CITIZENS
PROPERTY INSURANCE CORPORATION

The Office of the Internal Auditor 2018 Audit Strategy and Plan

Table of Contents

Introduction

This document serves as the Office of the Internal Auditor's (OIA) 2018 Audit Strategy and Plan (Plan) for Citizens Property Insurance Corporation (Citizens). The contents of this document have been shared with executive management and further address:

- Audit focus areas
- Plan analysis and areas not covered by the audit plan
- Service delivery and assurance
- Staffing and budgets

The Chief of Internal Audit currently oversees three complimentary assurance groups within Citizens which include Internal Audit, Enterprise Risk Management and Internal Control Monitoring. The 2018 Office of Internal Audit Strategy and Plan are presented to the Audit Committee for consideration and approval.

Executive Summary

The mission of Citizens' OIA is to provide an independent, objective assurance and consulting activity designed to add value and improve Citizens' operations.

2.1. Background on Citizens Property Insurance Corporation

Citizens operates according to statutory requirements created by the Florida Legislature and a Plan of Operation approved by the Florida Financial Services Commission. In essence, Citizens was formed to provide affordable property insurance to applicants who are in good faith entitled to procure insurance through the voluntary market but are unable to do so (i.e. the insurer of last resort). The corporation is subject to operational reviews and examinations by the Florida Office of Insurance Regulation and the Florida Auditor General, and its financial statements are a major component unit of the Florida Comprehensive Annual Financial Report. Citizens has offices in Tallahassee, Jacksonville and Tampa.

2.2. Audit approach

In alignment with our mission, OIA uses a Collaborative Audit approach in supporting Citizens in the achievement of its strategic goals and ultimately, to provide independent and objective assurance over the organization's internal control environment to the Audit Committee, Board of Governors and Management. The objective of this Plan is to provide the most timely and comprehensive scope of audit coverage to Citizens by using resources available to the OIA. Since it is impractical to provide audit coverage to the entire corporation on an annual basis, we, in consultation with management across the organization, performed a review of the audit universe and prioritized efforts consistent with risks recorded. As part of the analysis, we also determined the best type of service to address each set of risks and circumstances.

2.3. Audit plan & process

OIA follows a detailed annual planning process, which is regularly revisited throughout the year, and adjusted to accommodate for changes in the organization's risk/opportunity profile.

- *Defining the audit universe*

  In determining the corporation's audit universe (or range of all audit activities), we engaged with management across the organization and assessed potential auditable entities. These entities included a range of programs, activities, functions, structures and initiatives, which collectively contribute to the achievement of Citizens' strategic objectives. For 2018, Citizens' strategic goals are to:

  - Operate as an efficient residual market
  - Ensure a strong financial operating environment
  - Operate a streamlined, scalable and customer-focused organization
  - Protect the public interest and maintain the integrity of the Corporation
  - Identify, educate and effectively communicate with internal and external stakeholders

- *Prioritizing work to be performed by Internal Audit*

  The primary responsibility of the OIA is to determine whether Citizens' network of governance processes, risk/opportunity management, and internal control, as designed and represented by management, is adequate and functioning in a manner to ensure that:

  - Risks/opportunities are appropriately identified and managed.
  - Interaction with the various governance groups occurs, as needed.
  - Significant financial, managerial, and operating information is accurate, reliable and timely.
  - Employees' actions comply with policies, standards, procedures and applicable laws and regulations.
  - Resources are acquired economically, used efficiently, and protected adequately.
  - Programs, plans and objectives are achieved.
  - Quality and continuous improvement are fostered in Citizens' control process.
  - Significant legislative or regulatory issues affecting Citizens are recognized and addressed appropriately.
  - Prioritizing the units to be reviewed or audited was based on the relative risks/opportunities associated with each of them. Risk factors considered while reviewing the units in the Universe included the Control Environment; Business Exposure; Compliance Requirements; Reputational/Image Factor; Organizational Change or Growth; and Management and Internal Audit Discretion.

- *Determining the types of services to be performed*
  Following the completion of a detailed analysis of the Corporation's strategic goals and objectives, management's concerns and OIA's risk assessment, OIA determined and planned audit activities to provide coverage. Engagements carried out by OIA can take many forms. OIA realizes that pure assurance activities are not the only solution to accomplish our goals and offers other services to add value to the company. These alternative activities include, but are not limited to:

  - Audit (Assurance) activity – involves the objective examination of evidence for the purpose of providing an independent assessment on governance, risk management, and control processes for the organization. Through audits the OIA assesses, among other, the adequacy of: internal control; risk management; governance process; compliance with laws or regulations, project management process; occupational fraud mitigation practices.
  - Consulting (Advisory) services - are provided generally at the specific request of a member of management or a process owner in the organization and are intended to add value and improve Citizens' governance, risk management, and control processes without assuming management responsibility.
  - Investigations - research and validation activities support various constituents in the process of determining the legitimacy of a reported suspicion by providing independent, objective financial and process related expertise.
  - Training/Education - detailed training aimed at educating management, employees and associated third parties on risk, control, process and financial related matters, and
  - Risk Assessments - activities to assess, identify, and highlight current and emerging risks that may affect the Company.

- *Coordination with other Assurance Providers*
  In developing this audit plan and approach, OIA consulted with other internal and external assurance providers to ensure that 2018 operational plans support or complement the audit plan including Citizens' Inspector General. This ensures duplication of work is minimized. The audit schedule will be shared with the external auditors, Dixon Hughes Goodman, and we will continue our discussion with them as the year progresses and adjust the plan, where appropriate, in order to provide them the opportunity to rely on OIA's work product where appropriate.

OIA Mandate

The purpose, authority, and responsibility of the OIA are formally defined in the internal audit charter. This charter is consistent with the Definition of Internal Auditing, the Code of Ethics and the International Standards for the Professional Practice of Internal Auditing as defined by the Institute of Internal Auditors. The Chief of Internal Audit annually reviews the audit charter and presents it to senior management and the board for approval.

3.1. Duties and Responsibilities

In accordance with Section 627.351(6)(i) Florida Statutes, it is the duty and responsibility of the Chief of Internal Audit to:

- Provide direction for the OIA including supervising, conducting and coordinating audits, investigations and management reviews relating to Citizens' programs and operations.
- Conduct, supervise or coordinate other activities carried out or financed by Citizens for promoting efficiency in the administration of, or prevention and detection of, fraud, abuse and mismanagement in its programs and operations.
- Submit final audit reports, reviews or investigative reports to the Board, the Executive Director, the members of the Financial Services Commission, the President of the Senate and the Speaker of the House of Representatives.
- Keep the Board informed concerning fraud, abuses and internal control deficiencies relating to programs and operations administered or financed by Citizens; make recommendations for corrective action; and report on the progress made in implementing corrective action.
- Cooperate and coordinate activities with the corporation's Inspector General.

3.2. Standards of Audit Practice

In addition to the requirements specified by Section 627.351(6)(i) Florida Statutes, OIA elected to follow the International Standards for the Professional Practice of Internal Auditing for all engagements.

The OIA further uses accepted industry frameworks for guidance when conducting audits. These include the Committee of Sponsoring Organizations of the Treadway Commission (COSO) internal control framework for financial/operations/compliance audits; the Control Objectives for Information and related Technology (COBIT), the Information Technology Governance Institute (ITGI), the National Institute of Standards and Technology (NIST) and Information Technology Infrastructure Library (ITIL) when conducting technology audits.

Organization and Administration

The Chief of Internal Audit was appointed by the Audit Committee, a committee of the Board of Governors, and reports directly to and is under the general supervision of the Audit Committee. Under the guidance of the Committee and in support of Citizens' management, the Chief of Internal Audit established a team of audit, risk and control professionals to provide assurance and consulting activity, which is designed to add value and improve the corporation's operations.

