Office of the
Internal Auditor

Engagement Report

July 2025

SOC Review Process

CITIZENS
PROPERTY INSURANCE CORPORATION

Table of Contents: Page

Executive Summary

Background 1
Objectives and Scope 1-2
Engagement Results 2-3

Detailed Finding

1. SOC Review Governance & Oversight 4
Distribution 5

Executive Summary

Background

To manage third-party risk, Citizens obtains Service Organization Control (SOC) reports from prospective and active vendors that either access/house company data or impact financial reporting and are relied upon for core Citizens business functions. SOC reports are independent attestation reports issued by a Certified Public Accountant (CPA) that evaluate the design and effectiveness of a service provider's internal controls.

SOC reports are categorized based on their focus:

- **SOC 1** reports assess controls relevant to a service organization's financial reporting, typically requested for vendors in financial services.
- **SOC 2** reports evaluate controls related to security, availability, processing integrity, confidentiality, and privacy of data, commonly used for IT service providers.

The Vendor Management Office (VMO), in collaboration with Purchasing, Information Technology Security and Risk Management (ITSRM), Financial Services (FS) and other stakeholders, is responsible for determining when SOC reports are required for prospective or current vendors. Post vendor award through a competitive solicitation, vendors are managed by a Contract Manager (CM) in alignment with the business unit using the vendor's products or services. Once the contract is executed, the VMO works with the CM to obtain SOC reports and bridge letters from vendors when required due to the services being performed.

Once SOC reports are obtained, they are reviewed to determine whether the vendor maintains a sufficiently strong internal control environment, allowing Citizens to rely on their internal controls and processes. VMO facilitates the annual review process, coordinating with subject matter experts from ITSRM and FS who review the reports and submit the results back to VMO.

Individuals responsible for reviewing SOC reports should be knowledgeable and capable of identifying key elements within the report, including testing exceptions and their relevance and materiality to Citizens. A thorough review also involves evaluating complementary user entity controls (CUECs), which are controls that Citizens must implement to ensure the secure and effective use of relevant service providers.

As Florida's insurer of last resort, Citizens has a responsibility to safeguard policyholder data, protect employees' personally identifying information, and maintain operational resilience. Given its reliance on third-party vendors to support these objectives, a well-structured and diligent SOC report review process is essential to uphold security, compliance, and public trust.

Objectives and Scope

The objective of this advisory engagement was to support Citizens in strengthening its approach to reviewing SOC reports from third-party service providers. This engagement took a collaborative approach to assess current practices and identify opportunities for enhancement. Key focus areas included:

- Developing a clear and practical framework to guide management in determining whether a SOC report is required to be provided by a vendor.
- Assessing the current SOC report review process, focusing on opportunities to enhance consistency, thoroughness, and risk alignment.

Executive Summary

- Evaluate documents requested during the solicitation and ongoing annual review phases for appropriateness and timeliness.

Engagement Results

Through Internal Audit's collaboration with the VMO, ITSRM, and FS, it was noted that the SOC review process had many key elements in place and functioning. For example, the VMO had procedures for conducting reviews of SOC reports and requesting a deviation from SOC report requirements. Additionally, ITSRM had a procedure detailing how to perform their specialized SOC reviews.

During the review, we noted that the coordination between the groups lacked a clearly defined structure, as there was ambiguity regarding the roles and responsibilities of all stakeholders involved. As such, to supplement existing procedures with an overarching governing document, Internal Audit presented the VMO with the **SOC Report Requirements and Deviation Request Procedure** document, which provides a formalized structure, sequencing, and role delineation necessary to ensure consistency, accountability, and alignment across all parties involved in the SOC review lifecycle.

This overarching procedure integrates existing practices, introduces standardized templates and tools (e.g., SOC Review Tracking Spreadsheet, SOC Review RACI Matrix and Flowchart), and clearly defines how and when each stakeholder - VMO, ITSRM, FS, and others - is engaged during both the procurement and annual monitoring phases. By implementing this comprehensive framework, the VMO is better positioned to coordinate third-party assurance activities, ensure complete documentation, and support risk-informed decisions when evaluating vendors. As such, Internal Audit will track the above-described program for remediation. Details of the finding are on page 4.

