

Office of the Internal Auditor



Strategy & Plan 2026

December 2025



Table of Contents:

Page

	Executive Summary	1
	Conformance & Organizational Independence	1
	Vision, Mission, and Core Values	1
	Three Lines Model and Dual-Role Safeguards	2
	Strategic Objective	2
	Internal Audit Plan	3
	Enterprise Risk Plan	8
	Internal Control Plan	10
	Appendixes	
	1. Dual Role Safeguards	12
	2. Overview of Potential Audit Engagements	14
	3. Audit Universe	22



Executive Summary

This plan delivers explicit coverage over the Citizens Property Insurance value chain and defines how The Office of Internal the Auditor (OIA) will conform to the Global Internal Audit Standards (GIAS), the COSO Enterprise Risk Management (ERM), and Internal Control Frameworks (ICF), support strategic imperatives (Depopulation, Customer Experience, Emergency Assessments), and prepare for the 2026 Internal Audit External Quality Assessment (EQA). It includes a quantified capacity model, KPI definitions, a detailed engagement catalog with scope and data needs, and graphics guidance for Board reporting. Key focus for 2026 includes:

- Full GIAS mapping (Purpose/Ethics/Governing/Managing/Performing) and a conformance statement with disclosure protocol.
- Dynamic risk management methodology and an enterprise risk (ER) function that supports organizational resilience by embedding a common risk language, empowering leaders with tools and training, monitoring mitigation effectiveness, and delivering actionable risk insights to guide strategic decision-making
- An Internal Control (IC) function that supports the organization by providing practices that safeguard organizational integrity by managing the Internal Control Framework (ICF), strengthening accountability through standardized processes, monitoring control effectiveness, and providing assurance that operations align with strategic objectives and regulatory expectations.
- Five audit themes for 2026 that are tailored to Citizens' explicit strategic objectives, scope, controls focus, data sources, and estimated hours.
- Growing OIA's analytics & automation roadmap for continuous assurance within Internal Audit, Enterprise Risk, and Internal Control.
- 2026 EQA timeline with readiness artifacts (charter, methodology, file samples, competency/ CPE logs, independence safeguards, KPI evidence).
- Quarterly Audit Committee progress reporting, calendar and decision asks; KPI pack with formulas, thresholds, and ownership.

Conformance & Organizational Independence

OIA conducts work in conformance with the Global Internal Audit Standards and the Code of Ethics. The Chief of Internal Audit reports functionally to the Audit Committee and administratively to the CEO. Any material nonconformance and remediation actions will be communicated to senior management and the Audit Committee.

Vision, Mission, and Core Values

Vision: To be an innovative driver for positive change and continuous improvement of Citizens' governance and control environment, contributing to the corporation's achievement of its strategic objectives.

Mission: To provide independent, objective assurance and consulting services designed to add value and improve the organization's operations. We bring a systematic, disciplined, and aligned approach to evaluating and improving the effectiveness of risk management, control, and governance processes.



Core Values: Integrity, Objectivity, Professionalism, Collaboration, Innovation, Service to Policyholders.

Three Lines Model and Dual-Role Safeguards

Management is the First Line, ER and IC are the Second Line, and Internal Audit is the independent Third Line. (Refer to Appendix 1 for details)

Function	Purpose	Key Responsibilities	Prohibited Activities
Internal Audit, Third Line	Independent assurance	Risk-based plan, opinions, reporting, follow-up	No operational ownership of ERM or ICF, no design or approval of business controls, no management decisions
ER, Second Line	Risk facilitation and oversight	Risk policy and appetite, KRI library, top risk reporting, deep dives, scenario analysis	No executional ownership of First Line controls, no Internal Audit assurance issuance
IC, Second Line	Control policy and quality	Control framework and taxonomy, CSA and testing standards, documentation, and deficiency tracking	No ownership of First Line processes, no Internal Audit assurance issuance

Integrated Planning Approach (Internal Audit + ER + IC)

Each quarter, Internal Audit (as the Third Line) refreshes a rolling risk-based plan using current intelligence from ER (risk appetite/KRIs, top-risk changes, scenario results) and IC (CSA/testing outcomes, defect trends), plus Citizens-specific change signals (CAT outlook shifts, reinsurance placements, underwriting/eligibility overrides, depopulation, claims/litigation and ELMS data, regulatory updates, and prior audit results). Internal Audit reevaluates the audit universe (inherent/residual risk, fraud/regulatory sensitivity, data sensitivity), checks portfolio balance across themes, confirms reliance vs. duplication with IC, verifies independence safeguards when Internal Audit touches ER/IC areas, sizes work to capacity with a contingency buffer, and finalizes a Quarterly Rolling Plan for management socialization and Audit Committee confirmation. Outputs include:

- Quarterly Rolling Engagement Plan: objectives, risk link, scope boundaries, data sources, hours, timing, team/skills, dependencies.
- Independence & Reliance Statement: any co-sourcing/for ER/IC audits; reliance points on second-line testing; conflicts/cooling-off notes.
- Internal Audit Risk Heatmap with top-risk callouts as viewed by Internal Audit.
- Scoping Summaries (per engagement): objectives and risk rationale.

Strategic Objective

Our purpose is to provide independent assurance and practical advice that strengthens governance, risk management, and internal control across underwriting, claims, reinsurance, technology, data, compliance, and finance.



To achieve this, we run rolling risk assessments that blend enterprise risk signals, control results, regulatory changes, catastrophe modeling, reinsurance placement, litigation trends, and prior audit findings. We will use this view to refresh the audit universe, rebalance the plan, and target second-line testing and deep dives. We will favor analytics and automation where they reduce effort and improve coverage.

