Office of the
Internal Auditor

AUDIT REPORT

September 2022

Applications and Infrastructure Standards Conformance Audit

Report Number: 2022-AUD-08
Applications and Infrastructure Standards Conformance (AISC) Audit

CITIZENS
PROPERTY INSURANCE CORPORATION

Table of Contents: Page

Executive Summary

Background

Applications and infrastructure components are susceptible to attacks that may result in exposure or modification of sensitive data or impact the availability of services to authorized users. Applications and infrastructure testing is conducted to identify security flaws introduced in the design, implementation, or deployment of an application and infrastructure components. Software engineers, system engineers, data engineers, and administrators should identify functions that are critical to security and test those functions to verify correct operation.

Infrastructure components such as switches, routers, firewalls, and wireless networking equipment are critical components of the Citizens' IT environment and must always be secure and available. By auditing the conformance of applications and infrastructure with security standards and industry-leading practices, we decrease the chance that an application or infrastructure component will be compromised or fail due to configuration errors.

The CIS critical security controls (CIS controls) is a publication of leading practice guidelines for computer security developed by the Center for Internet Security (CIS). The CIS controls are a prioritized set of safeguards to mitigate the most prevalent cyber-attacks against systems and networks. They are mapped to and referenced by multiple legal, regulatory, and policy frameworks. CIS controls version 8 has been enhanced to keep up with modern systems and software. The movement to cloud-based computing, virtualization, mobility, outsourcing, work-from-home, and changing attacker tactics prompted the update. It supports an enterprise's security as they move to fully cloud and hybrid environments.

Citizens' information security policies are based on CIS control version 6.1, which was released in 2016. Since then, CIS has released Version 7 (in 2018) and Version 7.1 (in 2019). The latest version of CIS control is version 8.0, released in 2021. Security of computer systems is ever evolving, with new vulnerabilities uncovered almost daily. As a result, CIS guidance is updated frequently. Staying aligned with the latest CIS guidance will support the relevance of Citizen's information security requirements.

Objectives and Scope

The objective of the AISC audit was to validate whether the configuration of applications and infrastructure components are in alignment with the "information security policies" and "industry-leading practices" (such as NIST, CIS Framework). The Audit also confirmed Citizens' management and mitigation of security risks associated with cyber-attacks, ransomware, and business disruption.

The scope of the Audit included a specific focus on:

- Network device (firewall) configuration hardening to evaluate the configuration processes applied and tools used to help mitigate breach possibility.
- SQL Server Database and Windows Server Domain Controller hardware configuration processes as well as comparison of actual configuration with the applicable CIS benchmarks to assess hardening conformance.

Executive Summary

- Application control, which supports integrity and confidentiality of data processing, configuration, authentication of Guidewire ClaimCenter and PolicyCenter and related change management.
- Access role design for Guidewire ClaimCenter and PolicyCenter to confirm the concept of least privilege and segregation of duties are designed appropriately.

Windows Server Domain Controllers were excluded during the Audit, as IT self-disclosed that Windows Server Domain Controllers mostly, but not entirely, met CIS benchmarks.

Results

Internal Audit completed the assessment of applications and infrastructure standards conformance and noted the following positive practices:

- The IT Infrastructure organization is aware of the necessity of hardening and throughout the Audit proactively acknowledged wanting to pragmatically address deviations from the CIS benchmark. At the same time, the IT infrastructure organization is concurrently supporting the existing IT landscape and simultaneously migrating to the cloud.
- The Guidewire platform largely conforms with authentication standards and application controls around confidentiality and integrity of information.
- Information Security & Risk (IS&R) has initiated a hardening program, with Windows Server 2019 as the first candidate as a pilot.

Results of our assessment of the applications and infrastructure configuration components indicated that there is a need to:

- Formally define and implement comprehensive information systems hardening standards and guidelines.
- Reassess and recalibrate the Guidewire system access role design to conform with the principles of least privilege and segregation of duties.

We want to thank management and staff for their cooperation and professional courtesy throughout 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
Thomas Dubocq, Director – IT Infrastructure
Ravi Tadiparthi, Director – Application Development
Wendy Emanuelson, Director – IT Security & Risk
Derick Leonard, Director – Data & Analytics (IT)

Audit Committee:
JoAnn 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 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 Protiviti Inc, and Ajay Kumar, Director of Internal Audit
Under the Direction of Joe Martins, Chief of Internal Audit