



# OFFICE OF THE INTERNAL AUDITOR

2020 Strategy & Plan

December 10, 2019









## Executive Summary

---

### 1. Introduction

This document serves as the Office of the Internal Auditor's (OIA) 2020 Strategy and Plan (Plan) for Citizens Property Insurance Corporation (Citizens). The contents of this document have been shared with executive management and is presented to the Audit Committee for consideration and approval.

The Chief of Internal Audit currently oversees three complementary assurance functions within Citizens which include Internal Audit, Enterprise Risk Management and Internal Control Monitoring. This Plan provides a detailed description of our approach, focus and expected deliverables for 2020 for each of the three functions mentioned.

### 2. Background and Approach

The mission of Citizens' OIA is to provide independent, objective assurance and consulting services designed to add value and improve Citizens' operations. OIA assists Citizens in accomplishing its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

#### 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. Its mission is to provide insurance protection to Florida policyholders who are entitled to but are unable to find property insurance coverage in the private market. 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 form a major component of the Florida Comprehensive Annual Financial Report. Citizens has offices located in Tallahassee and Jacksonville.

#### 2.2. Approach

In alignment with our mission, OIA uses a collaborative 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, risk and control coverage by using resources available to the OIA. Since it is impractical to provide coverage to the entire corporation on an annual basis, the OIA, in consultation with business unit leadership, continuously considers risk across Citizens' process universe and determines the best type of service to address each set of risks and circumstances.



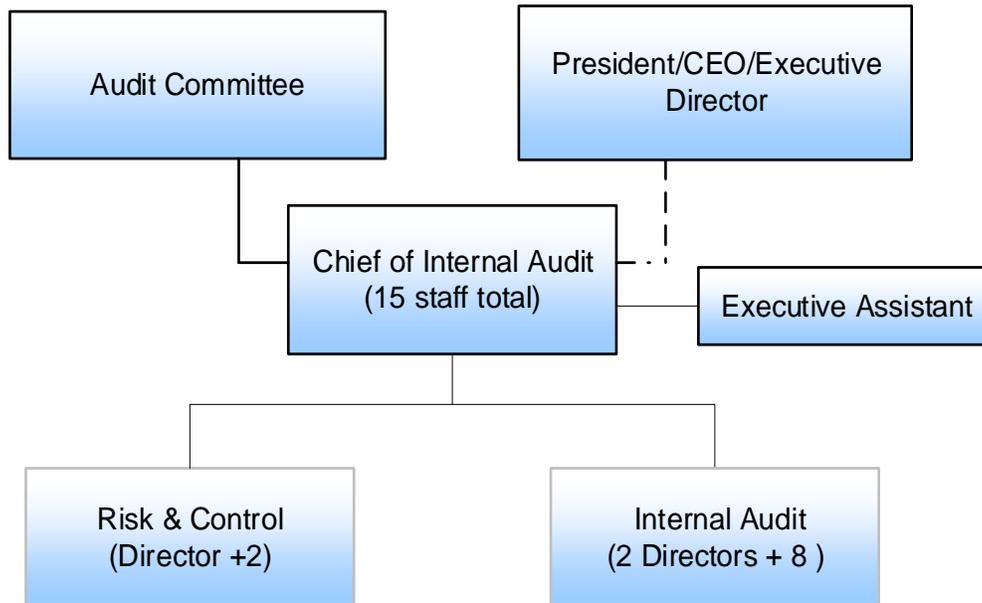
## Executive Summary

### 2.3. Coordination with other Assurance Providers

In developing this plan and approach, OIA consulted with other internal and external assurance providers, including Citizens’ Inspector General, to ensure that the 2020 OIA plan supports or complements other operational plans. This ensures duplication of work is minimized. Our 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.

### 3. Organization

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 services, which are designed to add value and improve the corporation's operations.



### 4. OIA Mandate

The purpose, authority, and responsibility of the OIA is formally established through Citizens’ enabling statute, specifically Section 627.351(6)(i) Florida Statutes. In addition, Citizens’ Audit Committee further clarified OIA’s role and authority through Citizens’ Internal Audit Charter. This charter is consistent with the Definition of Internal Auditing, the Code of Ethics and the



## Executive Summary

---

International Standards for the Professional Practice of Internal Auditing as defined by the Institute of Internal Auditors and is reviewed annually.

In addition to the International Standards for the Professional Practice of Internal Auditing, the OIA further uses accepted industry frameworks for guidance when conducting audits, risk assessments or internal control evaluations. These include the Control Objectives for Information and Related Technology (COBIT) as guidance for conducting IT audits; the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control Framework (COSO 2013) for the development and management of Citizens' Internal Control Framework; and the COSO Enterprise Risk Management Framework (COSO ERM) for the development and management of Citizens' Enterprise Risk framework.

### 5. 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 innovative.
- *Teamwork:* We are a solidified team that works together collaboratively and efficiently.
- *Trusted and Respected:* We embrace the highest level of confidentiality and integrity and treat all people with dignity and respect.
- *Professional and Courteous:* We respectfully follow the relevant standards while being polite and courteous to others.
- *Responsive to Risk and Customers:* We will understand the changing needs of Citizens and respond by being flexible in our planning and delivery.
- *Competent, Fair and Balanced:* We provide unbiased, balanced, and practical solutions.

### 6. OIA Strategy

OIA aligned its 2020 approach with Citizens' strategic objectives and goals in order to provide high quality audit, risk and control services. To be a valued partner, the OIA team seeks opportunities to enable the OIA to effectively allocate its financial and human resources to meet the expectations of its key stakeholders.

We seek creative ways to maximize the value and impact of available audit, risk and control resources and to be a valued partner. As such the OIA team seeks opportunities to:

- Learn about and understand our business partners' environment and the challenges they face.
- Provide progressive thinking toward internal and external factors and trends that may prevent Citizens from successfully meeting its goals and objectives.
- Be aware of and apply leading audit, risk and control practices.



## 7. Internal Audit

Internal Audit (IA) follows a detailed annual planning process and prepares a theme-based audit plan which considers the possibility of dynamic risk fluctuations and process changes throughout the year. This necessitates regular re-evaluation of audit approach and scope so that appropriate audit focus is always given to important strategic and operational issues and risks. Throughout the year, the audit plan continuously evolves to support our dynamic risk environment, focusing on current and emerging reputational, compliance, operational, information technology and financial risks. To achieve the greatest impact, IA “rebalances” internal audit activities in a rolling audit plan to ensure adequate focus is given to Citizens’ strategic issues and critical processes.

### 7.1. Defining the audit universe

In determining Citizens’ 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 2020, Citizens’ key strategic themes are:

- Strengthening Metric Driven Decision Making.
- Proactively Managing Claims and Litigation Avoidance.
- Ensuring Scalability and Flexibility in Our Operations.
- Investing in and Leveraging Citizens’ Greatest Resource - Our Employees.

### 7.2. Prioritizing work to be performed by Internal Audit

The primary responsibility of Internal Audit 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.



## Plan Detail

---

- Prioritization of the units to be reviewed or audited are based on the relative risks/opportunities associated with each of them. Risk factors considered while reviewing the units in the universe include the control environment; business exposure; compliance requirements; reputation factors; organizational change or growth; and management discretion.

### 7.3. Determining the types of services to be performed

Following the completion of a detailed analysis of the Citizens' strategic goals and objectives, considering management's concerns and Internal Audit's risk assessment, IA developed specific audit themes in identifying planned audit activities and audit coverage. Themes-based audit planning is a value-adding approach that helps the IA to determine, consolidate, and provide high-level insights into the following periods' audit focus areas to the Audit Committee, Chief Executive Officer (CEO) and other key stakeholders through the grouping of internal audit outcomes into related higher-level topic areas (or themes).

Activities carried out by IA can take many forms. IA realizes that pure assurance activities are not the only solution to accomplish our goals and offers other services to add value to the company. Engagements are defined within following categories:

- Audit (Assurance) engagement - involves the objective examination of evidence for the purpose of providing an independent opinion on the effectiveness of process governance, risk management, compliance and internal control practices for the organization.
- Consulting (Advisory) engagement - is provided at the request of management and is intended to add value and improve Citizens' governance, risk management, compliance and internal control processes without assuming management responsibility.
- Project engagement – provide a focused assessment on the effectiveness of the project development approach applied to ensure that fit for purpose processes, and systems are designed and implemented.
- Business Support - is provided at the request of management and is usually conducted to improve collaborative efforts and to assist in the identification of good business practice.
- Targeted audits or 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.
- Risk Assessments - activities to assess, identify, and highlight current and emerging risks that may affect the Company.



## Plan Detail

### 7.4. Internal Audit Planned Themes

IA documented specific audit themes which highlight 2020 planned audit coverage with a listing of potential audit engagements identified and agreed with business unit management. As the year progresses IA will present selected engagements quarterly to the Audit Committee for approval.



