IT Strategic Plan Update

Aditya Gavvala
Chief Information Officer

CITIZENS
PROPERTY INSURANCE CORPORATION

IT Vision and Mission

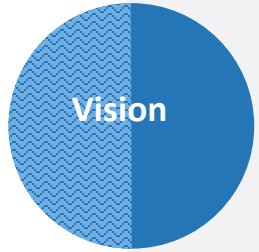
Corporate

We serve the people of Florida as the state's insurer of last resort, and as an innovative thought leader focused on promoting a healthy property insurance market.

We strive to promote access, stabilization, and market competitiveness for Florida consumers, carriers, investors, and the overall property insurance industry.

IT

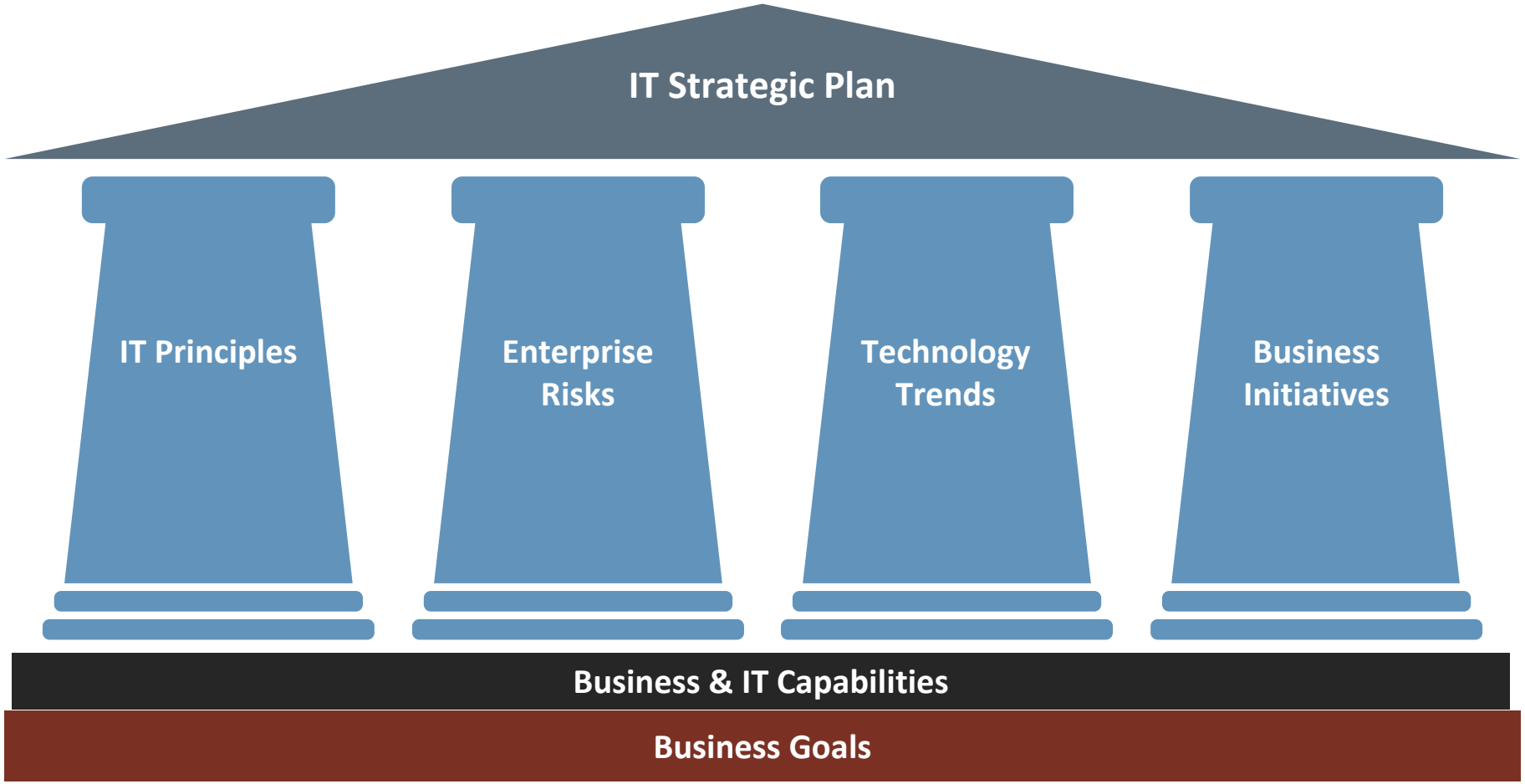
We provide and support secure, reliable and dependable technology infrastructure, and deliver high quality business solutions and data analytics to our internal and external customers.



We will relentlessly drive value to our customers through highly engaged, responsive and customer service-oriented IT workforce.

CITIZENS
PROPERTY INSURANCE CORPORATION

Strategic Plan



InfoTech research was used as the baseline for the IT Strategic Plan.

