Enterprise Risk Management Framework

Introduction
The framework for this program is based on the Committee of Sponsoring Organizations of the Treadway Commission’s (COSO) Enterprise Risk Management Framework. This framework describes responsibilities and governance structure, the foundation of this program, the components of this program, the external and internal environment to provide necessary context for assessment of Citizens risks, an introduction to risk appetite, and the methodology for developing our risk profile. The framework also provides the basis for the development of Citizens Enterprise Risk Management policy, procedures and report structures.

Definitions
Risk is the possibility that events will occur that can affect the achievement of strategy and business objectives.

Enterprise Risk Management is 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.

Risk Appetite is the degree of risk, on a broad-based level, that Citizens is willing to accept or take in pursuit of its objectives.

Risk Tolerance is the level of risk that Citizens is willing to accept in various risk areas. This can be measured in terms of both quantitative and qualitative dimensions.

The Enterprise Risk Office is the function responsible to coordinate, facilitate, and enable executive and business function management in the use of Citizens Risk Management policy and processes in the identification, assessment, and mitigation of risks.

Three Lines of Defense in effective risk management & control

<table>
<thead>
<tr>
<th>1st Line (Risk Management)</th>
<th>2nd Line (Risk Management &amp; Internal Control)</th>
<th>3rd Line (Internal Audit)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business</td>
<td>Manage risks on a daily basis and provide assurance regarding the effectiveness of controls</td>
<td>Steer, monitor and support line management in terms of managing risks and developing and maintaining an adequate internal control framework</td>
</tr>
</tbody>
</table>

First line of defense: Business
Citizens’ managers bear primary responsibility for identifying, controlling and monitoring the risks within their processes and for maintaining an appropriate internal control framework. These internal controls ensure the reliability of our processes and provide assurance to the second and third line and, ultimately, Executive Management and the Board of Governors.

Second line of defense: Risk Management & Internal Control
The Enterprise Risk Office is responsible for coordinating, developing and monitoring Citizens’ risk management framework and processes and supports and challenges the business with the identification, assessment and mitigation of current or emerging risks.

The Internal Control Office is responsible for coordinating, developing and monitoring Citizens’ internal control framework and processes and supports and challenges the business with the effective management of Citizens primary operating controls.
Enterprise Risk Management Framework

Third line of defense: Internal Audit
The Office of the Internal Auditor is responsible for developing of a comprehensive risk based internal audit program which provides assurance that Citizens internal control infrastructure is designed well and operating effectively.

Risk and Control Assurance Model

Key Principles on Managing Risk
• In order to achieve Citizens’ business objectives, risks must be considered and managed enterprise-wide;
• Risk management is integral to the strategic planning process, business decision making and day-to-day operations;
• Risks are identified, analyzed, responded to, monitored and reported on, in accordance with Citizens’ policies and procedures;
• Risk responses must be tailored to each particular business circumstance;
• Management must regularly assess the status of risks and risk responses; and
• Compliance with the Enterprise Risk Management Framework must be monitored and reported.

Components of the ERM Framework
Citizens’ Enterprise Risk Management Framework is made up of six process components derived from the Committee of Sponsoring Organizations of the Treadway Commission (COSO) ERM Framework. Our Policy on Business Conduct is the core of our business philosophy and set the tone and values of the organization. Objectives are set by the Executive Leadership Team in alignment with our Citizens’ Strategic Framework and are cascaded throughout the organization.

1. Establish the Context - understanding and articulating the internal and external environments of Citizens. The environment may generate risks that cannot be controlled,
Enterprise Risk Management Framework

or constrain the way we respond to a risk.

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

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

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

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

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

**Continuous Risk Identification** – identifying risk throughout the year. Risk identification is an iterative process and a shared responsibility of each employee.

Components of the ERM Framework

---

**Risk Perspective**
Risk can be viewed from three perspectives:

**Opportunity** - Risk of lost opportunity or something good not happening

By viewing risks from the perspective of opportunity, Citizens recognizes the inherent relationship between risk and return, i.e. the greater the risk, the greater the potential return or loss. In this context, Citizens must adopt suitable responses to maximize the upside opportunity within the constraints of its operating environment.
Enterprise Risk Management Framework

**Uncertainty** - Risk of not meeting expectations
When considering risks from the perspective of uncertainty, Citizens must determine how it can proactively prevent an uncertainty from having a negative impact. This will mainly be achieved through management of risks relating to operational performance.