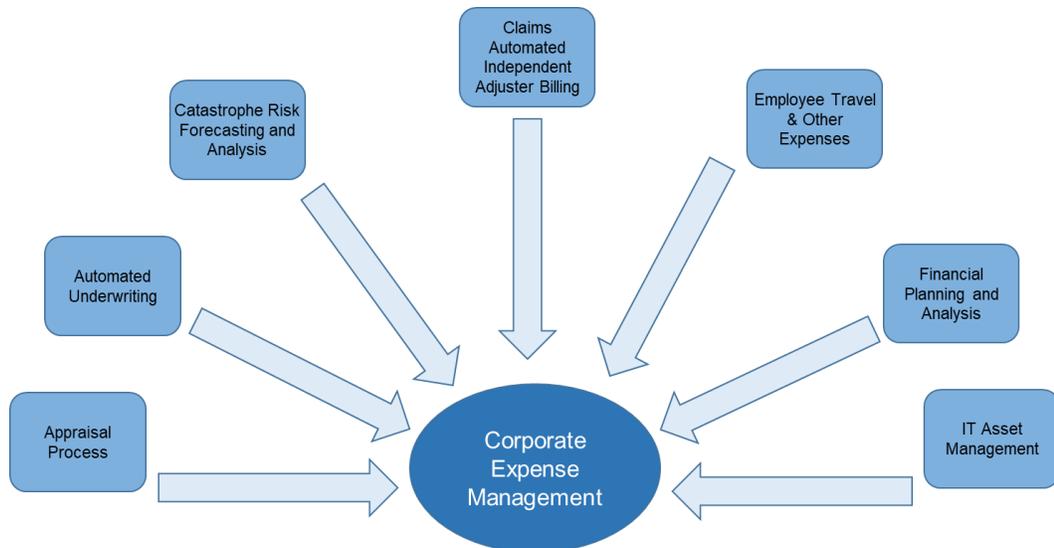
#### Theme 1: Corporate Expense Management

Citizens continues to develop and improve existing strategies, programs, and processes geared toward reducing operating expenses across the organization. Citizens management has implemented or is in the process of exploring expense reduction activities in the areas of enhanced budgeting process and tools, IT service management solution, independent adjusting invoice management software, automated underwriting process redesign and proof of repairs requirements. Additionally, the organization remains focused to achieve and maintain an expense ratio that is aligned with the private market. In considering potential audit engagements per division we focused on the following:

- Claims management is exploring the benefits provided by third-party Invoice Management software to monitor, track and manage the payment of independent adjusting firms. There is a need to automate and simplify the day rate time management and fee bill invoicing for independent adjusters in order to reduce expenses by minimizing manual touch points and improving accuracy.



## Plan Detail



- When a policyholder and Citizens have a disagreement regarding the cost of repairing or replacing damaged property, the policyholder has various forums to resolve this dispute. One way to resolve the dispute is to invoke the appraisal clause within the insurance policy. When conducted properly, an appraisal can be a very effective alternative dispute resolution process that can help reduce resolution time and legal spend.
- Financial Services successfully launched a budgeting module in Centerpoint during 2018 and training was conducted for budget users throughout the organization. Implementation was completed and new process adopted throughout Citizens with additional projection model features launched during 2019. When applied a budgeting process can help manage expenses and achieve objectives.
- Underwriting management is working on an Automated Underwriting Process Redesign project for the purpose of gaining efficiency in the underwriting effort for evaluating personal lines new business applications. The recommendations and results of this project will be forthcoming with possible process revisions implemented during 2020 and longer terms goals of improved loss frequency, critical rating variable accuracy, and lower expenses.
- An IT Service Management Solution was purchased which has several modules that provide request and problem management, configuration management and IT asset management. The asset management module will include both software and hardware assets and will assist with the configuration of asset roles and responsibilities, asset life cycles and reporting. Software asset management will also focus on licensing and optimization for third party software. The VMO is enhancing the software asset management program to incorporate the use of the new software, provide more robust

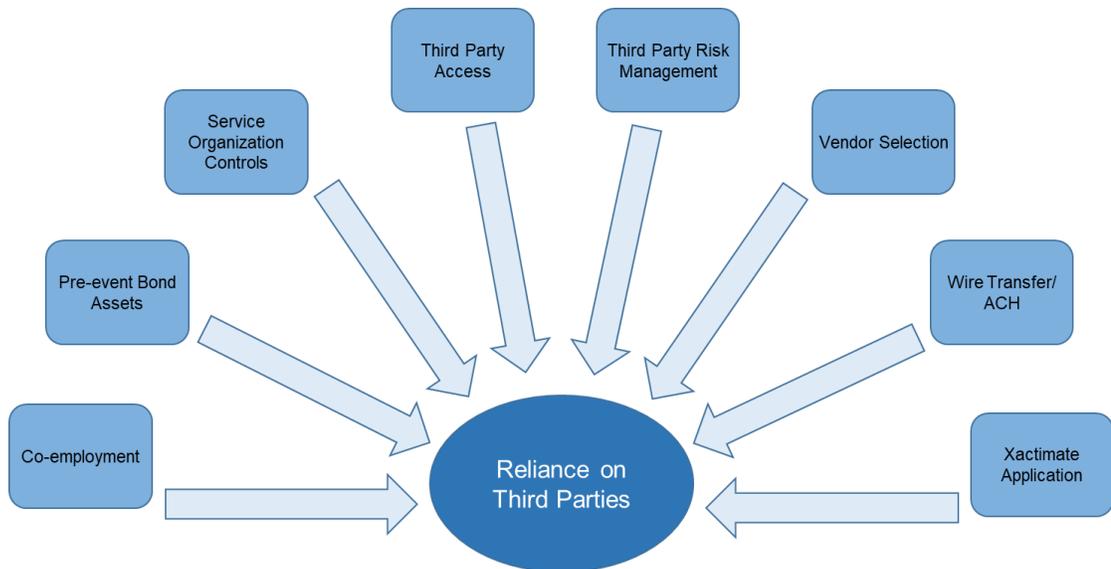


## Plan Detail

operational processes using industry frameworks and practices and developing a maturity model that is in alignment with Citizens' expense management objectives.

### Theme 2: Reliance on Third Parties

Citizens, in its capacity as an insurance company and as a government entity, relies upon vendors to carry out vital business functions, increase efficiencies in daily operations, boost productivity and create flexibility in resources. Reliance on third parties increases exposure to additional risks and potential compliance deficiencies which may result in business disruption. In considering potential audit engagements per division we focused on the following:



- The Vendor Management Office (VMO) in partnership with the Purchasing and Legal departments, support Citizens' vendor selection process. The collaboration of these departments provides oversight of the contract life cycle and ensures compliance with Florida Statutes governing the procurement process to ensure fair and equitable selection of vendors.
- The VMO enables Citizens to better control costs, drive service excellence, and mitigate risks throughout the contract life cycle, which includes engagement, selection, and management of vendors. The VMO and IT Security collaborated to implement a centralized collection, review and monitoring process for SSAE16 Service Organization Control (SOC) reports in 2019 with advisory guidance from IA. These processes and procedures were developed to ensure proper risk mitigation steps are being taken by Citizens when relying on the controls of 3<sup>rd</sup> party organizations.
- Given the nature of Citizens business model, staff augmentation is used throughout the organization to respond to the dynamic business needs. In 2019, Citizens' Contingent



## Plan Detail

---

Worker corporate policy was created to provide standards to assist the organization in all aspects of the utilization of contingent workers. Additional measures were implemented to differentiate contingent workers from employees and training was provided to contingent worker liaisons.

- Citizens Finance is migrating to a new vendor to provide organizational banking needs, including wire transfers and ACH services, which should be completed by year end 2019-year end. Citizens initiates wire transfers of large sums of money for various business purposes and relies on adequate processes, controls, and authorities to be in place for these activities.
- Citizens issued multiple senior secured bonds for the purpose of funding losses in the event of future catastrophes. If a claims catastrophe was to occur, Citizens would access the proceeds of these bonds held within secured trust accounts. Given the sheer value of these bonds, it is important that there are appropriate management oversight controls for these assets.
- Claims management is working with a nationally recognized third-party vendor, Xactimate, to develop and pilot a customized application for simplifying the estimating process during onsite inspections during a catastrophe event.
- 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, potential changes occurring on sensitive assets and appropriate monitoring. IT Security and Risk enhanced their third-party security access controls over the last year to provide a more comprehensive program. Third party IT security risk management continues to be a focus area for the IT Security and Risk department.

