CITIZENS
PROPERTY INSURANCE CORPORATION

ENTERPRISE RISK MANAGEMENT FRAMEWORK

Table of Contents

Introduction & Approach

Citizens' Enterprise Risk Management (ERM) Framework provides the foundation for our enterprise risk program designed to support the organization in the achievement of strategic and operational objectives through identifying, assessing, and mitigating risks.

The framework is based on the Committee of Sponsoring Organizations of the Treadway Commission's (COSO) Framework. COSO emphasizes the value of embedding enterprise risk management in strategic planning and performance throughout the organization as risk impacts performance and strategy. The components of our framework are modeled after COSO and customized to fit the unique needs of our organization.

Citizens' ERM Framework:

- Reinforces expectations of roles and the provision of guidance, training, and a software solution responsibility for risk management
- Aligns strategic initiatives and business objectives to the risk management process
- Promotes structure, transparency, consistency, and uniformity of ERM across the organization
- Defines the types of risk perspectives, risk categories, and risk evaluation guidance that provide input into our comprehensive risk portfolio
- Empowers management to make risk-informed decisions
- Provides guidance to ensure that residual risk exposure is aligned with risk appetite
- Enables management across all levels of the organization to proactively self-identify, evaluate, record, and manage risks
- Describes our governance and oversight structure for enterprise risk processes

Standards & Policies

Citizens' mission and Code of Ethics establish the standards that guide our business conduct and support a culture of accountability, transparency, and trust. Citizens' Enterprise Risk Management Framework is integrated throughout our corporate policies. The following policies specifically reference or directly align with the ERM Framework:

- Internal Audit
- Information Security & Privacy
- Vendor Management
- Enterprise Resiliency
- Physical Safety & Security
- End User Computing

Strategy & Objective Setting

Risk is the possibility that events will occur that can affect the achievement of strategy and business objectives. Risk management is integral to the strategic planning process, decision-making, and day-to-day operations.

Citizens' Strategic Plan outlines the strategic goals that support our core mission. Each goal is supported by strategic objectives that provide insight to track and measure progress towards achieving strategic goals. Objectives are set by the Executive Leadership Team in alignment with

Citizens' Strategic Plan and are cascaded throughout the organization. Enterprise Risk and Enterprise Strategy & Planning align Citizens' strategic risks to our strategic themes.

Roles & Responsibilities

The Enterprise Risk team within the Office of the Internal Auditor is responsible for the design and maintenance of the ERM framework. Citizens' management has the primary responsibility for identifying, mitigating, and monitoring the risks within their processes. The Chief of Internal Audit is appointed by the Board of Governors, reports to, and is under the general supervision of the Board and is not subject to supervision by any Citizens' employee. The Chief of Internal Audit reports to the Board through the Audit Committee. Apart from Internal Audit, the Chief of Internal Audit also has leadership responsibility for Enterprise Risk and the Internal Control functions.

Three Lines Model

The ERM Framework incorporates a widely accepted Three Lines Model approach to governance and risk. The model outlines the roles of various leaders within the organization to describe risk management and control responsibilities in three separate lines.

- **First Line: Business/Management**

  As Risk Owners, Citizens' managers bear primary responsibility for identifying, controlling, and monitoring the risks within their processes and for maintaining appropriate internal controls. Risk Champions may be designated as liaisons to Enterprise Risk for process area(s) or a division. The Risk Champion's responsibilities include coordinating with business area leaders and subject matter experts on the identification, categorization, assessment, and mitigation of operational risks; updating the enterprise risk registry; and validating any reporting of supporting metrics and measures.

- **Second Line: Enterprise Risk Management & Internal Control**

  Enterprise Risk is responsible for coordinating, developing, and monitoring Citizens' risk management framework and processes and supports the business with the identification, assessment, and mitigation of current or emerging risks.

  The Internal Control team is responsible for coordinating, developing, and monitoring Citizens' Internal Control Framework and processes and supports the business with the effective management of Citizens' primary operating controls.

- **Third Line: Internal Audit**

  The Internal Audit team is responsible for developing a comprehensive risk-based internal audit program that provides independent assurance that Citizens' internal control infrastructure is well designed and operating effectively.

