CITIZENS
PROPERTY INSURANCE CORPORATION

Office of the Internal Auditor

Confidentiality
Integrity
Ethics
Objectivity
Competency

AUDIT REPORT

Citizens Authentication Gateway (CAG)

December 17, 2015

Table of Contents: Page

Executive Summary

Appendices

Executive Summary

Background

The Citizens Authentication Gateway (CAG) is an internally developed user authentication system which was implemented in conjunction with the Citizens Insurance Suite to serve as a single sign-on system to the Insurance Suite modules. CAG validates the user ID and password entered on the login screen with its database of valid users and passes the user ID of authenticated users to the Insurance Suite modules, i.e., Citizens PolicyCenter®, Citizens BillingCenter®, Citizens ClaimCenter® and ContactManager, as well as the Clearinghouse application. The Insurance Suite modules and Clearinghouse are responsible for user authorization based upon a roles-based user account in each module/application.

Although CAG was initially intended as an interim Single Sign-On (SSO) system until a long-term SSO was implemented, the plan is that it will serve as the long-term sign-on solution. In line with the plan, CAG is being expanded to also manage access to the new VUE Producer Management Platform (PMP) and Global Policy Search (GPS) applications along with the new external website.

CAG user accounts are created by the following functions:

- Technical Support Center (typically internal users)
- Claims – Vendor Relationship Management (typically independent adjusters)
- Consumer and Agent Services (typically agents and depopulation companies)
- Budget and Financial Systems (typically internal users)

User accounts are created (provisioned) in CAG by three methods; Claims Administration Information System (CAIS) and Electronic Policy Administration System (ePAS) application automated interfaces; Service Desk tickets fulfilled by the Technical Support Center; and emails directed to CAG administrators. By default, CAG user accounts are assigned the 'User' role, which provides visibility to the Insurance Suite modules and other applications that they are configured to use. There are also other CAG user roles which provide varying degrees of elevated capabilities within CAG for security administration and technical configuration purposes.

Audit Objectives and Scope

The objective of this audit was to evaluate the design, implementation and operation of CAG in providing authentication for the Insurance Suite modules, ContactManager, Clearinghouse and other applications that are in process.

Specific areas reviewed were:

- Integration with source systems of record for user management (CAIS, ePAS, Active Directory, Service Desk).
- Implementation and adherence to Citizens information security policies, procedures and guidelines.
- Validation of controls over user provisioning, modification and de-provisioning.

This audit included activity which occurred between January 1, 2015 and October 29, 2015.

Executive Summary

Management's Assessment and Reporting on Controls

OIA provided management an opportunity to share known control weaknesses and their plans to remediate them. This process is intended to foster an environment whereby management and staff conduct periodic proactive reviews of controls and are aware of the risks to the business. It also enables OIA to focus its audit efforts on areas where it can add value to the organization.

At the start of the audit, CAS Management shared the following control weaknesses and remediation plans with OIA:

- Simultaneous use of a CAG user ID: A CAG user ID can be used simultaneously by more than one person within each agency. Management stated that this contradiction to the Citizens information security policy would be remediated by the implementation of the VUE Producer Management Platform (PMP) system by mid-2016.
- Inability to remove agent access:
  - If an agent loses an underlying appointment or their license due to lack of continuing education as determined by the Florida Department of Financial Services (DFS) weekly discrepancy report, access cannot be fully removed due to gaps in the current Agency Appointment Agreement. Management's research resulted in a decision to maintain the agent accounts in the system.
  - CAG user ID's for agents are not being disabled or deleted when system inactivity reaches 60 days to align with the IT Security Policy. This is due to the number of agencies (3123) with less than 50 active policies who do not frequently use the system. Management stated that access is maintained for these agents so that they may continue to serve the policy holders.
- CAG records are not reconciled with ePAS or Agency Appointment System (AAS): Management stated that work is in progress to develop reports that match ePAS and AAS records to CAG. Implementation of the VUE PMP system by mid-2016 will also provide the ability to reconcile user accounts with CAG.

Audit Opinion

Based upon our audit work, we noted that in general, the design, implementation and operation of CAG is rated as **Satisfactory**. Our audit work indicated an opportunity to strengthen the controls associated with a shared administrative account and account privileges as follows:

- **A need to eliminate the use of a shared administrator account.** There is an account with administrator privilege that is used to run scripts which update Citizens Insurance Suite data in production. The password for this account is known and shared by four IT support personnel. To address this finding, management has created a new password which is known only by the owner of the administrator account and the password has been stored in the password vault.
- **A need to prohibit the 'Technical Support Center User' role in CAG from promoting itself to the Security Administrator role.** The 'TSC User' role is assigned to 29 personnel who support all of the CAG users. Persons with the 'TSC User' role can elevate themselves to have the Security Administrator role which provides 11 additional administrative capabilities. To address this finding, TSC management will review the assignment of the 'TSC User' role on a monthly basis until a system enhancement is developed and implemented in June, 2016.

Executive Summary

Other low rated issues and process improvement opportunities were noted and discussed with management during the audit.

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

Appendix 1

Definitions

Audit Ratings

Satisfactory:

Critical internal control systems are functioning in an acceptable manner. There may be no or very few minor issues, but their number and severity relative to the size and scope of the operation, entity, or process audited indicate minimal concern. Corrective action to address the issues identified, although not serious, remains an area of focus.