Internal Audit Plan

Internal Audit follows a detailed annual planning process and prepares a themes-based audit plan, considering the possibility of dynamic risk fluctuations and process changes throughout the year. The audit plan continuously evolves to support our dynamic risk environment, focusing on current and emerging reputations, compliance, operational, information technology, and financial risks. The Internal Audit “rebalances” audit activities to achieve the most significant impact in a rolling audit plan, ensuring adequate focus on strategic issues and critical processes.

Internal Audit’s primary objective is to determine whether the internal network of governance processes, risk/opportunity management, and internal control, as designed and represented by management, is adequate and functions in a manner to ensure that:

- Risks/opportunities are appropriately identified and managed.
- Significant financial, managerial, and operating information is accurate and timely.
- Employee actions comply with policies, procedures, and applicable laws and regulations.
- Resources are sourced economically, used efficiently, and protected adequately.
- Programs, plans, and objectives are achieved.
- Significant legislative or regulatory issues affecting operations are recognized and addressed appropriately.

Audit Universe and Risk Assessment

The Internal Audit function maintains an up-to-date audit universe (*refer to Appendix 2*), which includes the corporation's key business processes, functions, and systems. A quarterly comprehensive risk assessment is conducted to identify and prioritize audit areas based on risk exposure, materiality, and potential impact on the corporation’s objectives.

Audit Plan Development and Execution

The annual audit plan was developed based on the results of our risk assessment and Citizens’ strategic priorities. The planned engagements include assurance, consulting, and special projects. The audit engagements will be executed with agility and adaptability, enabling adjustments to the business environment, emerging risks, and evolving regulatory requirements. The planned audit activities are bundled into audit themes to help us determine, consolidate, and provide high-level insights into potential 2026 audit focus areas.

Capacity, Hours & Flexibility

Plan hours are based on current staffing and expected sourcing. Maintain a 10–15% contingency for unplanned requests, investigations, and emerging risks.

Planned Audit/Advisory Projects	22-26
Follow-up & Validation	All high/medium issues within 180/270 days
Contingency	10–15% of available hours



Training & CPE	40 hours per auditor
Co-sourcing	Use of specialists, as needed, to supplement internal audit capabilities.

Types of Internal Audit Engagements, strategy view

Internal Audit utilizes a balanced portfolio to deliver assurance, insight, and capability building that is aligned with Citizens' strategy and risk profile.

Assurance core

- **Traditional audits**, independent opinions on design/operating effectiveness for priority processes. (~280–400 hrs.)
- **Precision audits**, analytics-led reviews that scan full populations to surface exceptions quickly, best for high-volume and rule-based areas. (~80–180 hrs.)
- **Targeted audits**, rapid checks to validate specific red flags or anomalies and decide on escalation. (~50 hrs.)

Change and execution

- **Project audit or advisory**, stage-gate and readiness views for major change/implementations. (~100 hrs.)

Performance enablement

- **Advisory**, management-requested design input that improves processes and controls while preserving independence. (~100 hrs.)
- **Business support**, short, collaborative problem solving to unlock quick wins and clarify handoffs. (~40 hrs.)
- **Training and education**, targeted capability building on risk, control, process, and financial stewardship, effort varies by audience.

Reporting, Follow-up, and Performance Metrics

Internal Audit provides regular status updates to senior management and the Audit Committee, including progress on the plan, significant observations, and thematic insights. Follow-up validates timely remediation. KPIs include plan delivery, cycle time, stakeholder satisfaction, recommendation implementation rates, coverage of top risks, adoption of automation and analytics, and QAIP conformance indicators.

KPI	Target	Definition	Data Source	Frequency	Owner
Plan Delivery	≥85%	Delivered/Committed hours (excl. approved deferrals)	AuditBoard	Quarterly	IA Directors
Cycle Time	≤12 weeks	Scope start → final report (median)	AuditBoard	Quarterly	IA Directors
On-time Remediation (High/Medium)	≥90%	Closed by due date/ total due	AuditBoard	Quarterly	Mgmt. + IA
Audit Productivity	≥80%	Time recorded (excl. Time-off and training)	AuditBoard	Quarterly	IA Directors



Stakeholder Satisfaction	≥4.0	Post-engagement survey average	Survey Monkey	Quarterly	CIA
Analytics Adoption	≥ 80%	Audits with scripted analytics	AuditBoard	Quarterly	DA Lead

Audit Themes

The 2026 themes are as follows:



- Effectiveness and Resiliency
- Expense and Capital Management
- Reporting and Data Accuracy
- Compliance and Litigation
- Data Management and Protection

Theme 1: Effectiveness and Resiliency

Traditionally, corporate effectiveness measures an organization's success in achieving its set goals. The right people, processes, and structure enable efficacy and efficiency, aligning with the corporation's strategic imperatives and initiatives. Various areas may contribute to corporate effectiveness, such as faster, leaner, and more cost-effective business processes, improved digital adoption, more efficient use of technology, management tools such as policies and procedures, and enhanced customer and employee experiences. The Internal Audit will assess several significant business processes that contribute to operational effectiveness and organizational resilience.



- Secondary Employment
- CAT Preparedness
- Automated Underwriting
- IT General Controls



Strategy & Plan

Theme 2: Expense and Capital Management

Citizens continues to develop and improve existing strategies, programs, and processes to reduce operating expenses and financial exposure. The organization remains focused on achieving a robust financial control environment and maintaining acceptable financial ratios. The Internal Audit will assess several key business processes that contribute to efficient financial planning, cost management, and reinsurance accounting.



- Commissions
- Claims Vendor Management
- FRISS
- Claims Check Processing
- E-Payments
- Rate Implementation
- CAT Bond Liquidity
- Premium Refunds & Suspense Account

Theme 3: Reporting and Data Accuracy

Analytics collect data and generate reports to inform critical business decisions and key metrics. As a result, a reliance on data being populated from many systems within the environment exists. Management must be confident of the completeness and accuracy of this data, which relies upon interfaces, batch jobs, and general IT controls to create appropriate and valuable metrics for decision-making. Internal Audit will provide assurance and advisory services to support these processes.



