IT Security and Risk Program Update

Robert Sellers, VP & CTO
Wendy Emanuelson, Director – IT Security & Risk

CITIZENS
PROPERTY INSURANCE CORPORATION

IT Security & Risk
Three Lines of Defense

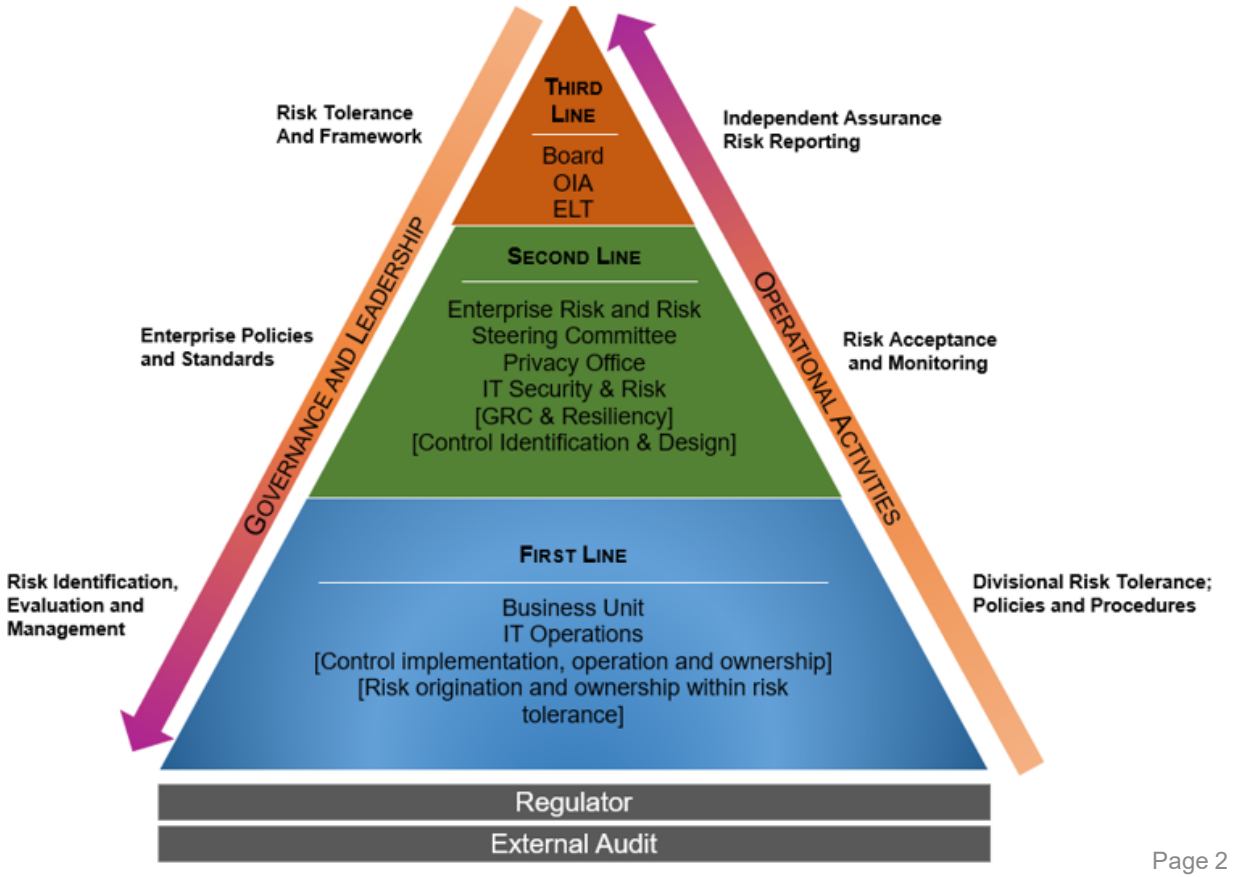
Three Lines of Defense Risk Management Model

See how foundational your cybersecurity individual leadership is in the Three Lines of Defense Risk Management Model

