

Enterprise Risk Management Framework

DYNAMIC RISK GOVERNANCE



WITH AGILITY



COLLABORATION



INNOVATION



INTEGRATION

Table of Contents

Roles & Responsibilities	3
Risk Perspectives	3
Risk Assessment	4
Risk Response	4
Risk Acceptance	5
Dynamic Risk Governance	5
With Agility	6
Collaboration	6
Innovation	7
Integration	7
Data Governance Strategy	8
Risk Impact Rating Guidance	9
Probability Rating Guidance	11
Overall Risk Rating Guidance	12
Definitions	13



Citizens' Enterprise Risk Management (ERM) Framework is the cornerstone of our enterprise risk program and serves as a comprehensive tool to proactively identify, assess, manage, and mitigate risks that could impede the achievement of strategic and operational objectives. By leveraging a dynamic and agile approach, we ensure that the organization is well-positioned to respond to emerging challenges and maintain resilience in an evolving business landscape.

Roles and Responsibilities

Citizens' ERM Framework follows the widely accepted Three Lines Model, which defines risk management responsibilities across three key lines: management, oversight, and independent assurance. The Chief of Internal Audit, who reports to the Board through the Audit Committee, provides leadership and ensures that risk management activities are executed in accordance with this framework.

The **Risk Steering Committee (RSC)** provides strategic oversight and ensures the alignment of risk management activities with organizational objectives.

❖ First Line - **Management** is primarily responsible for identifying, mitigating, and monitoring the risks within its processes.



❖ Second Line - **Enterprise Risk** provides oversight, guidance, and support to business functions. They facilitate risk identification, assessment, and mitigation while ensuring alignment with corporate risk appetite and strategy. **Compliance, IT Security & Risk, and Privacy** assess and mitigate risk in alignment with the ERM methodology within their specialty field.

❖ Third Line - **Internal Audit and the Inspector General** provide independent assurance on the effectiveness of risk management practices across the organization.

Essentially, all **Employees** act as risk managers contributing to effective risk management at all levels.

Risk Perspectives

The Enterprise Risk team partners with business areas to deliver a forward-looking and insightful risk perspective, enhancing decision-making and strategic performance. Our ERM program adopts a multi-dimensional approach to risk management, focusing on:

Strategic Risks	Assessed annually with executive leadership, incorporating internal and external factors like governance, market shifts, and regulatory changes.
Operational Risks	Monitored throughout the year, focusing on core processes and operational efficiencies.

Project Risks	Evaluated pre- and post-implementation to ensure risk mitigation aligns with project goals.
Emerging Risks	Continuously monitored to anticipate future challenges and opportunities.

Risk Assessment

Our risk assessment process is a systemic approach that includes six steps:

- 1 Identify Risks:** Recognize events that may prevent the organization from achieving its objectives.
- 2 Evaluate Risks:** Assess the impact (high, medium, or low) and probability (likely, possible, or unlikely) of these events.
- 3 Consider Mitigating Activities/Controls:** Review existing controls to determine residual risk levels.
- 4 Rate Risk:** Determine overall risk ratings by combining impact and probability.
- 5 Decide Acceptability:** Determine if risk levels are acceptable and whether further mitigation is required.
- 6 Monitor and Review:** Continuously review the risk and its controls to ensure it is managed effectively.



Risk rating guidance promotes consistency in assessing risks across the organization and is provided in Appendices A-C.

Risk Response

Management's response to risks is guided by risk ratings, severity, and prioritization, and can include:

Accept 	No further action is required if the risk is within tolerance.
Mitigate 	Reduce severity or probability through existing or new controls.
Transfer 	Share the risk with third parties, such as through outsourcing or insurance.
Pursue 	Take calculated risks to capture opportunities.

Risk Acceptance

Risk assessment results exceeding acceptable levels will be reviewed to determine if additional mitigating activities can be promptly designed and implemented or if escalation is warranted. When it is no longer feasible or reasonable to implement mitigation measures for significant risks due to organizational changes, costs, or other factors, risk acceptance will be presented to the Risk Steering Committee (RSC) for consideration.