Organization Chart
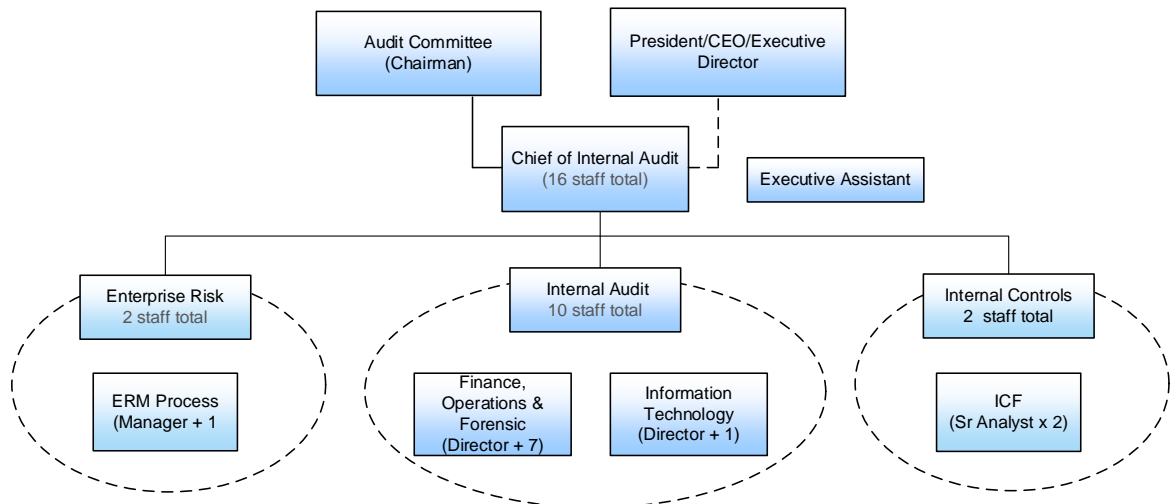
Apart from the Office of Internal Audit the Chief of Internal Audit also directs the scope and focus of the Enterprise Risk and Internal Control Offices. Within its mission statement the OIA is to accomplish its objectives by bringing a systemic disciplined approach to improve the effectiveness of governance, risk management, and internal control processes throughout Citizens. Benefits from combining these functions include reducing the span of control necessary to manage them individually; improving efficiency and synergies from having all expertise related to assurance, governance, risk, and internal control under one umbrella; a more holistic approach on risk and control activities driven by one shared vision; and the vision and strategy is executed by a group of professionals with a similar mindset as well as complementary competencies.

When combining internal audit and other assurance functions it is important that there is full transparency regarding the considerations involved in formalizing the organization's assurance model. This is important not only to ensure compliance with the international standards for the professional practice of internal auditing, but also to ensure the full support and commitment of senior management and the Audit Committee in order to remain true value-adding business partners.

Audit Strategy

OIA aligned the 2018 audit strategy with Citizens' strategic objectives and goals utilizing information derived from OIA's annual enterprise risk assessment and consultation with management. Additionally, OIA assesses risk at operational levels and performs detailed risk assessments on specific risks (i.e., occupational fraud, information technology, finance and operations) to understand likelihood and impact on the organization. This information is aggregated, allowing OIA to identify the risks that have the highest impact and likelihood of occurrence to preclude the company from achieving its' strategic goals and objectives. This "Top Down" approach allows for the proper alignment of audit activities to provide assurance and mitigate risk within the organization at the enterprise and process levels.

5.1. OIA Mission

Our mission is to enhance and protect organizational value by providing independent risk-based and objective assurance, advice, and insight.

5.2. OIA Vision

We are *innovative drivers for positive change* recognized for delivering excellence while striving to be the most trusted and respected service organization in Citizens.

5.3. OIA Values

In support of OIA's mission and aligned with Citizens values we adopted:

- *Forward Thinking*: We provide excellence by being insightful, proactive, and future focused.
- *Teamwork*: We are a solidified team that works together cooperatively and efficiently.
- *Trusted and Respected*: We embrace the highest level of integrity and treat all people with dignity and respect.
- *Professional and Courteous*: We respectfully follow the standards for professional practice of IA while being polite and courteous to others.
- *Responsive to Risk and Customers*: We will understand the changing assurance needs of Citizens and respond by being flexible in our planning and delivery.
- *Fair and Balanced*: We provide unbiased, balanced, and practical solutions.

Audit Approach, Plan, and Budget for 2018

Following the completion of a detailed analysis of the corporation, including an understanding of the organization's strategic direction and associated strategic objectives, an analysis of the organization's top business risks and their potential impact upon the audit universe, the OIA identified its audit priorities for 2018.

It should be noted that this plan is flexible and changes as the risk profile of the organization changes. This flexibility allows for realignment of audit focus to areas or issues of most importance.

6.1. Finance and Operations

The audit plan for Finance and Operations is focused on core business areas and support functions with generally higher levels of risk, and includes the following:

- Underwriting and Agency Services

  In 2016, Personal and Commercial Lines Underwriting were consolidated with Consumer and Agent Services. Throughout 2017, the area focused on several initiatives designed to increase efficiency:

  - The initial phase of the Automated Underwriting (AUW) Initiative focused on automating throughput of new business submissions and policy changes for all lines of business. In October 2017, 100% auto-issuance of submitted bound policies was achieved. As a result of the 2017 OIA AUW audit and the onboarding of the new Underwriting Vice President, several process improvements related to AUW are in the process of being implemented. For 2018, plans are to expand

automated capabilities to include risk parameters to automate underwriting decisions whenever possible. OIA will provide assurance services focused on enhancements to the automated underwriting process.

- New products and services will offer enhanced self-service capabilities to potential policyholders, and agents enabling more efficient, cost effective, and user friendly transactions. OIA will provide advisory support to management during the implementation of self-service capabilities.

- A solicitation is in progress to procure a replacement for the current agency management system that will support tracking and monitoring of agent licenses, commissions, investigations, complaints and key performance indicators. OIA will support management throughout the replacement of the agency management system to ensure appropriate controls are designed and implemented.

Consumer Services experienced significant increases in call volumes due to Hurricane Irma. Approximately 750 call vendor personnel were activated to answer calls. As of October 2017, over 90,000 Irma calls were received. Post Irma considerations may lead to process improvements and adjustments to the Catastrophe Plan for Underwriting and Agency Services. OIA will provide advice and support in identifying improvement opportunities based on Citizens' experience with Irma.

The Voice of the Customer Program measures customer satisfaction through surveys designed to assess service excellence and identify opportunities for improvement. During 2018, OIA will provide assurance services regarding the effectiveness and efficiency of the Voice of the Customer Program and to determine if improvements identified from the program are thoroughly validated, appropriately designed, and implemented.

- Claims

The Claims function implemented a Managed Repair Program, a key component of the water loss mitigation initiative. Effective July 2017, two new endorsements are attached to every new and renewed HO-3 and DP-3 policy. The endorsements allow Citizens to offer free water mitigation services for emergency water extraction and drying and a mutual consent Managed Repair Program for permanent repairs with the application of the policy deductible. The program initially applies to non-weather water claims with plans to expand to other peril losses. OIA will assess the deployment of the Managed Repair Program to ensure the program is operating as expected.

On September 10, 2017 Hurricane Irma created significant property damage in the Florida Keys and other portions of the state. Citizens activated the Catastrophe Response Plan prior to storm landfall in preparation to meet the needs of policyholders. The storm resulted in Citizens receiving over 60,000 claims, making it the second largest claim generating event in Citizens' history. OIA identified areas

with increased risk and developed targeted audits to provide operational assistance during the 4th quarter of 2017. Post Irma considerations may lead to process improvements and adjustments to the Catastrophe Plan for Claims. OIA will provide advice and support in identifying improvement opportunities based on Citizens' experience with Irma.

Guidewire software is utilized to support core insurance business functions in the Citizens Insurance Suite. In order to maintain Guidewire support and take advantage of improved functionality, an upgrade to version 9 will occur in a phased approach beginning with ClaimCenter. Advisory support will be provided to management for the Guidewire upgrade.

- Human Resources
In September of 2016, Citizens began offering formal alternative work arrangements (AWA) that permit eligible Citizens employees to work from an alternate worksite on specific days or the entire work week. As Citizens transitions out of the Tampa facility by June 2019, more employees may be eligible to participate in the program full time. An audit will be conducted to assess controls in place related to management of AWA employees, productivity monitoring and analysis, and compliance with corporate policy.

During the first part of 2018, Human Resources plans to develop and deliver a Strategic Workforce Program to determine current and future staffing needs which business units will be able to utilize for planning and budgeting purposes. OIA will provide advisory support for this initiative.

Centerpoint, Citizens' integrated ERP solution, will replace the existing Human Resource applications Kronos, Org Plus, and SuccessPath. The Human Capital Management (HCM), Recruiting and Advanced HCM phases of the project include self-service, benefits administration, timekeeping, payroll, recruiting, and performance and talent management. The phases are expected to be implemented December 2017 through May 2018. OIA will continue to provide advisory support throughout the implementation of Centerpoint.

- Vendor Management
The Vendor Management Office (VMO) was created in 2014. VMO facilitates Citizens' Vendor Management Strategy to effectively implement and oversee the vendor governance life cycle including vendor engagement, selection, management, and mitigation of risks. A comprehensive, mature VMO model has been established. In 2018, OIA will review the vendor management processes.

- Financial Services

Financial Services is comprised of four areas which include Actuarial Services, Corporate Analytics, Finance and Accounting and Treasury and Investments.