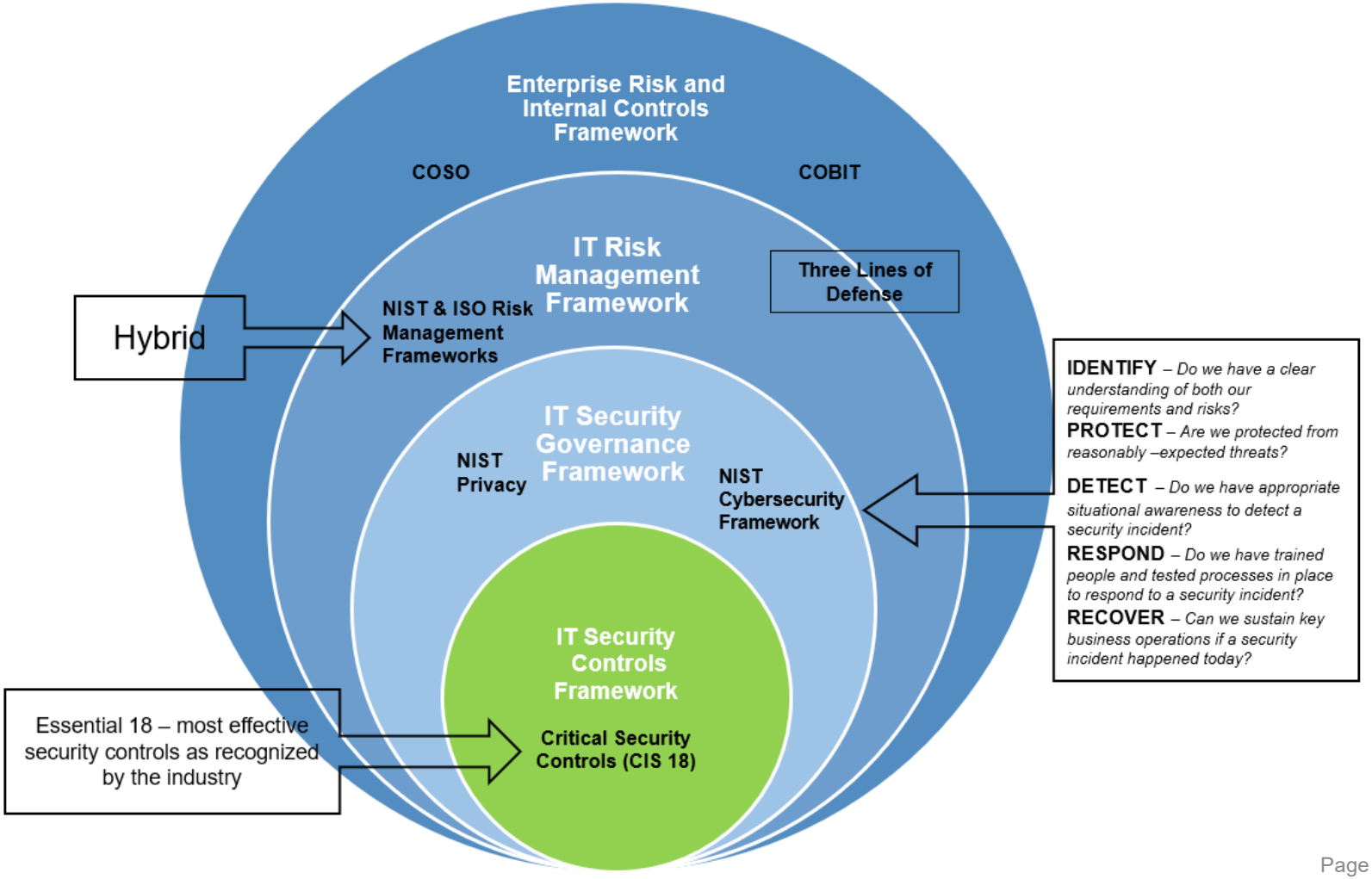
First Line of Defense – Business and IT Operations Management own the security controls and risk. They work closely with the Director of IT Security and Risk and the Director of Enterprise Risk and Controls to implement and maintain effective operational controls.

