CITIZENS
PROPERTY INSURANCE CORPORATION

Office of the Internal Auditor

Confidentiality
Integrity
Ethics
Objectivity
Competency

Advisory

Date: November 14, 2016

To: Robert Sellers, VP, IT Infrastructure and Operations

From: Karen Wittlinger, IT Audit Director

Subject: SQL Database Remediation Project

Background

A project was initiated in April 2014 to implement computer hardening standards developed for the Windows and SQL infrastructure platforms based upon audit observations raised during two prior audit engagements. The project scope was changed in July 2015, separating the implementation of hardening of both platforms into two projects in order to ensure adequate management focus. OIA has continued to monitor the SQL remediation project given the risk of potential data breaches should database security configurations not be adequate.

Conceptually, computer hardening refers to the process of securing a system by implementing appropriate security measures, resulting in a reduction of the attack surface. General examples of the security measures include updating software, removing unnecessary software or user accounts, implementing appropriate authentication, changing default passwords, and limiting account permissions. With a corporate goal to protect the public interest and maintain the integrity of the corporation, this project aligns with a strategic initiative aimed at protecting private data in Citizens' custody.

The primary objectives of the SQL security strengthening project include:

- Evaluation and finalization of security baseline configurations
- Installation of approved standard configurations for approximately 240 servers
- Determination and documentation of procedures to ensure approved configurations are applied to all new servers as well as those requiring remediation
- Development of a configuration validation process and IT scanning process for new server builds
- Documentation and approval of configuration exceptions

The project is 61% complete and is on target for completion in March 2017.

Scope and Objectives

Given the importance of system security and the need to apply appropriate standards with the hardening of the SQL servers, OIA has been monitoring this project and provided an assessment of the strength of project governance in place to ensure adequate consideration and implementation of a sound security infrastructure around SQL.

The scope of the advisory work included the following components that were identified as integral parts of project governance:

- A sound project governance structure has been established (project team and stakeholders group), objectives have been clearly defined and communicated and a clear escalation path is implemented.
- Required project artifacts are being created and stored in the appropriate location in line with the project methodology.
- Approvals have been obtained for artifacts and significant project decisions in line with the methodology.
- Roles and responsibilities have been delineated for project team members.
- Tasks, resources and target dates are being maintained up to date, and periodically reported to the project owner and sponsor.
- Project risks are being identified as part of project progression.
- Monthly status reports are being generated and distributed in line with the methodology time frame.
- Process documentation is completed to ensure ongoing configuration management and validation of SQL databases.
- Database configuration exceptions are being documented and provided to the IT security department for risk evaluation, approval and follow-up.

Results

Overall, we noted that adequate processes are in place to support and ensure the effective completion of the project. The governance structure is designed well with an effective escalation and approval path and monthly updates to the stakeholders group. Weekly meetings provide detailed progress updates to the project team, and processes have been documented to ensure new SQL servers are hardened when the devices are built.

OIA provided informal recommendations to project management throughout the process which have been appropriately addressed. However, hardening standards may not be able to be implemented within a SQL server due to negative operational impacts within the network environment. As such, these configuration exceptions are currently being documented and provided to IT Security for formal assessment. This process is not formally documented in current security procedures and it was agreed that it will be included as an IT security standard in the revised IT Technology Security Policy. The target date for standards completion is 12/31/16. Configuration exceptions arising from the project will be researched and documented in accordance with the new standard within the timelines of the project.

We would like to thank Management and staff in IT Operations and Infrastructure and IT Security for their cooperation and professional courtesy throughout the course of this engagement.

Distribution

Barry Gilway, President/CEO/Executive Director
Kelly Booten, Chief of Systems and Operations
Dan Sumner, Chief Legal Officer and General Counsel
Curt Overpeck, Chief Information Officer
Mario Andrade, Director, IT Infrastructure
Mitch Brockbank, Director, IT Security and Risk
Diane Walker, Director, IT Operations