Actuarial Services' primary responsibilities are loss reserving and support rate making. Rate making includes determining of actuarial sound rate levels for each product, and, where appropriate, file these results with the Florida Office of Insurance Regulation (OIR). Rate making is performed at least annually for all lines of business and completed in partnership between Actuarial Services and the Product Development function within UAS. Loss reserving involves the evaluation of various segments of business and determining the proper amount of additional funds that need to be put aside to pay for future claims losses on past events, which is performed quarterly.

Corporate Analytics' focus areas includes Catastrophe Modeling, Forecasting and Research, Geographic Information Systems and Reporting/Analytics. Catastrophe modeling is used to estimate Citizens' exposure to hurricane risk, a critical element in ratemaking, reserve review, liquidity and claims paying analyses, risk transfer decisions, legislative inquiries, and projecting live hurricane losses. Forecasting and research supports strategic planning, budgeting, and risk transfer programming for Citizens. Geographic Information Systems harnesses geographical and demographic data for a variety of purposes, including hurricane response during and after a storm. Finally, the Reporting/Analytics team provides critical data that helps senior executives inform Citizens stakeholders, including the Florida Legislature and Cabinet, as they make critical decisions regarding Citizens' role.

Finance and Accounting is continuing to focus on designing and implementing the Budgeting module as part of an integrated enterprise resource planning (ERP) system (referred to as Centerpoint). The Oracle Fusion Cloud Service, an ERP solution, was procured early in 2016 and is continuing to be implemented utilizing a phased approach. Specific process areas impacted by this implementation includes human resources, accounting, purchasing, and vendor management, among others. The 'Financials' phase of the ERP solution (Phase 1) replaced and enhanced the general ledger, accounts payable processing, cash management, employee expense processing, and purchase requisitioning, and was implemented in April 2017. The 'Budgeting' phase (Phase 3) will kick-off in January 2018 and is expected to be implemented July 2018. For 2018 we will continue to provide advisory services with focus on the Centerpoint project thereby ensuring that appropriate controls are in place throughout the ERP implementation. Furthermore, we will perform a post implementation audit of Centerpoint Phases 1 & 2 to provide assurance that processes and controls are designed and operating effectively.

Treasury & Investments is tasked with managing the Company's investment portfolio primarily through external investment money managers. During 2017, Citizens replaced the vendor application utilized to monitor investment manager performance and compliance with Citizens investment policies. OIA will focus on providing assurance that the new vendor application is effectively aligned to the Company's Investment policies and adequately monitoring investment activity. Furthermore, OIA will assist Citizens' Treasury function in identifying opportunities to automate the cash management function through industry best practices.

Citizens, as the insurance provider of last resort for the State of Florida, is entrusted with public funds through the collection of insurance premiums. Citizens annual financial planning and analysis process and ongoing income and expense management is an important element in the protection of assets and the management of cost. OIA will assess the efficiency of the newly developed ABC Budgeting process, including the ongoing monitoring and management of the budget variances throughout the year.

Resource Allocation (Fin/Ops)	Hours

Audit Engagements
Underwriting and Agency Services:
  (1) Automated Underwriting – 350 hrs
  (2) Voice of the Customer Program – 350 hrs
Claims:
  (3) Managed Repair Program – 350 hrs
  (4) Claims Coverage/Payment Process – 350 hrs
Financial Services:
  (5) ABC Budgeting – 350 hrs
  (6) Investment Management – 350 hrs
  (7) Centerpoint Phase 1 & 2 Post-Implementation – 350 hrs
Human Resources:
  (8) Alternative Work Arrangements – 350 hrs
Communications, Legislative & External Affairs:
  (9) Social Media – 350 hrs
Systems & Operations:
  (10) Vendor Management – 350 hrs
	3,500

Advisory Engagements
  (11) Treasury Management Automation Best Practices – 300 hrs
  (12) Strategic Workforce Planning – 300 hrs
	600

Project Monitoring (13) Centerpoint Phase 3 Budgeting - 100 hrs (14) Centerpoint Phases 4 & 5 Human Resources – 100 hrs (15) Guidewire V9 Upgrade – 100 hrs (16) Post Irma Considerations – 100 hrs (17) Special VMO Project – 100 hrs (18) Self-Service Strategy – 100 hrs (19) Agency Management System – 100 hrs	700
FIN/OPS TOTAL:	4,800
Data Analytics	1,200
TOTAL	6,000

(*See Appendix 3 for an overview of the planned Fin/Ops audits*)

6.2. Compliance and Forensic Audit

OIA continues to proactively develop and support a company culture that embraces mitigation efforts for fraud, waste and abuse and compliance with Company policy and State & Federal regulation, thus reducing cost associated with these activities. OIA is in the process of establishing a dedicated team of professionals whose focus is on forensic and compliance audit activities.

For forensic audit, OIA will focus on fraud deterrence by performing activities related to the following categories:

- Deterrence - assessing policies & procedures, performing risk assessments, and training, as well as other activities geared at improving the Company's anti-fraud culture.
- Detection - performing data analysis activities in an effort to proactively detect and mitigate fraud. OIA will continue developing "best practice" fraud analytic tests to be used in the general audit programs for monitoring.
- Investigation - responding to instances of fraud, waste, and abuse as well as initiating appropriate investigative methods through document and case management and collaboration.

The Company is currently implementing a comprehensive operational compliance governance framework. The ultimate goal of implementing the framework is to foster full compliance by Citizens to all relevant laws, rules and regulations (LRR). This will be accomplished by using a systematic, documented, enterprise approach that involves identification of all relevant LRRs, education and training of appropriate staff, integration of LRRs into work processes, procedures, and corporate policies, monitoring for adherence to LRR, updating as requirements change, and addressing areas of noncompliance in a strategic risk based fashion. In 2018, OIA will assess the effectiveness of the organization's compliance function and determine if formal procedures have been applied across the organization to ensure consistency in managing compliance governance.

Resource Allocation (Compliance and Forensic)	Hours
Audit Engagements (1) Compliance Governance Follow Up – 350 hrs (2) Unclaimed Property Operational Process – 400 hrs	750
Advisory Engagements (3) Legislative Changes – 100 hrs	100
COMPLIANCE TOTAL:	850
Forensic Audit	1,200
TOTAL	2,050

(*See Appendix 3 for an overview of the planned forensic and compliance engagements*)

6.3. Information Systems and Technology

In developing the 2018 audit plan, OIA met with individuals at all levels of IT management to discuss strategic and operational risks as well as current and upcoming projects. We also reviewed industry practice and surveys to determine potential IT risks that may be applicable to the Citizens environment. Together with IT management we identified engagements that support IT objectives and add value toward strategic initiatives and/or evaluate control practices that contribute to achieving appropriate risk tolerance within the organization. At the program level, four advisories were identified:

- Data Retention policies and procedures are required to ensure that documents are retained in accordance with laws and regulations as well as ongoing business needs. Absent formal guidance by Management, data may not be able to be retrieved when required and costs may outweigh benefits in retaining obsolete data. Management indicated there may be opportunities to improve the processes that are driven by regulatory compliance and business requirements. OIA will perform an Advisory engagement and assess the interpretation of the laws and corresponding practices to provide enhancement recommendations for retaining and disposing data.

- In 2017, IT management implemented a new enterprise planning and delivery methodology based upon an industry leading framework. "Enterprise Rhythm" is a transformative program with the goals of expanding economic decision making and improving delivery predictability, throughput and quality as well as development of pre-defined performance metrics, elimination of administrative overhead and improved employee engagement. OIA will evaluate program components and assess the effectiveness and efficiency of the program against industry practice and management's overall goals and objectives.

- A formal IT Security Compliance framework and self-assessment program are being deliberated. IT Security Compliance practices can comprise several elements within an organization, depending upon the compliance obligations and specific business

challenges. These elements should be considered in a business oriented approach that utilizes a risk based foundation to analyze, implement and monitor security controls. OIA will support management in the development of an effective compliance self-assessment program by researching leading frameworks, practices and information to create and implement this component of IT Security governance. Work completed as part of the Internal Controls Framework program will be leveraged for the engagement.

- IT initiated the Disaster Recovery Strategy Transition Plan project, in 2015, as a formal method to ensure that key objectives of the Disaster Recovery Strategic Plan are realized and that potential intersecting projects do not conflict with the strategic objectives. A component of the project will be to migrate the current backup data center located in Tampa to a new purpose-built co-location facility in 2018 that will support business continuity via a viable reactive plan and location to restore systems and services in the event of an outage. Due to the significance of disaster recovery in overall business resiliency, OIA will validate that the transition and new facility effectively support corporate resiliency objectives.