Collaboration

Enterprise Risk is focused on creating and maintaining a collaborative and engaging risk identification and assessment environment across the organization. Enterprise Risk frequently partners with IT Security and Risk, Ethics & Compliance, Enterprise Resiliency, and the Strategic Evaluation Group to conduct cross-functional risk assessments leveraging the ERM Framework. Results provide management with valuable insights that contribute to risk-informed decision-

making. Recurring touchpoint meetings are held to promote transparency, leverage resources, prevent duplication of efforts and ensure that higher rated risks are appropriately mitigated.

For IT risks, Enterprise Risk and IT Security and Risk align Citizens' Enterprise Risk Framework with the Security and Risk Framework that includes leading practices from Control Objectives for Information and Related Technologies (COBIT), National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO) and Critical Security Controls (CSC 18) Frameworks.

Risk Perspectives

Enterprise Risk facilitates, enables, and partners with business areas to deliver a forward-looking and insightful risk perspective that enhances the decision-making and strategic performance of Citizens. Our risk profile reflects a comprehensive view of risk from various perspectives.

Strategic	Annually, Enterprise Risk facilitates a strategic risk assessment with the Executive Leadership Team (ELT). Strategic risks are assessed by estimating the potential impact or severity level the risk may have on Citizens if the event occurs and by considering the probability of occurrence.
Operational	Enterprise Risk facilitates and enables Risk Champions and management to identify and assess operational risks for up to 81 business processes across Citizens from the OIA process universe.
Project	Pre- and post-implementation project risk assessments are performed to assist management with decision-making and to ensure mitigating activities are designed and implemented for higher-rated project risks.
Emerging	Scenario risk assessments are conducted to evaluate emerging risk scenarios that may impact Citizens.

Risk Assessment Process

Our risk assessment process begins with a review of the applicable strategic and business objectives for the process, project, or scenario to be evaluated. Risks that may impact Citizens' ability to achieve these objectives are identified and assessed. Mitigating activities, or controls, which are in place are reviewed and considered to determine the remaining, or residual, level of risks. In some instances, the level of risk may result in revisions to strategy or objectives.

The risk assessment process consists of seven steps:

1. Identify the objectives applicable to the type of risk assessment (i.e., business, project, or strategic initiatives).
2. Identify risks that may impact the ability to achieve the objectives.
3. Assess the impact and likelihood of the risk without controls (inherent risk).

4. Identify and record the mitigating activities/controls in place to reduce the risk.
5. Assess the likelihood of the risk considering mitigating activities (residual risk).
6. Determine and execute the appropriate risk response.
7. Evaluate and monitor performance to determine whether the implemented risk management options achieved the stated goals and objectives.

Risk Evaluation Criteria

Risk rating guidance promotes consistency in assessing risks across the organization. Risks are assessed by estimating the potential impact or severity level the risk event may have on Citizens if the event occurs and by considering the probability of occurrence. Specific guidance is located in Appendices A-C.

- **Risk Impact Rating:** The impact of each risk is rated as high, medium, or low based on guidelines for seven risk categories: strategic, financial, operational, systems/technology, compliance, reputational, and fraud. While a risk event may impact multiple categories, the one most severely impacted by the occurrence of the risk event is selected.
- **Probability Rating:** The probability or likelihood of the occurrence at the indicated impact level is assessed as likely, possible, or unlikely. Guidelines to assess the probability rating include the consideration of the percentage of failures that may occur and the complexity of the process**.**
- **Overall Risk Rating:** The severity of consequences (impact) is multiplied by the probability of occurrence (likelihood) to determine the overall risk rating: severe, high, medium, or low.

Risk Response

Management responds to risks by making decisions about the best alternative(s) and then prepares and executes the selected response strategy. The response to risks is primarily guided by the risk rating and considerations regarding severity and prioritization as well as the business context and associated business objectives. The internal or external environment may generate risks that cannot be controlled or constrain the way we respond to risk. Risk responses also include management's view of the risk, which may be perceived as opportunities, uncertainties, or hazards.