### Theme 3: Corporate Effectiveness

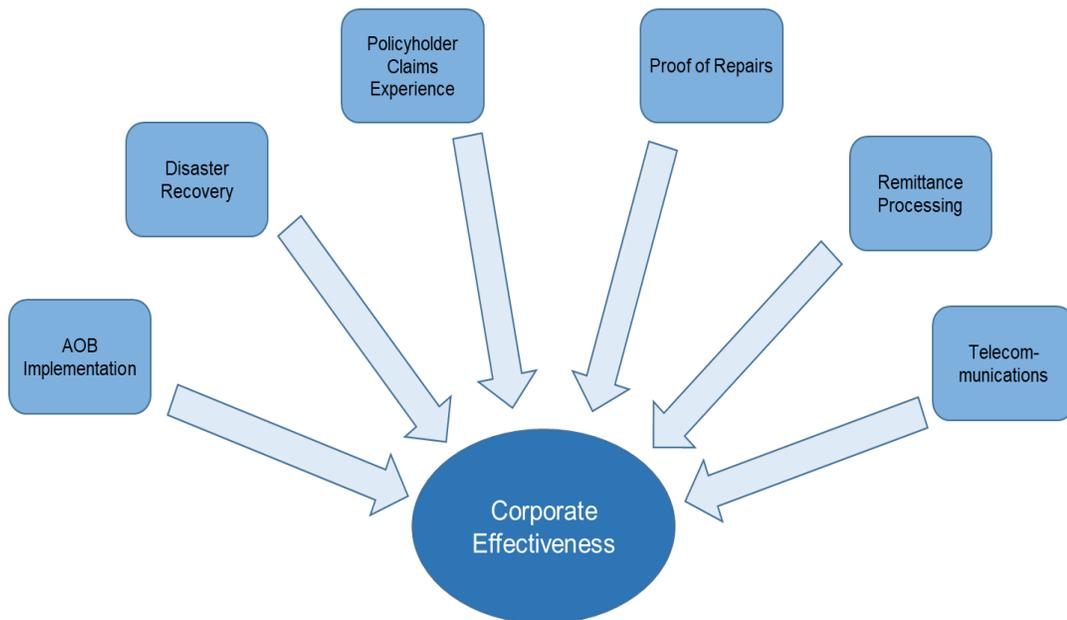
Citizens continues to implement numerous initiatives to improve operational processes, implement new regulatory requirements and to enhance organizational effectiveness. IA selected a few of these changes:

- Assignment of Benefit (AOB) legislation was passed during 2019, which led to the rapid design and implementation of processes and procedures to meet the July 1, 2019 statutory implementation date. Numerous system and process changes were successfully developed and implemented in a short period of time.
- Disaster Recovery (DR) is the process through which Citizens prepares for recovery or continuation of technology infrastructure critical to the organization after a natural disaster, cyber event or other unique occurrence. Disaster Recovery is generally a subset of overall Business Continuity planning and focuses on the technology systems that support the business functions. Recovery can be achieved by restoring information



## Plan Detail

technology (IT) business operations at an alternative location, using alternate equipment and files and/or performing some or all the affected business processes using manual methods. Citizens migrated the disaster recovery data center to a new location in Florida last year. Testing was performed by IT and/or product owners as part of the migration and again this year for a subset of the critical applications required for recovery. Additional process enhancements are in process and more testing is planned for 2020.



- In the past several years, insurance companies have seen an increase in fraudulent property claims. As a result, most insurers have strengthened their verification and added additional stipulations to their claims process. During 2018, Citizens began requiring proof of repairs for Hurricane Irma damage to determine renewal eligibility for policies renewing on or after March 6, 2019. Policyholders who have filed a claim for damage caused by Hurricane Irma must submit proof of repair documentation to Citizens as soon as any repairs are complete.
- In late 2018, Financial Services completed the migration of the remittance processing systems to RT Lawrence. The system is currently used to process more than \$800 million in policyholder premium payments annually.
- Citizens uses many types of communications to provide data, voice and video exchange across the local and wide area networks for employees, agents and contractors. Telephony services provided are both wired and wireless and include both local and 1-800 services for call center activities. New employee phones were rolled out and new mobile device management software will be implemented in 2020 to provide centralized device management services, including configurations and

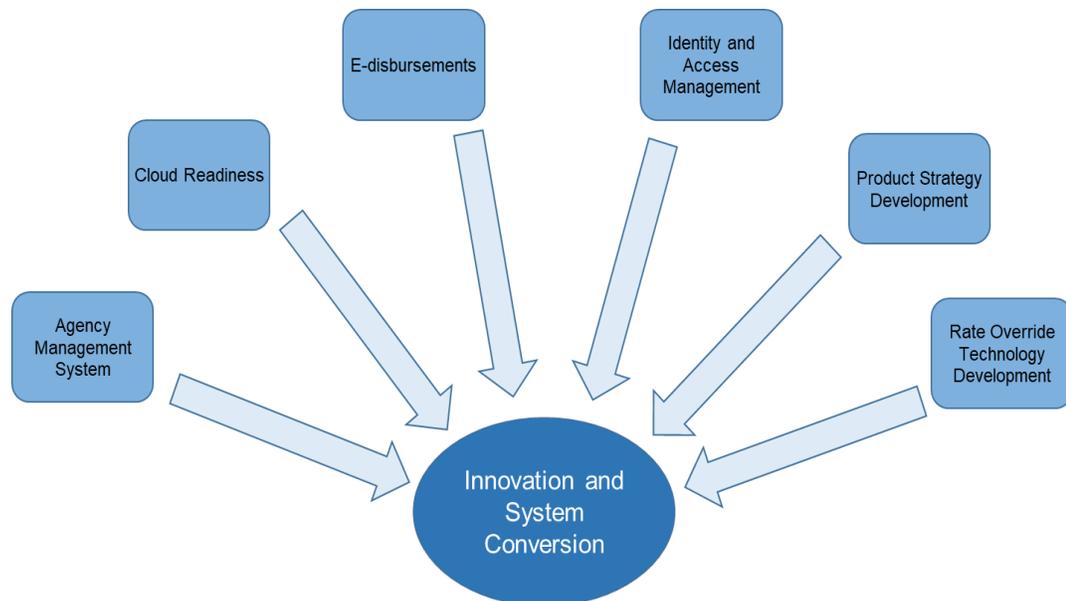


## Plan Detail

application upgrades. Text message archiving is also being implemented for both Citizens-owned and employee “Bring Your Own Device” phones. A new strategy is underway that will incorporate all communications in order to provide consistencies in processes.

### Theme 4: Innovation and Systems Conversion

Citizens’ core functions are continually innovating by exploring ways to leverage industry leading practices and tools to increase operational efficiency and focus on the customer experience. IA will focus attention on some of the most impactful initiatives scheduled for next year:



- An Agency Management platform is in process of being implemented that will replace three of the legacy systems that support the agency related functions. The new platform will improve functionality and provide a more integrated solution that will support tracking and monitoring of agent licenses, commissions, investigations, complaints and key performance indicators as well as provide self-service capabilities to agents. In lieu of an implementation vendor, Citizens’ internal departments are taking the lead to implement appropriate configurations, access controls and processes for this web-based cloud solution.
- IT strategies are in place for cloud solutions and enterprise information and data management. Migration to cloud services and solutions means reliance upon service providers for appropriate internal controls such as information security and privacy, legal compliance, backups and disaster recovery as well as general maturity of technology in the vendor network environment and business viability. Use of cloud solutions, when appropriate, drive process efficiencies by taking advantage of vendors



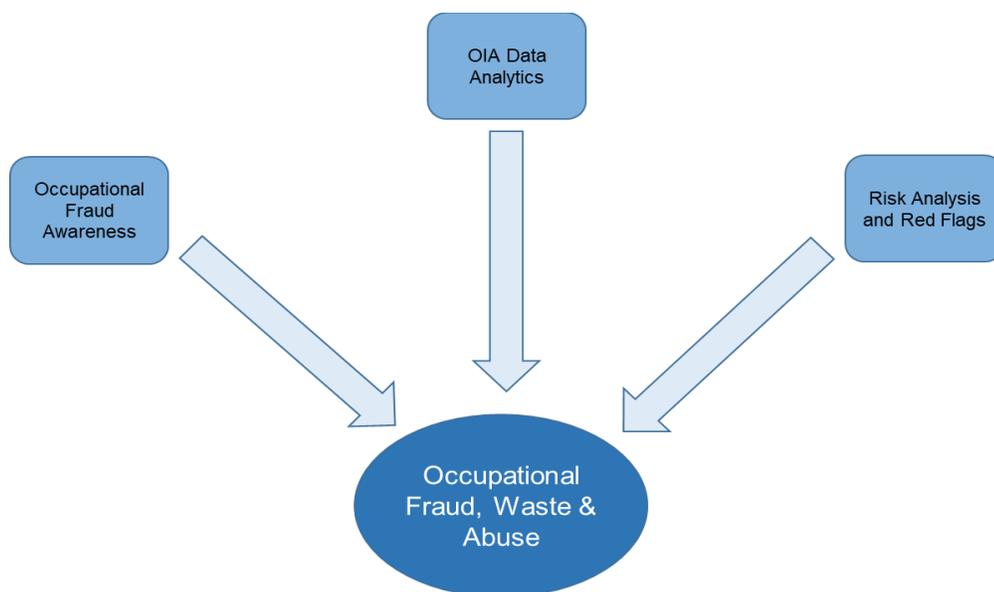
## Plan Detail

with specific, solution-based expertise, elasticity in system usage, automation, disaster recovery and high availability. Based upon the cloud opportunities and direction, governance practices and policies are currently being developed. Defined standards for security, operations and environment management are also being completed as well as some integration designs.