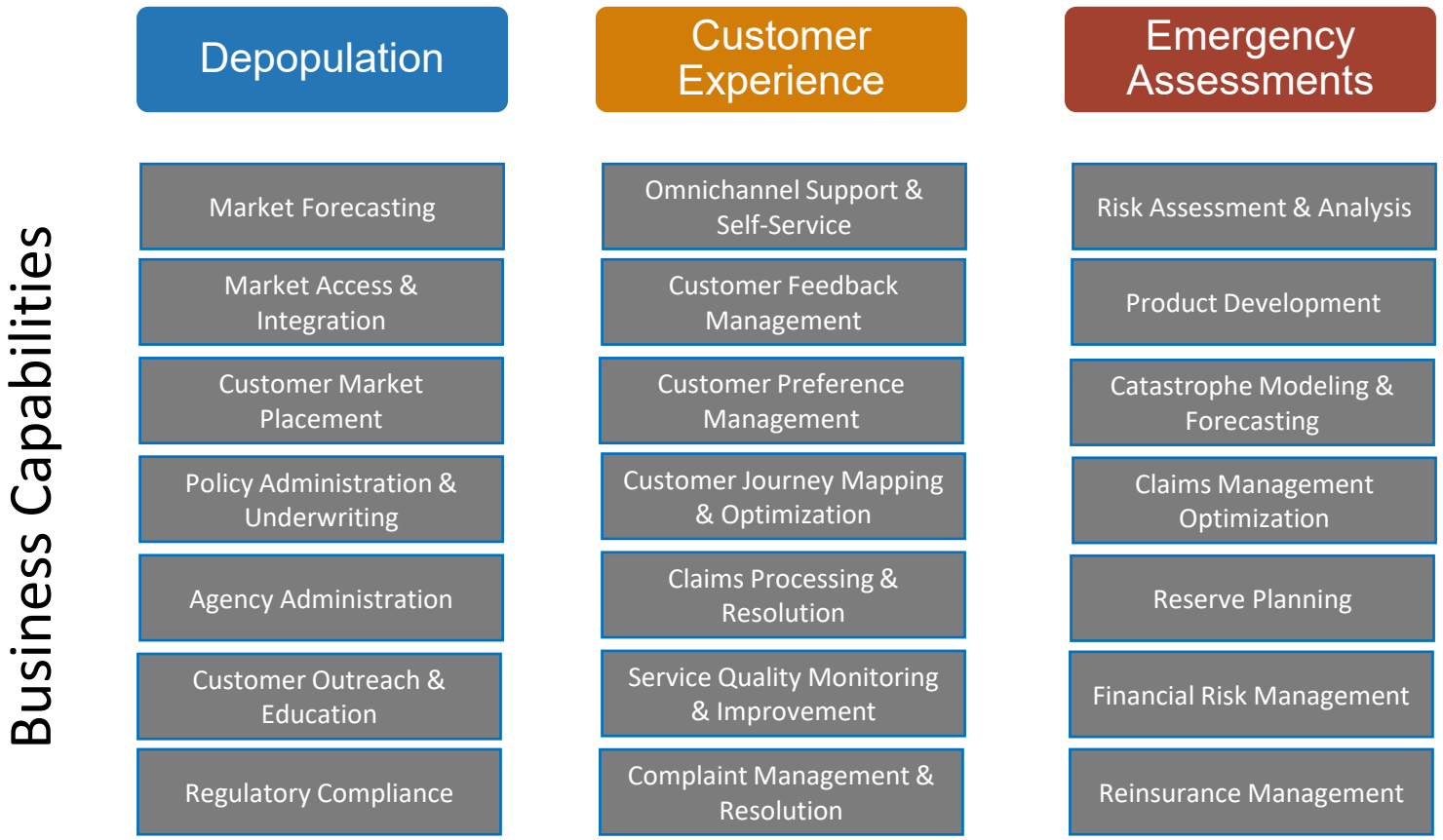
CITIZENS
PROPERTY INSURANCE CORPORATION

Business Goals

Depopulation	Customer Experience	Emergency Assessments
Promote depopulation and optimize access to private-market coverage for Citizens' applicants and policyholders.	Understand and enhance the customer experience by soliciting feedback, gauging satisfaction, and optimizing service capabilities and touchpoints.	Reduce or eliminate the risk of emergency assessments for Citizens' policyholders and all potentially impacted Florida policyholders.

CITIZENS
PROPERTY INSURANCE CORPORATION

Business Capabilities



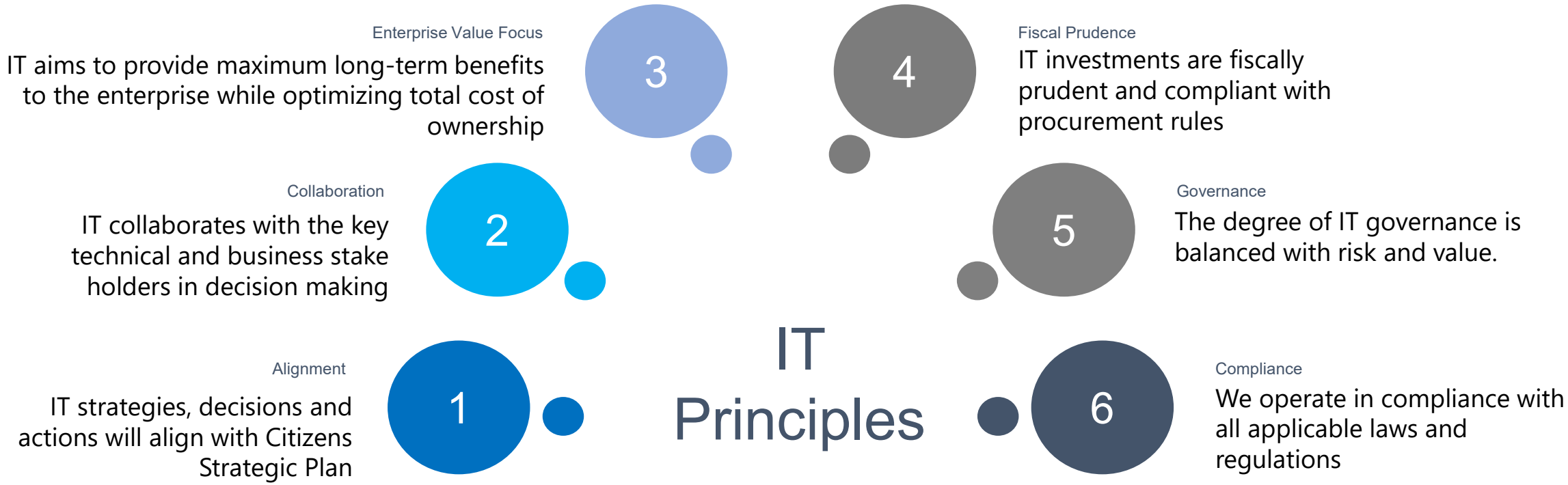
CITIZENS
PROPERTY INSURANCE CORPORATION

IT Goals

Operational Excellence	Reduced Risk
Run business operations with cost optimized, resilient, compliant and risk mitigated technical infrastructure.	Protect IT systems and infrastructure against security threats.