Risk Response	
Accept	No action is taken to change the severity or probability of the risk. The response is appropriate when the risk to strategy and business objectives is already within Citizens' risk tolerance or risk appetite.
Mitigate	Management takes action to reduce the severity or probability of the risk. Mitigating activities may be actions that are currently in place and/or future

	activities that may be in development that reduce the risk to an amount of severity that is within the organization's residual risk tolerance or appetite.
Transfer	Management takes action to reduce the severity of the risk by transferring or otherwise sharing a portion of the loss or liability to third parties to lower the risk severity in alignment with residual risk tolerance or appetite. Examples of risk transfer are outsourcing, reinsurance, or pre-event bonds.
Pursue	Action is taken that accepts increased risk to achieve improved performance. This may involve more aggressive strategies, expansion of operations or developing new products or services. When choosing to pursue risk, management understands that the nature and extent of the action required to achieve desired results will not exceed Citizens' risk tolerance or appetite.
Avoid	Action is taken to eliminate the risk which may consist of ceasing product offering. Choosing avoidance suggests that Citizens was not able to identify a response that would reduce the risk to an acceptable level of severity or probability.
Monitor	Management is actively monitoring the risk and will take action at the appropriate time. Other risk responses are not applicable in this situation. Examples include emerging risks that management is preparing to mitigate but cannot execute mitigation plans until the scenario materializes.

- Risk tolerance refers to the level of risk Citizens is willing to accept, in any area, without taking further action to mitigate risk impact.
- Risk appetite is the level of risk that Citizens is willing to accept while pursuing its objectives, and before any action is determined to be necessary in order to reduce the risk.

Risk assessment results that exceed acceptable levels will be further reviewed to determine if additional mitigating activities can be designed and implemented timely or if escalation is warranted. When the implementation of mitigating activities or a suitable alternative is no longer feasible or reasonable for significant risks because of organizational changes, costs, or other considerations, risk acceptance will be presented to the Risk Steering Committee for consideration.

Monitoring

Risk monitoring ensures that our risk portfolio continuously reflects current risks and allows proactive adjustments to risk mitigation strategies as needed. Risk assessments and mitigation plans are periodically updated throughout the year as changes occur. Enterprise Risk, Risk Owners, and Risk Champions proactively monitor Citizens' risk portfolio to provide assurance that risks are being managed as expected; assess whether the risk response plans remain relevant; ensure the risk profile anticipates and reflects any changes in circumstances and any new exposures and monitor inherent and residual risk profiles against the target risk profiles.

Reporting

Citizens operate according to statutory requirements established by the Florida Legislature and is governed by a Board of Governors. The Board of Governors and the Board Committees receive regular updates on top risks and mitigation efforts from Citizens' executive leadership and the Chief of Internal Audit. The status of the Enterprise Risk assessments and aggregate results by risk rating and other details as appropriate are reported quarterly to the Risk Steering Committee, Audit Committee, and Board of Governors.

Enterprise Risk enables management across all areas of the organization to self-identify, evaluate, record, and manage risks through the provision of guidance, training, and a software solution to establish and maintain a centralized risk registry that provides a holistic view of risks and enables reporting. Enterprise Risk, Risk Owners, and Risk Champions continuously update the risk registry as risks and mitigating activities change throughout the year. Management and Risk Champions have access to reporting capabilities within the risk module of the software solution.

Governance

The Risk Steering Committee is comprised of executive management that guides and monitors risk management processes deployed thereby ensuring adequate oversight in managing Citizens' exposure to significant risks. This committee's responsibilities are assigned by, and its authority is derived from, the President/CEO and the Executive Leadership Team. The Risk Steering Committee:

- Provides risk management leadership for Citizens through the alignment of operational risk mitigation activities with enterprise strategic objectives and processes
- Prioritizes Citizens' risk exposures and thresholds and resolves resource allocation issues based on risk prioritization
- Ensures optimal risk management by reviewing key risk indicators and other measures to monitor mitigation progress
- Ensures open communication between Enterprise Risk and the other functional units of Citizens to promote collaborative risk management

APPENDIX A: RISK IMPACT RATING GUIDANCE

Criteria for Risk Impact Rating – Using the following guidelines, indicate the potential severity of the risk event to Citizens, if it occurs. While a risk event may impact multiple Risk Categories, select the one most severely impacted by the occurrence of the risk event.