- Fraud Analytics/Continuous Monitoring
- Enterprise Data Governance/Data loss prevention



Theme 4: Compliance and Litigation

The Florida legislative session each year produces several bills that may affect corporate business processes and systems. The corporation responds to these changes by ensuring that internal processes and procedures are adjusted to accommodate compliance with current regulations. Compliance programs are designed to integrate ethical standards into an organization's daily business activities through communication, education, training, monitoring, investigation, detection, and reporting. It focuses on reducing claims litigation and enhancing litigation capabilities by developing and implementing innovative litigation and claims management practices. Internal Audit will provide assurance and advisory services to support the implementation of the processes and procedures.



- Ethics
- Privacy Program
- Division of Administrative Hearings (DOAH)
- Regulatory Support (Auditor General Operational Audit)
- Regulatory Support (OIR Market Conduct Exam)
- Period End Financial Reporting
- Loss Reserve Development, IBNR



Strategy & Plan

Theme 5: Data Management and Protection

Citizens is transforming how systems and services are delivered to employees and customers to enhance productivity, eliminate unnecessary capacity and associated costs, and meet the rapid increase in demand. As the focus on flagship and critical initiatives is changing, applications currently residing on premises are being migrated to Software as a Service (SaaS) solution, and several new products are being implemented for modernization and improved productivity. Internal Audit will participate in projects or perform audits to validate that appropriate controls remain in place as these changes occur.

Cybersecurity protects an organization's computer equipment and information from unintended or unauthorized access, modification, or destruction. Data can be in various forms, including customer lists, customer and financial details in databases, and paper documents. A cyber-attack may cause economic losses and damage the corporation's reputation, so sound practices must be applied to protect data. The IT Security and Privacy Office continues to review and refine security and privacy policies, standards, and procedures to ensure alignment with global events. The Internal Audit will conduct IT security audits due to the critical nature of these controls and assess the adequacy of the processes and controls. The Internal Audit function will provide assurance and advisory services to support the implementation of methods and procedures that ensure system security and data protection. Additionally, we will provide assurance services to opine on the effectiveness of IT General Controls for critical systems/applications.



- Enterprise Data Governance/Data loss prevention
- Technology Governance
- Patching & Vulnerability Management
- EZLynx (Clearinghouse)

Management and Data Analysis

Occupational fraud is a universally recognized business risk, and Internal Audit has a statutory commitment to prevent, detect, and respond to fraud, abuse, and mismanagement. This commitment is fulfilled through fraud training and awareness, risk assessment, analytics, and targeted audits.

Data analysis supports the integration of digital technologies into Internal Audit, Enterprise Risk, and Internal Control activities. In 2026, these integration efforts will be focused on:

- Consolidating our governance, processes, and data retention and reduction approaches.
- Strengthening our systems, infrastructure, and team.



Strategy & Plan

- Expanding analysis and automation for data anomalies, internal control testing, risk monitoring, and audit execution.

Enterprise Risk Plan

Citizens' ERM Framework provides a comprehensive and integrated approach to proactively identifying, assessing, managing, and mitigating risks that could impede the achievement of strategic and organizational objectives. The enterprise risk (ER) function is a strategic enabler of organizational resilience, embedding a proactive, risk-informed approach across the organization. The ER team provides visibility into key risk exposures and supports business units in anticipating, understanding, and responding to a dynamic risk landscape.

For 2026, the enterprise risk program will focus on four key priorities: enhancing risk visibility, strengthening alignment with enterprise tolerance, and supporting risk-informed decision-making.



- **Agile Risk Assessments:** Facilitate timely and adaptive assessments of strategic, operational, project, and emerging risks to deliver forward-looking insights that enhance organizational resilience and responsiveness to evolving threats and opportunities.
- **Strategic Collaboration:** Strengthen partnership with business areas, including IT Security and Risk, Business Systems Resiliency, and Strategy & Planning, to integrate tools and resources, enabling more comprehensive and efficient risk coverage.
- **Data-Driven Risk Intelligence:** Leverage innovative technologies, including analytics, to detect emerging risk trends and inform decision-making, providing a more comprehensive assessment of potential risks.
- **Alignment with Leading Practices:** Advance program maturity by introducing formal risk appetite statements and conducting quality reviews to ensure alignment with the framework and industry standards.

These priorities reflect a commitment to advancing risk management maturity and ensuring the organization remains adaptive and well-prepared in a dynamic risk environment.

Reporting, Follow-up, and Performance Metrics

ER provides regular status updates to senior management, quarterly updates to the Risk Steering Committee, and periodic updates to the Audit Committee, including plan progress, top and emerging risk insights.



KPI	Target	Definition	Data Source	Frequency	Owner
Risk Assessment Completion	≥95% of the plan	% of planned risk assessments completed	Risk Registry	Monthly	ER
Risk Appetite Statement Adoption	≥75%	% of business units adopting formal risk appetite statements	Risk Registry	Quarterly	ER
Acceptable Risk Exposure	≥95% key risks	% of top risks within approved appetite/tolerance thresholds	Risk Registry, Dashboards	Quarterly	ER
Mitigation Coverage	≥95%	% of risks out of thresholds with active mitigation plans	Risk Registry; Dashboards	Quarterly	ER
KRI Development	≥50%	% of KRIs implemented and monitored for high-impact risks.	KRI Dashboard	Quarterly	ER

Internal Control Plan

Dedicated to promoting a robust internal control environment, the internal control (IC) team partners with business units to implement and sustain effective internal control practices that minimize risk exposure, safeguard assets, and ensure accuracy and integrity in reporting. The Internal Control Framework (ICF) supports the design and monitoring of controls that promote operational consistency, accountability, and compliance.