CITIZENS
PROPERTY INSURANCE CORPORATION

IT Guiding Principles



Enterprise Strategic Risks

2024 Strategic Risks		
Risk Title	**Risk Description**	**Rating**
Rate Differential	As a result of Citizens' current rate making efficiencies and the glide-path application to Citizens' rates, Citizens' competitive position in the market is not aligned with being a residual market.	High
Market Conditions	Changing market conditions may adversely impact private carriers continued participation in the Florida insurance market or geographic locations due to insolvency resulting in fluctuations in Citizens' costs, financial condition, exposure, and number of policies in force.	High
Claims Abuse	Failure to identify and stay in front of fraud, and other claims abuse schemes that increase claim costs for Citizens.	High
Acquisition of Reinsurance	Citizens' inability to transfer risk through acquiring reinsurance in the global marketplace could lead to significant financial implications for Citizens, the State of Florida, and ultimately on Florida residents.	High
CAT Response	Failure to have adequate vendor resources to respond to a catastrophic event to meet customer expectations.	High
Strategic Workforce Planning	Citizens' increasing retirement eligible workforce, and business priorities may impact our organization's stability, culture, reputation, and high levels of employee engagement as well as the ability to attract, retain and/or develop employees to master critical skills.	High
External Influences	Uncertainty related to external events, including storms, new or changing laws and/or regulations, and changing market conditions that require rapid adjustments impacting Citizens' mission and operations may result in significant financial and operational challenges.	High
Cyber Threats	The increasing complexity and variety of cyber incidents may adversely impact organizations' performance and reputation.	High
Technical Debt	Technical debt refers to the cost incurred due to short-term technical decisions that prioritize immediacy, simplicity, or budget constraints. These decisions, while convenient initially, can lead to long-term consequences such as operational inefficiencies, increased costs, and heightened risks. Addressing this technical debt promptly is essential to maintain system integrity and efficiency.	Medium
Ethics, Integrity, Conflicts of Interest	Violation of Citizens' code of ethics, commitment of illegal and unauthorized acts, management fraud, employee fraud or situations where multiple, conflicting interests could possibly corrupt motivation or decision-making may result in criminal charges, reputational damage, or financial loss.	Low
End User Business Applications	Productivity tools/applications developed by business units using non-standard technologies have become indispensable for day-to-day operations. However, they introduce various challenges to the organization, including security, privacy, resilience, supportability, and maintainability.	Low

Technology Trends

InfoTech Tech Trends - 2024

Emerging
- Artificial Intelligence
- Robotic Process Intelligence (RPA) or Intelligent Process Automation (IPA)

Transformative
- Cloud Computing
- Cybersecurity solutions
- Application Programming interfaces (APIs)
- Data Management Solutions
- No-code/Low-code Platforms

Growing Investment

Niche
- Internet of Things (IoT)
- Drones
- Mixed Reality
- Blockchain
- Quantum Computing
- Private Cellular (LTE or SG)

Entrenched
- On-premises Servers

Not Growing Investment

Datos Top Tech Priorities for Personal Lines Carriers - 2024

- **Agent and Customer Access**
  - Customer portals (low code/no-code tools)
  - Mobile and Omnichannel functionality
  - Multi-factor authentication (MFA) for producers and policyholders
- **BI, Analytics, and Artificial Intelligence (AI)**
  - Data governance and quality
  - Third party data
  - Analytics inventory and model management
- **Policy Administration and Rating Systems**
  - Flexible Product Development
  - Automation to shorten cycle times
  - AI for underwriting
- **Billing Systems**
  - Mobile inquiry and payment processing
- **Claims Systems**
  - AI for efficiency and fraud detection/prevention

IT Capabilities and Domains

- An IT Capability is a specific ability or competency that the IT department possesses, enabling it to support and enhance business operations. These capabilities encompass the skills, processes, technologies, and resources that IT provides to help an organization achieve its business goals and deliver value.
- A Capability Domain is a high-level categorization of related capabilities within an organization, typically grouped by function or strategic purpose. Each domain encompasses multiple individual capabilities that collectively contribute to the achievement of specific business or IT objectives.