- User access controls and system configurations are foundational to application security and monitoring. Especially important are controls related to privileged users and audit logging. IT Security and Risk initiated a multi-year project to implement a strategy to consolidate and centralize user identity and access management processes and technology capabilities. The program includes a gap analysis, roadmap and implementation of a user identity and access management life cycle to address Citizens' risks.
- Technology changes are currently under development to allow rate override functionality for specific underwriting circumstances in PolicyCenter. The ability to adjust rates, for specific parameters, is a widely accepted industry practice. Currently, Citizens management performs rate override adjustments manually.

### Theme 5: Fraud Detection and Deterrence

IA continues its statutory commitment in preventing and detecting occupational fraud. Occupational fraud is universally recognized as a risk and as such, risk prevention and early detection have become good business practice. Even a remote possibility of fraud could lead to significant economic and reputational impacts to an organization. Internal audit provides an immediate response to suspected fraud, abuse, and mismanagement through ad-hoc forensic audits.





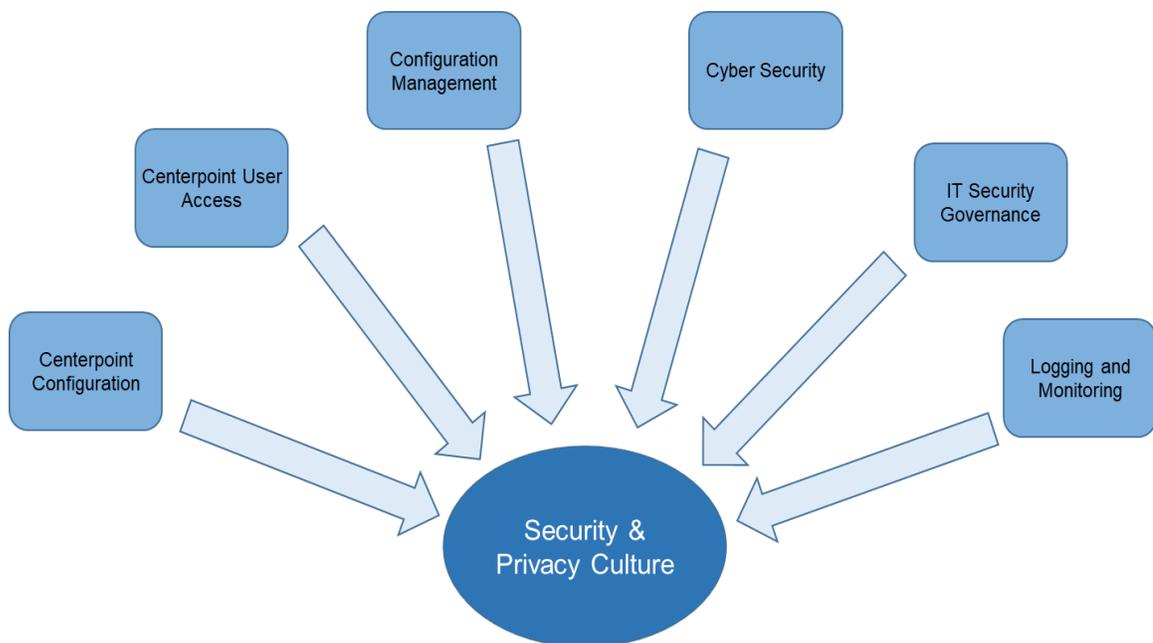
## Plan Detail

In addition to responding to suspected occupational fraud, IA plans to enhance our approach to the awareness of occupational fraud within the organization. According to the Association of Certified Fraud Examiners, 40% of fraud is identified through a tip or hotline call. Approximately another 40% of fraud is identified through general management processes. Therefore, as IA provides the knowledge and understanding of occupational fraud, and potential red flags, through awareness activities, IA will be enhancing approximately 80% of the methods of detection.

Finally, IA plans to support management in identifying, responding to and monitoring risks that may result in a material loss due to fraud. As an independent and objective function, with a strong knowledge of fraud, IA is in a prime position to address fraud risk management programs, and to affect change.

### Theme 6: Security and Privacy Culture

Cyber Security and privacy concerns remain on the radar of both corporate executives and IT Security professionals. Cyber-crime requires that Citizens remains vigilant, constantly reviewing risks and system vulnerabilities, and evolve protection mechanisms to adjust to the risk landscape. IT security initiatives should align to corporate goals and objectives, address legal regulatory compliance needs, support key operational risks, place appropriate resources against the highest risks and deliver value on IT security investments. Citizens currently has several key security initiatives underway to further mitigate risks and optimize security processes in an environment that continues to transition to cloud based solutions where appropriate in the future.





## Plan Detail

---

- With the implementation of the Centerpoint modules for Human Resources, Finance, and Procurement, the business is reviewing risks and revising some of the access controls to improve segregation of duties and oversight. Workflow configurations within the Procurement module are being updated to provide additional processing efficiencies. Some challenges are still being worked and additional access and configuration changes may be required to provide the maturity level and controls required by the organization
- Configuration management is an Information Technology Infrastructure Library (ITIL) and an IT Service Management process to track all configuration items in an IT environment. The software and associated processes establish and maintain consistency in devices including security configurations. This contributes to enhanced performance and reliability by documenting attributes of the system, ensuring that system changes are implemented as prescribed, and potentially alerting management of undocumented changes for further research. A new multi-module service management system is being implemented and the configuration management component of the software is scheduled to be operational by 2019 year-end.
- Citizens' network security policies require risk assessments and ongoing industry standard vulnerability testing to determine potential cyber security weaknesses. On a periodic basis, IT Security and Risk contracts an external firm to assess the network security environment and supporting processes. As part of the network security assessment, the contracted expert performs testing using simulations of malicious external and internal cyber-attacks. Test results are risk assessed, providing an opportunity for IT Management to enhance security processes and protection mechanisms, such as architectural and configuration changes, access controls, vulnerability patching and/or updated operating system and software versions in order to better align with risk tolerance levels.
- Several enhancements are underway within IT Security Governance that will contribute to a more positive outcome toward mitigation of risks and security compliance. These initiatives will provide more streamlined information in support of management decisions and IT Security investment. A formal IT Security Compliance standard was completed, and a self-assessment program is being implemented which will demonstrate policy compliance. A formal risk management standard is underway to improve risk assessments and awareness. In addition, Security policies are being reviewed for potential consolidation and enhancements to simplify understanding and responsibilities within the business units.
- System and application logging and monitoring have been enhanced with the implementation of additional logging agents deployed to servers and databases as well as a new Security Information Event Management (SIEM) software. The cloud based managed service provider system (the SIEM) will aggregate hardware and application logs from many systems and provide analysis and correlation, identify anomalies and

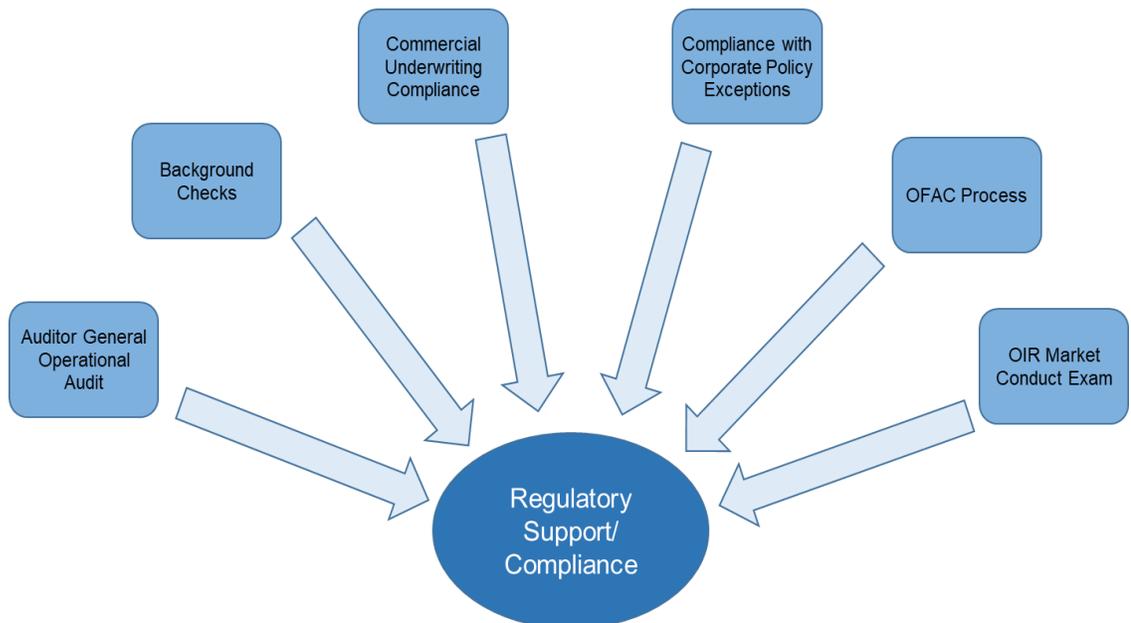


## Plan Detail

provide alerting. The implementation will have a direct and positive impact on incident response and management capabilities.