IT management continues to focus on cyber security and completed several initiatives this year. A risk management framework was developed with implementation underway. A new GRC tool was purchased to track compliance efforts. Security awareness was expanded to include additional employee informational bulletins and targeted communications. And new security standards reflect the adoption of the leading practices Critical Security Controls framework. IT Management is currently assessing process gaps against the new standards with plans to implement additional control practices as required. OIA will provide assurance related engagements that focus on cyber-security operational processes to support the standards implementation as well as other processes that are essential in supporting IT objectives. Three assurance engagements will be performed in the areas of Cyber Security and Infrastructure Management, both of which contribute to the success of corporate risk management objectives:

- OIA will evaluate project governance and the effectiveness of the standards implementation, including the gap analysis process, assessment and prioritization of new control practices and the compliance methodology used to validate the changes.

- Third party security comprises external connections and user activities for any third parties requiring access to applications or devices residing in the Citizens network and is a component of cyber security practices. Mitigation of third party risks such as data tampering or data compromise, requires an understanding of external user access levels and potential changes occurring on sensitive assets. OIA has not previously performed an assessment of these controls so will evaluate the risks and associated control practices related to third party risk mitigation to ensure appropriate visibility within this set of users and network connections.

- An IT Infrastructure Management audit will be performed to evaluate the design and effectiveness of control practices associated with capacity and performance management. These areas have also not been assessed previously. Additionally,

processes and procedures related to infrastructure hardening and maintenance will be evaluated against leading practices and the new IT Security standards.

Specific engagements included in the plan are:

Resource Allocation (IT)	Hours
Audit Engagements (1) IT Sec Critical Controls and Standards Implementation – 350 hrs (2) IT Infrastructure Management – 350 hrs (3) Third Party Access – 350 hrs	1050
Advisory Engagements (4) Data Retention – 100 hrs (5) Enterprise Rhythm – 300 hrs (6) IT Security Compliance Program – 300 hrs (7) Disaster Recovery Strategy Transition Program (Tampa Data Center Migration) – 100 hrs	800
TOTAL:	1850

(*See Appendix 3 for an overview of the planned IT audits*)

6.4. OIA Budget

The 2018 budget for Citizens' OIA presented is $2.26 million as compared to $2.28 million budgeted for 2017. As we continue to develop our staff and hire more business qualified individuals we improve upon the type and quality of audits we complete which has a direct impact upon cost.

2018 Budget Analysis					
OIA Expense Categories	**2016 Approved Budget**	**2017 Approved Budget**	**2018 Approved Budget**	**$ Change**	**% of Total Proposed Budget**
Salaries & Benefits	1,902,767	1,951,788	2,038,455	86,667	4%
Contingent Staffing	-	109,200	-	-109,200	-100%
Professional Services	50,000	75,000	75,000	-	0%
Training	30,000	29,800	31,200	1,400	5%
Operating Expenses	40,000	84,065	76,067	-7,998	-10%
Legal	55,950	40,000	40,000	-	0%
Total	**2,078,717**	**2,289,853**	**2,260,722**	**-29,131**	**-1%**

- **Salaries & benefits**: Salaries & Benefits reflect the annual inflationary merit as well as the onboarding of a Forensic Audit Manager and his staff.
- **Professional Services & Contingent staffing**: Traditionally this amount is a placeholder should the department need external support. This year we do not think that there will be a need for contingent staff.
- **Training**: Training is based on a dollar allocation per staff member to upkeep professional CPE requirements and develop professionally. Staff is required to complete at least 80 hours of productive training (combination of external and internal).
- **Legal**: Traditionally this amount is a placeholder should the department need to use external legal services.
- **Operating expenses**: Year on year operating expenses are relatively stable.

6.5. Allocation of Audit Hours

In developing the audit plan, we ensure that we allocate sufficient time for the completion of other non-audit related tasks as well as personal time off. At the same time we plan so that approximately 70% of all available hours in a year are directed towards assurance and consulting (advisory). The table below provides a breakdown of direct audit hour allocation in 2018.

| Audit Plan Component	Allo-cation	Explanation
Planned Audits	59%	Includes audits selected through the risk assessment and prioritization process.
Planned Advisories	31%	This category includes requests from the Audit Committee, Executive/Senior Management, etc. This may be planned requests or contingency for unplanned events (such as investigations). Requests are within the internal audit mandate and include advisory engagements, as long as such engagements have the potential to improve management of risks, add value and improve operations.
Observation follow-up	5%	Represents approximately one day at each month end to follow-up on open findings and validate closure of closed findings.
Contingency	5%	Part of the audit plan set aside for other and unforeseen items such as assistance for external auditors and quality assurance reviews, employee turnover, overruns, etc.
Direct hours	100%	Total hours available for audit (total hours net of vacation, statutory holidays, sick time, administration, training, etc.)

Citizens Enterprise Risk Management

Citizens' Enterprise Risk Office (ERO) 2018 focus areas will be to:

- Roll-out a refined Strategic Risk Management process.
- Continue embedding an Operational Risk Management process and conducting operational risk assessments throughout the organization.
- Complete the implementation and roll-out of a new ERM platform.

In 2017 the ERO identified three focus areas: Strategic Risk Management; Operational Risk Management; and Project Risk Management
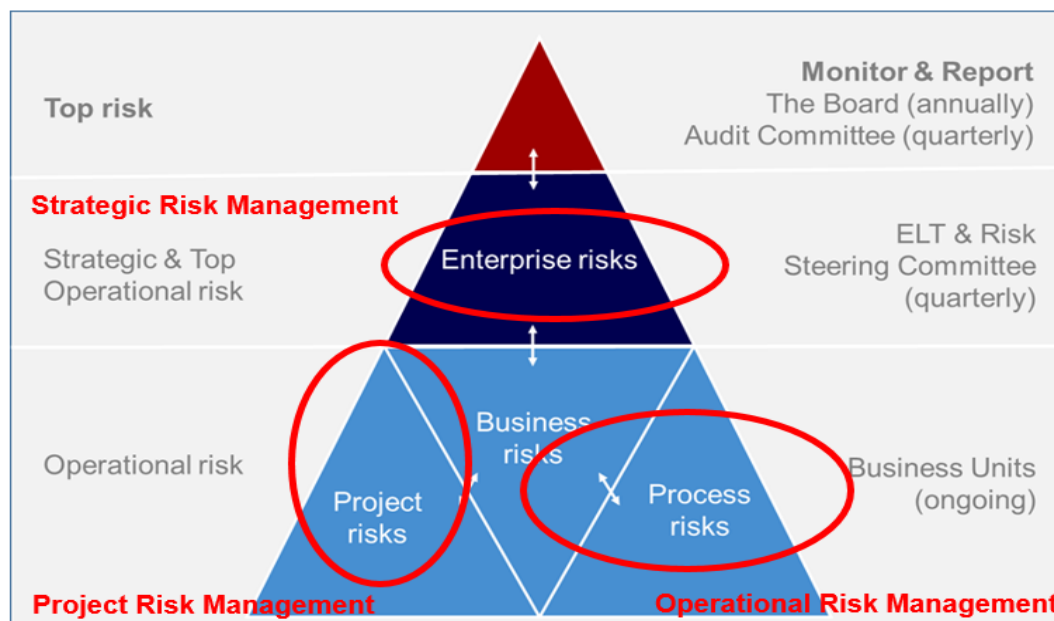
7.1. Strategic Risk Management

The primary focus of Strategic Risk Management (SRM) will be the identification, assessment, mitigation, monitoring and reporting of the key enterprise risks that may prevent Citizens from achieving its Strategic Objectives and Key Strategic Initiatives identified in the Strategic and Annual Plans. Key stakeholders for SRM include:
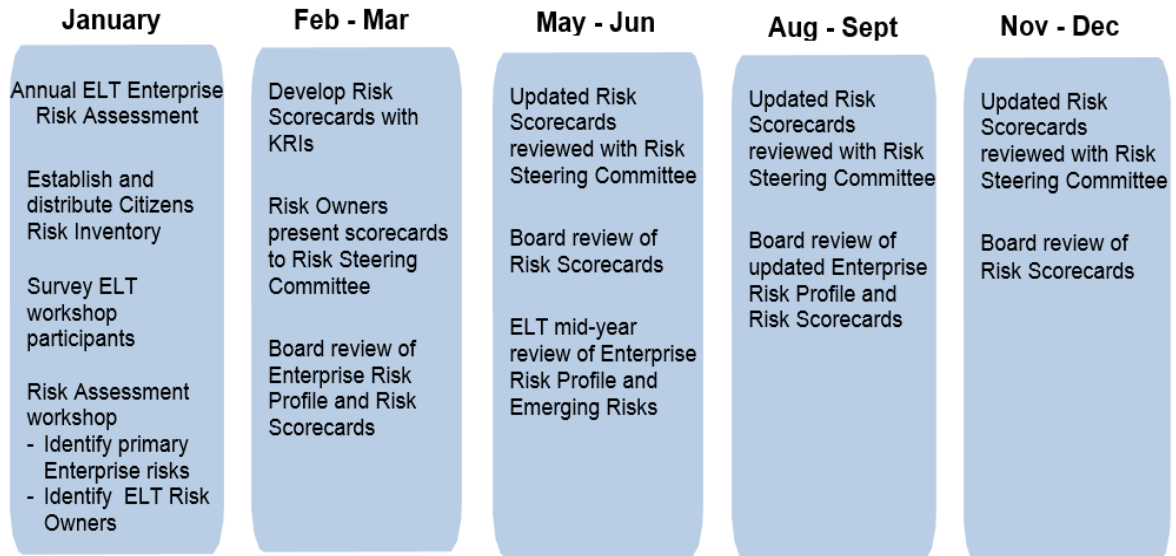
- Board and Audit Committee
- Executive and Senior Leadership Teams – ELT and SLT
- Risk Steering Committee (RSC)
- Business Unit leadership
- Assurance functions – Compliance, Internal Audit, IT Security, Internal Controls Office

SRM will be embedded within the Strategic and annual planning processes and aligned with the annual Board calendar and will enable the discussion and prioritization of the key enterprise risks by the Executive Leadership Team (ELT).