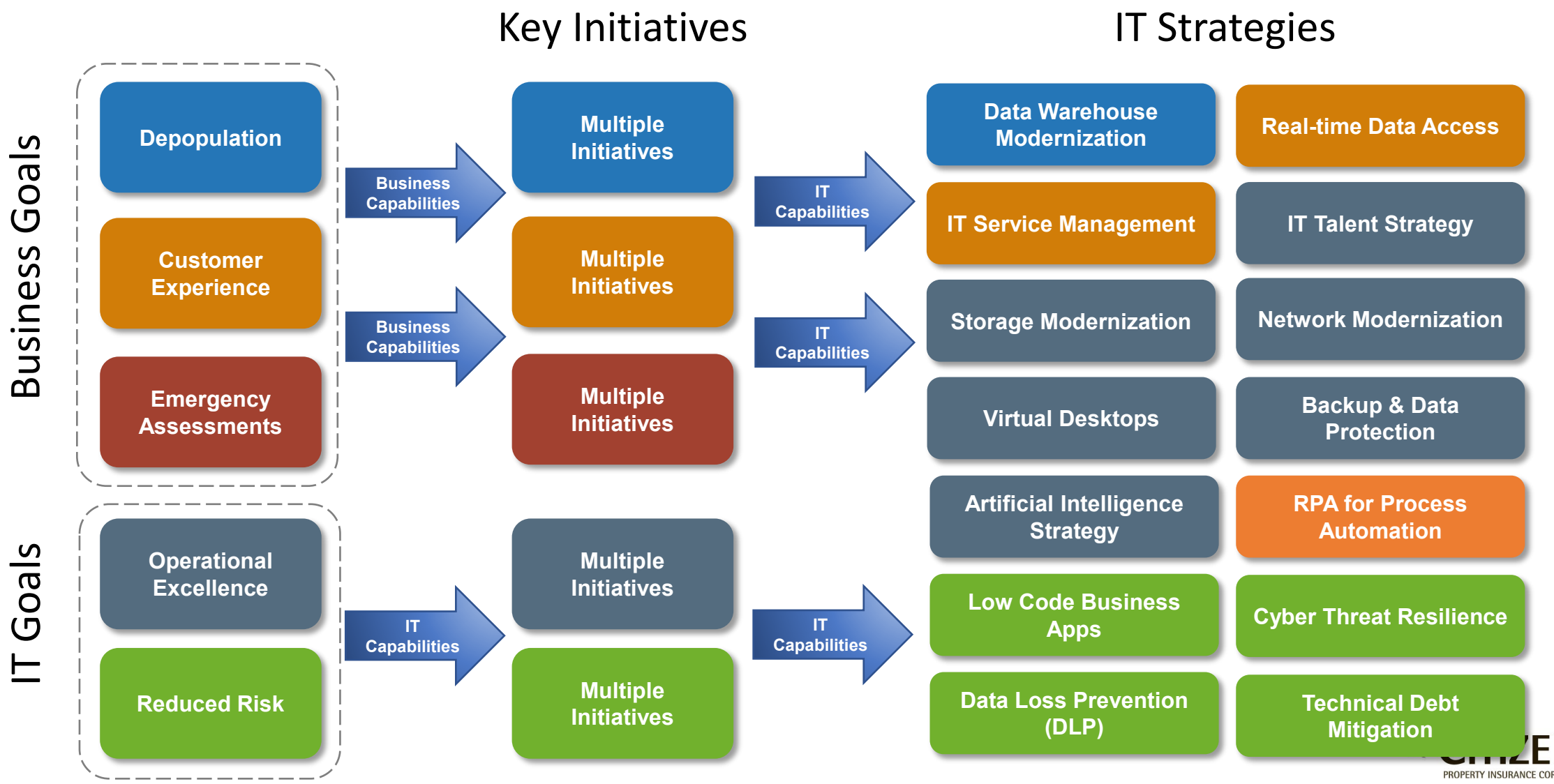
Citizens IT Capability Domains

Strategic Planning	People and Resources	Architecture and Planning	Infrastructure and Operations
Service Delivery	Application Delivery	Data and Business Intelligence	Security & Risk

CITIZENS
PROPERTY INSURANCE CORPORATION

**IT Capability Domain to IT Capabilities are listed in Appendix D.*

Aligning Business Goals with IT Strategies



CITIZENS
PROPERTY INSURANCE CORPORATION

Appendices

The following slides provide supplementary information that supports the main presentation.

- Appendix A: Business Capabilities to IT Capability Domain Mapping
- Appendix B: IT Strategy-on-a-Page Example
- Appendix C:
  - ✓ Depopulation Related IT Strategies
  - ✓ Customer Experience Related IT Strategies
  - ✓ Emergency Assessments Related IT Strategies
  - ✓ Operational Excellence Related IT Strategies
  - ✓ Reduced Risk Related IT Strategies
- Appendix D: IT Capabilities
- Appendix E: Glossary of Terms

CITIZENS
PROPERTY INSURANCE CORPORATION

Appendix A: Business Capabilities to IT Capability Domain Mapping

		IT Capability Domains							
Business Goal	**Business Capability**	**Strategic Planning**	**People & Resources**	**Architecture & Planning**	**Infrastructure & Operations**	**Service Delivery**	**Application Delivery**	**Data & BI**	**Security & Risk**
Depopulation	Market Forecasting							X	
	Market Access & Integration	X	X	X	X		X	X	X
	Customer Market Placement	X	X	X			X	X	X
	Policy Administration & Underwriting					X	X		
	Agency Administration					X	X		
	Customer Outreach & Education					X	X	X	
	Regulatory Compliance								X
Customer Experience	Omnichannel Support & Self-Service		X			X	X	X	
	Customer Feedback Management							X	
	Customer Journey Mapping & Optimization		X			X		X	
	Customer Preference Management					X		X	
	Claims Processing & Resolution					X	X		
	Service Quality Monitoring & Improvement					X		X	
	Complaint Management & Resolution					X		X	
Emergency Assessments	Risk Assessment & Analysis							X	X
	Product Development	X	X	X			X		
	Catastrophe Modeling & Forecasting	X						X	X
	Claims Management Optimization		X			X	X		
	Reserve Planning							X	
	Financial Risk Management								X
	Reinsurance Management	X						X	
Operational Excellence	Process Optimization & Automation		X			X	X		
	Cost Management & Efficiency	X		X	X			X	
	Performance Monitoring & Reporting		X			X		X	
	Quality Assurance & Control		X			X	X		X
	Asset Optimization	X			X				
	Operational Resilience & Adaptability				X				X
	Compliance Management								X
Reduced Risk	Risk Management & Mitigation		X						X
	Disaster Recovery		X		X				X
	Contingency Planning & Resource Allocation		X		X				X
	Incident Response & Management		X			X			X
	Data Protection & Encryption								X
	Audit & Compliance Monitoring								X
	Security Policy Development & Governance								X

Appendix B: IT Strategy-on-a-Page Example

DLP Strategy on a Page

Purpose: DLP is designed to stop data from being used or stored where it should not. Typically, DLP is the last line of defense against a data breach when all other measures have failed. DLP use the concepts of data at rest, data in motion and data in use to structure DLP architectures.

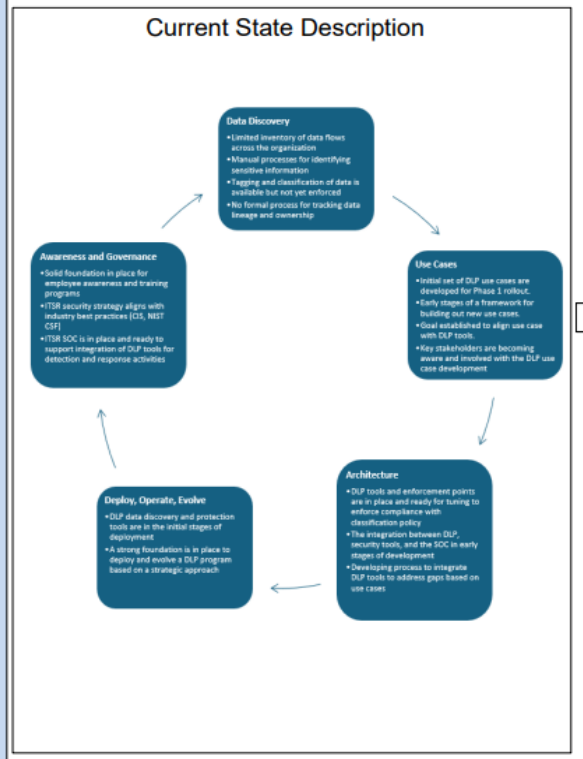
Current Challenges

- Difficulty in maintaining visibility and control of data spread across on-premises, cloud, mobile devices, and hybrid environments.
- Challenges in integrating DLP solutions with existing security infrastructure, scaling across diverse environments, and achieving a unified view of data protection efforts.
- Many enforcement points where DLP should be deployed that require multiple DLP solutions increasing complexity and allocation of resources.
- Poor or informal business processes can lead to inconsistent application of DLP policies.
- DLP policy matching solutions producing an overabundance of false positives and false negatives.
- Employees may resist adopting new DLP tools and procedures due to lack of education and communication.