In 2026, the IC team will focus on advancing control maturity, enhancing transparency, and driving innovation in monitoring and testing practices. These efforts are designed to reinforce the organization's control environment and expand coverage of higher-risk areas and compliance requirements. The four priorities are outlined below:



- **Control Assessments:** Control self-assessments are performed for Citizens' top primary controls that may significantly impact achieving objectives and mitigating higher-rated risks. The assessments enhance operational resilience by delivering actionable insights that help business



Strategy & Plan

leaders strengthen control effectiveness, reduce risk exposure, and drive sustainable performance improvements.

- **Analytics-Enabled Monitoring:** Implement analytics-enabled monitoring solutions that detect anomalies, support proactive risk mitigation, and reduce manual control testing to provide broader and efficient control coverage.
- **Alignment with Leading Practices:** Provide internal control consultations for new and higher-risk processes. Conduct quality reviews of control self-assessments to ensure alignment with leading practices and framework standards.
- **Maximize Efficiency through Strategic Connections:** Strengthen strategic partnerships with business areas to align efforts, share tools, and optimize resources across control and compliance activities. Leverage the control self-assessment process to obtain evidence that demonstrates compliance with higher-risk laws, rules, and regulations (LRRs).

Reporting, Follow-up, and Performance Metrics

IC provides regular status updates to senior management and periodic updates to the Audit Committee, including progress on the plan, significant observations, and insights into controls. To measure the effectiveness and maturity of the ICF, the following KPIs track progress across control assessments, remediation, documentation standards, and compliance validation.

KPI	Target	Definition	Data Source	Frequency	Owner
CSA Completion Rate	≥95% critical processes	% critical processes completing CSA	CSA tracker	Quarterly	IC
Control Remediation	≥90%	% controls deficiencies successfully remediated.	ICF testing	Quarterly	IC
Documentation Conformance	≥95%	% of CSAs meeting standards	QA sampling	Quarterly	IC
Regulatory Compliance Coverage	≥95% high-risk LRRs	% of high-risk LRRs with CSAs that include evidence of compliance	CSA tracker	Quarterly	IC



Appendix 1 – Dual Role Safeguards

OIA operates a three-line model tailored for Citizens: management is the First Line; enterprise risk (ER) and internal control (IC) provide the Second Line; Internal Audit is the independent Third Line.

Roles and Boundaries

Function	Purpose	Key Responsibilities	Prohibited Activities (to protect IA independence)
Internal Audit (Third Line)	Independent assurance	Risk-based plan; opinions; reporting; follow-up	No operational ownership of ERM/ICF processes, no design/approval of business controls, no management decisions
ER (Second Line)	Risk facilitation & oversight	Risk framework; appetite; KRI library; top-risk reporting; deep-dives; scenario analysis	No executional ownership of First-Line controls; no Internal Audit assurance issuance
IC (Second Line)	Control policy & quality	Internal control framework (ICF) & taxonomy; control self-assessment CSA/testing standards; documentation; deficiency tracking	No ownership of First-Line processes; no Internal Audit assurance issuance

Dual-Hat Structure & Safeguards

The Chief of Internal Audit (CAE) has administrative oversight over ER and IC. The following safeguards maintain the independence and objectivity of the Internal Audit activity:

- Structural: Distinct leaders for ER and IC with clearly documented mandates, separate budgets, and performance objectives.
- Governance: Internal Audit reports functionally to the Audit Committee; ER/IC risk/control matters are discussed with Management committees; Audit Committee retains oversight of all three functions' plans/KPIs.
- Assurance over ER/IC: When Internal Audit engagements cover ER or IC activities, the CAE delegates engagement oversight to co-sourced external specialists to perform testing; any impairment is disclosed.
- Conflict Management: Annual and ad-hoc independence declarations; conflicts register; rotation of IA staff away from areas where they had performed second-line responsibilities.
- Policy & Methodology: Documented prohibitions on IA assuming management responsibilities; IA methodology requires explicit independence assessment at planning; quality reviews validate objectivity.

Reporting Lines

Area	Administrative Reporting	Functional Reporting	Primary Committee
Internal Audit	CEO	Audit Committee	Audit Committee



Appendix 1 – Dual Role Safeguards

ER	CAE (administrative)	Audit Committee, Risk Steering Committee visibility	Audit Committee
IC	CAE (administrative)	Audit Committee visibility	Audit Committee

Mandates and Charters (IA, ER, IC)

Internal Audit (Third Line)

- Provide independent, objective assurance and advisory services that add value and improve operations.
- Maintain a risk-based plan; communicate results and overall opinions; verify remediation; coordinate with other assurance providers.
- Conform to the IIA Global Internal Audit Standards (GIAS) and the Code of Ethics; maintain a Quality Assurance Improvement Program (QAIP); undergo an External Quality Assurance review (EQA) in 2026.

Enterprise Risk (Second Line)

- Maintain risk framework, the ERM register, appetite statements/tolerances, and the KRI library; facilitate risk identification and assessment.
- Coach First Line on Risk methodology, deliver top-risk reporting; run scenario analysis and deep-dive reviews; coordinate risk workshops.
- Support plan rebalancing with timely risk signals; no operational control ownership.

Internal Control (Second Line)

- Define control standards and taxonomy; own control self-assessment (CSA) and testing methodology; and set documentation, evidence, and records retention requirements.
- Coach First Line on control design; maintain the Corporate Controls Register; track and report control deficiencies.
- Run thematic quality assessments (QA) on self-assessments; coordinate with Internal Audit on reliance and avoid duplicative efforts.



Appendix 2 - Overview of Potential Audit Engagements

The following table lists audit engagements selected for 2026 and provides a detailed overview of Internal Audit's view of risk and the engagement objective.