Key Features of the new SOC Report Requirements and Deviation Request Procedure:

- VMO decision authority on SOC report requirements and review outcomes
  - The new procedure clarifies that the Vendor Management Office (VMO) holds final authority not only in determining whether a SOC report or equivalent assurance is required for a vendor, but also in making the final judgment on whether the results of the SOC report review provide sufficient assurance to proceed with the vendor engagement, or if a formal deviation must be initiated by the Business Unit. However, this determination is made in consultation with the subject matter experts in ITSRM and FS, whose specialized reviews inform the VMO's decision. VMO acts as the coordinating function and ultimate decision-maker but relies on the expertise of ITSRM and FS to evaluate technical and financial risks associated with the report's findings.
- Responsibilities of each team involved in the process
  - The delivered documents outline the authority of VMO to make a determination of requirements related to obtaining the SOC reports for certain vendors or sub-vendors. They also define the responsibility of the subject matter expert reviewers, including the evaluation of exceptions, CUECs, and the impact of 3rd party attestation reports on CPIC, both in the procurement lifecycle and annual review stages.
- Standardization of Financial Services specialized reviews
  - While ITSRM had established procedures for SOC report reviews, FS did not have a formalized review protocol. The new procedure provides the necessary structure to

Executive Summary

  - guide FS in evaluating financial reporting controls and documenting associated risks, including CUEC implementation and exception analysis.
- Centralized repository and year-over-year risk tracking
  - A centralized SOC Review Tracking Spreadsheet, maintained by the VMO, now serves as the single source of truth for recording exceptions, CUEC assessments, subservice organizations, and risk ratings. This consolidation not only improves visibility and consistency across teams but also enables meaningful year-over-year analysis. FS and ITSRM are expected to use this centralized repository to identify recurring exceptions and CUEC implementation issues across reporting periods, even in cases where the SOC auditor issued unqualified opinions. The effectiveness of this enhancement will rely on consistent use of the spreadsheet and intentional cross-year comparisons during annual reviews.
- SOC Deviation Process clarified
  - The new procedure makes it clear that a "Deviation" refers to a scenario in which VMO has determined that a SOC report should be obtained for a vendor, but that vendor does not have a SOC report to provide. In this case, the Business Unit must initiate the Deviation Process to continue to pursue or keep using that vendor's products or services. This process covers a number of concepts, including risk mitigation, risk acceptance, and alternative solutions to SOC report comfort.
- Training requirements
  - Stakeholders responsible for reviewing SOC reports, including those in FS and ITSRM, should receive standardized training on how to evaluate exceptions, assess CUECs, and document findings in alignment with the new procedure. VMO should maintain ownership of a recurring training protocol to promote consistent execution and interpretation across reviews. The new procedure details the main elements that should be covered in the training.

Additionally, throughout this engagement, OIA noted the following in-process improvements by VMO independently of the review process:

- Ticketing system improvements, which will allow VMO to track the workflow of SOC reports via Service Now. This will replace the current process of sharing via email.
- Enhancement of information gathered during the contracting/procurement phase of the vendor cycle to include information regarding SOC report availability and any relevant subservice organizations from the potential vendor.
- Expanding and documenting the understanding of services provided in order to improve the reliability of information and accuracy of determinations related to the need for SOC reports from vendors.
- Establishing more reliance on existing risk/control processes and activities in an effort to reduce duplication of work between SOC report reviewers and existing assurance providers within CPIC.

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

Detailed Finding

1. SOC Review Governance & Oversight

Classification	Medium	**Control Evaluation**	Control is not appropriately designed
Observation	During the review, Internal Audit noted that the coordination between the groups lacked a clearly defined structure, as there was ambiguity regarding the roles and responsibilities of all stakeholders involved. There is no standard tracking of year-over-year SOC report reviews.		
Cause	Multiple business units perform overlapping and disparate procedures that have not been centrally tracked, defined or coordinated.		
Consequence	Risks associated with vendors are not continuously considered, SOC reports are not always requested and reviewed when appropriate. When obtained, SOC reports may not be reviewed appropriately.		
Recommendation	Design and implement a **SOC Report Requirements and Deviation Request Procedure** document, which provides a formalized structure, sequencing, and role delineation necessary to ensure consistency, accountability, and alignment across all parties involved in the SOC review lifecycle.		
Agreed Management Response	Management agrees with the above recommendation and is working to implement the suggested practices and procedures.		
Responsible Individual	**Keri Dennis**, Asst Director - Vendor Relationship Mgmt.	**Completion date**	12/31/2025

Distribution

Addressee(s) Spencer Kraemer, Senior Director, Vendor Management & Purchasing

Business Leaders:
Tim Cerio, President/CEO/Executive Director
Jennifer Montero, CFO
Mark Kagy, Inspector General
Keri Dennis, Asst Director - Vendor Relationship Mgmt.

Audit Committee:
Jamie Shelton, Citizens Audit Committee Chair
Carlos Beruff, Citizens Audit Committee Member and Chairman of the Board
Robert Spottswood, Audit Committee Member

Following Audit Committee Distribution:
The Honorable Ron DeSantis, Governor
The Honorable Blaise Ingoglia, Chief Financial Officer
The Honorable James Ulthmeier, Attorney General
The Honorable Wilton Simpson, Commissioner of Agriculture
The Honorable Ben Albritton, President of the Senate
The Honorable Daniel Perez, Speaker of the House of Representatives

The External Auditor

Completed by Mark Giardino, Internal Audit Manager and Kyle Sullivan, Director of Internal Audit.

Under the Direction of Joe Martins, Chief of Internal Audit.