Second Line of Defense – IT Security and Risk, with close support from Enterprise Risk and Privacy establishes and implements information security vision; program management, enterprise policies, standards and control design; and information security risk management while providing oversight, support, monitoring and reporting of operational controls.

Third Lind of Defense – The office of Internal Audit provides independent and objective assurance. It validates the effectiveness of the operational controls and overall risk management framework while keeping the Executive Leadership Team and Board of Governors informed to make educated IT and security risk management decisions within Citizens' risk tolerance levels



IT Security & Risk
Security and Risk Framework



Mission

Educate, advise, and empower our workforce to make informed cyber-risk decisions and partner with internal and external teams to make Citizens operating environment safe, secure, and resilient.

CITIZENS
PROPERTY INSURANCE CORPORATION

Enterprise Operations, IT Security & Risk Guiding Principles

Mission: *Educate, advise, and empower our workforce to make informed cyber-risk decisions and partner with internal and external teams to make Citizens operating environment safe, secure, and resilient.*

IT Security and Risk Provides Value through the following Guiding Principles

Protect Confidentiality, Integrity and Availability (CIA Triad): Deliver controls that are designed to progressively mitigate risk and protect data.

Partner with Stakeholders: Partner with stakeholders to protect against cybersecurity threats while promoting accountability and risk ownership.

Enable Risk Based Decisions: Provide transparency around cyber security risk to educate and enable risk-based decision making.

Present Options for Risk Treatment: Recommend options for compensating controls and risk treatment to support organizational priorities.

Invest in appropriate resources to balance risk: Align use of investments and resources with organizational needs to properly manage risk.

IT Security & Risk
2019-2022 Accomplishments

Multi-Factor Authentication now required on > 98% of user accounts to use our systems remotely

Local administrators removed from >80% of computers, significantly reducing risk of malware spread

Facilitated closure of over 80% of Exceptions to Policy

Facilitated closure of 97% of open risk gaps related to security controls

Facilitated closure of items related to 16+ audit projects with open items tracked in GRC solution

Consolidated documentation into one high level policy and multiple detailed standards for easier consumption and compliance readiness.

Server patching has been above 90% consistently since moving to monthly cycle

Average of 150 phishing attempts per month, averaging 2-3 user clicks per month.

75+ security reviews completed, including IT Security Standards Assessments (ISSAs), security contract language, etc.

Consulted in 200+ engagements throughout the organization

Phishing reporting increased over 100% following campaigns

Only 8.25% of our staff are "phish prone“ during last quarter

Enterprise Data Incident Response Plan (EDIRP)

Notable Improvements and Accomplishments 2021-22

EDUCATE AND EXERCISE

- Met with Executive leadership to Brief them on the process for responding to ransomware demands (June 2021)
- Successful 2021 Tabletop exercise led by 3rd Party Vendor(October 2021)

ENHANCED PROCESS

Enhanced process for response to third party incidents

- Agency Management Software Incidents (May 2021)
- Print Vendor Incident (June 2022)
- Developed questionnaire for Third Party incident Reports(July 2022)

INTERNAL REVIEW

Internal review to ensure rapid response capabilities for major incidents

- Reviewed agreements with MSSP and Cyber Insurer (May 2021)
- Concluded combination of MSSP capabilities and Cyber Insurer resources provided sufficient early response coverage (July 2022)

PLAN UPDATES

- Ransomware Runbook (June 2021)
- Change in Director of IT security and Risk (April 2022)
- Updated EDIRP Quick Reference Guides (April 2022)

IT Security & Risk
Strategic Objectives

2021 - 2023 Security Strategy Objectives	2022 - 2024 Security Strategy Objectives
Control access and distribution of sensitive data to reduce loss	Control access and distribution of sensitive data to reduce loss
Increase security analysis and protection of CPIC's applications and integrations	Increase security analysis and protection of CPIC's applications and integrations
Advance incident, threat and vulnerability detection, protection and response practices	Optimize IT Security Operations and Architecture Capabilities
Optimize Citizen's cloud security platforms and architecture	
Mature IT governance, risk, & compliance	Mature IT Security Governance, Risk & Compliance
Improve Citizens' cyber risk culture	Improve Citizens' Cyber Risk Culture

Executive Summary
ITSR Strategy on a Page

Citizens One-Page Security & Risk Strategic Plan

ITSR Mission

Educate, advise, and empower our workforce to make informed cyber-risk decisions and partner with internal and external teams to make Citizens operating environment safe, secure, and resilient.