January	Feb - Mar	May - Jun	Aug - Sept	Nov - Dec
Annual ELT Enterprise Risk Assessment Establish and distribute Citizens Risk Inventory Survey ELT workshop participants Risk Assessment workshop - Identify primary Enterprise risks - Identify ELT Risk Owners	Develop Risk Scorecards with KRIs Risk Owners present scorecards to Risk Steering Committee Board review of Enterprise Risk Profile and Risk Scorecards	Updated Risk Scorecards reviewed with Risk Steering Committee Board review of Risk Scorecards ELT mid-year review of Enterprise Risk Profile and Emerging Risks	Updated Risk Scorecards reviewed with Risk Steering Committee Board review of updated Enterprise Risk Profile and Risk Scorecards	Updated Risk Scorecards reviewed with Risk Steering Committee Board review of Risk Scorecards

7.2. Operational Risk Management

The focus of the Operational Risk Management (ORM) will be the identification, assessment, mitigation, monitoring and reporting of the risks to day-to-day operations at Citizens. Operational risks typically deal with people, processes and systems. In addition, a primary objective of the ORM process will be to enhance Citizens' risk culture within operational management, business units and functional areas. The ORM process is intended to foster a culture where the organization embraces incorporating risk management decisions into their daily decision making and activities.

In 2018 the operational risk assessments will be coordinated with the Internal Controls Framework processes and follow that program timeline. By integrating the ERM and ICF processes we will have completed operational risk assessments and internal control reviews for 71 of the 76 defined Citizens' processes (93% coverage) by early 2019. (See Appendix 1)

Below is a summary of Operational Risk Management work completed in 2017 and planned for 2018:

- In 2017, completed operational risk assessments for 21 processes – 28% of the 76 defined processes
- 2018 plan is to complete operational risk assessments for another 50 processes – bringing the total to 71 of the 76, 93% coverage
- In 2019 we will complete the remaining 5 processes and initiate updates for processes completed in 2017

7.3. Project Risk Management

The focus of the Project Risk Management (PRM) process will be twofold:

- Enhance the existing process within the Project Initiation and Analysis Phase of Citizens' project management methodology to assist the business unit and project managers with evaluating project risk.

- Develop and implement a project risk management process to assist project managers and the Project Management Office (PMO) with the identification, assessment, mitigation and monitoring of key project risks for selected high-priority and key strategic projects.

- The PRM work in 2018 will be addressed following the roll-out of the Strategic Risk Management process and completion of the Operational Risk Management initiatives.

7.4. ERO Budget

The 2018 budget for Enterprise Risk presented is $421 thousand as compared to $524 thousand budgeted for 2017.

2018 Budget Analysis					
ERO Expense Categories	**2016 Actual**	**2017 Approved Budget**	**2018 Proposed Budget**	**$ Change**	**% of Total Proposed Budget**
Salaries & Benefits	379,483	411,916	292,869	-119,047	-29%
Contingent Staffing	51,692	-	-	-	0%
Professional Services	972	50,000	15,000	-35,000	-70%
Training	7,872	7,600	5,200	-2,400	-32%
Operating Expenses	89,448	55,250	108,500	53,250	96%
Legal	-	-	-	-	0%
Total	**529,467**	**524,766**	**421,569**	**-103,197**	**-20%**

- **Salaries & benefits**: Salaries & Benefits reflect the reduction in staff following changes within the ERO structure.
- **Professional Services**: This amount is a placeholder should the department need external support.
- **Training**: Training is based on a dollar allocation per staff member to upkeep professional CPE requirements and develop professionally. Staff is required to complete at least 80 hours of productive training (combination of external and internal.
- **Operating expenses**: The increase reflects the anticipated acquisition and implementation of an ERM application.

Citizens Internal Control Framework

The Internal Controls Office ("ICO") continues to make progress on its review of Citizens' Internal Control Framework. Following a collaborate effort between OIA, ERO and ICO a single process universe with 76 processes, of which 69 are eligible for inclusion in the ICF, have been identified. As of November 2017, 37 out of the 69 process and control reviews have been completed (See Appendix 1 for detail of the process universe). The ICO will continue process and control reviews on additional process areas through 2019.

Each review involves understanding, documenting, and testing identified primary controls in line with COSO 2013, the industry standard for internal control frameworks. There are 16 process and control reviews planned for 2018. Of these 16 reviews, 11 process and control reviews are in the Information Technology ("IT") function. In performing the IT reviews, we will be following the COBIT 5 framework in alignment with COSO 2013 to complete the internal control assessments. See the "Process Reviews" section of the ICO Resource Allocation schedule below for detail of these 16 processes.

In addition to the 16 process and control reviews planned for 2018, the ICO will continue transitioning a larger majority of the ownership of control assessments and documentation updates to the business functions in alignment with control awareness and accountability objectives through control self-assessments. This transition includes the continued development, refinement, and administration of training to business unit representatives in the areas of control self-assessment execution as well as training within the control management system used to facilitate the control self-assessments. Finally, as significant changes occur in these processes undergoing control self-assessments, management may also engage the ICO to perform hands-on consultation to refine process documentation and testing procedures in accordance with the standards of the Internal Control Framework.

In 2018, 34 processes will be subject to a control self-assessment. As 2018 will be the first year most of the Framework, the ICO will initiate a quality assurance program in 2019 for reviews completed during control self-assessment year 2018. In order to maximize effectiveness as well as efficiently utilize management's time, the ICO will work closely with the Enterprise Risk Office ("ERO") to execute the 2018 plan and gain efficiencies where plans align. See Appendix 4 for additional detail on the 2018 ICO plan.

We anticipate the following will be required to execute on the ICO plan above:

Resource Allocation (ICF)	Hours
Process Reviews: Legal & Compliance: Corporate Insurance (100hrs) Records Management (100hrs) Purchasing (Non-competitive) (120hrs)	320
Finance & Accounting: Financial Planning & Analysis (120hrs)	120

Systems & Operations: Facilities Management (120hrs) IT Change Management (120hrs) Technical Operations Center (120hrs) IT Strategy and Planning (120hrs) IT-Business Unit Communications (60hrs) IT Finance Management (120hrs) Enterprise Architecture (120hrs) IT Operations (180hrs) Application Development (280hrs) Application Delivery (120hrs) Application Quality Assurance (120hrs) IT Infrastructure (180hrs)	1660
Control Self-Assessment Administration: Business Unit Scheduling Period (40hrs) Hands-on Assistance with CSA Performance (480hrs) Issue Follow-up (60hrs) Business Unit Calibration / Post Mortem (80hrs)	40 480 60 80
TOTAL:	**2760**

8.1. ICO Budget

The 2018 budget for Citizens' ICO presented is $286 thousand as compared to $262 thousand budgeted for 2017.

2018 Budget Analysis					
ICO Expense Categories	**2016 Actual**	**2017 Approved Budget**	**2018 Proposed Budget**	**$ Change**	**% of Total Proposed Budget**
Salaries & Benefits	116,613	232,003	245,796	13,794	6%
Contingent Staffing	-	-	-	-	0%
Professional Services	6,000	0	15,000	15,000	100%
Training	3,358	4,000	5,200	1,200	30%
Operating Expenses	29,371	26,009	20,427	-5,582	-21%
Legal	-	-	-	-	0%
Total	**155,342**	**262,012**	**286,423**	**24,411**	**9%**

- **Salaries & benefits**: Salaries & Benefits reflect onboarding of the Sr IT Analyst.
- **Professional Services & Contingent staffing**: This amount is a placeholder should the department need external support.
- **Training**: Training is based on a dollar allocation per staff member to upkeep professional CPE requirements and develop professionally. Staff is required to complete at least 80 hours of productive training (combination of external and internal).
- **Operating expenses**: The reduction is due to a decrease in software licensing fees.