### Theme 7: Regulatory Support / Compliance

Internal Audit in its liaison role is responsible for coordinating with the Florida Office of Insurance Regulation (OIR) Market Conduct examiners and the State of Florida Auditor General auditors. The OIR exam is performed every two years and the Auditor General operational audit is performed every three years. In 2020 both engagements are scheduled to be performed and will be commencing in September. Most of the coordination efforts constitutes meeting planning, information request tracking and delivery and overall ensuring the examiners/auditors receive the correct information timely.



With the new cloud solutions as well as updated policies and standards, there may be approved reasons for short term non-compliance to policies. Formal exception processes with appropriate tracking and reporting have been implemented using the IT Security and Risk compliance tool. Exceptions to policy may create business risks that require additional scrutiny and a formal process ensures appropriate risks have been identified, a risk value has been determined, and any potential mitigating controls have been applied.

### 8. Enterprise Risk and Internal Control

As part of the Enterprise Risk (ER) and Internal Control (IC) mission to embed comprehensive Enterprise Risk and Internal Control frameworks throughout the organization, the ER & IC will collaborate to strengthen the risk and control culture throughout Citizens. This collaborative approach will enhance management's risk assessment and internal control processes and the



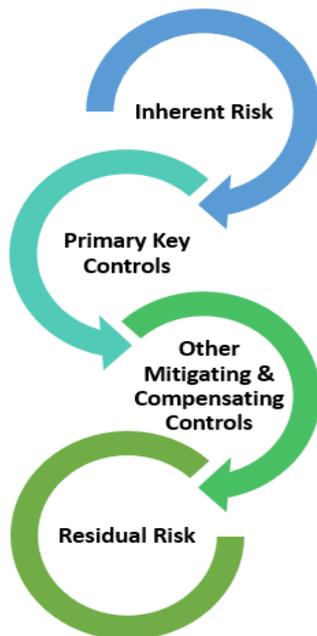
## Plan Detail

risk and control maturity level of the organization. By incorporating a risk and controls consideration, from the day-to-day activities to corporate strategic plans, business leaders will be better equipped to manage their risks and internal controls.

The ER & IC will focus on three key goals that align with Citizens' strategic goals and objectives in order to provide high quality risk and control services:

- Strengthen and maintain Enterprise Risk and Internal Control frameworks by creating and maintaining a collaborative and engaging risk and control identification and assessment environment across the organization.
- Promote a more comprehensive understanding of risk and controls concepts and related tools to improve the business areas' ability to proactively manage risks and strengthen controls
- Leverage technology to provide a holistic view of risks and controls. Enable management across all levels of the organization to self-identify, evaluate, record and manage controls and risks through the provision of guidance and training of software solutions.

By closely aligning the ER & IC processes we will provide a comprehensive approach to embed the Enterprise Risk and Internal Control frameworks throughout Citizens. As both ER and IC collaborate and assist the organization to achieve its business and strategic objectives through the ERM and IC frameworks, the team will coordinate key risk and control touch points and co-facilitate some business area meetings to ensure a cohesive roll out of the frameworks is executed. This alignment will enhance operational effectiveness by strengthening controls in the mitigation of risks.



- **Inherent Risk:** The natural level of risk that exists in a process in the absence of any action management might take to alter the risk's impact or probability. Identified through an inherent risk assessment.
- **Primary Controls:** Controls that have a significant impact on the ability to achieve key business objectives. Primary key controls are identified through both IC and management process reviews.
- **Other Mitigating & Compensating Controls:** Activities in place to reduce risk. Identified through IC and management process reviews as well as ER risk assessments.
- **Residual Risk:** Remaining risk after management has taken actions to alter the risk's impact or probability by establishing primary key controls and/or other mitigating and compensating controls. Determined by management in a residual risk assessment facilitated by ER.



## Plan Detail

### 8.1. Enterprise Risk Plan

ER delivers a forward-looking and insightful risk perspective that enhances the decision-making process and strategic performance of Citizens. ER is focused on enabling the achievement of Citizens' strategic objectives, goals, and business initiatives by coordinating, developing and monitoring Citizens' Enterprise Risk Management (ERM) framework. The established ERM framework supports and challenges the business with the identification, assessment, and mitigation of current or emerging risks. Citizens' management and business leaders have the primary responsibility for identifying, mitigating, and monitoring the risks within their processes and for maintaining an effective Internal Control Framework.

#### Components of the ERM Framework

Citizens' Enterprise Risk Management Framework is made up of six process components derived from the Committee of Sponsoring Organizations of the Treadway Commission (COSO) ERM Framework.



- **Establish the Context** - understanding and articulating the internal and external environments of Citizens. The environment may generate risks that cannot be controlled or constrain the way we respond to a risk.

- **Initial Risk Identification** - using a structured and systematic approach to recognizing where the potential for undesired outcomes or opportunities can arise.

- **Analyze and Evaluate Risks** - considering the causes, sources, probability the risk will occur, the potential positive or negative outcomes, and then prioritizing the results of the analysis.

- **Develop Alternatives, if applicable** - systematically identifying and assessing a range of risk response options guided by risk appetite.

- **Respond to Risks** - making decisions about the best option(s) among several alternatives, and then preparing and executing the selected response strategy. Risk responses will involve one or more of the following: mitigate, exploit, accept, transfer, avoid.

- **Monitor and Review** - evaluating and monitoring performance to determine whether the implemented risk management options achieved the stated goals and objectives.

#### Enterprise Risk Goals and Maturity Model

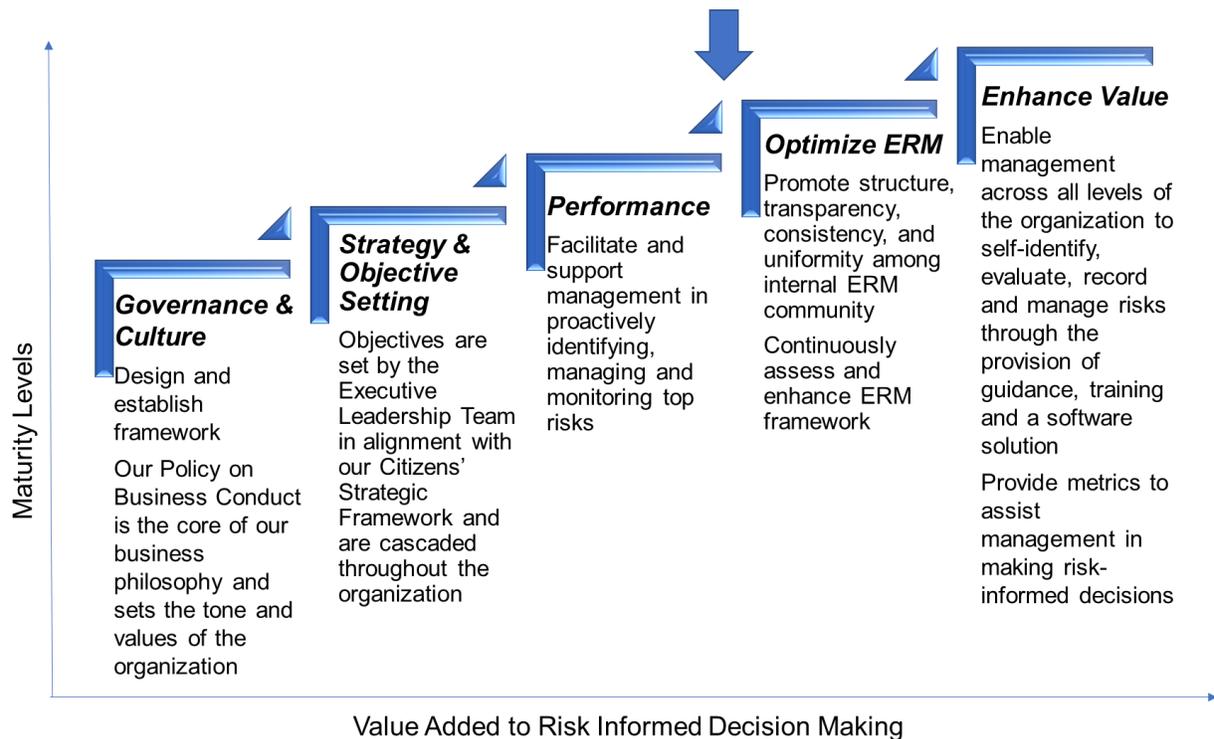
In 2020, ER will leverage the solid foundation of the Enterprise Risk Framework as the team continues progress towards a more mature model that will optimize and enhance value by:

- Promoting structure, transparency, consistency, and uniformity among internal ERM community.



## Plan Detail

- Refreshing and maintaining a collaborative and engaging risk identification and assessment environment across the organization.
- Facilitating the identification and evaluation of risks throughout the organization and supporting the use of a consistent aligned approach across Citizens.
- Enabling management across all levels of the organization to self-identify, evaluate, record, monitor and manage risks through the provision of guidance, training and a risk software solution, Resolver.
- Providing clear and transparent risk reporting to key stakeholders to support decision making processes.
- Proactively identify, assess, measure, manage and monitor Citizens' risk portfolio.
- Validating that current residual risk exposure is aligned with risk appetite.



### 2020 Planned Deliverables

Risk management assessments are conducted from three different perspectives: top-down (strategic risk); bottom-up (operational risk); and project risk.