Strategy Rationale (Why?)

Summary

Security & Risk Management encompasses all the ways in which we identify, treat and monitor risk while protecting our information assets and digital platform from malicious intent, thereby safeguarding Citizens' operations, reputation and brand.

Target Customers

Citizens collects, process and stores information assets from policy holders, agents, adjusters and employees. Their information and their trust are a valuable company asset that we are obligated to protect.

Strategic Drivers

- Protect the confidentiality, integrity and availability of data \ systems
- The Rise of Ransomware
- The Age of Cloud Computing
- Advancement of Technology
- Distributed Workforce

Current Security and Risk Challenges

- **Security Culture:** Less than 60% of employees complete security awareness videos and decrease of phishing attempt reporting.
- **Incident and Threat Management:** Expand visibility into our network while reducing noise to allow more efficient and effective response to threats.
- **Access and Data Loss:** Underdeveloped Identity and Access Management (IAM) and Data Leak Protection (DLP) processes and platforms that pose risk.
- **Risk-Based Decision Making:** Opportunity for maturing risk management practices to support decision making.
- **Application Security:** Low visibility of security related vulnerabilities and security logging in our applications.

Strategic Objectives (What?)

Strategic Objectives and Focus Areas
Objective 1: Improve Citizens' Cyber Risk Culture
Objective 2: Control access and distribution of sensitive data to reduce loss
Objective 3: Optimize Security Operations and Architecture Capabilities
Objective 4: Increase security analysis and protection of Citizens' apps and integrations
Objective 5: Mature IT Governance, Risk and Compliance

IT Security and Risk Provides Value through the following Guiding Principles

Strategy Execution Approach (How?)

Risks
Security technology integration with legacy systems may not be possible
Achieving thorough visibility into supply chain partners' security and compliance posture may be challenging
Unexpected changes in the regulatory and threat landscape
Integration of security and monitoring tools with SaaS-based application may not be possible

Assumptions
Citizens leadership will support program and decisions through risk-based data
All areas of IT will support ITSR with implementation, integration and operation some of the security platforms
Activity that rises to enterprise level will be managed through enterprise level governance processes
Current security technology stack may need to be expanded to fulfil program

APPENDIX A
Cybersecurity Terminology

Common Security Cybersecurity Terminology

ACCESS MANAGEMENT (AM): Is the oversight of who can access what resource based on their role and need to know basis.

CIS CONTROLS (CIS Essential 18, Critical Security Controls): The CIS Controls are a prioritized set of Safeguards developed by the Center for Internet Security (CIS) to mitigate the most common cyber-attacks against systems and networks.

COBIT (Control Objectives for Information and Related Technologies): This is an IT management framework developed by the ISACA to help businesses develop, organize and implement strategies around information management and governance.

COSO (The Committee of Sponsoring Organizations of the Treadway Commission): COSO is a joint initiative of five professional organizations and is dedicated to helping organizations improve performance by developing thought leadership that enhances internal control, risk management, governance and fraud deterrence.

DAST TOOL: A Dynamic Analysis Security Testing tool is an application security solution that can help to find certain vulnerabilities in web applications while they are running in production.

DATA LOSS PREVENTION (DLP): DLP refers to software and processes to identify sensitive and to detect and prevent potential data loss/data ex-filtration.

IDENTITY GOVERNANCE AND ADMINISTRATOR (IGA): The continuous management of User IDs and Roles through their lifecycle.

NIST CYBERSECURITY FRAMEWORK (NIST CSF): The NIST CSF Framework consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The Framework was originally designed to foster risk and cybersecurity management communications among both internal and external stakeholders.

