Office of the Internal Auditor

Confidentiality
Integrity
Ethics
Objectivity
Competency

CITIZENS
PROPERTY INSURANCE CORPORATION

AUDIT REPORT

Information Technology Change Management Audit

November 15, 2016

Table of Contents: **Page**

Executive Summary

Background

Information Technology change management is an organization's process to manage changes to software applications and IT infrastructure. These changes arise both proactively and reactively to facilitate system enhancements, service improvements and system incidents. Change management comprises important foundational controls within an IT environment and seeks to balance the efficient handling of changes with an appropriate level of review to maintain processing integrity and reduce the risk of disruption to information systems and business operations.

Change management at Citizens is managed by the Director of IT Operations and a Change Manager. IT Operations has documented policies and procedures to guide management and personnel in performing change management responsibilities that include evaluating, authorizing, prioritizing, communicating and validating systems changes. Governance is accomplished through meetings of IT representatives (Change Control "Board") who have decision-making authority to approve, disapprove, or defer implementation of proposed changes. From January to July 2016, IT Operations managed an average of 153 changes and 18 emergency changes per month, which aligns with 2015, where the average monthly changes totaled 155 with 13 being emergency changes.

A separate change management review committee, created in early 2015, provides an additional level of control for the Citizens Insurance Suite (CIS) of products and the Citizens Data Warehouse. This process adds a review of proposed application changes with a cross-functional group of IT and business representatives as changes are requested for development. Additional focus is placed on system impacts from an integration standpoint due to complexities and interfaces within these systems.

An effort was undertaken in 2015 to strengthen the change management program and solidify areas of perceived weakness that could present unnecessary risks to the systems environment. Updated policies and procedures were approved and implemented in late 2015. Enhancements included identifying and requesting changes earlier in the process; increasing the frequency in which the change control board reviews proposed changes; requiring review of all proposed changes; and prescribed definitions and strict enforcement over pre-authorized and emergency changes.

Audit Objectives and Scope

The objective of this audit was to evaluate the adequacy and effectiveness of controls related to change management. The scope of the audit included an assessment of:

- Governance of change management activities:
  - Policies and procedures
  - Management review of change management metrics
- Review, approvals and documentation quality for a sample of changes for the period June to August 2016.
- Segregation of duties for execution of change management roles and responsibilities.
- Administrator and user access within change management software tools.

Management's Assessment and Reporting on Controls

OIA met with Management to determine if there were any internal control issues related to the audit scope that Management would like to report. Management indicated that there were no significant internal control issues to relay.

Executive Summary

Audit Opinion

Based upon our audit work, the overall effectiveness of policies, procedures, processes and controls evaluated during the audit of Information Technology Change Management is rated as **Satisfactory.**

With the development and implementation of enhanced change management policies and processes, IT has strengthened controls in several areas. The change management review committee imposes a multi-dimensional view of potential changes related to the Guidewire product suite and the Citizens data warehouse prior to moving to development. Other improvements to the operational change process reduced production implementation risks through the development of formal definitions of automatically authorized changes, a focus on emergency changes, detailed metrics and other process enhancements.

In our work, we noted some minor observations which are being addressed.

We would like to thank management and staff in IT Operations and Strategy Planning and Continuous Improvement 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)	Diane Walker, Director of IT Operations Brian Weaver, Sr. Director, Strategy Planning and Continuous Improvement
Copies	**Business Leaders:** Barry Gilway, President/CEO/Executive Director Kelly Booten, Chief – Systems and Operations Curt Overpeck, Chief Information Officer Dan Sumner, Chief Legal Officer & General Counsel Robert Sellers, VP – IT Infrastructure and Operations Christine Turner Ashburn, VP-Communications, Legislative & External Affairs Clint Roszelle, Assistant Director – Business Process Excellence 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	Kirk Elmore, Senior Auditor
Audit Director	Karen Wittlinger, IT Audit Director
Under the Direction of	*Joe Martins* *Chief of Internal Audit*