Title	Audit Engagement Justification and Objective
Automated Underwriting	<p>Risk Rationale: Automated underwriting systems are essential for efficient and consistent risk evaluation, pricing, and application processing in property and casualty insurance. While they enhance speed and accuracy, reliance on these systems introduces risks such as system errors, outdated rules, poor data quality, and weak controls over updates or overrides. These issues could result in misclassification, mispricing, higher loss ratios, or regulatory non-compliance.</p> <p>Objective: Confirm the system makes accurate, policy-compliant decisions, with sound rule governance, quality data, and controlled overrides that protect pricing and compliance.</p>
CAT Bond	<p>Risk Rationale: Catastrophe bonds apply trigger formulas tied to modeled losses, industry indices, or location-specific metrics. Weak validation of models and terms, unclear monitoring of triggers, or valuation errors can lead to missed recoveries or unexpected investor obligations. This affects liquidity during peak CAT seasons, financial reporting, and market credibility.</p> <p>Objective: Verify that the bond structure, modeling, valuation, and disclosures are governed well, monitored continuously, and aligned to risk appetite and regulation.</p>
CAT Preparedness	<p>Risk Rationale: Hurricanes create concurrent stress on people, vendors, systems, and cash flow. If surge staffing, call center capacity, claims intake, field adjusting, and technology recovery are not exercised and coordinated, customer wait times increase, and loss leakage grows. Vendor bottlenecks and data breakdowns also raise fraud and compliance risk during emergencies.</p> <p>Objective: Assess governance, surge capacity, vendor readiness, technology recovery, and lessons learned practices, to confirm Citizens can respond fast and compliantly during CAT events.</p>
Claims Check Processing	<p>Risk Rationale: The use of large volumes and multiple payment channels increases the likelihood of duplicate, erroneous, or fraudulent disbursements. Control failures in approval workflows, bank file security, positive pay, and daily reconciliations can lead to unrecoverable losses and reporting issues. Weak access control or segregation also magnifies insider risk.</p> <p>Objective: Test that payments are authorized, accurate, timely, and well-controlled, with strong segregation of duties, monitoring, and exception handling.</p>
Claims Vendor Management	<p>Risk Rationale: Adjusting firms, IME providers, mitigation contractors, and legal vendors directly affects loss cost and cycle time. Inadequate onboarding, weak due diligence, unclear SLAs, or poor invoice controls drive leakage, service complaints, and security exposures. Concentration risk and gaps in backup vendors can stall the CAT response.</p>



Appendix 2 - Overview of Potential Audit Engagements

Title	Audit Engagement Justification and Objective
	Objective: The objective of the claims vendor management audit is to evaluate the effectiveness of the organization's processes for monitoring and managing third-party vendors involved in the claim lifecycle, including SLAs, performance monitoring, security, and billing controls, to ensure reliable service and controlled claim costs.
Commissions	Risk Rationale: Commission rules vary by product, channel, and timing. Errors in rate tables, overrides without approval, or interface failures between policy and commission systems cause over- or underpayments and disputes. This creates financial misstatements and reputational damage with agents and regulators. Objective: Assess strategy, calculations, approvals, and system controls to confirm commissions are accurate, timely, and consistent with Board-approved terms.
Division of Administrative Hearings (DOAH)	Risk Rationale: Disputes moved to DOAH require strict timelines, complete documentation, and consistent legal positions. Backlogs, case management gaps, or evidence defects can lead to increased adverse rulings and drive additional litigation costs. Patterns of errors can attract external scrutiny. Objective: Review governance, timeliness, documentation, and outcome monitoring to support fair, consistent, and compliant dispute resolution.
Enterprise Data Governance and Data Loss Prevention	Risk Rationale: Inadequate data governance and weak DLP controls can lead to data breaches, regulatory penalties, loss of customer trust, inadequate monitoring and alerting, and poor data quality and integrity. Objective: Assess classification, ownership, quality, and DLP controls to ensure sensitive data is accurate, protected, and used appropriately.
E Payments	Risk Rationale: Electronic receipts and disbursements reduce cycle time but expand the attack surface. Fraud attempts exploit compromised credentials, vendor banking changes, and gateway outages. Without strong authentication, change controls, settlement reconciliations, and uptime monitoring, we risk financial loss and customer impact. Objective: Advisory support to help ensure adequate segregation of duties is designed into the process and well-controlled for the outgoing payment processes, and that strong monitoring and reconciliations are in place.
Ethics	Risk Rational: A credible ethics program prevents harm, reduces regulatory risk, and improves culture. If training is sporadic, hotlines are not trusted, or investigations lag, issues surface late, and patterns remain hidden. Poor trend reporting limits leadership action and drives repeat findings. Objective: Evaluate training, reporting, and response processes to confirm expectations are clear, issues surface early, and actions are consistent.
EZLynx (Clearinghouse)	Risk Rationale: The transition from Clearinghouse to EZLynx must maintain statutory eligibility rules and data quality. Mapping errors, interface defects, or unclear exception handling can misdirect risks and lead to non-compliance. Agent adoption and support quality also affect service levels.