- *Strategic Risk* - In 2019 the ELT, in a facilitated risk workshop, documented and prioritized 17 key strategic risks. During 2020, ER will continue to work with the assigned Risk Owners to further develop risk mitigation activities and where appropriate develop key risk indicators (KRIs) that can be used to monitor the efficiency and



## Plan Detail

effectiveness of mitigation efforts. In addition, a refresh workshop will be held during the first quarter of 2020.

- *Operational Risk* - During 2020, ER will continue to introduce business unit management and their delegates, to Citizens' operational risk management methodology with the primary objective to enhance Citizens' risk culture within operational management, business units and functional areas. Our operational risk management approach is intended to foster a culture where the organization embraces incorporating risk management decisions into their daily decision making within and across functional areas.
- *Project Risk* - Project risk management has been in place within the project life cycle for many years at Citizens. During 2019, ER and the Project Portfolio Management and Standards team collaborated to begin to align the project risk management process to Citizens' Enterprise Risk Management Framework and related methodology where possible. During 2020, ER will continue to assist project management in redefining and enhancing the project risk assessment and recording process.

### 8.2. Internal Controls Plan

IC is responsible for maintaining and monitoring Citizens' Internal Control Framework (ICF), which is designed to strengthen the governance, oversight, and accountability of Citizens' internal control environment. ICF leverages the 2013 Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control Integrated Framework as the benchmark for operational, financial, and compliance objectives and controls. IC's core objectives for 2020 consist of the following key topics:



- Maintain consistency and sustainability across the Internal Controls Program.
- Collaborate, plan, and assess the annual Control Self-Assessments (CSA) for each business area.
- Develop and report on control metrics to key stakeholders.

COSO provides internal control principles that Citizens can utilize as a benchmark. ICF incorporates those COSO principles that complement the uniqueness of Citizens' operations, business goals and objectives. In addition, there are three major objectives that ICF focuses on: operations, financial and non-financial reporting, and compliance



## Plan Detail

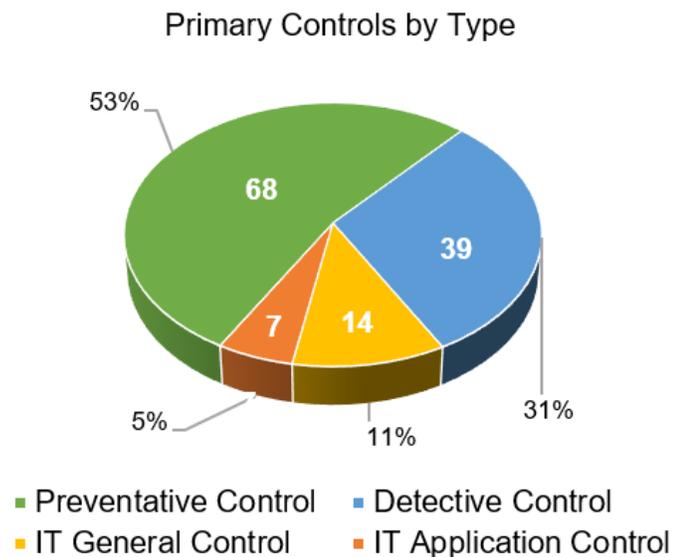
objectives. Through ICF, IC guides and assists management to enhance internal controls, while also helping Citizens transform with the changing and complex insurance environment.

### IC Planned Deliverables

- Maintain Consistent & Sustainable Program

During 2019, the IC successfully implemented the Internal Control Framework across the 71 business processes based on the defined process universe. The established Framework enabled IC to identify the top primary controls for each business process. Primary controls are those key activities performed by the business that help mitigate high inherent risks identified by management. These inherent risks are those top risks that prevent the business from meeting their core objectives, such as strategic, compliance, or reporting objectives.

As of year-end 2019, IC and management identified 128 primary controls across the 71 business processes. Shown in the graph below, the primary controls consist of 39 detective controls, 68 preventative controls, 14 IT general controls, and 7 IT application controls.



During 2020, IC will continue to maintain the ICF program and assist management with the evaluation and enhancement of their current processes, procedures, and controls. Through our monitoring process, we will continue to improve the internal control maturity level of the organization.

- *Evaluate New Business Processes* - IC continues to assess and evaluate the current ICF business process universe. As the internal control maturity level evolves, IC will focus on identifying additional business processes that may need to be incorporated within the scope of the ICF program. Based on our evaluation, we identified additional



## Plan Detail

---

business processes in four (4) divisions to include in ICF: i.e. Human Resources; Legal Services; Underwriting & Agency Services; and Financial Services. IC will collaborate with ER to identify inherent risks and will work with the respective business units to identify primary controls and other mitigating activities.

- *Evaluate & Enhance Control Self-Assessments* - IC works toward continuous improvement, assesses the effectiveness of Citizens' system of internal controls, and identifies opportunities to enhance Citizens' internal control environment. Our efforts will add value to the business and improve control design and operating effectiveness. During 2020, IC will review and enhance selected control self-assessments within five (5) of the divisions. The enhancements will include evaluating new inherent risks, documenting updated process narratives/flowcharts, enhancing current primary control design, and recommending new primary controls.

Control Self-Assessment (CSA) is a defined ICF process through which business unit management verify and validate whether the primary controls are operating as expected. Business Units are responsible for performing an annual CSA for every primary control documented which includes an evaluation of control design and control operational effectiveness.

- *Develop & Report Internal Control Metrics* - As we leverage the leading industry standards for the Internal Control Framework (ICF) as a benchmark, IC will develop ICF scorecards to provide awareness of controls throughout Citizens and for each division.



## Appendix 1: Aligning the Audit Plan to Citizens' Strategic Themes

The OIA uses a collaborative risk-based approach in supporting Citizens in the achievement of its strategic goals. The following table aligns the audit plan with Citizens' strategic themes for 2020.

Citizens' Strategic Themes	OIA Themes	Potential Engagements
Strengthening Metric Drive Decision Making	Corporate Expense Management	<ul style="list-style-type: none"> <li>• CAT Risk Forecasting &amp; Analysis</li> <li>• Financial Planning &amp; Analysis</li> <li>• OIA Data Analytics</li> <li>• OIA Risk Analysis &amp; Red Flags</li> </ul>
Proactively Managing Claims and Litigation Avoidance	Corporate Effectiveness Corporate Expense Management Occupational Fraud, Waste & Abuse	<ul style="list-style-type: none"> <li>• Appraisal Process</li> <li>• AOB Implementation</li> <li>• Claims IA Auto Billing</li> <li>• E-Disbursements</li> <li>• Policyholder Claims Experience</li> <li>• Pre-event Bond Assets</li> <li>• Proof of Repairs (Irma)</li> <li>• Xactimate Application</li> </ul>
Ensuring Scalability and Flexibility in Our Operations	Corporate Effectiveness Corporate Expense Management Innovation & System Conversion Occupational Fraud, Waste & Abuse Regulatory Support/Compliance Security & Privacy Culture	<ul style="list-style-type: none"> <li>• Agency Management System</li> <li>• Automated Underwriting</li> <li>• Centerpoint Configurations</li> <li>• Centerpoint User Access</li> <li>• Cloud Readiness</li> <li>• Configuration Management</li> <li>• Disaster Recovery</li> <li>• Identity and Access Management</li> <li>• IT Asset Management</li> <li>• IT Security Governance</li> <li>• Logging and Monitoring</li> <li>• OFAC Process</li> <li>• Policy Exception Management</li> <li>• Remittance Processing</li> <li>• Service Organization Controls (SOC)</li> <li>• Software Asset Management</li> <li>• Telecommunications</li> <li>• Third Party Access</li> <li>• Third Party Vendor Risk Mgt</li> <li>• Vendor Selection</li> <li>• Wire transfer/ACH</li> </ul>
Investing in and Leveraging Citizens' Greatest Resources - Our Employees	Corporate Expense Management Corporate Effectiveness Regulatory Support/Compliance	<ul style="list-style-type: none"> <li>• Background Checks</li> <li>• Co-employment</li> <li>• Employee Expense Reimbursement</li> <li>• OIA Fraud Awareness and Training</li> </ul>