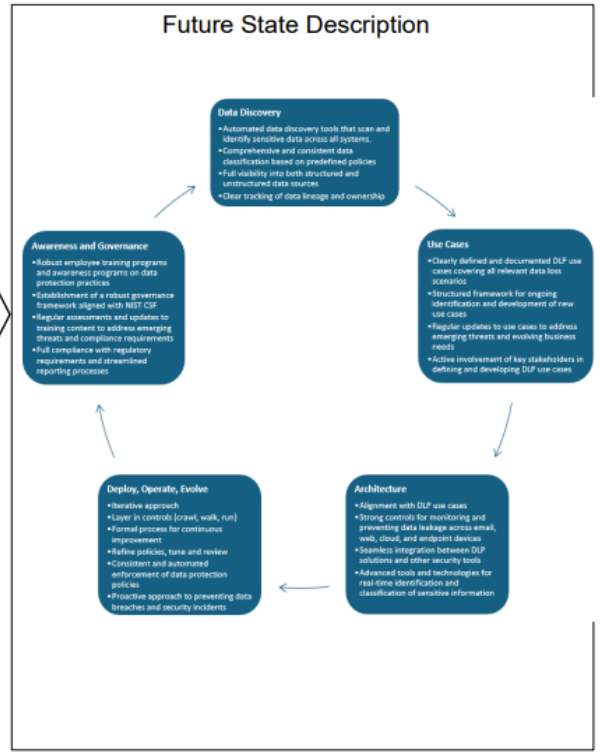
Objectives

- **Data Discovery, Mapping, Classification:**
  - Identify sensitive data, its movement, and location.
  - Prioritize based on risk.
  - Map data sources and destinations.
  - Classify and tag data for DLP inspection.
- **DLP Business Use Cases:**
  - Develop use cases for security controls.
  - Focus data security on use cases vs attempting to tackle all aspects at once.
- **DLP Initial Architecture:**
  - Identify product options based on use cases.
  - Identify what capabilities exist today.
  - Map all DLP controls to data sources and destinations.
  - Identify where DLP is lacking or nonexistent.
  - Deploy controls in areas and order based on risk/likelihood of occurrence.
  - Choose vendors/tools that can protect data in multiple use cases.
- **Deploy, Operate, and Evolve:**
  - Implement in monitoring only and enable active control once acceptable.
  - Refine DLP policies for accuracy.
  - Define what success looks like to each DLP use case.
  - Implement metrics to support continuous improvement and to measure DLPs impact on reducing risk.
- **Awareness and Governance:**
  - Establish communication and end user training framework.
  - Identify and improve business practices for data handling.
  - Develop feedback and consulting opportunities.

Current State Description



Future State Description



Strategic Alignment

Business Goal	IT Goal	IT Capabilities to Enhance	ITSR Components Needed
Reduced Risk	Protect IT Systems and Infrastructure against Security Threats	Data Protection & Privacy	• Data Classification Tools • Data Discovery Tools • DLP Policy Management • Encryption • Reporting

Information Security and Privacy Policy

- **Data Security:** Manage Citizens' critical data based on identified risk designed to safeguard the confidentiality, availability, integrity, and resiliency of critical data assets.
- **Data Classification Handling:** The ITSR operational unit and the Privacy Officer must develop and maintain Data Classification and Handling Procedures.
- **Identity Management and Access Control Management**: Limit access to Citizens' network and assets to ensure users have the least access they need to complete business objectives.

Transition Narrative

Where we are today

- A data classification policy has been established.
- Security solutions that provide DLP capabilities are deployed, but not aligned with use cases or business requirements.
- A robust data security program is in place, but a data-centric architecture model has not yet been adopted.

Transition

- Identify sensitive data, develop business use cases, and prioritize.
- Classify and tag sensitive data.
- Focus DLP on use cases with well defined success metrics.
- Invest in automated tools that seamlessly integrate with our existing systems and provide comprehensive coverage.
- Promote a centralized approach to data management to achieve a unified and consistent application of the data classification policy.
- Launch comprehensive training programs and awareness campaigns.
- Implement real-time monitoring and robust reporting mechanisms to track compliance and address non-compliance proactively.
- Adopt a data-centric approach aligned with the NIST CSF framework and industry best practices.

Where we want to be

- Adoption of DLP tools that align with a data-centric security model.
- Clear accountability for data classification across all departments.
- Integration of specialized DLP tools to address gaps in coverage.
- Data classification policy is established and effectively enforced.
- Ability to adapt to new threats, changes, and technology advancements.
- DLP tools integrated into SOC with automated incident detection and response capabilities.
- Documented and formalized data handling and DLP policy enforcement across the organization.
- Culture of security awareness and proactive behavior to protect data.

Relevant Standards

Data Protection

- **3.1:** Establish and a Maintain Data Management Process
- **3.2:** Establish and Maintain a Data Inventory
- **3.3:** Configure Data Access Control Lists
- **3.4:** Enforce Data Retention
- **3.5:** Securely Dispose of Data
- **3.6:** Encrypt Data on End-User Devices
- **3.7:** Establish and Maintain a Data Classification Scheme
- **3.8:** Document Data Flows
- **3.9:** Encrypt Data on Removable Media
- **3.10:** Encrypt Sensitive Data in Transit
- **3.11:** Encrypt Sensitive Data at Rest
- **3.12:** Segment Data Processing and Storage Based on Sensitivity
- **3.13:** Deploy a Data Loss Prevention Solution
- **3.14:** Log Sensitive Data Access