Impact Categories	(1) Low	(2) Medium	(3) High
Strategic Impacts to Citizens' ability to achieve our strategic objectives and key strategic initiatives, ability to adapt to changes in the business environment, etc.	• Little or no impact on the achievement of corporate mission, vision and/or key strategic objective(s). • Requires little intervention.	• Moderate impact on the achievement of corporate mission, vision and/or key strategic objectives. • Can be rectified with moderate change in processes / systems.	• Prevents the achievement of corporate mission, vision and/or key strategic objectives. • Major changes in processes/systems required with significant reengineering and significant changes to organizational structure.
Financial Improper reconciliation of general ledger accounts, inaccurate financial reporting, unfavorable contract terms, and overpayment for products and services, loss of capital, etc.	• Financial impact that may reduce cash flow by less than USD 5 million.	• Material financial impact that may reduce cash flow by more than USD 5 million but less than USD 20 million.	• Significant material financial impact that may reduce cash flow by more than USD 20 million.
Operational Risks that impact daily business activities such as inadequate information systems, physical security, quality, cycle times, training, resources, management oversight, reporting, segregation of duties, unforeseen catastrophes, business continuity, etc. will result in unexpected losses.	• Mature processes and strong internal control environment. • Limited impact on the achievement of key operational objective(s).	• Processes under development, known control deficiencies may result in a disruption to normal operation or monetary loss. • Moderate impact on the achievement of key operational objective(s).	• High percentage of transactions subject to complex and changing policies, procedures, and/or regulations; leading to ineffective or inefficient processes; high probability of monetary loss. • May prevent the achievement of key operational objective(s).
Systems/Technology Technology or system delays or failures, unauthorized access, data and systems protection, cybersecurity, cloud security and privacy, etc.	• Temporary (less than 1 hour) loss of IT / business support system. • No loss of data, no data recovery required. • Key functions or locations unavailable < 24 hours. • 1% - 5% of policyholders impacted.	• Loss of key IT / business support systems for 1-5 days throughout the company. • Some loss of important data, data recovery required. • Key functions or locations unavailable for 1-5 days. • 5% - 10% of policyholders impacted.	• Loss of key IT / business support systems for >5 days throughout the company. • Loss of vital data. • Key functions or locations unavailable >5 days. • >25% of policyholders impacted

APPENDIX A: RISK IMPACT RATING GUIDANCE (CONTINUED)

Criteria for Risk Impact Rating – Using the following guidelines, indicate the potential severity of the risk event to Citizens, if it occurs. While a risk event may impact multiple Risk Categories, select the one most severely impacted by the occurrence of the risk event.

Impact Categories	(1) Low	(2) Medium	(3) High
Compliance Non-conformance with laws, rules and regulations, prescribed practices or ethical standards which result in a disruption in business and financial loss.	• Incident non-reportable to regulator/authorities, or reportable with no penalty for non-compliance. • Minimal, if any, changes required to implement new or changing regulations.	• Material compliance deviation. Potential for OIR action or penalties. Some business unit specific regulations with potential for OIR or legislative criticism for non-compliance. • Moderate changes required to implement new or changing regulations.	• Criminal offense. Non-compliance leads to prosecution and fines, litigation including class actions and incarceration of leadership. • Extensive system changes and significant changes to business model required.
Reputational Negative publicity, whether valid or not may cause policyholder concern, costly litigation, and/or unfavorable revenue projections. Includes consideration for public and political sensitivity.	• Limited media coverage or public interest. • Adverse exposure potential is relatively immaterial. • Isolated or general morale problems among staff/management with little turnover.	• Extensive media coverage, noticeable to customers. • Adverse external publicity somewhat sensitive, but interest is narrowly focused to a limited audience. • Moderate reputational sensitivity. Widespread general morale problems among staff/management with high turnover.	• State CFO / Governor action. • Public / media outrage, major customer exposure (contact & interest), extreme public interest. Massive reduction in company's credibility with customers, suppliers, staff and public. • Senior / key experienced staff leave.
Fraud Intentional acts intended for financial or personal gain, violations of code of ethics, commitment of illegal or unauthorized acts, situations where multiple, conflicting interests could possibly corrupt motivation or decision-making which may result in civil or criminal charges, reputational damage or financial loss.	• Financial loss is less than $5,000 • Limited media coverage • Isolated employee dissatisfaction • Incident does not need to be reported to authorities or is reportable to authorities but no follow-up is needed.	• Financial loss between $5,000 - $250,000 • Extensive media coverage • Widespread employee morale problems. • Reported to authorities and immediate corrective action is needed.	• Financial loss to company in excess of $250,000 • Public / media outrage, major customer exposure (contact & interest), extreme public interest. Massive reduction in company's credibility with customers, suppliers, staff and public. • Widespread employee morale issues and turnover; multiple senior leaders leave • Incident must be reported to authorities and significant sanctions and financial penalties result.