Appendix 2 - Overview of Potential Audit Engagements

Title	Audit Engagement Justification and Objective
	Objective: Confirm the new process works as intended, data is reliable, and statutory requirements are met.
Fraud Analytics and Continuous Monitoring (Recurring)	<p>Risk Rationale: Fraud evolves with new channels and vendors. Manual controls alone fail to identify organized patterns in claims, payments, and procurement. Weak model governance, poor data, or limited coverage reduce detection and overwhelm investigators with false positives.</p> <p>Objective: Expand the design and coverage of monitoring and analytics to detect anomalies early and strengthen controls across the lifecycle.</p>
FRISS	<p>Risk Rationale: Friss is a fraud detection tool that leverages advanced analytics, external data, and internal operations data, introducing opportunities and risks for the organization. If tuned and governed well, the tool intends to reduce loss and cycle time. Incomplete data feeds, mis-calibrated thresholds, and inconsistent alert triage cause missed fraud and customer friction. A lack of outcome measurement can hide performance issues.</p> <p>Objective: Evaluate governance, data quality, model performance, and alert handling to ensure the tool prevents fraud without disrupting legitimate business.</p>
IT General Controls	<p>Risk Rationale: Critical systems support policy, claims, finance, and reporting. If access management, change control, and operations monitoring fail, we risk unauthorized activity, service outages, and data errors. These failures cascade into financial statements and regulatory filings.</p> <p>Objective: Test core ITGCs for critical systems to confirm that integrity, confidentiality, and availability are protected.</p>
Loss Reserve Development, IBNR	<p>Risk Rationale: The reserve setting relies on data quality, actuarial methods, and effective governance to ensure accuracy and reliability. Model errors, parameter bias, or weak change control can misstate liabilities and impair decision-making. External reviews expect clear documentation and challenge assumptions.</p> <p>Objective: Evaluate methods, governance, and controls for reserve setting, including IBNR, to confirm accuracy and oversight.</p>
Patching and Vulnerability Management of Critical Applications	<p>Risk Rationale: Attackers weaponize known vulnerabilities within days. Delayed patch cycles, incomplete asset inventories, or weak change validation leave exploitable gaps. Third-party components and SaaS apps add complexity that can be overlooked.</p> <p>Objective: Evaluate vulnerability discovery, patch prioritization, deployment, and verification to confirm timely risk reduction.</p>
Period End Financial Reporting	<p>Risk Rationale: Month- and quarter-end closings touch many systems and teams. Breakdowns in reconciliations, cutoff, or review controls drive misstatements and restatements. Staff turnover and manual workarounds raise error risk during peak load.</p> <p>Objective: Assess key closing steps, reconciliations, review controls, and ownership, to confirm accurate, timely, and compliant reporting.</p>



Appendix 2 - Overview of Potential Audit Engagements

Title	Audit Engagement Justification and Objective
Premium Refunds and Suspense Accounting	<p>Risk Rationale: Customer refunds and suspense movements are highly sensitive and subject to scrutiny. Weak payee validation, missing reason codes, or poor aging oversight can lead to mishandled funds and regulatory attention. High transaction volumes magnify even the most minor control gaps.</p> <p>Objective: Test accuracy, timeliness, and traceability of refunds and suspense activity, to ensure customer funds are safeguarded and reported correctly.</p>
Privacy Program	<p>Risk Rationale: The increased use of cloud services, data sharing, and AI raises privacy obligations. Unclear data inventories, weak consent and retention controls, or slow incident response heighten the likelihood of breaches and penalties. Prior gaps should show measurable remediation.</p> <p>Objective: Follow up on prior work and assess maturity against accepted frameworks, with a focus on governance, data handling, and response practices.</p>
Rate Implementation	<p>Risk Rationale: Implementing approved rates into production poses a high risk. Configuration errors or skipped testing can result in mispricing thousands of policies. Weak defect management and change control could lead to silent revenue leakage and regulatory exposure.</p> <p>Objective: Verify rates and rules are accurately configured, thoroughly tested, and governed with timely defect remediation and transparent reporting.</p>
Regulatory Support, Auditor General Operational Audit	<p>Risk Rationale: The Auditor General requires timely and accurate responses across various functions. Poor coordination, inconsistent evidence, or missed deadlines increase findings and audit hours, pulling focus from operations.</p> <p>Objective: Coordinate requests, meetings, and deliverables across the enterprise to ensure accurate, timely responses.</p>
Regulatory Support, OIR Market Conduct Exam	<p>Risk Rationale: Market Conduct exams review underwriting, claims, complaints, and reporting. Disorganized evidence collection, control gaps, or late corrections can drive repeat findings and corrective orders.</p> <p>Objective: Coordinate requests and evidence delivery to support a timely, accurate, and complete examination.</p>
Secondary Employment	<p>Risk Rationale: Outside work can create conflicts of interest, lead to the misuse of company information, and result in time theft. Without clear disclosure, approval, and monitoring, leaders cannot manage reputational and legal risk.</p> <p>Objective: Evaluate disclosure, approval, and monitoring controls to manage conflicts and protect company interests.</p>
Technology Governance, Follow-up	<p>Risk Rationale: Unresolved audit and risk recommendations signal control weaknesses and program drift. Weak tracking, unclear ownership, or deadline extensions without rationale leave exposures open and invite repeat issues.</p> <p>Objective: Assess management's progress on prior recommendations and map governance practices to relevant frameworks.</p>



Appendix 2 - Overview of Potential Audit Engagements

The following table lists potential additional audit engagements that could be selected within this multi-year audit plan.