Needs Improvement:

Internal control systems are not functioning in an acceptable manner and the control environment will require some enhancement before it can be considered as fully effective. The number and severity of issues relative to the size and scope of the operation, entity, or process being audited indicate some significant areas of weakness. Overall exposure (existing or potential) requires corrective action plan with priority.

Unsatisfactory:

One or more critical control deficiencies exist which would have a significant adverse effect on loss potential, customer satisfaction or management information. Or the number and severity of issues relative to the size and scope of the operation, entity, or process being audited indicate pervasive, systemic, or individually serious weaknesses. As a result the control environment is not considered to be appropriate, or the management of risks reviewed falls outside acceptable parameters, or both. Overall exposure (existing or potential) is unacceptable and requires immediate corrective action plan with highest priority.

Appendix 2

Issue Classifications

Control Category	High	Medium	Low
Financial Controls (Reliability of financial reporting)	• Actual or potential financial statement misstatements >USD 5 million • Control issue that could have a pervasive impact on control effectiveness in business or financial processes at the business unit level • A control issue relating to any fraud committed by any member of senior management or any manager who plays a significant role in the financial reporting process	• Actual or potential financial statement misstatements between USD 2.5 million to 5 million • Control issue that could have an important impact on control effectiveness in business or financial processes at the business unit level	• Actual or potential financial statement misstatements below USD 2.5 million • Control issue that does not impact on control effectiveness in business or financial processes at the business unit level
Operational Controls (Effectiveness and efficiency of operations)	• Actual or potential losses >USD 2.5 million • Achievement of principal business objectives in jeopardy • Customer service failure (e.g., excessive processing backlogs, unit pricing errors, call center non responsiveness for more than a day) impacting 10,000 policyholders or more or negatively impacting a number of key corporate accounts • Actual or potential prolonged IT service failure impacts one or more applications and/or one or more business units • Actual or potential negative publicity related to an operational control issue • An operational control issue relating to any fraud committed by any member of senior management or any manager who plays a significant role in operations	• Actual or potential losses between USD 0.5 to 2.5 million • Achievement of principal business objectives may be affected • Customer service failure (e.g., processing backlogs, unit pricing errors, call center non responsiveness) impacting 1,000 policyholders to 10,000 or negatively impacting a key corporate account • Actual or potential IT service failure impacts more than one application for a short period of time	• Actual or potential losses below USD 0.5 million • Achievement of principal business objectives not in doubt • Customer service failure (e.g., processing backlogs, unit pricing errors, call center non responsiveness) impacting less than 1,000 policyholders • Actual or potential IT service failure impacts one application for a short period of time

Appendix 2

Control Category	**High**	**Medium**	**Low**
	• Any operational issue leading to death of an employee or customer	• Any operational issue leading to injury of an employee or customer	
Compliance Controls (Compliance with applicable laws and regulations)	• Actual or potential for public censure, fines or enforcement action (including requirement to take corrective actions) by any regulatory body which could have a significant financial and/or reputational impact on the Group • Any risk of loss of license or regulatory approval to do business • Areas of non-compliance identified which could ultimately lead to the above outcomes • A control issue relating to any fraud committed by any member of senior management which could have an important compliance or regulatory impact	• Actual or potential for public censure, fines or enforcement action (including requirement to take corrective action) by any regulatory body • Areas of non-compliance identified which could ultimately lead to the above outcomes	• Actual or potential for non-public action (including routine fines) by any regulatory body • Areas of noncompliance identified which could ultimately lead the above outcome
Remediation timeline	Such an issue would be expected to receive immediate attention from senior management, but must not exceed 60 days to remedy.	Such an issue would be expected to receive corrective action from senior management within 1 month, but must be completed within 90 days of final Audit Report date.	Such an issue does not warrant immediate attention but there should be an agreed program for resolution. This would be expected to complete within 3 months, but in every case must not exceed 120 days.

Appendix 3

Distribution

Addressees: Aditya Gavvala, VP – Application Delivery
Robert Sellers, VP – IT Infrastructure and Operations
Mitch Brockbank, Director – Information Security and Risk

Copies: **Business Leaders**:
Barry Gilway, President/CEO/Executive Director
Jay Adams, Chief – Claims
Steve Bitar, Chief - CAS
Kelly Booten, Chief – Systems and Operations
Jennifer Montero, Chief Financial Officer
John Rollins, Chief Risk Officer
Dan Sumner, Chief Legal Officer and General Counsel
Curt Overpeck, Chief Information Officer
Christine Ashburn, VP, Legislative and External Affairs and Communications
Bruce Meeks, Inspector General

Audit Committee:
Juan Cocuy, Citizens Audit Committee Chairman
Bette Brown, Citizens Audit Committee Member
Jim Henderson, Citizens Audit Committee Member

Following Audit Committee Distribution:

The Honorable Rick Scott, Governor
The Honorable Jeff Atwater, Chief Financial Officer
The Honorable Pam Bondi, Attorney General
The Honorable Adam Putnam, Commissioner of Agriculture
The Honorable Andy Gardiner, President of the Senate
The Honorable Steve Crisafulli, Speaker of the House of Representatives
Dixon Hughes Goodman LLP

Audit Performed By

Auditor in Charge	Gary Sharrock, Manager – IT Audit
Audit Director	Karen Wittlinger, Director – IT Audit
Under the Direction of	*Joe Martins* *Chief of Internal Audit*