APPENDIX B: PROBABILITY RATING GUIDANCE

Probability Rating - Indicate the likelihood of occurrence of the potential causes of the failure.		
Rating	**Probability**	**Criteria**
Likely (3)	**> 75%**	High likelihood of occurrence (repeated failures). Will probably occur in most circumstances; complex process with some controls; mostly manual processes; impacting factors outside control of organization.
Possible (2)	**25% - 75%**	Moderate likelihood of occurrence (occasional failures). Might occur at some time; previous audits/reports indicate non-compliance; complex process; mix of manual & automated processes; control conscious environment is in place; impacting factors outside control of organization.
Unlikely (1)	**< 25%**	Low likelihood of occurrence (relatively few failures). Could occur at some time; noncomplex process; mostly automated processes; control structure is in place.

APPENDIX C: OVERALL RISK RATING GUIDANCE

Probability & Impact Matrix			Unlikely	Possible	Likely
			1	2	3
IMPACT	Complex Issue with high Impact and likely Probability for which the solution is outside of the ability of Citizens management and intervention is required through Board of Governors or the Legislature.				Severe Risk
	High	3	Low Risk	Medium Risk	High Risk
	Medium	2	Low Risk	Medium Risk	Medium Risk
	Low	1	Low Risk	Low Risk	Low Risk

Note: The risk rating is an estimate of the potential impact or severity level the risk event may have to Citizens if the event occurs.

APPENDIX D: DEFINITIONS

Emerging Risk	Newly developing risk that should be monitored for potential impacts to Citizens.
Enterprise Risk	Function responsible to coordinate, facilitate, and enable executive and business function management in the use of Citizens' Enterprise Risk Framework and processes in the identification, assessment, and mitigation of risks.
Enterprise Risk Management	The culture, capabilities, and practices, integrated with strategy-setting and operational execution that Citizens relies on to manage risk in creating, preserving, and realizing value.
Impact	Potential severity of the risk event to Citizens if it occurs. Impacts are rated as high, medium or low.
Inherent Risk	Level of risk without implementation or consideration of mitigating activities.
OIA Process Universe	Consists of primary business processes of the organization and provides the population for operational risk assessments.
Probability	Likelihood of the occurrence at the indicated impact level. Probability is rated as likely, possible, or unlikely.
Residual Risk	Level of risk that remains after considering mitigating activities, or controls, in place to reduce the risk.
Risk	Possibility that events will occur that can affect the achievement of strategy and business objectives.
Risk Appetite	Degree of risk, on a broad-based level, that Citizens is willing to accept or take in pursuit of its objectives.
Risk Category	Provides a structured approach to support risk identification, assessment, analysis and reporting.
Risk Profile	Consists of a comprehensive view of risks from various perspectives: strategic, operational, project and emerging.
Risk Rating	The severity of the consequences (impact) multiplied by the probability of occurrence (likelihood) to determine the overall risk rating of severe, high, medium or low.
Risk Response	Strategies to respond to risk: accept, mitigate, transfer, pursue, avoid or monitor.
Risk Steering Committee	Provides guidance and oversight of Citizens' risk management processes.
Risk Tolerance	Level of risk that Citizens is willing to accept in various risk areas.