**Hazard** - Risk of loss or something bad happening
While managing risk from the perspective of hazard, Citizens must mitigate the degree of damage to critical business assets (people, property, earning capacity and reputation) that would be caused if the hazard occurs.

**Risk Appetite & Risk Tolerance**
Defining risk appetite is challenging, particularly when applying the COSO definition of risk appetite (“the amount of risk, on a broad level, an organization is willing to accept in pursuit of value”). In consultation with Executive Management the Enterprise Risk Office will define Citizens risk appetite as part of the annual performance planning process.

One of the considerations affecting risk appetite is risk tolerance. According to COSO, this is defined as the “acceptable level of variation an entity is willing to accept regarding pursuit of its objectives.” A separate document will be prepared to communicate Citizens approach to risk appetite and tolerance.

**Risk Management Accountability**
Citizens’ executive management and business leaders are accountable for identification and managing risks affecting the business.

**Enterprise Risk Office Responsibility**
The Enterprise Risk Office has the responsibility for establishing and embedding an enterprise risk oversight framework and culture consistent with our risk appetite that protects and enhances Citizens’ embedded value.

Our Enterprise Risk Framework describes our approach to risk management, including provisions for risk governance arrangements; our appetite and limits for risk exposures; policies for the management of various risk types; risk culture standards; and risk reporting.
Enterprise Risk Management Framework

As an integrated part of all business processes, the Enterprise Risk Office is responsible for the definition and the deployment of the Enterprise Risk Management (ERM) framework within Citizens by enabling management to assess manage and assess risk utilizing an aligned terminology, process, and tool.

The role the Enterprise Risk Office in management of the ERM Framework

<table>
<thead>
<tr>
<th>Vision</th>
<th>Desired Outcomes</th>
</tr>
</thead>
<tbody>
<tr>
<td>To enable ERM through the integration of risk and control activities</td>
<td>• Promote structure, transparency, consistency, and uniformity among internal ERM</td>
</tr>
<tr>
<td>across the enterprise to support a common, holistic, prioritized view</td>
<td>community.</td>
</tr>
<tr>
<td>of risks and controls.</td>
<td>• Facilitate the identification and evaluation of risks throughout the</td>
</tr>
<tr>
<td></td>
<td>organization and support the use of a consistent aligned approach across</td>
</tr>
<tr>
<td></td>
<td>Citizens.</td>
</tr>
<tr>
<td></td>
<td>• Enable management across all levels of the organization to self-identify,</td>
</tr>
<tr>
<td></td>
<td>evaluate, record and manage risks through the provision of guidance, training</td>
</tr>
<tr>
<td></td>
<td>and a software solution.</td>
</tr>
<tr>
<td></td>
<td>• Convert disparate risk and control data into integrated informational views.</td>
</tr>
<tr>
<td></td>
<td>• Proactively identify, assess, measure, manage and monitor Citizens risk</td>
</tr>
<tr>
<td></td>
<td>portfolio.</td>
</tr>
<tr>
<td></td>
<td>• Empower management to make risk-informed resource utilization decisions.</td>
</tr>
<tr>
<td></td>
<td>• Validate that current residual risk exposure is aligned with risk appetite.</td>
</tr>
</tbody>
</table>

Pre-requisites include common views of language, framework, organization, and process.

ENTERPRISE RISK MANAGEMENT PROCESS

OVERVIEW

The basis of Citizens Enterprise Risk Management Process is a continuous cycle anchored in the six steps of establish, identify, evaluate, develop, respond and monitor as shown below. Within each step of the process, regular and meaningful communication is essential to improve the likelihood of success. By viewing this cycle as a continual loop, managers are reminded of the need for thoughtful and regular feedback, as improvement is critical to successful risk management.
Enterprise Risk Management Framework

**Step 1: Establish**

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

**Step 2: Identify**

Systematically and continuously identify risks faced in meeting strategic and operational objectives. For each business objective, it is necessary to identify the key risks that might impede the achievement of the respective strategic or operational objectives. Risk identification should initially be performed as part of all major decision making processes:

- **Each major decision level**
  - Group strategy planning
  - Business Unit operating plans
  - Core processes
  - Project plans
  - Investment (Buy/Sell) decisions
  - Personal plans

- **Process or system changes**
  - Change requests

Collective and individual assessment of risks

- By individuals in groups using techniques such as brainstorming, internal and external input, e.g. project sub-contractor presentations

- **New Projects**
  - Project team planning
  - Project paper presentation and discussions

Thereafter, risks can be updated on an ongoing basis by integrating the identify step with core business management processes.