Common Security Cybersecurity Terminology

PENETRATION TESTING: This is a security practice where a real-world attack on a subset of an organization's IT ecosystem is simulated in order to discover the security gaps that an attacker could exploit.

RANSOMWARE: Is a form of malware that leverages encryption to hold the operations of an organization hostage in exchange for a ransom payment. In ransomware attacks, an attacker gains access to a victim's data, encrypts it such that the victim can no longer access it, and holds the data hostage unless an extortion payment is made.

RED TEAMs: Red Teams consist of security professionals who are integral to maintaining and improving an organization's security posture. They are "attackers" who deploy ethical hacking methods such as penetration testing to simulate an attack and improve defenses.

RISK-BASED VULNERABILITY MANAGEMENT: This is a process that emphasizes prioritizing the most severe security vulnerabilities and remediating according to the risk that they pose to the organization.

SECURITY INCIDENT: A security incident is a confirmed attempt or actual unauthorized access, use, disclosure, modification, or destruction of information.

TECHNICAL DEBT: What results when development teams or project teams take actions to expedite the delivery of a piece of functionality or project deliverable which later needs to be refactored. Typically, this refers to prioritizing speedy delivery over perfect code, from a cybersecurity perspective it could be in form of security control or feature requiring exception or risk acceptance to be remediated in future.

THREAT: In IT security, a threat is a potential negative action or event facilitated by a vulnerability that results in an unwanted impact to a computer system or application.

VULNERABILITY: Is a weakness or issue within a system, software, or application that could be exploited by a malicious party to gain unauthorized access to an organization.

Enterprise Resiliency Update

Robert Sellers, VP & CTO

CITIZENS
PROPERTY INSURANCE CORPORATION

Enterprise Resiliency

Enterprise Resiliency Program

- Provides the methodology for Citizens to anticipate, absorb, respond to, and mitigate negative impact to the business from unexpected crisis events and business interruptions