APPENDIX E: OIA PROCESS UNIVERSE

OIA Process Universe		
Assurance	• Enterprise Risk Management	• Internal Control Framework
Claims	• Catastrophe Planning, Testing & Coordination • Claims Governance • Claims Legal Billing	• Claims Litigation • Claims Operations • Claims Vendor Management • Special Investigative Unit
CLEA	• Corporate Communications • Insurance Technical Communications	• Legislative & Cabinet Affairs • Public External Relations & Outreach
Consumer & Policy Services	• CPS Processes	• Customer Correspondence
Enterprise Governance	• Corporate Governance	
Enterprise Operations	• Agency Management • Clearinghouse Operations • Commercial Lines Underwriting • Continuous Improvement • Depopulation Operations • Enterprise Performance Metrics • Enterprise Strategy & Planning Support • FMAP	• Personal Lines Underwriting • Product Dev – Applications, Forms & Rules • Product Dev & Rate Implementation • Project Portfolio Management • Purchasing • Software Asset Management • Quality Improvement Services • Vendor Management
Enterprise Operations (IT)	• IT Application Delivery • IT Application Development • IT Application Quality Assurance • IT Change & Release Management • IT Configuration Management • IT Enterprise Architecture • IT Enterprise Resilience (BCP & DRP) • IT Governance	• IT Information Management • IT Infrastructure • IT Knowledge Management • IT Operations • IT Problem Management • IT Security & Risk • IT Service Request Management • IT Systems Application Development
Financial Services	• Accounts Payable • Cash Management & Treasury • Claims Accounting & Disbursements • Commissions Payments & Accounting • Compliance FS • Corporate Analytics • Depop Billing, Settlements & Acc. • Escheatment Processing & Accounting • Financial Close • Financial Planning & Analysis • Financial Reporting	• Investments Accounting • Investments Management & Compliance • Loss Reserve Development IBNR • Pre- & Post-Event Liquidity Bond Financing • Premium Accounting • Premium Invoicing, Refunds & Suspense • Premium Remittance Processing • Rate Development Actuarial • Reinsurance Servicing & Accounting • Risk Transfer Strategy & Execution
Human Resources	• Compensation • Employee Benefits • Facilities Management • HR Systems & Reporting	• Learning & Development • Payroll • Talent Acquisition
Office of the General Counsel	• Claims Legal • Compliance • Corporate Insurance • Corporate Legal	• Ethics • Privacy • Records Management

APPENDIX F: ALIGNMENT TO COSO

The chart below provides a high-level overview of how COSO's five key framework components and supporting principles align to Citizens' ERM Framework.

	Governance & Culture	Strategy & Objective Setting	Performance	Review & Revision	Information, Communication & Reporting
COSO	- Exercises Board Risk Oversight - Establishes Operating Structures - Defines Desired Culture - Demonstrates Commitment to Core Values - Attracts, Develops, and Retains Capable Individuals	- Analyzes Business Context - Defines Risk Appetite - Evaluates Alternative Strategies - Formulates Business Objectives	- Identifies Risk - Assesses Severity of Risk - Prioritizes Risks - Implements Risk Responses - Develops Portfolio View	- Assesses Substantial Change - Reviews Risk & Performance - Pursues Improvements in Enterprise Risk Management	- Leverages Information & Technology - Communicates Risk Information - Reports on Risk, Culture, and Performance
CITIZENS ERM	- Introduction & Approach - Standards & Policies - Roles & Responsibilities - Governance	- Strategy & Objective Setting - Risk Response	- Risk Perspectives - Risk Assessment Process - Risk Evaluation Criteria - Risk Response	- Risk Response - Monitoring	- Collaboration - Reporting

APPENDIX G: ALIGNMENT OF STRATEGIC THEMES & RISKS

2022 Strategic Themes	2022 Strategic Risks
Strategic Theme 1: Identify and Implement Strategies to Reduce Citizens' Exposure	• Market Instability • Rate Differential • Acquisition of Reinsurance • Underwriting Data Integrity
Strategic Theme 2: Ensure Scalability, Flexibility and Resiliency in Our Operations to Optimally Serve Customers	• External Influences • CAT Response • Data Security & Privacy • Vendor Management/Oversight • Product Offerings • Leveraging Data & Technology
Strategic Theme 3: Identify and Implement Strategies to Reduce Litigation and Enhance Litigation Capabilities	• Claims Abuse • Litigation Management Solution • Attorney Fee Reform
Strategic Theme 4: Invest In and Leverage Citizens' Greatest Resource – Our Employees	• Strategic Workforce Planning • Compliance with Laws & Regulations • Ethics, Integrity & Conflicts of Interest