OIA
OFFICE OF THE INTERNAL AUDITOR

CITIZENS
PROPERTY INSURANCE CORPORATION

INTERNAL AUDIT

IT Critical Security Controls Implementation Audit Report

April 15, 2019

Report Number: 2019-03 IT Critical Security Controls Implementation

Table of Contents

Executive Summary

Background

As part of the IT Security and Risk Department's goals to improve enterprise security governance and risk management, a suite of policies and standards was developed following the National Institute of Standards and Technology IT Security Standards and Cyber Security Framework (NIST CSF). Parallel to this effort was the adoption of the Center for Internet Security's Critical Security Controls (CSCs), which are a set of best practices initially designed as a response to extreme data losses experienced by organizations in the US defense industrial base. The goal in the use of these practices is to secure IT systems and data against the most pervasive attacks. These standards are continuously refined by a global group of experienced IT security practitioners. The updated IT Security standards reflect a combination of NIST CSF and CSC based controls and practices.

The CSC controls implementation process consisted of the selection of Critical Security Controls that would be adopted, IT management surveys to determine which practices were not implemented and controls validation of implementation of the adopted practices. IT Operations has been tracking implementation progress against the initial target date of December 31, 2018 and provides metrics to IT management weekly. The IT Systems Security Committee is provided a monthly status and metrics. Of the initial 222 controls identified for implementation, 189 were noted by the control owners as having been remediated by December 31, 2018.

Audit Objectives and Scope

The objective of this audit was to evaluate the successful implementation of the IT Critical Security Controls adopted by the organization. The scope included an assessment of the following as of December 31, 2018:

- Validation of CSC controls implementation including the approval of systems based evidence of control practices by IT Security management
- IT Security standards reflecting the addition of CSC controls or modification of the NIST based standards to align with the CSCs
- An assessment of CSC controls not selected for implementation
- An assessment of risk values established within the RSAM compliance database for each of the CSC controls
- Controls implementation exception processing

Audit Opinion

The implementation of the critical security controls and supporting processes is rated as **Satisfactory**.

OIA testing of controls evidence from control owners as well as online systems confirmed that controls were implemented or projects are underway to establish the controls. The IT Security standards were modified to include the adopted CSC controls. Controls not selected for

Executive Summary

implementation at project inception and control risk values established in the compliance software tool appear to be reasonable. There have been no exceptions requested whereby a specific control is not able to be implemented due to extenuating circumstances within the network environment.

Our work resulted in two low risk observations indicating that processes should be strengthened related to oversight and approval of CSC controls which were not selected for adoption as well as controls evidence documentation and approval. Other minor test result anomalies were also provided to management so that process refinements may be considered as part of the establishment of the compliance and risk management programs.

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	• 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

Appendix 2

Control Category	High	Medium	Low
	• Any operational issue leading to death 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

Addressee(s) Carlos Rodriguez, Director, IT Security and Risk

Addressee(s) **Business Leaders:**
Barry Gilway, President/CEO/Executive Director
Kelly Booten, Chief – Systems and Operations
Christine Turner Ashburn, Chief, Communications, Legislative & External Affairs
Robert Sellers, V.P., Chief Technology Officer
Aditya Gavvala, V.P., IT Services and Delivery
Mark Kagy, Acting Inspector General

Audit Committee:
Bette Brown, Citizens Audit Committee Chairperson
James Holton, Citizens Audit Committee Member
Marc Dunbar, 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 Bill Galvano, President of the Senate
The Honorable Jose R. Oliva, Speaker of the House of Representatives

The External Auditor

Audit performed by Karen Wittlinger, Director, IT Audit
Under the Direction of Joe Martins, Chief of Internal Audit