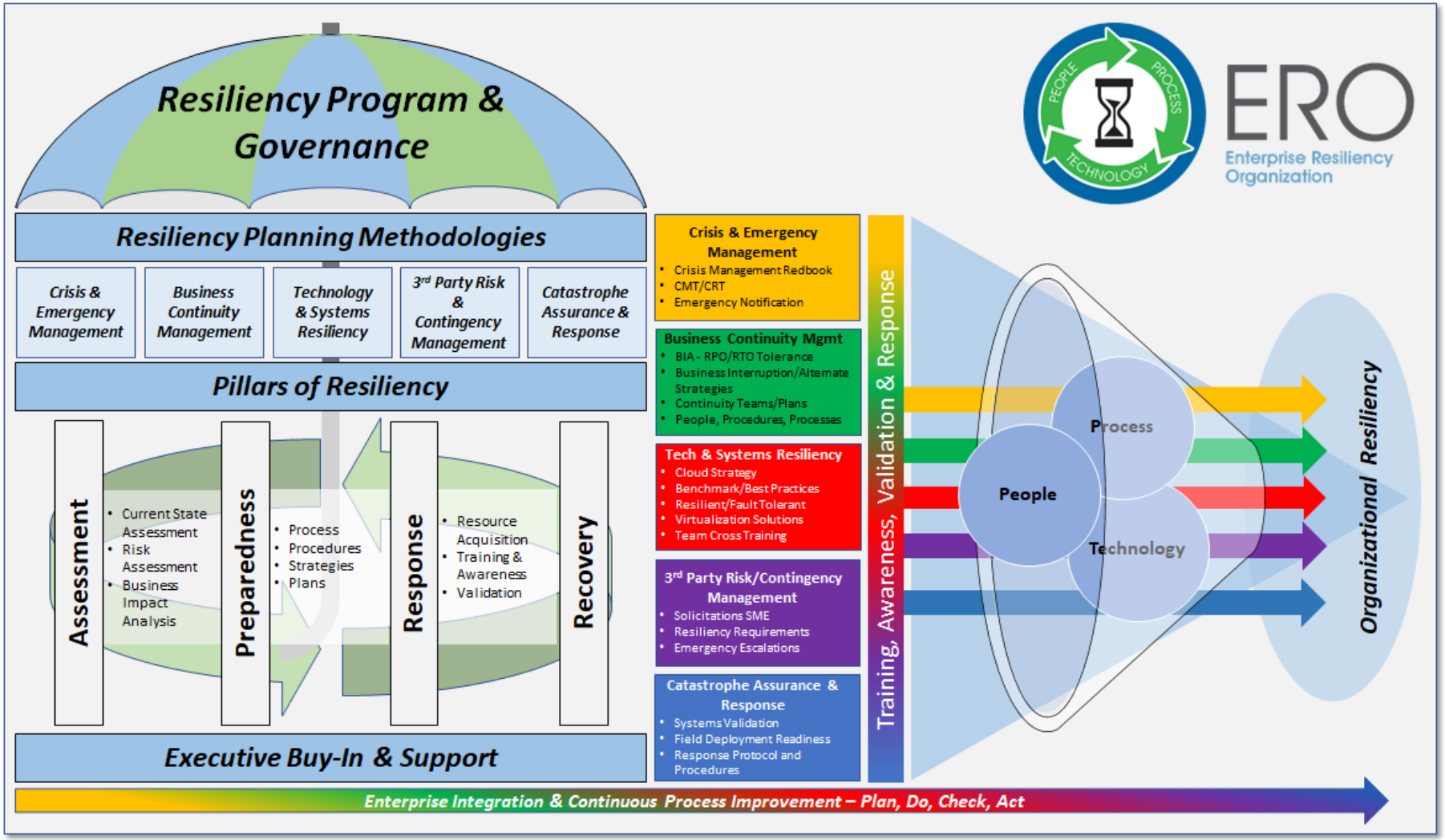
Citizens Business Impact Analysis

- Establishes the scope, requirements and practices for resiliency
- Identifies the people, processes, technology, dependencies and resources
- Analyzes the impact and maximum allowable downtime that is tolerable
- Identifies existing strategies, gaps and risk mitigations to minimize impact

Operational Resilience

- Consists of the specific initiatives that expand business continuity management programs to focus on the impacts, connected risk appetite and tolerance levels for disruption of product or service delivery to internal and external stakeholders (such as employees, customers, citizens and partners).

Enterprise Resiliency Program



Enterprise Resiliency Governance

Program Governance and Activities

Governance

- Information Systems Advisory Committee
- Citizens' Enterprise Risk Management Organization
- Enterprise Resiliency & IT Security Advisory Committee
  - Quarterly meetings ongoing for oversight and support of Enterprise Resiliency and IT Security program activities. Senior leaders and Enterprise Risk representation
- IT Governance Committee and IT Risk Management Committee
  - Monthly meetings with IT leadership and Chief of Enterprise Operations
- Program Updates/Activities 2022-2023
  - Operational Resiliency – Organization and Systems
  - Enterprise Crisis Management Planning & Response
  - Catastrophe Assurance Preparedness and Response
  - Enterprise Business Continuity Planning & Exercises
  - Business Impact Analysis (Q3 through Q4)
  - IT Systems Recovery (DR) and Resiliency Planning & Exercises
  - Support of major system solicitations and new system implementations

Operational Resiliency Risks – PIF Increase

Operational Resiliency PIF Increase Impact Assessment

- PIF increase assessments for four scenarios with 48 teams conducted
- Impacts identified and assessed included People, Process, Internal/ External Systems and Vendors
- Results included ideas and mitigation actions for scalable, flexible and resilient strategies:
  - Increase staff / adjust workforce scheduling
  - Optimize technology / implement automation
  - Expand self-service / improve agent education
  - Improve monitoring / improve systems and business processing
  - Assess and execute service contracts / minimize single points of failure
- Mitigations
  - Citizens has resiliency actions identified and either in progress or already implemented as part of our on-going strategic, themed focus on Scalability and Resiliency for the enterprise