Appendix 1: Audit Universe

Financial & Operational Processes

Claims
- 🟨 Catastrophe Planning, Testing, Coordination
- 🟩 Claims Governance
- 🟧 Claims Litigation
- 🟨 Claims Operations
- 🟩 Special Investigations Unit (SIU)
- 🟩 Subrogation and Salvage Recovery
- 🟨 Vendor Management - Claims

Communication, Legislative & External Affairs
- 🟩 Corporate Communications
- 🟩 Insurance Communications - Customer Correspondence & Complaint Handling
- 🟩 Insurance Communications - Technical Communications
- 🟨 Legislative Affairs
- 🟨 Public/External Relations & Outreach

Operations
- 🟨 Continuous Improvement
- 🟨 Enterprise Metrics
- 🟩 Enterprise Portfolio Management (PMO)
- 🟩 Enterprise Strategy & Planning Support
- 🟩 Facilities Management
- 🟨 Vendor & Contract Management
- 🟨 Corporate Governance

Assurance
- 🟧 Enterprise Risk Management
- 🟩 Internal Control Framework

Legal
- 🟨 Claims Legal
- 🟩 Compliance
- 🟩 Corporate Insurance
- 🟩 Corporate Legal
- 🟩 Purchasing
- 🟩 Records Management

Underwriting & Agency Services
- 🟨 Agency Management
- 🟩 Clearinghouse Operations
- 🟩 Commercial Lines Underwriting
- 🟨 Consumer & Policy Services
- 🟨 Depopulation Operations
- 🟩 FMAP
- 🟨 Personal Lines Underwriting
- 🟩 Product & Rate Implementation
- 🟩 Product Development -Applications, Forms, Rules
- 🟨 Underwriting & Agency Governance

Financial Services
- 🟨 Accounts Payable
- 🟩 Cash Management & Treasury
- 🟨 Claims Accounting & Disbursements
- 🟩 Commissions Payments & Accounting
- 🟩 Corporate Analytics
- 🟩 Depopulation Billing, Settlements & Accounting
- 🟩 Escheatment Processing & Accounting
- 🟨 Financial Close
- 🟨 Financial Planning & Analysis
- 🟩 Financial Reporting
- 🟨 Investment Accounting
- 🟨 Investments Management & Compliance
- 🟨 Loss Reserve Development/IBNR
- 🟩 Pre- & Post-Event Liquidity Bond Financing
- 🟩 Premiums
- 🟩 Rate Development & Filing
- 🟩 Reinsurance Servicing & Accounting
- 🟩 Risk Transfer Strategy & Execution

Human Resources
- 🟩 Compensation & Benefits
- 🟨 HR Supporting Services
- 🟨 Payroll Administration
- 🟩 Recruiting & Contingent Staffing

Information Technology Functions

- 🟩 Application Delivery
- 🟩 Application Development
- 🟩 Configuration Management
- 🟩 Enterprise Architecture
- 🟨 Enterprise Resilience (BCP/DRP)
- 🟩 IT Strategy & Planning

- 🟩 Finance Management
- 🟩 Incident & Problem Management
- 🟩 IT Business Unit Communications
- 🟩 IT Change Management
- 🟩 IT Governance

- 🟩 IT Infrastructure
- 🟩 IT Knowledge Management
- 🟨 IT Security & Risk
- 🟩 IT Operations
- 🟩 Technical Operations Center

Risk Legend
- 🟩 Low
- 🟨 Medium
- 🟧 High
- 🟥 Severe

Appendix 2: Risk Impact Definition

Potential Impact		Potential Probability	
Severe	Refers to complex issues with high impact and likely probability for which the solution is outside of the ability of Citizens management and intervention is required through Board of Governors or the Legislature.		
HIGH > $20M	*Potential loss of ability to sustain ongoing operations* • Major impact to company's brands/reputation • Increase in costs with major impact on long term profitability/viability • Major inability to maintain current operational performance • Downgrade of credit rating with major impact on costs • Major Federal, State or International legal action	Likely	*Will probably occur in most circumstances*
MEDIUM $5M to $20M	*Moderate impact on achievement of business objectives* • Temporary, but recoverable, reduction in company reputation • Increase in costs with a moderate impact to cash flow • Federal, State, International, Local, Civil legal action with moderate implications	Possible	*Might occur sometime*
LOW < $5M	*Insignificant impact on the achievement of business objectives* • Notable event with insignificant impact	Unlikely	*Low likelihood of occurrence.*

Appendix 3: 2018 *Overview of Audits*

Title	Type	Audit Justification and Objective
Underwriting Agency Services		
Automated Underwriting	Audit	**Risk Rationale:** Citizens utilizes an automated underwriting process for policy issuance. As a result of the 2017 OIA audit and the onboarding of the new Underwriting Vice President, many process changes have been implemented and further changes are being considered for 2018. Plans include expanding the automated capabilities to include risk parameters to automate underwriting decisions whenever possible. Inadequate design and implementation of automated business rules could prevent the identification of all exposures associated with a property, resulting in insufficient coverage and/or assignment of inaccurate premiums, permit binding or issuing of ineligible policies, and allow unauthorized access to modify automated business rules. **Objective:** Determine the efficiency and effectiveness of controls established for enhancements to the automated underwriting process.
Voice of the Customer Program	Audit	**Risk Rationale:** The Voice of the Customer Program provides information to identify business trends, discover the root cause of customer behavior, and enable the right decisions to ensure service excellence while achieving continuous performance improvement across the organization. The success of the program may be impacted by failure to provide timely and accurate customer service including average speed of answer (ASA), abandoned calls, and other issues that may contribute to a negative customer experience. **Objective:** Validate the effectiveness and efficiency of the Voice of the Customer Program and to determine if improvements identified from the program are thoroughly validated, appropriately designed, and implemented.
Agency Management System	Project	**Risk Rationale:** Solicitation in progress to replace the current Agency Management System, which includes ePas and AAS/ARS. The new Agency Management System will support tracking and monitoring of agent licenses, commission, performance, investigations, complaints, and key performance indicators. This is the second solicitation for a system replacement as the previously selected system replacement, PMP, did not meet expectations. **Objective:** Provide support to management during the implementation of the new Agency Management System.

Appendix 3: (continued…)

Title	Type	Audit Justification and Objective
Claims		
Managed Repair Program	Audit	**Risk Rationale:** Effective July 2017, two new endorsements are attached to every new and renewed HO-3 and DP-3 policy. The endorsements allow Citizens to offer free water mitigation services for emergency water extraction and drying and a mutual consent Managed Repair Program for permanent repairs with the application of the policy deductible. The program initially applies to non-weather water claims with plans to expand to other peril losses. The Managed Repair Program is a key component of Citizens' Water Loss Mitigation strategic initiative to mitigate the risk associated with water loss to protect the Policyholder and Citizens premium reserves and sustain financial strength by identifying, evaluating, and addressing non-weather related claim cost trends, and mitigating the potential for litigation. Success of the program may be impacted by the volume of voluntary participants and external influences such as negative press and attorneys that oppose managed repair programs. **Objective:** Assess the deployment of the Managed Repair Program against the stipulations of the agreement and evaluate the efficiency and effectiveness of internal controls developed and implemented to ensure that the program is operating as expected.
Claims Coverage/Payment Process (Cat & Non-Cat)	Audit	**Risk Rationale:** Hurricane Irma was the second largest claims generating event in Citizens' history. More than 300 Citizens' adjusters were dedicated to the Irma response and approximately 800 independent adjusters were deployed along with the use of contractors with emergency adjuster licenses. The amount of additional new resources along with the increased volume of claims, extended work hours, and possible manual workarounds may impact the accuracy of claim payments. In addition, the large contingent adjuster workforce combined with the legally restrained ability to train contingent staff increases the risk that policy coverage may not be interpreted and/or applied correctly while adjusting claims. **Objective:** Evaluate controls in place for the CAT and non-CAT claims payment processes to ensure that policy coverage is accurately interpreted and consistently applied across all claims.