Enterprise-Wide User Access Review	<p>Risk Rationale: New hires, transfers, and terminations create constant access churn. If reviews are infrequent, attestations are weak, or role designs are overly permissive, excess access accumulates, increasing insider and privacy risks.</p> <p>Objective: Confirm access is role-appropriate, reviewed regularly, and promptly adjusted with role or employment changes.</p>
AI Governance and Model Inventory	<p>Risk Rationale: The use of AI and ML is expanding in claims, underwriting, and service. Without a clear inventory, risk classification, and testing standards, models can embed bias, drift silently, and breach emerging regulations. Vendor models also need governance.</p> <p>Objective: Review governance, inventory completeness, risk assessment, and monitoring for AI and ML models.</p>
IT Asset Management	<p>Risk Rationale: Hardware, software, and data-bearing devices must be tracked from purchase to disposal. Gaps in inventory, tagging, or sanitization lead to loss, wasted spending, and data exposure, especially during refresh cycles and remote work.</p> <p>Objective: Evaluate lifecycle controls, from acquisition to disposal, and confirm records are accurate and assets are safeguarded.</p>
Attack and Penetration Testing	<p>Risk Rationale: In today's threat landscape, organizations face constant exposure to cyberattacks from external adversaries and insider threats. Without a robust and well-governed penetration testing program, critical weaknesses may remain undetected, leaving systems vulnerable to exploitation.</p> <p>Objective: Assess scope, frequency, remediation, and reporting of testing, to drive timely risk reduction.</p>
Background Checks	<p>Risk Rationale: Incomplete or inconsistent screenings raise legal exposure and insider threat risk, particularly for sensitive roles. Vendor quality, turnaround time, and exception handling all contribute to effectiveness.</p> <p>Objective: Provide control advice and support to confirm that screenings are complete, compliant, and well-documented.</p>
Claims Legal Billing	<p>Risk Rationale: Defense counsel billing is high-dollar and complex. Undervalued legal matter budgets, vague guidelines, and limited sampling lead to overbilling and inconsistent cost control, resulting in tension with counsel and regulators.</p> <p>Objective: Evaluate billing review consistency, oversight, and results, to support fair, controlled litigation spend.</p>
Claims Litigation	<p>Risk Rationale: Fragmented matter management, uneven strategy, or delayed decisions escalate costs and increase adverse outcomes. Limited management information on cycle time and outcomes hides trends that could inform settlements and defense posture.</p> <p>Objective: Assess strategy, counsel oversight, matter tracking, and outcomes against leading practice, to strengthen control and consistency.</p>



Appendix 2 - Overview of Potential Audit Engagements

Compliance Program	<p>Risk Rationale: Regulatory change is frequent and cross-cutting. If ownership and certifications are unclear, or if monitoring is reactive, compliance gaps persist and create findings in external reviews.</p> <p>Objective: Assess governance, responsibilities, annual reviews, and reporting, to confirm compliance risks are identified and managed.</p>
Contract Management Review Process	<p>Risk Rationale: Contracts encode service, cost, data, and risk terms. Missing clauses, expired agreements, or poor change control create legal and financial risks. Fragmented repositories and manual processes lead to increased error rates.</p> <p>Objective: Assure contracting practices and controls, focusing on compliance, performance, and renewal discipline.</p>
Employee Retirement Plan	<p>Risk Rationale: Benefit plans are regulated and sensitive. Errors in eligibility, contributions, or fees, as well as weak vendor oversight, harm employees and invite penalties and litigation.</p> <p>Objective: Assess fiduciary governance, transactions, reporting, and communications, to confirm compliance and asset protection.</p>
IGA Program Development	<p>Risk Rationale: Identity governance is foundational to access control. Design gaps in connectors, role models, or certification campaigns can lead to toxic combinations and orphaned accounts. Implementation must strike a balance between security and usability to be widely adopted.</p> <p>Objective: Evaluate SailPoint design, build, and governance to confirm lifecycle controls and compliance obligations are met.</p>
Insurance Operations Legal Counsel	<p>Risk Rationale: Timely and consistent legal support reduces cycle time and adverse outcomes. If intake is unclear, workloads are unmanaged, or guidance is uneven, operations slow and legal exposures grow, especially in high-volume periods.</p> <p>Objective: Assess workload management, collaboration with claims, documentation, and oversight of legal risks.</p>
IT Budget and Spend	<p>Risk Rationale: Technology spend is material and dynamic. Weak planning and tracking lead to overruns, stranded investments, and misaligned priorities. Vendor changes and cloud consumption models introduce volatility if not closely monitored.</p> <p>Objective: Evaluate planning, approvals, tracking, and reporting to confirm that spending aligns with strategy and policy.</p>
Office of Foreign Assets Control, OFAC	<p>Risk Rationale: Sanctions screening must be complete and timely to avoid severe penalties. If watchlists are stale, matching logic is weak, or alerts are not functioning, and prohibited parties may be onboarded or paid, creating legal and reputational risks.</p>
Office of Foreign Assets Control, OFAC	<p>Risk Rationale: Sanctions screening must be complete and timely to avoid severe penalties. If watchlists are stale, matching logic is weak, or alerts are not functioning, and prohibited parties may be onboarded or paid, creating legal and reputational risks.</p> <p>Objective: Assess policies, systems, and case handling for sanctions screening to confirm timely, accurate, and well-governed processes.</p>



Appendix 2 - Overview of Potential Audit Engagements

Performance Violations and Late Submission Program	<p>Risk Rationale: The performance violations & late submission program was updated with changes to the disciplinary process, and a new discipline program must be applied consistently to be credible. Uneven documentation, unclear definitions, or delayed decisions can create fairness concerns and expose organizations to legal liability. Poor reporting can hide trends and impede corrective action.</p> <p>Objectives: Determine whether violations are handled consistently, thoroughly documented, and resolved promptly, with apparent oversight and reporting.</p>
Project Portfolio Management	<p>Risk Rationale: Without disciplined selection and capacity management, projects outstrip resources and delay value. Benefits are rarely measured when governance is weak, making it hard to stop or redirect struggling work.</p> <p>Objective: Evaluate selection, prioritization, capacity, and benefits tracking to align projects with strategy and risk tolerance.</p>
Purchasing Compliance	<p>Risk Rationale: After-the-fact reviews often reveal policy exceptions, missing competitive bids, and split purchases. Weak controls here lead to cost leakage, vendor favoritism perceptions, and unfavorable audit findings.</p> <p>Objective: Review post-purchase compliance with policy, contract, and law, and recommend control improvements.</p>
Rate Indication	<p>Risk Rationale: Rate indication combines actuarial methods, experience data, and assumptions. Data quality issues, undocumented judgment, or inconsistent governance can misstate indicated rates and trigger regulatory challenges.</p> <p>Objective: Assess governance and transparency of assumptions, data, and methods that drive indicated rates.</p>
Records Management and Requests	<p>Risk Rationale: Public records obligations require strong retention, retrieval, and redaction practices. Disorganized repositories, unclear ownership, or manual redaction increase the chance of late or incorrect responses and privacy breaches.</p> <p>Objective: Evaluate retention, retrieval, request handling, and safeguards to ensure compliance and efficient operations.</p>
Risk Transfer Strategy and Execution	<p>Risk Rationale: Risk transfer choices affect earnings stability and capital. If treaties, limits, and attachment points are misaligned with appetite, or if placements and contracts are not executed cleanly, we face higher net losses and recovery disputes.</p> <p>Objective: Review design, governance, and execution of reinsurance and other transfer tools, to confirm coverage meets appetite and standards.</p>
System Integrations	<p>Risk Rationale: Integrations connect policy, claims, finance, and analytics to facilitate seamless operations. Incomplete requirements, weak data mappings, and limited testing lead to service disruptions, corrupted data, and reporting errors. Vendor coordination and cutover control are critical.</p> <p>Objective: Assess planning, controls, and testing for integrations, to protect operations and data integrity.</p>



