Technology for SOX



Advisory Memorandum

We also completed a gap assessment of the IT Security and Logging & Monitoring Standards against the information security leading practices listed above. Information Security & Risk revised/published both IT governing documents in 2022. We noted no significant gaps.

To support Management in their continuous improvement of IT governing documents, we compiled a library of references for security governing documents from NIST and SANS. We also purchased two libraries of general IT management governing documents based on ITIL from established consulting firms in this area.

We encourage Management to consider the following suggestions to enhance the completeness and coverage of IT governing documents:

- Evaluate the need to add/revise IT policies and standards to incorporate additional coverage for critical areas that were already shared with management under separate cover.
- Assess the feasibility of refreshing the content of the software development lifecycle (SDLC). As well as upgrading the SDLC from a departmental (IT) to a corporate policy to address contemporary risks in this area.
- Finalize change management standards initiatives to further mature change management controls and practices.
- Further utilization and implementation of IT's Governance Risk and Compliance platform to support lifecycle management and embedding of IT governing documents in IT processes and practices.

We want to thank management and staff for their cooperation and professional courtesy throughout this audit.



Distribution

Addressee(s) Wendy Emanuelson, Director – IT Security & Risk
Chris Jobczynski, Director – Enterprise Architecture & IT Strategy

Business Leaders:

Tim Cerio, President/CEO/Executive Director
Kelly Booten, Chief Operating Officer
Aditya Gavvala, VP – Chief Information Officer
Robert Sellers, VP – Chief Technology Officer
Christine Turner Ashburn, Chief, Communications, Legislative & External Affairs
Jennifer Montero, Chief Financial Officer
Mark Kagy, Inspector General

Audit Committee:

JoAnn Leznoff, Citizens Audit Committee Chair
Carlos Beruff, Citizens Audit Committee Member and Chairman of the Board
Scott Thomas, Citizens Audit Committee Member

Following Audit Committee Distribution:

The Honorable Ron DeSantis, Governor
The Honorable Jimmy Patronis, Chief Financial Officer
The Honorable Ashley Moody, Attorney General
The Honorable Wilton Simpson, Commissioner of Agriculture
The Honorable Kathleen Passidomo, President of the Senate
The Honorable Paul Renner, Speaker of the House of Representatives

The External Auditor

*Completed by Peter Schellen, Internal Audit Manager,
Under the Direction of Joe Martins, Chief of Internal Audit*