Appendix 3: (continued…)

Title	Type	Audit Justification and Objective
Claims		
Post Irma Considerations	Project	**Risk Rationale:** Citizens has developed a Catastrophe (CAT) Plan to provide scalability for handling the increased volume of claims in the event of one or more storms or other weather events affecting Florida. The plan identifies the roles and responsibilities of every business unit in a CAT and establishes the operational framework for the CAT response and claims handling activities. In September, the CAT Plan was executed for a major storm, Hurricane Irma. Responses to Irma included mobilizing Catastrophe Response Centers (CRC's) as field claims centers, placing adjusters in a satellite office in hard hit areas, providing a focused training program for contractors to receive an emergency adjuster license and utilizing aerial technology. There is an opportunity to leverage any lessons learned from this storm to enhance the CAT plan. **Objective:** Monitor the process, provide advice, and assist management with identifying and validating post Irma considerations for process improvements and adjustments to the CAT Plan.
Citizens Insurance Suite/Guidewire V9 (ClaimCenter 2018)	Project	**Risk Rationale:** Guidewire software is utilized to support core insurance business functions in the Citizens Insurance Suite. The current platform version 7 is more than 5 years old. In order to maintain Guidewire support and take advantage of improved functionality, an upgrade to version 9 will occur in a phased approach beginning with ClaimCenter. Coding freezes may result in delays for enhancements. Rework may occur if system customizations cannot be maintained and additional Acuity system changes are needed to maintain integration with ClaimCenter. **Objective:** Monitor project process and progress and provide advice and support to management during the Guidewire V9 upgrade.

Appendix 3: (continued…)

Title	Type	Audit Justification and Objective
Human Resources		
Alternative Work Arrangements	Audit	**Risk Rationale:** In September of 2016, Citizens began offering formal alternative work arrangements (AWA) that permit eligible employees to work from an alternate worksite on specific days or the entire work week. As Citizens transitions out of the Tampa facility by June 2019, more employees may be eligible to participate in the program full time. There is an increased risk that productivity may suffer as business leaders may not be adequately trained to effectively manage and monitor employees participating in AWA. **Objective:** Evaluate performance management processes developed to ensure adequate oversight is in place to manage and monitor AWA employee performance, productivity, and compliance with corporate policy.
Strategic Workforce Planning	Advisory	**Risk Rationale:** Throughout the organization, the ability to effectively analyze current and future staffing needs is limited. In addition, parts of the organization may not have a sufficient number of employees with the appropriate skills to achieve its objectives. During the first part of 2018, Human Resources plans to develop and deliver a Strategic Workforce Program to inform on current and future staffing needs. Business units will be able to utilize this information to support staffing needs for planning and budgeting purposes. **Objective:** Provide advisory support in the development of a value add program that will enable business units to accurately plan, forecast, and acquire the appropriate resources.
Centerpoint Phase 4 and 5 HR (HCM and Recruiting)	Project	**Risk Rationale**: In support of Citizens' strategic objective to continuously improve and implement process and technology advancements that realize cost savings and enhance performance, a long term Enterprise Resource Planning (ERP) strategy was developed. As part of this strategy, Oracle Fusion Cloud Service, an integrated ERP solution, was purchased to address administrative processing needs. The integrated ERP solution, Centerpoint, will replace existing Human Resource applications Kronos, Org Plus, and SuccessPath. The Human Capital Management (HCM), Recruiting and Advanced HCM phases of the project focus on self-service, benefits administration, timekeeping, payroll, recruiting, and Performance and Talent management. The phases are expected to be implemented December 2017 through May 2018. Appropriate controls must be in place to mitigate risks related to user access, segregation of duties, reporting capabilities, data conversion, system/application interfaces, and data security. **Objective**: Continue to monitor project processes and progress and provide advisory support to the project team and business areas in the identification and mitigation of risks as needed.

Appendix 3: (continued…)

Title	Type	Audit Justification and Objective
Communications, Legislative & External Affairs		
Annual Legislative Changes	Project	**Risk Rationale:** Annually the Florida Legislature meets and establishes new laws and regulations that have various degrees of impact on Citizens, its' customers and stakeholders, and the processes the company uses to serve as the insurer of last resort. Impact of potential changes generated by the 2018 legislature, monitor the identification, evaluation, tracking and the integration of the necessary changes to our processes and systems.
Social Media	Audit	**Risk Rationale:** Social media is in many respects an unstoppable cultural force, in spite of some organizations' attempts to block or curtail its use. A significant sticking point when it comes to properly leveraging social media is dealing with the many risks to which companies are exposed. Negative exposure on social media sites, or inappropriate or unauthorized action in the company's name, can significantly impact reputation resulting in lost trust from Citizens stakeholders. If not effectively mitigated, these reputational risks (along with other risk types) can lead to serious negative consequences including fraud, financial loss, privacy violations and failure to comply with laws and regulations. Further, Social Media is used internally to communicate across the organization and can cause misunderstanding or friction if not meeting expectations. **Objective**: Ensure adequate and effective controls are in place to support internal clients and protect Citizens against reputational damage through proper use of supporting social media tools, monitoring and reporting (metrics), training, proper authorizations, administrator and user access, and compliance with corporate policy and procedures.
Finance & Accounting		
ABC Budgeting	Audit	**Risk Rationale:** The annual Financial Planning & Analysis (FP&A) process is maturing and becoming more complex each year and is an important finance element for any organization to meet their goals and objectives. OIA has collaborated with the Finance area through an advisory during 2016 and will be following-up on the implementation and maturing of ABC Budgeting segment of the FP&A process. It is important to provide assurance around financial processes as Citizens is the insurance provider of last resort for the State of Florida and is entrusted with public funds resulting from insurance premiums. **Objective:** Assess the efficiency and effectiveness of processes and controls around the annual budgeting process and the ongoing monitoring and management of the budget throughout the year.

Appendix 3: (continued…)

Title	Type	Audit Justification and Objective
Finance & Accounting		
Centerpoint Phase 1 and 2 Post-Implementation Review (Financials and Procurement)	Audit	**Risk Rationale:** In support of Citizens' strategic objective to continuously improve and implement process and technology advancements that realize cost savings and enhance performance, a long term Enterprise Resource Planning (ERP) strategy was developed. As part of this strategy, Oracle Fusion Cloud Service, an integrated ERP solution, was purchased to address administrative processing needs. Phases 1 and 2 of the integrated ERP solution, Centerpoint, replace Financial and Procurement applications ProFinancials and CAPS. The Financials and Advanced Procurement phases of the project focus on replacing the general ledger, accounts payable processing, cash management, employee expense processing, purchase requisitioning, contract management, supplier portal, competitive solicitation management. Phase 1 was implemented in April 2017, while Phase 2 is expected to be fully implemented January 2018. Appropriate controls must be in place to mitigate risks related to user access, segregation of duties, reporting capabilities, data conversion, system/application interfaces, and data security. **Objective**: To provide assurance that processes and controls are designed and operating effectively following the Phase 1 and 2 implementation of Centerpoint.
Treasury Management Automation Best Practices	Advisory	**Risk Rationale:** The ability to efficiently prepare periodic treasury and cash management reports is increasingly important to enable management to make effective day-to-day, as well as long-term financial decisions. The current process of compiling such data is very manual and labor intensive for the individuals preparing and reviewing the data prior to being forwarded to management. Also, this time could potentially be better spent on strategic and dynamic thinking if certain aspects of the cash management function were to become more automated. **Objective:** To assist management in identifying opportunities to automate the cash management function through industry best practices.

Appendix 3: (continued…)

Title	Type	Audit Justification and Objective
Finance & Accounting		
Investment Management	Audit	**Risk Rationale:** Citizens' total portfolio market value for April 2017 was $12.26 billion with an average duration of 3.35 years and average credit ratings of "A+/A1/A+". As of July 2017, 88% of the total investment portfolio is managed by 15 external investment managers, or $10.76 billion, and 12% is internally managed, or $1.50 billion. Citizens has four investments policies which are monitored using a new Investment Performance and Compliance software (Factset). **Objective**: To provide assurance that processes and controls to monitor external investment managers are adequately designed and operating effectively. This includes ensuring the investment compliance software is adequately monitoring investment activity. Also, to provide assurance that processes and controls surrounding internally managed investments are designed and operating effectively.
Centerpoint Phase 3 Project Monitoring (Budgeting)	Project	**Risk Rationale:** In support of Citizens' strategic objective to continuously improve and implement process and technology advancements that realize cost savings and enhance performance, a long term Enterprise Resource Planning (ERP) strategy was developed. As part of this strategy, Oracle Fusion Cloud Service, an integrated ERP solution, was purchased to address administrative processing needs. The integrated ERP solution, Centerpoint, will replace existing Budgeting applications TM1. This phase is expected to be implemented January 2018 through July 2018. Appropriate controls must be in place to mitigate risks related to user access, segregation of duties, reporting capabilities, data conversion, system/application interfaces, and data security. **Objective**: Ensure that there is proper oversight and change management control procedures are followed throughout implementation and provide key consulting guidance when necessary.
Unclaimed Property Operational Process	Audit	**Risk Rationale:** Escheatment is the process of identifying customer's uncashed claims payments or premium refunds that are considered abandoned and remitting the funds to the appropriate state if the customer cannot be contacted. Because there is no "owner" of these funds they are potentially subject to misappropriations. **Objective**: Perform a forensic audit to determine if the appropriate anti-fraud controls are in place and operating effectively as well as perform forensic audit procedures to test for misappropriation.