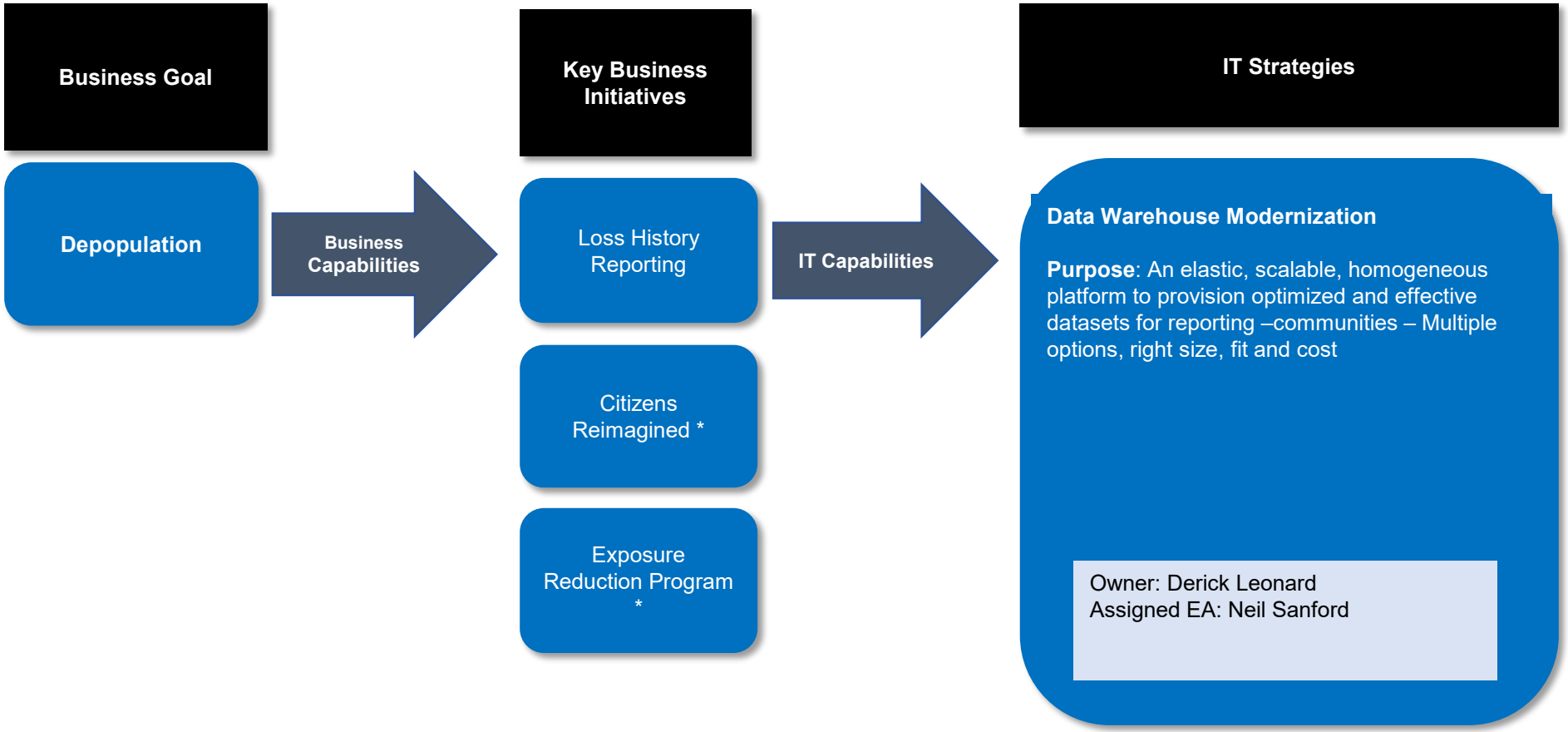
References

This strategy was inspired by:

- NIST CSF 2.0 Feb.2, 2024
- CIS Critical Security Controls Ver.8
- Gartner: Choosing the Right Data Loss Prevention Architecture April 3, 2023

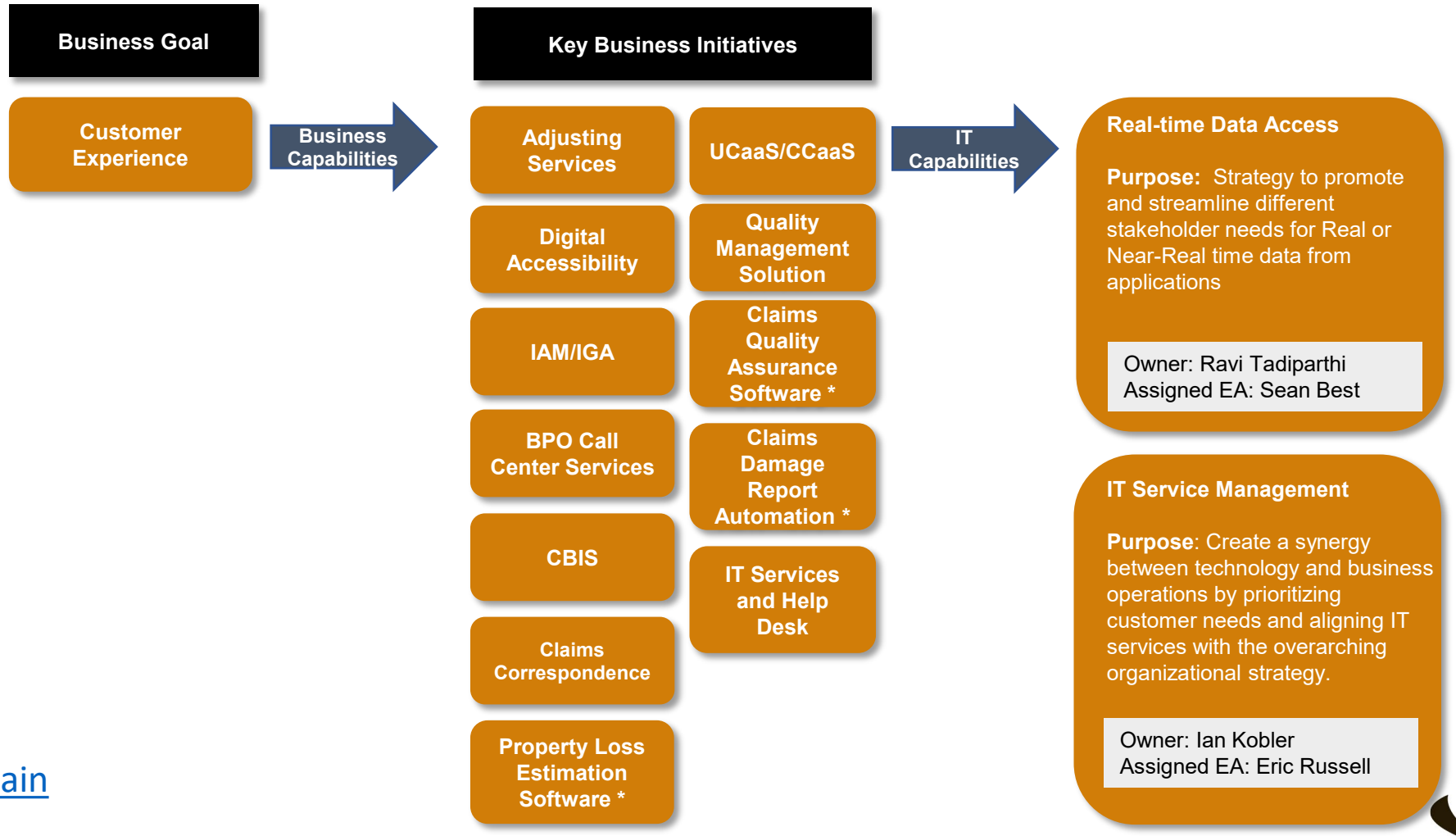
Disclaimer: This strategy document is intended to outline Citizens' aspirational goals and overall direction regarding [specific area]. While this strategy has been informed by industry standards, it is not intended to establish or guarantee a specific level of compliance.

