Office of the Internal Auditor

AUDIT REPORT 2023

Third-Party Technology Risk

Table of Contents: Page

Executive Summary

Background 1

Audit Objectives and Scope 1

Results 2

Appendix

Distribution 3

Executive Summary

Background

Citizens relies on third-party technology vendors to enable business processes through the utilization of technology, systems, and related services. According to a 2022 Gartner survey, 81% of organizations said their third-party network has increased in the past three years. Seventy-seven percent of organizations say their third-party network now includes third parties that perform more new-in-kind services (analytics, automation, artificial intelligence), and 72% say their third parties provide services outside the core business model. However, increasing third-party relationships also lead to increased risk.

Third-party technology risk at Citizens is managed through established processes and dedicated teams within Enterprise Operations, including Vendor Management and Purchasing (VMAP), the Information Security & Risk team (ITSR), and the Enterprise Architecture team. Key processes in place around third-party technology risk before a vendor is selected include vendor review and due diligence (solicitations, responsible vendor review) and security evaluation (questionnaires, review of public information, use of a third-party vendor risk tool). After onboarding, vendor performance and security reviews (including review of Service Organization Controls (SOC) reports provided by vendors) are incorporated into periodical vendor review processes. In addition, Enterprise Resiliency evaluates single points of failure as part of the solicitation process. This includes consideration of resiliency measures.

Objectives and Scope

The objective of this audit was to validate if third-party technology risk management aligns with Citizens' policies, standards, and leading practices. The scope of this audit included these specific areas:

- Determine that vendor performance is monitored periodically, and where applicable, service credits and remediation are sought and received.
- Determine whether dependency on vendors is assessed, and where applicable, resilience measures are implemented and alternatives are identified and tested.
- Review the adequacy and completeness of the SOC report review process. This will include coverage of user control considerations and related control self-assessments.
- Confirm continued vendor suitability assessments are performed periodically, inclusive of both performance and information security considerations, as applicable.
- Assess the timeliness, completeness and thoroughness of information security questionnaires completed by vendors.
- Review the coverage of Citizens' training requirements for vendor personnel, integration with Citizens' security technology and contractual obligations of vendors of notification of security incidents.

The scope of this audit excluded processes and controls around solicitations (security questionnaires will be included), vendor selection, and purchasing.

Results

Based on our review, the following areas were identified as strengths:

- **Vendor Management and Purchasing Governance**: VMAP collaborates with business partners to procure and contract for business needs, optimize vendor relationships, and

Executive Summary

promote contract management best practices. The VMAP Program includes established, comprehensive governing documents around third-party vendor management.

- **Information Security & Risk Governance**: ITSR provides oversight and assessments of third-party cybersecurity risk. Information Security Standards Assessments, Business Impact Assessments, and SOC report reviews are completed, gaps are remediated, or risk accepted. ITSR also utilizes leading third-party intelligence to provide real-time insight into vendor risk metrics.
- **Internal Controls**: Citizens has established an Internal Controls (IC) function within the Office of the Internal Auditor that facilitates and enables management's identification and continued improvement of primary controls. IC also maps SOC reports Complementary User Entity Controls (CUECs) to Citizens' primary controls where applicable, as control self-assessments provide additional support for the effectiveness of controls.
- **Scalable, Secure Technology**: Citizens has implemented leading technology to support third-party (technology) risk management. VMAP uses Cobblestone for centralized vendor and contract management and Exiger for ongoing monitoring of vendor health. ITSR uses ServiceNow Governance, Risk and Compliance (GRC), supporting risk and control mapping, including CUEC alignment to ITSR security standards controls. The IC Team uses AuditBoard, an integrated GRC system, which includes self-service capabilities for Control Champions and management to perform annual control self-assessments of the effectiveness of Citizens' primary controls.
- **Service Organization Controls (SOC) Report Monitoring**: VMAP, Financial Services, and ITSR collaborate in obtaining, reviewing, validating, and following up on SOC reports, the risks, and the CUEC considerations described in the SOC.
- **Vendor Performance Assessments:** VMAP requires Contract Managers to complete Vendor Performance Assessments based on Vendor Classification periodically. These assessments can be used as a tool to identify opportunities for continuous vendor improvements. Contract Management Reviews are completed by VMAP based on a frequency of two Contract Managers per quarter. A Contract Management Review is designed to ensure that Contract Managers are successfully performing their Contract Management duties, including the appropriate completion of Vendor Performance Assessments. Additionally, Contract Managers undergo Citizens and State of Florida training and, in certain cases, are required to be certified by the State of Florida.
- **Solution Suitability Assessments:** The suitability of solutions is periodically addressed through Contract Manager and Business Unit collaboration, Architecture Review Committee review of proposed solutions, the Lean Portfolio Management process, Market Analysis Reviews, and solicitation of alternative vendors/solutions.

Conclusion

There was one low-rated finding regarding enhancing SOC report monitoring and review for sub-service vendors. This observation was discussed with management, and remediation plans are in progress. In addition, some improvement opportunities to increase the efficiency and effectiveness of third-party technology risk management were considered and discussed with Management.

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

Distribution

Addressee(s): Wendy Emanuelson, Director – IT Security & Risk
Keri Dennis, Asst Director – Vendor Relationship Management

Business Leaders:
Tim Cerio, President, CEO & Executive Director
Kelly Booten, Chief Operating Officer
Mark Kagy, Inspector General
Aditya Gavvala, VP Chief Information Officer
Stephen Guth, VP – Enterprise Services
Robert Sellers, VP Chief Technology Officer
Spencer Kraemer, Sr Director – Vendor Management & Purchasing
Deena Harrison, Director – Risk & Controls

Audit Committee:
Joanne 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