Risks should be considered within the following main risk categories:

- **Strategic**
- **Operational**
- **Financial**
- **Systems**
- **Compliance**
- **Reputation**

**Step 3: Evaluate**

Analyze and evaluate risks by considering the causes, sources, probability the risk will occur, potential positive or negative outcomes, and then prioritizing the results of the analysis. Once the risks have been identified, the probability of the risk occurring and the potential impact if the risk does occur are assessed using the risk rating table below.
Enterprise Risk Management Framework

### Risk Impact Rating:

Criteria for Risk Impact Rating - Indicate the severity of the failure to Citizens, or the magnitude of the impact if the failure occurs. Only values of 1, 2, 3. Use the following guidelines:

<table>
<thead>
<tr>
<th>Risk Categories</th>
<th>(1) Low</th>
<th>(2) Medium</th>
<th>(3) High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategic</td>
<td>Minor impact on the achievement of corporate mission, vision and/or strategic objective(s). Requires little intervention.</td>
<td>Moderate impact on the achievement of corporate mission &amp; vision. Can be rectified with moderate change in processes/systems and can significantly delay the accomplishment of strategic objective(s).</td>
<td>Major changes in processes/systems required with, significant reengineering, explosive growth, significant changes organizational structure. Failure to meet key strategic objective(s).</td>
</tr>
<tr>
<td>Financial</td>
<td>Financial impact that may reduce cash flow by less than USD 5 million.</td>
<td>Material financial impact that may reduce cash flow by more than USD 5 million but less than USD 20 million.</td>
<td>Significant material financial impact that may reduce cash flow by more than USD 20 million.</td>
</tr>
<tr>
<td>Processing/Operational</td>
<td>Mature processes and strong internal control environment. Limited impact on key operational objectives.</td>
<td>Processes under development (moderate change), known control deficiencies which may result in a disruption to normal operation or monetary loss, with a limited effect on achievement of corporate strategy and objectives.</td>
<td>Significant or high percentage of transactions subject to complex and changing policies, procedures, and/or regulations (major change); leading to ineffective or inefficient processes; high probability of monetary loss. Extensive use of third-party processors with no monitoring. Could prevent the achievement of key operational objective(s).</td>
</tr>
<tr>
<td>Systems/Technology</td>
<td>Minor outage with no impact on service or recovery of data required. Some loss of data; Breach of IT Systems, Key functions or locations unavailable &lt; 24 Hours. Outage affects 1% - 5% of policyholders.</td>
<td>Limited scope, short duration outage. Minor service impact. Data required to be recovered. Some loss of important data; breach of IT Systems resulting in damage. Key functions unavailable &gt; 1 - 5 days. Outage affects 5% - 10% of policyholders.</td>
<td>Significant or high percentage of transactions subject to complex and changing policies, procedures, and/or regulations (major change); leading to ineffective or inefficient processes; high probability of monetary loss. Extensive use of third-party processors with no monitoring. Could prevent the achievement of key operational objective(s).</td>
</tr>
<tr>
<td>Compliance</td>
<td>Incident non-reportable to regulator/authorities, or reportable with no penalty for non-compliance. Limited regulations, flexibility permitted in meeting policies, procedures, and regulations.</td>
<td>Potential for OIR action or penalties for non-compliance. Some business unit specific regulations with potential for OIR or legislative criticism for non-compliance. Ethical standards are communicated but not enforced; or not monitored.</td>
<td>Criminal offense. Extensive, directly related statutes or regulations or accounting principles. Previous regulatory criticisms or sanctions. No ethical standards. Large scale action, major breach of legislation with very significant financial or reputational consequences.</td>
</tr>
<tr>
<td>Reputational</td>
<td>Limited media coverage or public interest. Adverse exposure potential is relatively immaterial. Limited or general morale problems among staff/management with little turnover.</td>
<td>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.</td>
<td>State CFO/Governor action. Public/media outrage, major customer exposure (contact &amp; interest), extreme public interest. Massice reduction in company's credibility with customers, suppliers, staff and public. Senior/key experienced staff leave.</td>
</tr>
</tbody>
</table>

---

[Continued on next page.]
Enterprise Risk Management Framework

Probability

<table>
<thead>
<tr>
<th>Likelihood Rating -</th>
<th>Indicate the likelihood of occurrence of the potential causes of the failure.</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Rating</strong></td>
<td><strong>Probability</strong></td>
<td><strong>Criteria</strong></td>
</tr>
<tr>
<td>3</td>
<td>Likely</td>
<td>75% - 90%</td>
</tr>
<tr>
<td>2</td>
<td>Possible</td>
<td>25% - 75%</td>
</tr>
<tr>
<td>1</td>
<td>Unlikely</td>
<td>&lt; 25%</td>
</tr>
</tbody>
</table>