Appendix C: Depopulation Related IT Strategies



Appendices Main

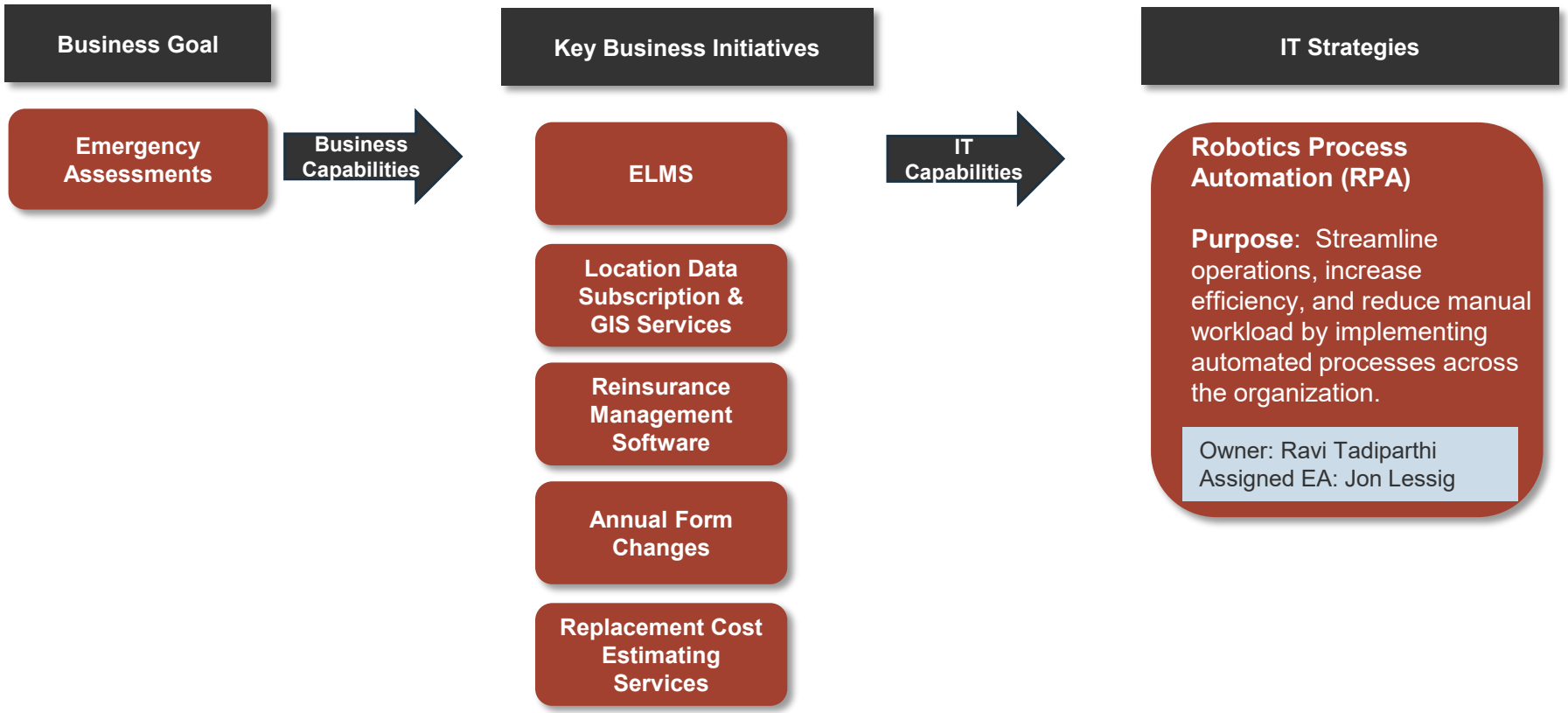
Appendix C: Customer Experience Related IT Strategies



Appendices Main

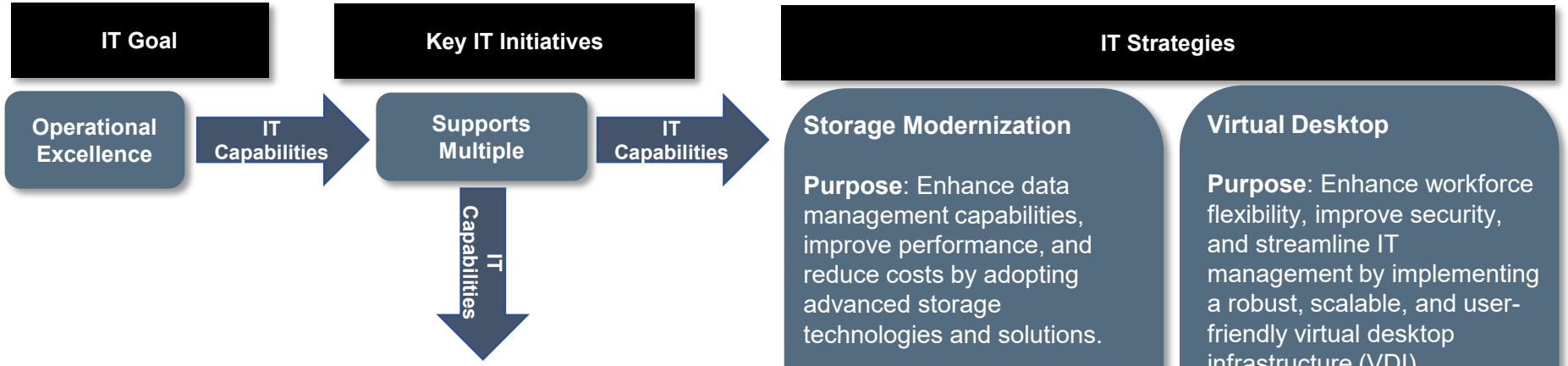
CITIZENS
PROPERTY INSURANCE CORPORATION

Appendix C: Emergency Assessments Related to IT Strategies



Appendices Main

Appendix C: Operational Excellence Related IT Strategies



Storage Modernization

Purpose: Enhance data management capabilities, improve performance, and reduce costs by adopting advanced storage technologies and solutions.

