Office of the Internal Auditor

Confidentiality
Integrity
Ethics
Objectivity
Competency

CITIZENS
PROPERTY INSURANCE CORPORATION

AUDIT REPORT

Systems Development Lifecycle (SDLC)

March 3, 2016

Report Number: 2015-AUD-IT-07 SDLC

Table of Contents: Page

Executive Summary

Background

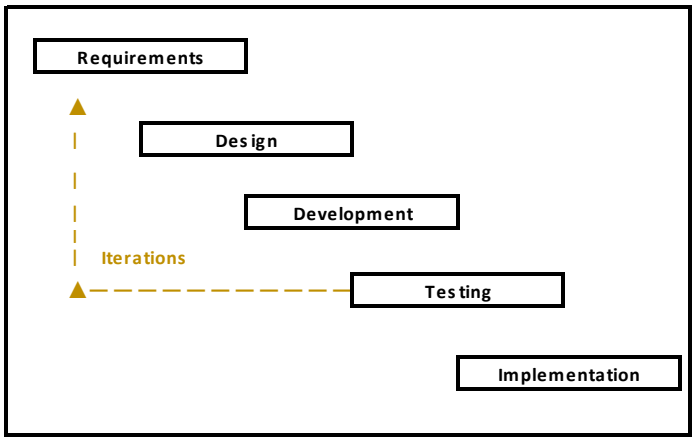
A Systems Development Life Cycle (SDLC) is a sequence of phases that must be followed in order to convert business requirements into an IT system or application and to maintain the system in a controlled method. While there are many development life cycle models available, the three most common objectives contained in the models are:

- Ensuring that high quality systems are delivered on-time and on-budget
- Providing strong management controls over development activities
- Maximizing the productivity of the development team

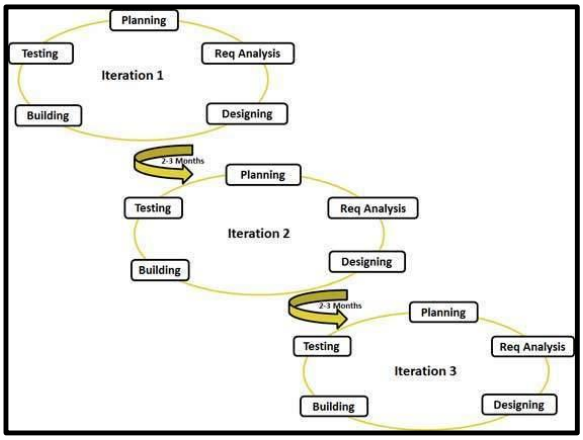
The 'Waterfall Model' was the earliest SDLC approach to be used for software development. In a waterfall model, each phase must be completed before the next phase can begin and there is no overlapping in the phases. In this approach, the whole process of software development is divided into separate phases, and the output of each becomes the input for the next sequential phase.

The 'Agile' model is the most popular SDLC model used in software development today. Agile introduces the concept of fast delivery to customers using a prototype approach. Projects are divided into small iterations with specific deliverable features. Customer interaction following each iteration is the backbone of the Agile methodology, and open communication with minimum documentation are the typical features of an Agile development environment.

Waterfall Model



Agile Model



Citizens uses both Waterfall and Agile software development models and while both models follow the Citizens SDLC methodology, management continues to adapt SDLC documentation to support the Agile model.

The SDLC Policy was implemented in 2014 and with this version, the related process was abridged, taking into consideration the complexity and rigor of the previous framework, process, deliverables and the Citizens environment.

Executive Summary

ISO/IEC 12207:2008 (Systems and software engineering - Software life cycle processes) an international standard for software lifecycle processes) and COBIT5 (Control objectives for information and related technology, V5) which provides a comprehensive framework of globally accepted practices, analytical tools and models for the governance and management of information and technology were used as guidance materials for this audit. In addition, the COBIT5 and ISO/IEC 15504:2004 (Information Technology – Process Assessment) Capability Level model as shown below was used to assess the operating level of Citizens' SDLC.

COBIT 5 / ISO/IEC 15504 Based Capability Levels	Definitions - COBIT 5 / ISO/IEC 15504 Based Capability Levels	Context
5. Optimized	Continuously improved to meet relevant current and projected enterprise goals.	Enterprise view/ Corporate knowledge
4. Predictable	Operates within defined limits to achieve its process outcomes.	
3. Established	Implemented using a defined process that is capable of achieving its process outcomes.	
2. Managed	Implemented in a managed fashion (planned, monitored and adjusted) and its work products are appropriately established, controlled and maintained.	Instance view/ individual knowledge
1. Performed	Process achieves its process purpose.	
0. Incomplete	Not implemented or little or no evidence of any systematic achievement of the process purpose.	