Risk Matrix

<table>
<thead>
<tr>
<th>Probability and Impact Matrix</th>
<th>PROBABILITY</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Unlikely</td>
</tr>
<tr>
<td>1</td>
<td>Low</td>
</tr>
<tr>
<td>2</td>
<td>Medium</td>
</tr>
<tr>
<td>3</td>
<td>High</td>
</tr>
</tbody>
</table>

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

Step 4: Develop
Develop alternatives, systematically identifying and assessing a range of risk response options guided by risk appetite. Decide and formulate effective risk response strategies and plans. Once risks have been analyzed, appropriate risk responses can be determined to mitigate risk to an acceptable level within reasonable costs. Citizens’ inherent and residual risk profile presented on the Risk Map are monitored against the target risk profile.

![Diagram showing the process of risk management with inherent risk, residual risk, and target risk]
**Step 5: Respond**
Respond to risks by making decisions about the best options(s) among a number of alternatives, and then preparing and executing the selected response strategy. Risks can be dealt with in various ways. The risk response options should include all possible management response to risk, whether viewed as opportunities, uncertainties or hazards. The risk response options and examples of activities under each option are outlined below:

<table>
<thead>
<tr>
<th>MITIGATE</th>
<th>TRANSFER</th>
<th>AVOID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Steps taken to reduce either the probability of an occurrence or impact or both such as:</td>
<td>Steps taken to shift the loss or liability to third parties, such as:</td>
<td>Steps taken to prevent the occurrence of hazards, such as:</td>
</tr>
<tr>
<td>Monitoring budgets/forecast</td>
<td>Insurance, Re-insurance / pre-event bonds</td>
<td>Ceasing activity</td>
</tr>
<tr>
<td>Defining accountability</td>
<td>Outsourcing</td>
<td>Divestment of operations</td>
</tr>
<tr>
<td>Ensuring adequate skill sets</td>
<td>Diversifying investments</td>
<td>Changing objective, scale of operations or scope of coverage</td>
</tr>
<tr>
<td>Improving staff morale</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Implementing a business continuity program</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>EXPLOIT</th>
<th>ACCEPT</th>
<th>AVOID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Steps taken to leverage opportunities, such as:</td>
<td>Informed decision to accept both the impact and the probability of risk events</td>
<td></td>
</tr>
<tr>
<td>Influencing regulators, public perception</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Renegotiating contracts</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reorganizing and restructuring</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Step 6: Monitor and report**
Evaluating and monitoring performance to determine whether the implemented risk management options achieved the stated goals and objectives. Continuously ensure that the risk response plans are operational and relevant. The purpose of the review is to:

- Provide assurance that risks are being managed as expected;
- Assess whether the risk response plans remain relevant; and
- Ensure that the risk profile anticipates and reflects changed circumstances and new exposures.

Risk monitoring consists of a combination of regular communication, periodic reviews or audits and evaluation by independent executives at appropriate levels. Assurance techniques include: periodic or random testing of controls, risks and control environment; quality assurance reviews; post-implementation reviews; performance appraisals.
Enterprise Risk Management Framework

Risk response should be measured in terms of efficiency and effectiveness. Efficiency measures the cost of implementing risk management responses in terms of time, money and resources, whereas effectiveness measures the relative degree to which the responses reduce the impact or probability of the risk occurring.

To maximize efficiency and effectiveness of risk responses, monitoring and reporting should be integrated with existing business processes and reporting as far as possible. While everyone in Citizens is responsible for enterprise risk management in their respective areas, some staff have specific responsibilities. The policy, design and framework for enterprise risk management is driven by the Board and managed by the Enterprise Risk Office.

The reporting structure ensures that risk response gaps are addressed and the risk responses are operating effectively under changing conditions. Enterprise risk management activities should be monitored and reported upwards throughout Citizens as illustrated in the following diagram.

Overview of Citizens approach to integrated enterprise risk management
Enterprise Risk Management Framework

Other Considerations
This document does not provide a detailed view of Citizens:

- Risk policy,
- Risk identification, assessment and monitoring procedures
- Report structures
- Approach to assess risk appetite and tolerance

As the Enterprise Risk Office develops and matures consideration will be given to fully operationalize enterprise risk management throughout the organization.