Office of the
Internal Auditor

AUDIT REPORT

November 2021

Logging and Monitoring

Report Number: 2021-AUD-01
Logging and Monitoring Audit

CITIZENS
PROPERTY INSURANCE CORPORATION

Table of Contents: Page

Executive Summary
Background 1
Audit Objectives and Scope 1
Results 2

Appendix
Distribution 3

Executive Summary

Background

Logging procedures ensure that computer activity and transaction records are recorded and stored in sufficient detail for a suitable period. Monitoring, in the form of manual or automated review and analysis of log contents, is important for identifying security incidents, policy violations, fraudulent activity, and operational problems shortly after they have occurred, and for providing information useful for resolving such matters.

Logs can also be useful for performing auditing and forensic analysis, supporting the organization's internal investigations, establishing baselines, and identifying operational trends and long-term problems. Besides these inherent benefits of logging and monitoring, several laws and regulations further compel organizations to store and review certain logs, e.g., the Gramm-Leach-Bliley Act (GLBA) requires that financial institutions protect their customers' information against security threats.

Citizens' system and application logging and monitoring have been enhanced with the implementation of logging agents on servers and databases. In addition, a more effective third-party, cloud-based Security Information Event Management (SIEM) service has recently been deployed which aggregates logs from many systems and provides analysis and correlation, identifies anomalies, and provides alerts for potential malicious behavior. The implementation will have a direct and positive impact on incident response and management capabilities.

Objectives and Scope

The objective of this audit was to assess whether the logging and monitoring of systems, applications and databases is aligned with Citizens' policies and standards, authoritative guidance, and regulatory requirements.

The scope of the audit included:

- Determining whether events and activities were being logged in alignment with authoritative guidance, leading practices, Citizens' policies and standards, and business needs.
- Reviewing the monitoring of log events and records to ensure that reviews were performed and were adequate to support business operations.
- Determining whether log management practices, including, but not limited to reporting, metrics, access controls, and retention, were in alignment with authoritative guidance, Citizens' policies and standards, and business needs.
- Assessing whether logging and monitoring supported the incident response process.

Audit Results

Internal Audit has completed an assessment of logging and monitoring, and noted that the following good practices are in place:

- Logging has been implemented on most systems and various types of monitoring are performed for operational and security purposes.

Executive Summary

- The Technical Operations Center (TOC) procedural documentation for monitoring and event response is thorough, and daily TOC activities are aligned with the documentation.
- A managed security service provider (MSSP) has been engaged to provide Security Information and Event Management (SIEM) services using logs from Citizens' information assets.

Following our assessment of the Logging and Monitoring practices applied, we noted that **the maturity level of logging and monitoring governance should be elevated.** Details of our observation were discussed with Management and corrective action is in progress.

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

Distribution

Addressee(s)

Aditya Gavvala, VP – IT Services and Delivery
Robert Sellers, VP – Chief Technology Officer

Business Leaders:
Barry Gilway, President/CEO/Executive Director
Kelly Booten, Chief Operating Officer
Mark Kagy, Inspector General

Audit Committee:
Erin Knight, 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 Nikki Fried, Commissioner of Agriculture
The Honorable Wilton Simpson, President of the Senate
The Honorable Chris Sprowls, Speaker of the House of Representatives

The External Auditor

Completed by Gary Sharrock, Internal Audit Manager – IT
Under the Direction of Joe Martins, Chief of Internal Audit