PIF Impacts Assessed – Technology

Impact assessment included Technology risks and defining actions to mitigate

- **Applications** – Current and future platforms
- **Capacity** – Memory, CPU Cycles, Storage, Monitoring Thresholds and Archives
- **Data Protection / Resiliency** – Replication, Backups, Payload Size, and Retention Management
- **Network** – Redundant Routes, Firewall Rules, and Role-Based Access Routing
- **Operations** – Integration Points/Payload, Batch Processing & Scheduling, Logging (Type & Timing), Concurrent Users / Access Management, Output & Uploads, Third-Party Components & Dependencies, Online Processing Inquiries (SIT), Workforce Scheduling, Mobile Support & Deployment / Code Push

Business Continuity Plans

2022 Maintenance Schedule – 18 Continuity Plans

- Claims
- Communications, Legislative & External Affairs
- Consumer Policy Services
- Enterprise Operations (3)
- Financial Services (5)
- Human Resources (3)
- Office of General Counsel (2)
- Office of Internal Audit
- Office of Inspector General

2022 Business Continuity Plan Maintenance Schedule												
Division/Department/Business Unit	**Jan**	**Feb**	**Mar**	**Apr**	**May**	**Jun**	**Jul**	**Aug**	**Sep**	**Oct**	**Nov**	**Dec**
Claims												
Claims												
Communications, Legislative & External Affairs												
Communications, Legislative & External Affairs												
Consumer and Policy Services												
Consumer and Policy Services												
Enterprise Operations												
Agency, Underwriting and Product Development (AUP)												
Enterprise Services & VMAP												
Information Technology												
Financial Services												
Accounting Operations - Jacksonville												
Actuarial Services												
Financial Services - Tallahassee												
Corporate Analytics												
Treasury & Investment												
Human Resources												
Human Resources Division												
Human Resources - Total Rewards												
Facilities Management												
Office of General Counsel												
Claims Legal Counsel												
Legal Services - TLH												
Office of Inspector General												
Office of Inspector General												
Office of Internal Audit												
Office of Internal Audit												

Legend

- Due EoM
- In Process
- Complete

Business Continuity Validation

Business Continuity Exercises

20 Table-top Exercises Scheduled

- 2021 Scenario: Cyber-Security Attack
- 2022 Scenario: Mission Critical System(s) Outage

2022 Business Continuity Exercise Schedule												
Division/Department/Business Unit	**Jan**	**Feb**	**Mar**	**Apr**	**May**	**Jun**	**Jul**	**Aug**	**Sep**	**Oct**	**Nov**	**Dec**
Claims												
Claims												
Communications, Legislative & External Affairs												
Communications, Legislative & External Affairs												
Consumer & Policy Services												
Consumer & Policy Services												
Enterprise Operations												
Agency, Underwriting and Product Management (AUP)												
Enterprise Services & VMAP												
Information Technology												
Financial Services												
Accounting Operations - Jacksonville												
Actuarial Services												
Corporate Analytics												
Financial Services - Tallahassee												
Treasury & Investments												
Human Resources												
Human Resources Division												
Human Resources Total Rewards												
Facilities Management & Real Estate												
Office of General Counsel												
Claims Legal Counsel												
Legal Services TLH												
Office of Inspector General												
Office of Inspector General												
Office of Internal Audit												
Office of Internal Audit												

Legend

- Scheduled
- Complete
- 2021 Deferred/Complete

IT Systems & Business Process Recovery Requirements

IT System & Business Process Criticality

Citizens' Business Impact Analysis process established the system recovery order of all systems, including 33 Mission Critical Systems that must be recovered within 24 hours or less to support Citizens' business units.