Owner: Sudheer Kondabrolu
Assigned EA: Ben Varnes

Virtual Desktop

Purpose: Enhance workforce flexibility, improve security, and streamline IT management by implementing a robust, scalable, and user-friendly virtual desktop infrastructure (VDI).

Owner: Sudheer Kondabrolu
Assigned EA: Ben Varnes

Network Modernization

Purpose: Enhance connectivity, improve performance, and ensure security by adopting advanced networking technologies and solutions.

Owner: Sudheer Kondabrolu
Assigned EA: Ben Varnes

Backup & Data Protection

Purpose: Ensure the integrity, availability, and security of our critical data by implementing comprehensive backup solutions and robust data protection measures.

Owner: Sudheer Kondabrolu
Assigned EA: Ben Varnes

Artificial Intelligence

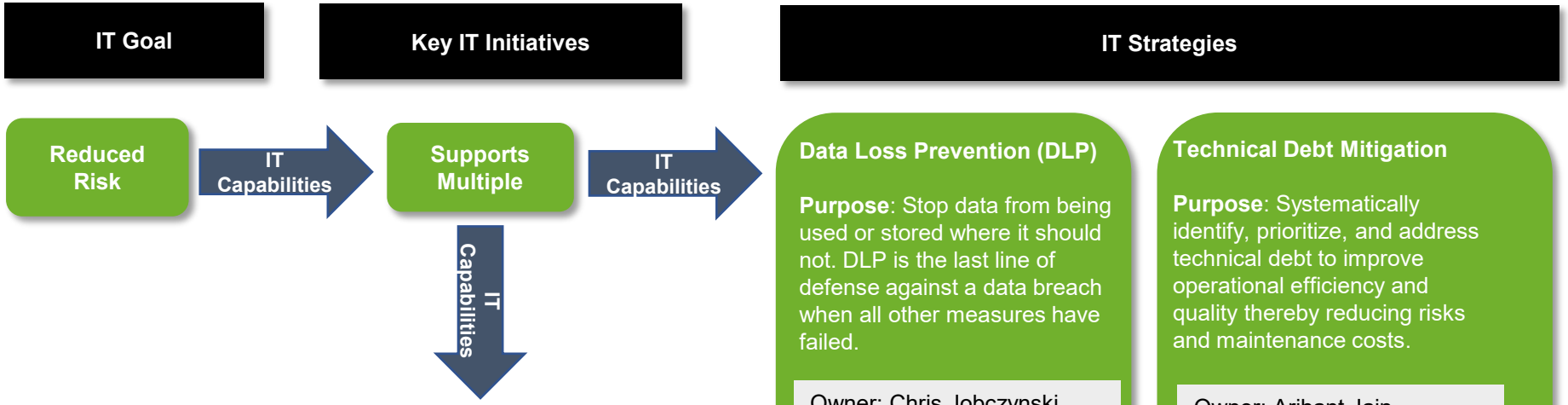
Purpose: A roadmap for integrating AI into an organization's operations, aligning it with broader business goals and automation initiatives.

Owner: Chris Jobczynski
Assigned EA: Mike Barksdale

Appendices Main

CITIZENS
PROPERTY INSURANCE CORPORATION

Appendix C: Reduced Risk Related to IT Strategies



Appendices Main

CITIZENS
PROPERTY INSURANCE CORPORATION

Appendix D: IT Capabilities

Strategic Planning	• IT Governance • IT Management and Policies • Strategic Planning • Performance Management • R&D and Innovation • Stakeholder Relations
People and Resources	• Strategic Communications • People Resource Mgmt. • IT Training • Workforce Strategy Planning • Financial / Budget Mgmt. • IT Knowledge Mgmt.
Architecture and Planning	• Enterprise Arch. • Business Arch. • Solutions Arch. • Technology Arch. • Data Arch. • Security Arch. • Arch. Governance Mgmt. • Implementation Planning
Infrastructure and Operations	• Availability and Capacity Mgmt. • IT Asset Management • IT Asset Deployment • Configuration Mgmt. • Cloud Orchestration • Network & Infr. Mgmt. • Infr. Portfolio Strategy
Service Delivery	• IT Change Mgmt. • Service Desk Mgmt. • Incident Mgmt. • Problem Mgmt. • Service Enhancement • Operations Mgmt. • Release Mgmt.
Application Delivery	• App. Lifecycle Mgmt. • Systems Integration • App. Development. • App. Maintenance • UX • QA/UAT • Intel. Automation Mgmt. • Tech Debt Mgmt. • CI/CD • AI Mgmt.
Data and Business Intelligence	• Analytics & Reporting • Data Quality Mgmt. • Ent. Content Mgmt. • Inform. Governance • Data Strategy • Data Integration • Inform. Lifecycle Mgmt. • Inform Self-Service
Security & Risk	• Security Strategy • Risk Mgmt. • Compliance Mgmt. • Security Mgmt. • Resp/Recovery Mgmt. • Cyber Threat Intel. • Controls & Audit. • Security/Access Admin. • Data Protection • Physical/IT Security

Appendix E: Glossary of Terms

Term	Definition
AI	Artificial Intelligence
API	Application Programming Interface
BI	Business Intelligence
BPO	Business Process Outsourcing
CAT	Catastrophe
CBIS	Citizens Business Insurance Suite
CI/CD	Continuous Integration (CI) and Continuous Delivery (CD)
DLP	Data Loss Prevention
ELMS	Enterprise Litigation Management Solution
IAM / IGA	Identity and Access Management (IAM) and Identity Governance and Administration (IGA)
IPA	Intelligent Process Automation
IoT	Internet of Things
IT	Information Technology
MFA	Multi-factor Authentication
QA / UAT	Quality Assurance (QA) and User Acceptance Testing (UAT)
R&D	Research and Development
RPA	Robotic Process Automation
UCaaS / CCaaS	Unified Communications as a Service (UCaaS) and Contact Center as a Service (CCaaS)
UI	User Interface
UX	User Experience

Appendices Main

CITIZENS
PROPERTY INSURANCE CORPORATION