Office of the Internal Auditor

Confidentiality
Integrity
Ethics
Objectivity
Competency

CITIZENS
PROPERTY INSURANCE CORPORATION

AUDIT REPORT

Citizens Insurance Suite Access

February 1, 2017

Table of Contents: Page

Executive Summary

Background 1
Audit Objectives and Scope 2
Audit Opinion 2

Appendix

Definitions 4
Issue Classifications 5
Distribution 7
Audit Performed By 7

Executive Summary

Background

The Citizens Insurance Suite replaced Citizen's policy, billing, and claims legacy systems with implementation occurring in several phases throughout 2013 and 2014. The Citizens Insurance Suite provides a complete set of applications to support core operations including underwriting, policy administration, billing, and claims management. As of June 2016, the Citizens Insurance Suite supports 489,138 polices with premium plus surcharges totaling $980,664,620. The suite includes the following applications:

- BillingCenter® enables performance of accounting functions including receipts, disbursements, general ledger, and remittance processing.
- ClaimCenter® provides support to adjusters across the entire claims cycle from the first notice of loss through settlement.
- PolicyCenter® supports agents, underwriters, and service representatives with policies from quote and issuance through changes and renewals.
- Contact Manager integrates with ClaimCenter® to update the selection of non-contracted payees for claims payments.

Citizens' employees as well as external parties including agents, independent adjusters and underwriters require system access to Citizens Insurance Suite to perform their job functions. In addition, take-out companies assuming policies from Citizens are granted view only access to their policies. As of July, approximately 12,332 users have access to view or update information within the Citizens Insurance Suite:

Center	Active Users
Policy (Agents)	8,608
Claim	1,514
Policy (Non-agent)	1,014
Billing	623
Policy (Take-out Company Users)	432
Contact	141
Total:	12,332

During 2015, OIA consulted with Project Management to educate and develop processes and controls to mitigate segregation of duties concerns across the suite. As a result, standards were rolled out to all business owners and application administrators to help ensure adequate access controls were followed. Responsibility for access management is decentralized with a designated business process owner for each application. Access management includes creating, modifying, terminating, and monitoring user identities and related access roles and permissions to proprietary information. Continued maintenance and recertification are necessary to ensure user access to information remains appropriate.

Executive Summary

Audit Objectives and Scope

The objective of this audit was to evaluate the adequacy and effectiveness of access controls for Billing, Claim, Policy Centers, and Contact Manager within Citizens Insurance Suite. The scope of the audit included an assessment of controls over each center for Citizens' employees, agents, vendors and take-out companies in the following areas:

- User provisioning of new hires and role changes due to promotions, demotions, lateral moves or changes in job duties
- User de-provisioning of voluntary and involuntary terminations
- Segregation of duties
- Monitoring activities and account validation including recertification

Management's Assessment and Reporting on Controls

OIA provided management responsible for provisioning within the Citizens Insurance Suite 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 this audit, BillingCenter management shared the following control weaknesses and remediation plans with OIA, which have subsequently been completed:

- BillingCenter did not have the capability to provide a history of changes made to users, roles, permissions or authority limits. Effective November 19, 2016 an admin history functionality was added to BillingCenter.
- During 2015, the annual recertification of BillingCenter users was not performed. In July of 2016, the annual recertification was initiated and completed.

Audit Opinion

The overall effectiveness of the controls evaluated during the audit of Citizens Insurance Suite Access is rated as **Needs Minor Improvement.**

Results from our audit work indicate that the provisioning processes are well managed with effective internal controls over the provisioning team screening of requests, confidentiality and non-disclosure agreements with agents regarding their system access and use of data, and annual recertification.

Our work also indicated specific areas where opportunities for improvement were noted:

- **Privileged users are not adequately monitored.** Privileged users have elevated permissions in order to perform their work. In the Citizens Insurance Suite, privileged users have permissions to change their own roles, permissions, and authority limits. In some instances, the users are also assigned to additional roles for various business purposes which may create segregation of duty conflicts. Inadequate monitoring of privileged users may result in misuse or misappropriation resulting in business interruption or financial loss. Implementation of alerts or exception reports to identify any changes to the privileged users' roles, permissions, and authority limits would ensure that inappropriate transactions are prevented or detected in a timely manner.

Executive Summary

- **Permissions within certain roles exceed the least privilege necessary for the user to perform their job functions.** Excessive permissions identified during our review include the ability to create, delete, and edit certain transactions. Granting access to unnecessary privileges can compromise security of data and may lead to disclosure of confidential or sensitive information, loss of data integrity, loss of proprietary information, business or system disruption, and increases the opportunity for fraudulent activity.

- **Service desk user profiles were not appropriately updated which impacted the deactivation process for terminated employees.** OIA identified 12 former employees who still had active accounts in the Citizens Insurance Suite after their separation dates. Five of the 12 users were also active in the Citizens Authentication Gateway which provides single sign-on access to the centers within the Citizens Insurance Suite. Failure to terminate user access may result in disclosure of confidential or sensitive information, business or system disruption, and fraudulent activity. Management deactivated the users.

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

Appendix 1

Definitions

Audit Ratings

Satisfactory:
The control environment is considered appropriate and maintaining risks within acceptable parameters. 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.

Needs Minor Improvement:
The number and severity of issues relative to the size and scope of the operation, entity, or process being audited indicate some minor areas of weakness in the control environment that need to be addressed. Once the identified weaknesses are addressed, the control environment will be considered satisfactory.

Needs Improvement:
The audit raises questions regarding the appropriateness of the control environment and its ability to maintain risks within acceptable parameters. The control environment will require meaningful enhancement before it can be considered as fully satisfactory. The number and severity of issues relative to the size and scope of the operation, entity, or process being audited indicate some noteworthy areas of weakness.

Unsatisfactory:
The control environment is not considered appropriate, or the management of risks reviewed falls outside acceptable parameters, or both. 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.

Appendix 2

Issue Classifications

Control Category	High	Medium	Low
Financial Controls (Reliability of financial reporting)	• Actual or potential financial statement misstatements > $10 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 > $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 < $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 > $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 • Any operational issue leading to death of an employee or customer	• Actual or potential losses > $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 • Any operational issue leading to injury of an employee or customer	• Actual or potential losses < $2.5 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
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	• Actual or potential for public censure, fines or enforcement action (including requirement to	• Actual or potential for non-public action (including routine fines) by any regulatory body

Appendix 2

Control Category	High	Medium	Low
	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	take corrective action) by any regulatory body • Areas of non- compliance identified which could ultimately lead to the above outcomes	• 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

Addressee(s)	Jay Adams, Chief Claims Steve Bitar, Chief Consumer and Agent Services Kelly Booten, Chief Systems and Operations Jennifer Montero, Chief Financial Officer
Copies	**Business Leaders:** Barry Gilway, President/CEO/Executive Director Dan Sumner, Chief Legal Officer & General Counsel Christine Turner Ashburn, VP-Communications, Legislative & External Affairs 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 Joe Negron, President of the Senate The Honorable Richard Corcoran, Speaker of the House of Representatives The External Auditor

Audit Performed By

Auditor in Charge	Deena Harrison
Audit Director	John Fox
Under the Direction of	*Joe Martins* *Chief of Internal Audit*