Business Recovery Order per Business Process by Division and Criticality

8 – 24 Hours

Claims
- Catastrophe Operations
- Field Operations
- Litigation
- Special Investigation Unit (SIU)
- Vendor Relationship Management
- Adjusters & Quality Assurance

CLEA
- Legislative and Cabinet Affairs
- Media Relations
- Technical Education & Communications
- Digital Communications
- Corporate Communications

Human Resources
- HR Business Partners

Enterprise Operations
- IT Security & Risk
- ITSD – IT Shared Services
- ITSD – IT Operations
- ITSD – IT Infrastructure & Engineering
- ITSD – Information Management
- Vendor Management and Purchasing
- Product Management Systems

1 – 2 Days

Financial Services
- Business Analysis

Human Resources
- Facilities Management

8 – 24 Hours

Consumer & Policy Services
- C&PS Inbound Calls/WFM/Policy Svcs./CIS
- Customer Correspondence (CCT)

Enterprise Operations
- Application Development
- Enterprise Architecture & IT Strategy
- Personal Lines Underwriting Services
- Product Development
- Commercial Lines Underwriting Services
- Vendor Management and Purchasing

Financial Services
- Treasury & Investment
- Corporate Analytics
- Financial Reporting & Accounting
- Actuarial Services

Human Resources
- Total Rewards
- Talent Experience
- Facilities Management/Mail Operations

2 – 3 Days

Financial Services
- Accounting Operations – JAX
- Accounting Operations – TLH
- Budget

Human Resource
- HRIM (HR Information Management)

Enterprise Operations
- Agency & Market Services

3 Days – 1 Week

Human Resource
- Learning & Development

Office of General Counsel
- Records Management
- Privacy
- Legal Services/Insurance

Enterprise Operations
- Strategy, Planning & Continuous Improvement
- Agency & Market Services

1 – 2 Weeks

Office of General Counsel
- Claims Legal Counsel

Enterprise Operations
- Enterprise Services – Quality Improvement

>2 Weeks

Office of General Counsel
- Ethics/Compliance

Office of Inspector General
- OIG – Investigations

Office of Internal Audit
- Internal Audit
- Enterprise Risk
- Internal Controls

Enterprise Operations
- Enterprise Programs

IT Resiliency and Disaster Recovery

IT Resiliency & Disaster Recovery Posture

- Continuous improvement ongoing in new Strategies for Systems and Infrastructure
- Systems Resiliency - Cloud Infrastructure strategy planning and migration ongoing with resiliency testing as part of each migration
- Failover Testing activities
  - Citizens Insurance Suite (CIS), Voluntary, CAIS, External Website, DoX and other supporting systems and infrastructure validated in 2021
  - Bubble testing conducted quarterly to validate Winter Haven (DR) and CSX (production) site infrastructure and systems capability and readiness
  - Pending Exercise – Citizens Website in Q3. CIS in planning for Q4-22/Q1-23
- Continuous unit testing and health checks of new and existing technology
- Monitoring and validating system enhancements for stability and resiliency in support of increasing PIF counts

IT Resiliency Readiness State 2022		
Functional Area	**Components**	**Readiness**
Storage	EMC/Infinidat/Networker/Replication	
Systems Engineering	VM Ware/System Start up/Citrix	
Telephony	Equipment Setup (telephony gear)	
Networking	Routers/Firewalls/VPN	
Data Center Services	Power, Connectivity, Cooling	
Facilities Management (Locations)	Office Space, Power, Connectivity	

CAT Assurance and Response

- Annual Assurance process completed (140 checklist items)
  - Testing of systems under anticipated volumes of claims, new business and other transactions anticipated for CAT volumes identified for 2022 storm season has been completed
- Field Services Readiness
  - Field Service Vehicles, Claims Service Vehicles and Satellite services ready
  - Mock Exercises completed August 2, 2022
- Significant Response Readiness Activities
  - Technical enhancements to support Remote Work capabilities for Independent Adjusters (Citrix, Softphones, Zoom)
  - Virtual Onboarding for Storm Response
  - Catastrophe Response Centers prepared for complying with CDC guidelines
  - Exercises completed to validate Information Technology Support Posture

#	Category/Assurance Item	Category Count	Status Readiness			Percent Ready
			Red	Yellow	Green	
**	Cumulative CAT Prep Assurance Totals/Percentage	140	0	0	140	✓ 100.0%

Enterprise Resiliency Program