## Appendix 2: Overview of Potential Audit Engagements

Title	Audit Justification and Objective
Agency Management System	<p><b>Risk Rationale:</b> The current agency management system, that supports agent distribution relationship management, is being replaced with the Salesforce Service Cloud Platform. This platform will support the tracking and monitoring of agent licenses, commission, performance, investigations, complaints, and key performance indicators.</p> <p><b>Objective:</b> Provide control advice and project support during the system configuration and implementation.</p>
Appraisal Process	<p><b>Risk Rationale:</b> A significant portion of claims are being referred to appraisal in order to settle claims. In addition, there was a litigated settlement offer made earlier in the year to help move claims out of litigation to be resolved in appraisal.</p> <p><b>Objective:</b> Evaluate the adequacy and effectiveness of controls related to the Appraisal process.</p>
Assignment of Benefits (AOB) Implementation	<p><b>Risk Rationale:</b> AOB legislation passed during 2019, resulting in the quick design and implementation of processes and procedures to meet the 7/1/2019 statutory implementation date.</p> <p><b>Objective:</b> Validate that the processes developed are operating as intended and in compliance with the statute.</p>
Automated Underwriting	<p><b>Risk Rationale:</b> Underwriting management is working on a project to redesign the current automated underwriting process, as staff currently touch 80% of automated underwriting files. The purpose of the project is to gain efficiency in the underwriting effort for evaluating personal lines new business applications.</p> <p><b>Objective:</b> Provide control advice and project support to the automated underwriting redesign.</p>
Background Checks	<p><b>Risk Rationale:</b> The organization performs background checks during the pre-employment phase of the hiring process and is evaluating expanding the process to include periodic checks on staff and agents. These background checks are important to ensure Citizens does not employ anyone in violation of Florida Statutes or laws.</p> <p><b>Objective:</b> Provide control advice and project support to help ensure that a comprehensive, consistent and defensible process is in place.</p>



## Appendix 2: Overview of Potential Audit Engagements

Title	Audit Justification and Objective
Catastrophe Risk Forecasting & Analysis	<p><b>Risk Rationale:</b> Citizens' Corporate Analytics Department calculates and provides catastrophe risk forecasting and modeling for the organization. The department annually calculates and reports aggregate net probable maximum losses by utilizing proprietary modeling applied to Citizens policies-in-force. This information, along with other risk forecasting and analysis, is relied on by Citizens to make risk transfer decisions.</p> <p><b>Objective:</b> Evaluate processes and controls surrounding catastrophe forecasting and modeling.</p>
Centerpoint Configurations	<p><b>Risk Rationale:</b> Oracle Fusion Cloud Service modules for human capital management, financials, and procurement were implemented (referred to as Centerpoint). Centerpoint replaced independent applications previously used by Human Resources, Finance and Procurement. Oracle module configuration is complex and proper configuration of the modules is necessary to adequately restrict and/or eliminate the ability to override controls in place to prevent inappropriate transactions. Improper application configuration may lead to unauthorized transactions that may impair business operations or allow nefarious transactions.</p> <p><b>Objective:</b> Confirm that Centerpoint modules are properly configured to ensure that security is adequate and prevents the override of key controls, appropriate logging is turned on and business operational process needs are met with configurations that are installed.</p>
Centerpoint User Access	<p><b>Risk Rationale:</b> Centerpoint process owners, supported by IT, implemented additional user access controls including monitoring of privileged users and reducing segregation of duty conflicts. Additional automation and enhancements are being considered to further strengthen controls.</p> <p><b>Objective:</b> Provide advice on the efficiency and adequacy of access controls and planned enhancements.</p>
Claims Automated Independent Adjuster Billing	<p><b>Risk Rationale:</b> Independent adjusters are paid on either a day rate or fee bill basis. Day rate payments are calculated on a flat rate per day of work completed while fee bill payments are based on a variable percentage of the gross claim amount calculated. Currently most of the day rate and fee bill payment processes are manual and claims management is considering the use of third-party software to automate the management of independent adjuster payments.</p>



## Appendix 2: Overview of Potential Audit Engagements

Title	Audit Justification and Objective
	<p><b>Objective:</b> Provide control advice and project support to ensure automation provides timely and accurate payments.</p>
Cloud Readiness	<p><b>Risk Rationale:</b> Migration to cloud services and solutions means reliance upon service providers for proper information security and privacy, legal compliance, disaster recovery, maturity of technology and business viability.</p> <p><b>Objective:</b> Assess Citizens' cloud migration program to ensure that adequate plans, processes, contract language, and cost models have been developed and appropriate risk mitigation activities are incorporated to minimize or avoid business disruption as additional cloud products are obtained.</p>
Co-employment	<p><b>Risk Rationale:</b> Citizens leverages temporary contingent workers as needed for a variety of operational reasons. Advantages of using contingent workers include scalable staffing flexibility, enabling access to broad talent pools, as well as reduced costs and increased operational efficiencies in some cases. While substantial practical benefits often accompany such arrangements, equally substantial legal and practical pitfalls can occur if risks surrounding contingent staffing are not fully understood and/or properly managed including misclassification and the unintentional creation of an employer-employee relationship between Citizens and a contingent worker.</p> <p><b>Objective:</b> Evaluate the adequacy and effectiveness of current policies, practices, and controls surrounding contingent staff management to ensure an effective program is properly managed and executed.</p>
Commercial Underwriting Compliance	<p><b>Risk Rationale:</b> There are various State of Florida Statutory underwriting requirements which Citizens needs to follow for properties to be eligible for coverage under specific product types. An example would be coverage eligibility for properties with transient public lodging.</p> <p><b>Objective:</b> Evaluate the adequacy and effectiveness of controls in place to meet State of Florida Statutory underwriting requirements.</p>
Compliance with Corporate Policy Exceptions	<p><b>Risk Rationale:</b> Compliance with corporate policy exception procedures and monitoring may be occurring in several business areas. These processes, associated risk levels and monitoring may not be consistent across Citizens.</p> <p><b>Objective:</b> Identify all policy exception processes within Citizens and determine focus, consistency in processes and that appropriate levels of</p>



## Appendix 2: Overview of Potential Audit Engagements

Title	Audit Justification and Objective
	management are included in tracking and reporting. Validate that high-risk issues are raised to Enterprise Risk for consideration and decisions by executive management
Configuration Management	<p><b>Risk Rationale:</b> Absent a complete asset inventory as well as secure configurations installed and maintained for operating systems and software, assets may not be properly protected, leading to undocumented changes that may cause business disruption or a security breach.</p> <p><b>Objective:</b> Evaluate the effectiveness of policies and processes requiring that secure configuration baselines are defined and documented for all environments and consistently reflected on hardware, software and images.</p>
Cyber Security	<p><b>Risk Rationale:</b> The integrity and privacy of data for which Citizens is the custodian, should be well controlled to avoid malicious internal or external attacks that may result in data exposure, data loss and/or reputational damage.</p> <p><b>Objective:</b> Evaluate the effectiveness of the processes comprising periodic network penetration testing, vulnerability management and malware prevention. Validate that the test objectives and security processes are assessed against Citizens' internal cyber security standards as well as industry leading practices.</p>
Disaster Recovery	<p><b>Risk Rationale:</b> The backup data center was moved to a new Florida location in 2018 and the plan was updated subsequent to the migration. Critical systems and data are replicated and backed up at the new site to provide continuity in the event of a natural disaster, cyber-attack or other unique occurrence. The disaster recovery program is important to the business not only from a business continuity perspective, but also due to the heightened risks posed by Florida weather events.</p> <p><b>Objective:</b> Evaluate the disaster recovery program, plans and testing strategy to ensure the program incorporates output from the business continuity efforts, critical applications and data required for recovery are incorporated in data replication and testing is comprehensive to ensure that the data center and associated processes will meet business needs in a recovery event.</p>
E-Disbursements	<p><b>Risk Rationale:</b> Citizens is seeking a solution which leverages debit card and Automated Clearing House (ACH) technology for two types of claims payments: Additional Living Expense payments to policyholders via vendor issued debit card and/or ACH options; and ACH payments to policyholders</p>



## Appendix 2: Overview of Potential Audit Engagements

Title	Audit Justification and Objective
	<p>and/or other parties for claim related disbursements; including multi-party payment options and multiple external approvals (both in the event of a catastrophe and in usual operations).</p> <p><b>Objective:</b> Provide consultative advice during design and implementation to assess the security of debit cards and ACH transactions.</p>
Employee Travel & Other Expenses	<p><b>Risk Rationale:</b> Citizens management and staff routinely travel between office locations, as well as to various industry and training events. The Business Travel Policy has established standards for the payment or reimbursement of travel costs consistent with state laws and regulations and for ensuring that expenses incurred are appropriate and prudent in the context of Citizens' governmental functions.</p> <p><b>Objective:</b> Evaluate the adequacy and effectiveness of controls related to Citizens' travel expense policy using targeted analytical procedures.</p>
Financial Planning and Analysis	<p><b>Risk Rationale:</b> Citizens successfully launched the Budgeting module in Centerpoint in 2018 and training was conducted for budget users throughout the organization. As a result, a continuous budgeting model was adopted throughout the organization in 2019. The need for continuous budgeting, strategic forecasting, and reforecasting is critical to have clear understanding and communication surrounding financial expectations to make strategic decisions and adjust resource allocations in response to changing conditions</p> <p><b>Objective:</b> Evaluate the adequacy and effectiveness of controls related to the Financial Planning and Analysis process.</p>
Identity and Access Management	<p><b>Risk Rationale:</b> Citizens' IT Security and Risk department is implementing an enterprise wide strategy to consolidate and centralize user identity and access management processes and technology capabilities. Complexity will continue to increase as new cloud solutions, systems and applications are adopted and integrated into the current environment. These complexities should be understood and appropriate controls for authentication and authorization should be implemented to mitigate risks associated with user access/privileged access, segregation of duties, oversight and monitoring and reporting capabilities.</p> <p><b>Objective:</b> Assess project governance and progress during the multi-year implementation of a comprehensive identity and access management solution and corresponding processes and provide advice throughout the project as needed.</p>