Appendix 3: (continued…)

Title	Type	Audit Justification and Objective
Legal & Compliance		
Compliance Governance Follow Up	Audit	**Risk Rationale:** This organization faces potential scrutiny and/or fines for non-compliance with federal and state regulations as well as the state of Florida's insurance regulatory mandates. With such a plethora of compliance rules and laws it is customary for organizations to employ a Compliance governance function to manage its regulatory requirements. **Objective**: Assess the effectiveness of the organizations compliance function and determine if formal procedures have been applied across the organization to ensure consistency in managing compliance regulation.

Title	Type	Audit Justification and Objective
Systems and Operations		
Data Retention (Rollover from 2017)	Advisory	**Risk Rationale:** Data Retention policies and procedures are required to ensure that documents are retained in accordance with laws and regulations as well as ongoing business needs. Absent formal guidance by Management, data may not be able to be retrieved when required and costs may outweigh benefits in retaining obsolete data. **Objective:** Assess current policies and practices and determine if they are appropriately applied within the organization.
Enterprise Rhythm	Advisory	**Risk Rationale:** IT Management implemented a new planning and delivery methodology in 2017 based upon the industry leading "Scaled Agile Framework (SAFe)", coined internally as "Enterprise Rhythm". The objectives of the SAFe framework as designed, allow organizations to synchronize alignment, collaboration and delivery of multiple agile development teams. The process also heightens visibility to capacity and projects and aligns product owners and individuals to a common purpose while continuously apprising management of the work in progress. Citizens' IT has placed significant resources toward this transformative program with the goals of expanding economic decision making to the product level and improving delivery predictability, throughput and quality. **Objective:** Evaluate program governance components and assess the effectiveness and efficiency of the Enterprise Rhythm program against management's overall program goals and objectives.

Appendix 3: (continued…)

Title	Type	Audit Justification and Objective
Systems and Operations		
IT Security Compliance Program	Advisory	**Risk Rationale** An information technology security compliance program ensures that activities conform to relevant mandatory and voluntary laws and requirements. Compliance challenges can negatively affect operational processes or cyber security safeguards within an IT organization. Accordingly, regulatory changes, fraud, security issues and operational delivery add a heightened focus on corporate governance and security compliance oversight within organizations. **Objective:** Support management in the development of an effective IT Security compliance self-assessment program based upon industry standards and benchmarks.
IT Infrastructure Management	Audit	**Risk Rationale:** Infrastructure management is key in providing consistent IT services to the organization. Infrastructure hardening is the act of applying security to each component of a network environment's infrastructure including web servers, application servers, database systems and other technical solutions to reduce the surface of vulnerability. Finding the right balance between hardening systems against potential threats and maintaining usability is an important component of IT security. Performance monitoring and capacity management processes determine the amount and timing of computing resources that are required. Hardware that is ineffective in meeting business needs and supporting security objectives may negatively affect business operations. **Objective:** Ensure that infrastructure build, maintenance, capacity and performance management processes are effective and that relevant components follow the new IT Security Standards. Focus areas include infrastructure protection, availability and monitoring.
Third Party Access	Audit	**Risk Rationale:** Third party security access and visibility and monitoring controls are key to safeguarding the network and data from nefarious/malicious external users. A recent US survey indicated that third party activities are not fully controlled in over 50% of 700+ companies. Absent appropriate control of external connections and user activities, the number of IT incidents and corresponding business impact may rise. **Objective:** Validate that third party policies, inventories, user account management, connections and monitoring are appropriate for the organization.

Appendix 3: (continued…)

Title	Type	Audit Justification and Objective
Systems and Operations		
IT Security Critical Controls and Standards Implementation	Audit	**Risk Rationale:** Citizens' IT Security department adopted the internationally accepted "Critical Security Controls" framework to uplift and standardize IT security controls. New information technology security standards were approved in 2016 to align with the updated IT Security Policy. A gap analysis was performed and work is underway to implement any process gaps. Absent appropriately designed and implemented cyber security safeguards, unknown data access or changes may occur within the network, potentially causing business disruption, financial implications or reputational damage. **Objective**: Assess the adequacy of the IT Security gap analysis and evaluate progress on the effective resolution of identified gaps and compliance to standards.
Disaster Recovery Strategy Transition Program (Tampa Data Center Migration)	Project	**Risk Rationale:** The current backup data center is being migrated to a new location to reduce risk and cost and to enhance system related disaster recovery processes. Lack of an appropriate and tested corporate resiliency plan and backup facility may increase the risk of outages or threat events, impairing the ability of the business to achieve its objectives. **Objective**: Validate the transition of the Tampa data center to a new facility is effective and that the new data center supports corporate resiliency strategies and objectives. Provide advice related to project governance, operational controls and practices in support of the migration.
Vendor Management	Audit	**Risk Rationale:** Vendor Management is tasked to assist the organization in making informed vendor engagement decisions, procure the right vendors, actively manage vendor relationships to realize expected benefits to optimize value, and mitigate risks when using vendors. Substantial reliance on third parties, complexities in vendor risks and relationships and potential regulatory compliance are key drivers in appropriately managing vendor relationships. **Objective:** Ensure adequate and effective controls are in place to identify, assess, and mitigate vendor risks and satisfactorily manage the vendor in alignment with corporate vendor management governance practices.
Self Service Strategy	Project	**Risk Rationale:** A strategic initiative is underway to extend current self-service capabilities for customers, agents, policyholders and claims adjusters to new products and services which will enable more efficient, cost effective, and user-friendly transactions. The current products and services offer limited capabilities that do not align to industry standards and best practices. **Objective:** To provide advice and support to management during the development and implementation of self-service capabilities.

Appendix 4: 2018 ICO Plan Breakdown

ICO Progress on Process Universe
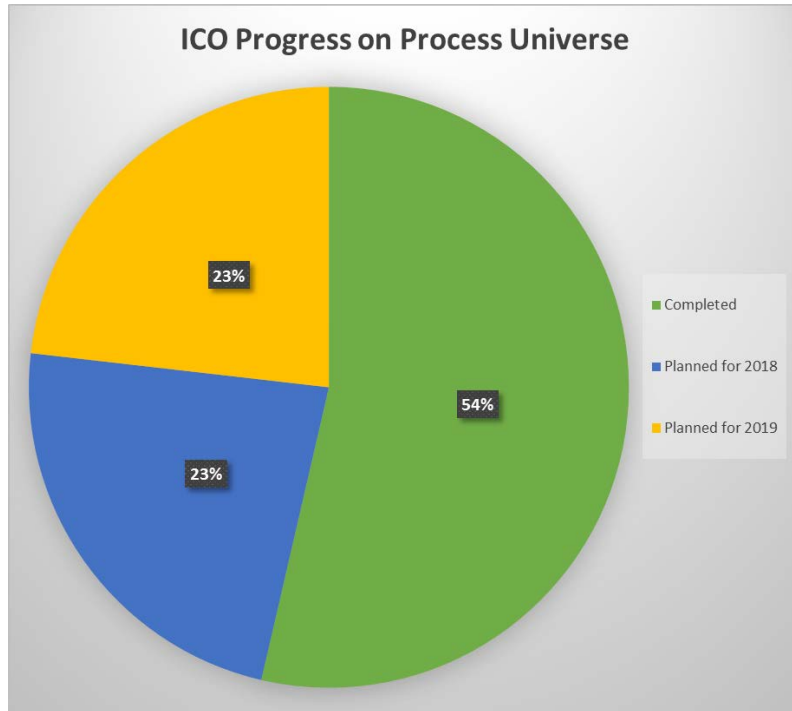
Functional Area	Completed	Planned for 2018	Planned for 2019	Out of Scope*	Control Self-Assessments**
Enterprise	1	0	0	0	1
Assurance	0	0	1	1	0
Claims	6	0	1	0	6
Communications, Legislative & External Affairs	3	0	2	0	3
Financial Services	15	1	1	1	15
Human Resources	3	0	1	0	3
Legal	1	3	2	0	1
Systems & Operations	4	12	5	2	1
UW & Agency Services	4	0	3	3	4
Total	37	16	16	7	34

* Process and control reviews where neither a primary control nor primary risk was identified. Classification is subject to change through ICO's annual planning and/or results of future ERO risk assessments.

** 3 IT Processes have been completed but will not be subject to a control self-assessment in 2018.