INTERNAL AUDIT

Service Organization Controls (SOC) Audit Report

September 2, 2020

Report Number: 2020-AUD-13 Service Organization Controls (SOC)

Table of Contents

Executive Summary

Background

Citizens relies on a network of vendors to support its mission to provide insurance to Florida consumers who are unable to find property insurance in the private market. Unless there is an approved exception, Citizens requires prospective and current vendors to provide a Service Organization Controls (SOC) report when services that are procured are either cloud based with access to Citizens' confidential or restricted confidential data or services that are procured that could have a potential impact to Citizens internal controls over financial statement reporting. For vendors with executed contracts, Citizens' Vendor Management Office (VMO) is responsible for assessing the SOC reports as a part of the vendor due diligence process to ensure that the proper risk mitigation steps have been taken or that additional stakeholders in the process such as the Contract Managers or IT Security and Risk have been notified of complementary controls. For prospective vendors that provide a SOC report as part of their response to a procurement, VMO is responsible for reviewing vendor provided SOC reports and notifying Purchasing about the results of the review. If a prospective vendor does not have or does not provide a SOC report, then they are asked to complete an IT Security Questionnaire which is evaluated by IT Security and Risk.

SOC reports are designed to help service organizations that operate information systems and provide information system services to other entities, build trust and confidence in their service delivery processes and controls. These reports are administered in accordance with the Statement of Standard Attestation Engagements No. 18 (SSAE18) which is a Generally Accepted Audit Standard that was established and published by the American Institute of Certified Public Accounts (AICPA) Auditing Standards Board. SOC reports are produced annually by third-party auditors and provide assurance to service organizations' clients, management, and user entities about the suitability of the design and operating effectiveness of the service organization's internal controls that are relevant to security, availability, processing integrity, confidentiality, and/or privacy of the hosted systems and the data stored or processed.

Citizens IT department has implemented a cloud strategy to move applications, as they expire and are reproduced, to a Cloud Software as a Service (SaaS) environment. As 6/25/2020, there are approximately 44 vendors who are required to provide annually SOC reports to Citizens for review.

Audit Objectives and Scope

The objective of this audit was to evaluate the adequacy and effectiveness of the processes, procedures, and controls over the SOC report governance process. Our scope included a review of the following areas:

- SOC Report Oversight and Monitoring
- SOC Report Review Process
- SOC Report Policies and Procedures
- SOC Report Escalation Process

Executive Summary

Audit Results

Results from our audit work indicate that key controls and processes over the SOC report governance process are adequate to ensure annual SOC reports are obtained from the vendors in accordance with the contractual agreement.

Specifically, we observed:

- A centralized SOC report repository has been developed to track and monitor critical vendors who are required to provide annual SOC reports.
- As a part of the Vendor Management Office's (VMO) due diligence process, annual SOC reviews are performed for critical vendors to evaluate whether vendor' internal controls are appropriately designed and are operating effectively to protect the organization from errors or potential wrong-doing. In addition, to identify risks that are not addressed by the vendor and the need to implement controls to mitigate those risks.

Our work also indicated specific areas where opportunities for improvement were noted:

- **The need to implement a SOC control exception tracking and monitoring process to ensure the vendor remediation plans have been completed to resolve the exception.** Vendor remediation plans for open control exceptions identified in the SOC report are reviewed by the Vendor Management Office (VMO) Reviewer for adequacy. However, follow-up should also be performed to ensure the vendor has implemented the remediation plan to resolve the open exception for applicable and material controls. Validation of the vendor's remediation plan ensures Citizens is not exposed to unmitigated risk.

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

Appendix

Distribution

Addressee(s) Keri Dennis, Manager, Vendor Relationship Management

Addressee(s) **Business Leaders:**
Barry Gilway, President/CEO/Executive Director
Kelly Booten, Chief Operating Officer
Christine Turner Ashburn, Chief, Communications, Legislative & External Affairs
Mark Kagy, Acting Inspector General
Stephen Guth, VP of Enterprise Services
Robert Sellers, VP Chief Technology Officer
Carlos Rodriguez, Director IT Security & Risk

Audit Committee:
Marc Dunbar, Citizens Audit Committee Chair
James Holton, Citizens Audit Committee Member
Bette Brown, 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 Nikki Fried, Commissioner of Agriculture
The Honorable Bill Galvano, President of the Senate
The Honorable Jose R. Oliva, Speaker of the House of Representatives

The External Auditor

Audit performed by Kay Weldon, Internal Audit Manager and Angela Smith, Senior Internal Auditor

Under the Direction of Joe Martins, Chief of Internal Audit