## Appendix 2: Overview of Potential Audit Engagements

Title	Audit Justification and Objective
IT Asset Management	<p><b>Risk Rationale:</b> IT hardware/software assets are inventoried and tracked to avoid redundant purchases and allow operations personnel to proactively replace outdated hardware/software that is nearing the end of its life cycle. Citizens may face licensing fines if adequate controls are not in place to validate installed software against licenses.</p> <p><b>Objective:</b> Assess controls associated with the hardware lifecycle to ensure data is reliable for decisions associated with asset expenses and disposal. Validate that processes are implemented to manage and monitor system capacity and performance.</p> <p>Also, as part of an operational initiative, the IA was approached to provide consultative advice through a validation of frameworks, policies and processes associated with the ongoing development work to enhance the software asset management program.</p>
IT Security Governance	<p><b>Risk Rationale:</b> Sound policies and processes within the IT Security department ensure appropriate risk management and effective use of resources. Strategies and objectives should be developed to align with business goals with underlying foundational programs and processes supporting those objectives. Absent appropriate oversight, lack of appropriate IT security risk mitigation may impair business performance.</p> <p><b>Objective:</b> Evaluate governance processes related to the strategy, policies, programs and metrics to direct, manage and monitor IT Security for the enterprise.</p>
Logging and Monitoring	<p><b>Risk Rationale:</b> System and application logging is required to provide an audit trail of business and system transactions to monitor access and correlate events that may require additional research and follow-up. The Corporate information classification and handling policy requires that certain audit and logging configurations are implemented for systems which are handling restricted confidential and confidential data. Absent appropriate logging practices being implemented, there is a risk for lack of accountability and potentially an inability to surface information to detect or reconstruct system events when required.</p> <p><b>Objective:</b> Assess the implementation of system logging and monitoring to ensure that risks have been determined, appropriate logs have been turned on and event monitoring is occurring. Validate that logging also fully supports the incident response process.</p>



## Appendix 2: Overview of Potential Audit Engagements

Title	Audit Justification and Objective
Occupational Fraud Awareness	OIA will leverage extensive industry knowledge, experience, and expertise to drive a message that everyone has a duty to understand occupational fraud to ensure any potential misconduct is identified and addressed timely. This will be accomplished through proactive training programs that are business unit specific and leveraging the communication platforms available within the company.
OFAC Process	<p><b>Risk Rationale:</b> Activities were transferred to Financial Services from the Legal area during the fall of 2017 as a result of realignment stemming from an Audit. Follow-up is needed to ensure compliance with the Federal Regulation.</p> <p><b>Objective:</b> Evaluate the adequacy and effectiveness of controls related to OFAC validation process.</p>
OIA Data Analytics	OIA will be expanding upon its own data analytics audit program. This will be accomplished using state-of-the-art tools and techniques to develop tests that OIA can apply across the organization, going beyond sampling into early warning and continued monitoring.
Policyholder Claims Experience	<p><b>Risk Rationale:</b> There are many facets to the different types of claims losses which drive claims to be handled through various business models and rely on Citizens staff and independent adjusters to meet policyholder claim processing needs.</p> <p><b>Objective:</b> Evaluate the adequacy and effectiveness of controls related to Claims Customer Experience.</p>
Pre-event Bond Assets	<p><b>Risk Rationale:</b> Citizens has issued multiple senior secured bonds for the purpose of funding losses in the event of future catastrophe. If a claims catastrophe should occur, Citizens would access the proceeds of these bonds held within secured trust accounts. It is critical that there is appropriate management of these assets and proper controls exist surrounding the ability to access the proceeds located in the trust account in order to pay out claims to the Company's policyholders.</p> <p><b>Objective:</b> Evaluate the adequacy and effectiveness of controls related management of assets and access to trust account proceeds.</p>
Product Strategy Development	<b>Risk Rationale:</b> There is no formal product guiding principle or strategy to help align products across Citizens. The project will identify product requirements in the Florida Statutes, Florida Administrative Codes, and



## Appendix 2: Overview of Potential Audit Engagements

Title	Audit Justification and Objective
	<p>similar documents and use the resulting analysis to develop consensus and ultimate approval for a foundational product doctrine.</p> <p><b>Objective:</b> Provide control advice and project support during the foundational product doctrine development.</p>
Proof of Repairs	<p><b>Risk Rationale:</b> During October 2018, Citizens began requiring proof of repairs for Hurricane Irma damage to determine renewal eligibility for policies renewing on or after March 6, 2019. Policyholders who have filed a claim for damage caused by Hurricane Irma are required to submit proof of repair to Citizens as soon as any repairs are complete. For claims with repairs not completed by the policy's renewal date Citizens will accept documentation such as a contract that demonstrates repairs are underway to process the renewal.</p> <p><b>Objective:</b> Evaluate the adequacy and effectiveness of controls for the request and receipt of proof of repairs and the determination of renewal eligibility.</p>
Rate Override Technology Development	<p><b>Risk Rationale:</b> Technology changes are currently under development to allow rate override functionality for specific underwriting circumstances in PolicyCenter. The ability to adjust rates, for specific parameters, is a widely accepted industry practice. Currently, Citizens management performs rate override adjustments manually.</p> <p><b>Objective:</b> Provide control advice and project support during the application development and pilot.</p>
Remittance Processing	<p><b>Risk Rationale:</b> In late 2018, remittance processing completed the migration of the remittance systems to the RT Lawrence software. Post implementation, it was noted that patches were needed to fix processing constraints that were experienced during implementation. The system is used to process more than \$800m in premium payments annually.</p> <p><b>Objective:</b> Evaluate the adequacy and effectiveness of controls related to remittance processing.</p>
Risk Analysis & Red Flags	<p>The cornerstone of OIA's fraud awareness program, transactional risk analysis and identifying red flags, provides the context needed to share the knowledge with the company through training sessions, but also direct our data analytics and targeted audit efforts to the most relevant risks that cannot be avoided.</p>



## Appendix 2: Overview of Potential Audit Engagements

Title	Audit Justification and Objective
Service Organization Controls (SOC)	<p><b>Risk Rationale:</b> The Vendor Management Office has implemented new processes and procedures to obtain 3<sup>rd</sup> party vendor Service Organization Controls (SOC) reports during the solicitation process and has centralized the ongoing SOC review process as of Q2 2019.</p> <p><b>Objective:</b> Evaluate the adequacy and effectiveness of controls related to the SOC process.</p>
Telecom's	<p><b>Risk Rationale:</b> Citizens relies on voice and data communications to support employee, customer and vendor activities in daily operational activities. Communication services such as voice, mobility, presence information, instant messaging, audio, web and video conferencing, voicemail, etc. should be secure, reliable and assessed periodically to validate that services meet business requirements and risks are mitigated to avoid business disruption.</p> <p><b>Objective:</b> Assess policies, processes and standards and ensure that wire, wireless and data communication services are planned, procured, configured, secured, monitored and reviewed, to support changing telecommunications business needs.</p>
Third Party Access	<p><b>Risk Rationale:</b> Third party security access, 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.</p> <p><b>Objective:</b> Evaluate risks associated with third party access to the Citizens network and validate that third-party policies, inventories, user account management, connections and monitoring are appropriate for the organization in mitigating those risks.</p>
Third-party Risk Management	<p><b>Risk Rationale:</b> The VMO has established guidelines and tools for contract managers to use to manage vendor relationships. Each third-party relationship brings with it several risks that need to be identified and assessed. These risks are often multi-dimensional as they extend across suppliers, vendors, contractors, service providers, and other parties, and can have an impact on different levels of the organization.</p> <p><b>Objective:</b> Evaluate the adequacy and effectiveness of controls related to VMO's Third-party Risk Management process.</p>



## Appendix 2: Overview of Potential Audit Engagements

Title	Audit Justification and Objective
Vendor Selection	<p><b>Risk Rationale:</b> Citizens' vendor selection processes have been updated within the past year to improve vendor identification and due diligence assessments.</p> <p><b>Objective:</b> Evaluate the adequacy and effectiveness of processes/ controls implemented to ensure adequate vendors are selected.</p>
Wire Transfer/ ACH	<p><b>Risk Rationale:</b> Citizens is migrating to a new vendor to provide all Company banking needs, including wire transfers and ACH services. Since Citizens periodically has the need to wire large sums of money, the Company must ensure the processes, controls, and authorities to do so are set up correctly and securely. The most significant risk of transferring to the new bank is to ensure the wire process is set up correctly with the appropriate access, segregation of duty controls and monitoring.</p> <p><b>Objective:</b> Evaluate the adequacy and effectiveness of controls related to the wire transfer and ACH processes.</p>
Xactimate Application	<p><b>Risk Rationale:</b> Citizens is working with a nationally recognized third-party vendor, Xactimate, to develop and pilot a customized application for simplifying the estimating process during onsite inspections during a catastrophe event. Pilot testing is planned during Q1 or Q2 2020.</p> <p><b>Objective:</b> Provide control advice and project support during the application development and pilot.</p>