All risk acceptance proposals must follow a specific business case methodology mandated by the RSC and supported by the relevant ELT member(s) and sponsor(s) responsible for implementing plans to mitigate the identified risks. The RSC reserves the right to disapprove or monitor any proposal it considers an insufficient attempt to manage risks or that does not significantly contribute to the strategic imperatives of the organization.

Dynamic Risk Governance

Our ERM Framework leverages a dynamic approach focusing on agility, collaboration, innovation, and integration. The dynamic approach:

- ❖ Emphasizes collaboration and communication across the organization and leverages data and analytics to help organizations make better risk-based decisions.
- ❖ Provides a comprehensive view of risks, including internal and external factors. This insight enables informed decisions about risk, including how to allocate resources and mitigate risks.
- ❖ Helps to reduce risk exposure by identifying and addressing risks early through implementing proactive risk controls and monitoring risk indicators.
- ❖ Enables more timely and effective responses to changes in the risk landscape. This agility and resilience can help to weather disruptions and avoid costly losses.
- ❖ Enables more timely and effective responses to changes in the risk landscape. This agility and resilience can help to weather disruptions and avoid costly losses.



With Agility

Enterprise Risk enables management across all areas of the organization to self-identify, evaluate, record, and manage risks through guidance, training, and a software solution that provides a holistic view of risks and enables reporting. To remain agile, timely, and aligned with the organization and external influences, both facilitated and self-service capabilities are available for identifying and assessing risks.



- ❖ Self-service capabilities drive front-line ownership and engagement enabling the business areas to report risks identified and assess the risk rating along with updating mitigation plans.
- ❖ Interactive dashboards provide insight into our current risk levels and a connected approach to risk, internal control, and compliance.
- ❖ Risk monitoring ensures that our risk portfolio continuously reflects current risks and allows proactive adjustments to risk mitigation strategies as needed. Enterprise Risk, risk owners, and risk leaders proactively monitor Citizens' risk portfolio to assure 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 residual risk profiles against the target risk profiles.

The ERM Framework enables timely and proactive risk identification, assessment, mitigation, and monitoring that supports Citizens in navigating the continual changes necessary to serve the needs of Floridians.

Collaboration

Enterprise Risk creates and maintains 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, which includes leading practices from the 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) Frameworks.

Partnerships with business areas promote transparency and synergy resulting in comprehensive risk perspectives and solutions to mitigate current and emerging risks.

Innovation

Engaging ERM approaches are utilized to increase employee risk management competencies, adapt to changing organizational needs, and align with the latest leading risk practices:

- ❖ Creative approaches to promote risk awareness.
- ❖ Research and training on the latest risk practices.
- ❖ Industry maturity self-assessments to continually improve the framework.
- ❖ Post-assessment surveys to solicit ideas for improvement.



Integration

Citizens' strong risk culture is embedded throughout the organization by integrating ERM into various corporate policies, decisions, and leadership. Our GRC solution seamlessly integrates risks, controls, and compliance.

Citizens' Vendor Management Strategy integrates a risk-based approach designed to prevent business disruption and negative impacts on business performance. The approach is woven throughout vendor engagement, selection, and management. Vendor Management and Purchasing, in collaboration with Enterprise Risk and other stakeholders, facilitates this risk-based approach that includes:

- | | |
|---|--------------------------------------|
| ❖ Vendor Engagement Risk Identification | ❖ Vendor Risk Profile |
| ❖ "Responsible Vendor" Review | ❖ Risk Mitigation & Monitoring Plans |
| ❖ Vendor Classification | ❖ Active Contract Management |