Based on our audit work, it is OIA's conclusion that Citizens' SDLC is operating at Level 1 – Performed.

Audit Objectives and Scope

IT Management requested OIA to include this audit in the 2016 plan. The objective of this audit was to assess the adequacy of the governance structure and procedures and validate that the process is well controlled and has been implemented consistently and effectively.

This audit included activity which occurred between August 1, 2014 and December 31, 2015. Specific areas reviewed were:

- Alignment of Citizens' SDLC with ISO/IEC 12207:2008 and COBIT5
- Application of Citizens' SDLC criteria to software projects
- Compliance with Citizens' SDLC for qualifying software projects
- Availability of training materials

Management indicated at the onset of the audit that the process is still being matured and as such, OIA agreed to provide advisory services which could assist in accelerating the pace of the potential process improvements.

These services included:

- Reviewing the existing SDLC documents and offering process improvement recommendations.
- Locating any missing reference documents and resolving missing or broken document links. If there are multiple versions of a reference document, a recommendation is provided regarding the version to be used.
- Creating a mapping from the SDLC Planning and Compliance Checklist and Activity Guide for Deliverables to best practices ISO 12207 and COBIT5 to assist in ensuring compliance going forward.

The process improvement opportunities were discussed with management and OIA provided related materials.

Management's Assessment and Reporting on Controls

OIA provided IT Application Delivery 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 SDLC audit, IT Application Delivery management shared the following control weaknesses and remediation plans with OIA:

- Metrics have not yet been developed to measure and report on the performance of SDLC. Management stated that metrics will be developed to measure the performance of the SDLC by September 30, 2016, and that the performance of SDLC will be monitored and evaluated on a regular basis.
- SDLC has not been routinely and consistently applied to software enhancements. Management stated that criteria will be developed to determine those enhancements which require the application of SDLC by September 30, 2016.

Audit Opinion

Based upon our audit work, it is OIA's opinion that the design, implementation and operation of Citizens' SDLC is rated as **Needs Improvement**.

We noted that IT Application Delivery Management has keen knowledge of SDLC methods and is committed to developing a strong SDLC process. While the risk is not significant in terms of financial impact, solid foundational procedures and controls in software and systems development strengthen the quality of results and help improve productivity by limiting errors and re-work in projects.

Our audit work indicated the following opportunities to strengthen the controls associated with the alignment of SDLC to global standards and best practices and internal procedures, including:

- **The need to ensure that SDLC processes and deliverables are aligned with best practices based on global standards.** There is not an overarching procedures document which explains the SDLC process and the related documents. In addition, the basic elements of SDLC are not identified in SDLC processes and deliverables, and therefore may not be consistent among projects. Also, there are not links to templates for the activities related to integration, including the

system test plan, which is stated to address integration testing. Management has stated that SDLC processes and deliverable templates, including those related to integration, will be reviewed and revised to ensure that they are complete and effective. In addition, an overarching document which explains the SDLC process and the related documents will be created and published. The targeted completion date for these activities is 6/30/2016.

- **The need to ensure that SDLC is applied to projects which meet the SDLC criteria.** In assessing the application of the SDLC process, we noted that it was not consistently applied to all relevant development initiatives. As a result, these projects did not conform to organizational defined development requirements which include standard deliverables that should be considered. Management has stated that the project intake process was changed effective January 1, 2016 to ensure all new projects are brought to the IT Governance Committee (ITGC) to determine the need for SDLC Compliance. This process improvement will ensure that all projects are assessed with regards to the need to comply with SDLC. A report that shows the status of SDLC compliance on projects will be produced and reviewed at the ITGC meetings. This change will be implemented by 6/30/2016.
- **The need to ensure that SDLC checklists are properly prepared and kept updated as activities are completed.** Our assessment of projects that followed the defined SDLC process revealed that the SDLC checklist which is used to ensure that the process is followed, was not consistently created or maintained and supporting deliverables were not linked to the projects. As a result, these projects were not in compliance with the company policy and could have been at risk of requiring additional re-work subsequent to project completion. Management has stated that a quality assurance process will be developed to ensure that SDLC checklists are updated as activities are completed, including links to supporting documents. The target implementation date of the quality assurance process is 6/30/2016.

We would like to thank IT Application Delivery Management 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

Copies:

Business Leaders:
Barry Gilway, President/CEO/Executive Director
Kelly Booten, Chief – Systems and Operations
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
Chris Jobczynski, Director, Planning and Delivery

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*