



INTERNAL AUDIT

Third-Party Access
Audit Report

August 28, 2020



Table of Contents

	Page
	
Executive Summary	
Background	1
Audit Objectives and Scope	1
Audit Opinion	2
	
Appendix	
Distribution	3



Executive Summary

Background

Citizens, in its capacity as an insurance company and as a government entity, relies upon third parties to perform vital business activities, increase efficiencies in daily operations, boost productivity and create flexibility in resources. Reliance on these third parties increases exposure to additional risks and potential compliance deficiencies which may result in business disruption.

Third-party access, visibility and monitoring controls are key to safeguarding the network and data from nefarious or malicious acts by external users. Without appropriate control of external connections and user activities, the number of cyber incidents and the corresponding adverse impact on business operations may increase.

IT Security and Risk (ITSR), in collaboration with the appropriate business units, is responsible for the governance of third-party access which includes managing the communication of applicable requirements. As part of Citizens' cybersecurity program, ITSR establishes the policies and standards for security over external connections, and user administration and monitoring activities for third parties that have access to applications or devices residing in the Citizens network.

Business unit management is responsible for requesting and approving access to Citizens information resources for third-party users, as well as integrations or file transfers between Citizens information systems and third-party systems.

Third-party access was last audited during 2018. In that audit we noted a need to improve governance over third-party access, focused on clarifying responsibilities with implementing IT security standards related to third-party access.

Audit Objectives and Scope

The objective of this audit was to evaluate risks associated with third-party access to the Citizens information resources and validate that third-party access policies, inventories, user account management, connections and monitoring are appropriate for the organization in mitigating these risks.

For the purposes of this audit, a third party is any entity other than a Citizens employee. Similarly, third-party access refers to any third party that connects to or accesses Citizens' information resources including, but not limited to, applications, services, infrastructure, or data.

Our work focused on the following types of third parties:

- Contingent workers
- External auditors, regulators, external legal counsel (especially Acuity users), hardware and software service technicians, et al.
- Business Process Outsourcing Providers (BPO's) (e.g., First Notice of Loss personnel, Customer Care Center agents, Underwriting personnel)
- Independent adjusters
- Customers (myPolicy users)
- Insurance agents and Clearinghouse users



Executive Summary

- Suppliers in Centerpoint (Supplier Portal users)
- Software as a Service (SaaS) providers, service organizations, external entities which hold Citizens' data
- Systems Integration Tool (SIT) process senders/receivers
- FTP/SFTP (File Transfer Protocol/Secure File Transfer Protocol) external senders and receivers

Audit Opinion

IA noted policy and process improvements since our last audit of third-party access. The Information Technology Security Policy, Information Technology Security Standards, the Vendor Management Office (VMO) contract template and the Vendor and Contract Management Playbook have been updated to include specific provisions concerning third-party access. IA also noted that a Third-Party IT Security Governance and Access RACI (Responsible, Accountable, Consulted, Informed) Matrix has been developed to delineate program responsibilities.

Our work indicated two areas where operational controls can be strengthened to ensure that third-party access to Citizens' information resources is properly managed. In addition, IA noted two opportunities to improve processes which are integral to managing third-party access. Corrective action for these issues has been agreed with management.

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



Appendix

Distribution

Addressee(s) Carlos Rodriguez, Director – IT Security and Risk
Diane Walker, Director – IT Operations

Addressee(s) **Business Leaders:**
Barry Gilway, President/CEO/Executive Director
Kelly Booten, Chief Operating Officer
Aditya Gavvala, V.P., IT Services and Delivery
Robert Sellers, V.P., Chief Technology Officer

Audit Committee:
Marc Dunbar, Citizens Audit Committee Chairperson
Bette Brown, Citizens Audit Committee Member
James Holton, 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

*Audit performed by Gary Sharrock, IT Audit Manager
Under the Direction of Joe Martins, Chief of Internal Audit*