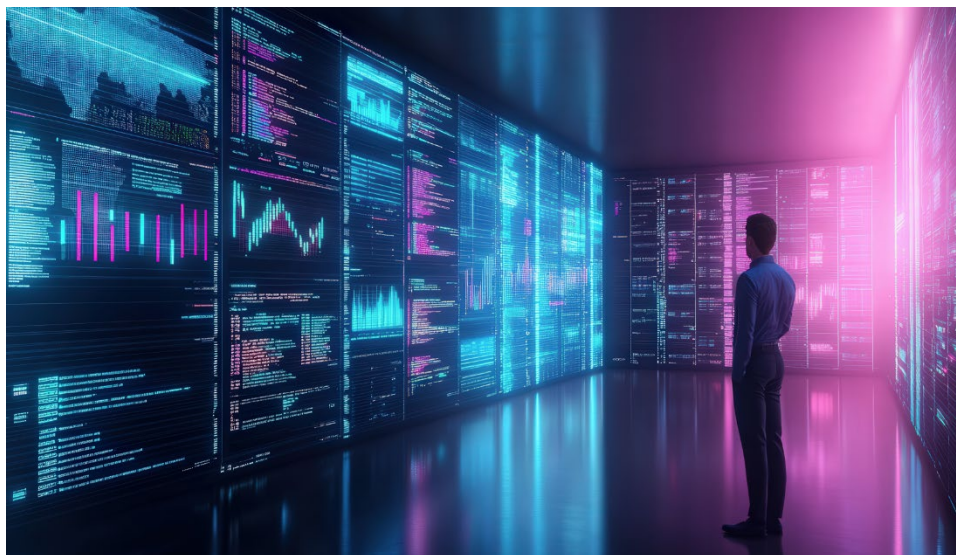
**Additional details regarding vendor risk management are included in Citizens' Vendor Management and Purchasing Playbook.*

Data Governance Strategy

Access to timely and reliable data is integral to our dynamic approach. As the framework evolves, the Enterprise Risk team, in collaboration with subject matter experts, will integrate data to assist with monitoring and assessing risks. Insights derived from data support:

- ❖ Understanding risk exposure
- ❖ Detecting and tracking emerging risk trends
- ❖ Facilitating risk-informed decision-making
- ❖ Enhancing and refining mitigation strategies

Key risk indicators (KRIs) and data analytics may be employed to evaluate and monitor risks. Where feasible, existing data and metrics will be utilized.



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 on 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 achieving corporate mission, vision and/or key strategic objective(s). - Requires little intervention.	- Moderate impact on achieving 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 significant reengineering and significant changes to organizational structure.
Financial Improper reconciliation of general ledger accounts, inaccurate financial reporting, unfavorable contract terms, 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 over 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).	- A high percentage of transactions are subject to complex and changing policies, procedures, and/or regulations, leading to ineffective or inefficient processes and a 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 results 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 have the potential for OIR or legislative criticism for non-compliance. - Moderate changes are 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 the business model are required.
Reputational Negative publicity, whether valid or not, may cause policyholder concern, costly litigation, and/or unfavorable revenue projections. This 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 is somewhat sensitive, but interest is narrowly focused on 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 the company's credibility with customers, suppliers, staff and the public. - Senior/key experienced staff leave.
Fraud Intentional acts intended for financial or personal gain, violations of the code of ethics, the 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 a company over \$250,000 - Public/media outrage, major customer exposure (contact & interest), extreme public interest. Massive reduction in the company's credibility with customers, suppliers, staff and the 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%	There is a high likelihood of occurrence (repeated failures). It will probably occur in most circumstances; it will be a complex process with some controls, mostly manual processes, impacting factors outside the organization's control.
Possible (2)	25% - 75%	Moderate likelihood of occurrence (occasional failures). It might occur at some time; previous audits/reports indicate non-compliance; complex processes; a mix of manual & automated processes; the control-conscious environment is in place; impacting factors outside the control of the 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 issues with high impact and likely probability for which the solution is outside of the ability of Citizens management and intervention is required through the 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 on Citizens if it occurs.

APPENDIX D: DEFINITIONS

Emerging Risk	Newly developing risks should be monitored for potential impacts on Citizens.
Enterprise Risk	Function responsible for coordinating, facilitating, and enabling 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 are integrated with strategy-setting and operational execution that Citizens rely on to manage risk in creating, preserving, and realizing value.
Impact	The 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 the 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, to reduce the risk.
Risk	There is a 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) is 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	The level of risk that Citizens is willing to accept in various risk areas.