Appendix 2 - Overview of Potential Audit Engagements

Third Party Risk Management, SOC Process	<p>Risk Rationale: Service organizations host sensitive data and critical services. If SOC reports are not obtained, reviewed, and translated into actionable steps, gaps in vendor controls become a source of our exposure. Contractual rights and monitoring must match the risk tier.</p> <p>Objective: Validate the end-to-end SOC report process and broader TPRM controls to ensure risks are identified, assessed, and mitigated.</p>
Contingent Staffing	<p>Risk Rationale: Contingent staffing supports flexibility in the property and casualty insurance industry, but it also poses risks related to compliance, oversight, data security, and performance. Without proper controls, the company may face worker misclassification, inconsistent onboarding, regulatory issues, and reputational or operational harm.</p> <p>Objective: This audit will assess whether proper governance, contracting, and oversight controls are in place to effectively manage contingent labor. It will help ensure alignment with legal requirements, mitigate operational risks, and support overall workforce integrity.</p>
Employee Onboarding	<p>Risk Rationale: Late background checks, delayed access provisioning, and incomplete training slow productivity and increase security and compliance risk. If onboarding controls are inconsistent across departments, we see audit exceptions later in user access, privacy, and ethics testing.</p> <p>Objective: Confirm new hires receive timely training, access, and policy guidance aligned with legal and company requirements.</p>
Customer Experience and Advocacy	<p>Risk Rationale: Policyholder trust depends on consistent, timely service across quoting, billing, claims, and complaints. Fragmented processes, inconsistent scripts, and opaque handoffs lead to dissatisfaction, increased escalations, and potential regulatory scrutiny. Poor feedback loops miss patterns and slow fixes.</p> <p>Objective: Identify pain points across key journeys, confirm standards are applied consistently, and recommend practical fixes that lift satisfaction and loyalty.</p>



Appendix 3 – Audit Universe

Administrative Services

Agency & Market Services

- Agency Management
- Clearinghouse Operations
- Depopulation Operations
- FMAP

Communications & Strategic Services

- Corporate Communications
- Digital Communications
- Insurance Technical Communications

Consumer & Policy Services

- Citizens Insurance Services
- Consumer & Policy Services Quality
- Customer Care Center
- Customer Correspondence
- Policy Services
- Workforce Management

Facilities Management

Human Resources

- Compensation
- Employee Benefits
- HR Information Management
- Learning & Org. Development
- Payroll
- Talent Experience

Public Affairs & Strategy

Enterprise Business Agility

Legislative & Cabinet Affairs

Project Portfolio Management

Financial Services

Accounting

- Accounts Payable
- Claims Accounting & Disbursements
- Commissions Payments & Accounting
- Depop. Billing, Settlements & Accounting
- Unclaimed Property Accounting

Actuarial

- Loss Reserve Development IBNR
- Rate Development Actuarial

Corporate Analytics

Financial Services Compliance

- OFAC

Financial Planning & Analysis

- Budgeting
- Forecasting

Investments

- Cash Management & Treasury
- Investment Accounting
- Investments Mgmt. & Compliance
- Pre- & Post-Event Liquidity Bond Financing

Period End Financial Reporting

- Financial Close
- Financial Statements

Premiums

- Premium Accounting
- Premium Invoicing, Refunds & Suspense
- Premium Remittance Processing

Reinsurance

- Reinsurance Servicing & Accounting
- Risk Transfer Strategy & Execution

Vendor Management & Purchasing

- Purchasing
- Software Asset Management
- Vendor Management

Information Technology

App. Access & Security Controls

- Admin. Activity Logging & Monitoring
- Application Access
- User Access Review

Change/Configuration Management

- IT Change & Release Management

Computer Operations

- Batch Job Processing
- Job Scheduler Access

Cybersecurity

- Attack & Penetration Testing
- Backup & Recovery
- Data Governance
- Patching & Vulnerability Mgmt.

Program Development

- IT Application Delivery
- IT Application Development
- IT Application Quality Assurance

Infrastructure & Operations

- Incident & Problem Mgmt.
- Network Infrastructure Mgmt.
- Physical Access to Assets

Entity Level Controls

- Enterprise Business Solutions
- IT Asset Management
- IT Budget & Spend
- IT Governance

Insurance Operations

Claims

- Catastrophe Planning, Testing & Coordination
- Claims Legal Billing
- Claims Litigation
- Claims Operations
- Claims Quality

Claims

- Claims Vendor Management
- Special Investigative Unit

Underwriting

- Commercial Lines Underwriting
- Personal Lines Underwriting
- Underwriting Quality Improvement

Product Development

- Insurance Product Management
- Systems Product Management

Office of the General Counsel

Corporate Services

- Corporate Insurance
- Corporate Legal
- Records Management

Insurance Ops Legal Counsel

- Ethics
- Compliance
- Privacy

Information Security

- IT Security & Risk
- Information Security Ops & Monitoring
- Business Systems Resiliency