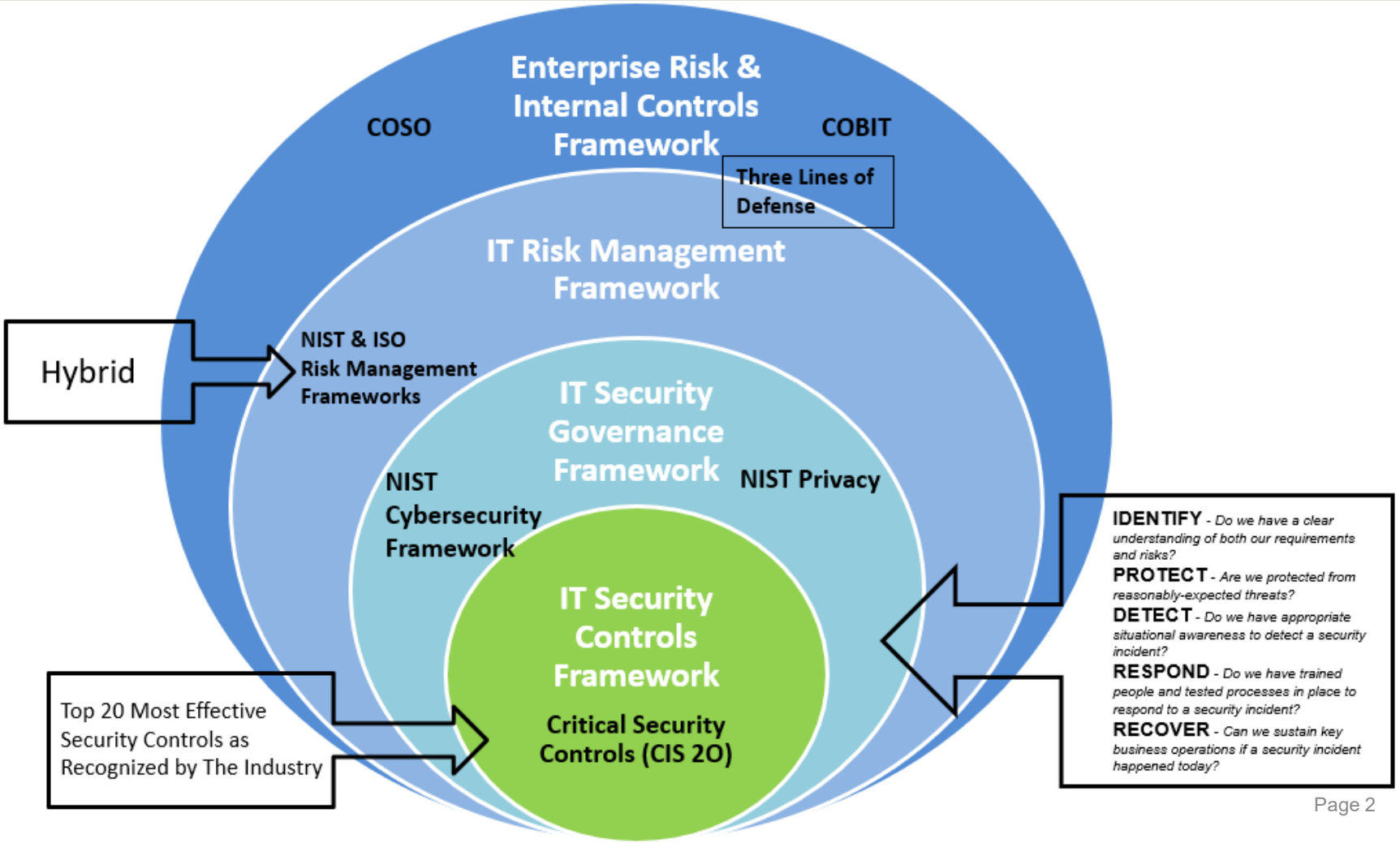
Enterprise Security and Risk Program Update

September 8, 2021

CITIZENS
PROPERTY INSURANCE CORPORATION

Enterprise Security & Risk
Security and Risk Framework

Mission: ***"Educate and empower our workforce to make informed cyber-risk decisions that are supported by proper security controls."***
Vision***: "Maintain cyber hygiene control assurance supported by data to make risk-based decisions and reduce the probability of material impact."***



Enterprise Security & Risk
Three Lines of Defense

Mission: ***"Educate and empower our workforce to make informed cyber-risk decisions that are supported by proper security controls."***
Vision***: "Maintain cyber hygiene control assurance supported by data to make risk-based decisions and reduce the probability of material impact."***

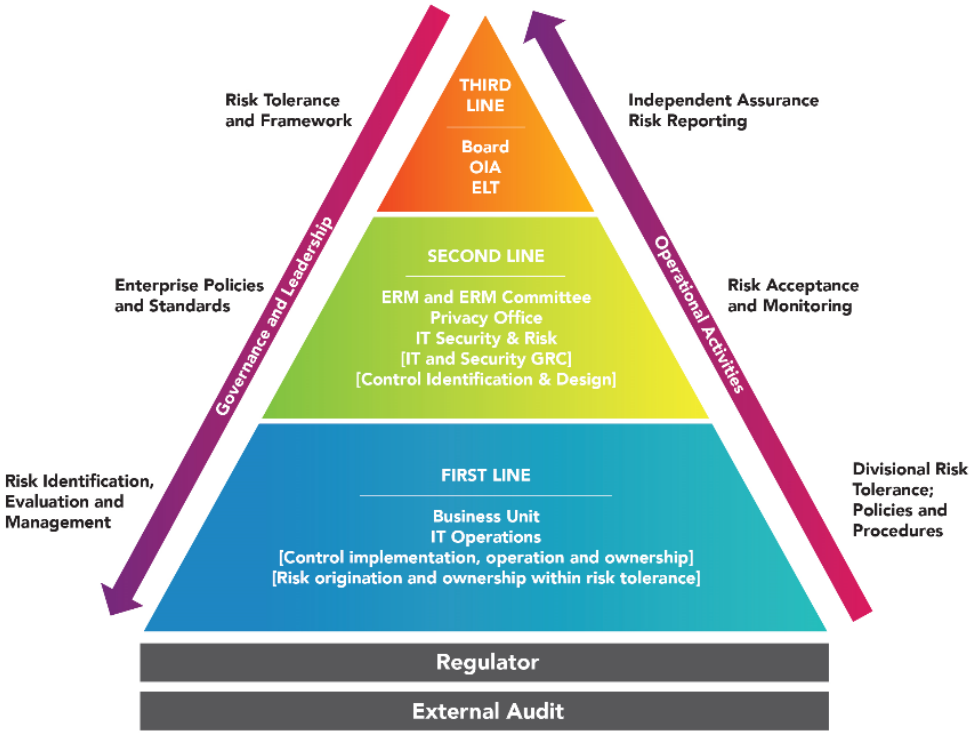
Three Lines of Defense Risk Management Model

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 Enterprise Risk Management (ERM) to implement and maintain effective operational controls.

Second Line of Defense – IT Security and Risk, with close support from ERM 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 Line 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.



Enterprise Security & Risk Strategic Objectives

Mission: ***"Educate and empower our workforce to make informed cyber-risk decisions that are supported by proper security controls."***
Vision***: "Maintain cyber hygiene control assurance supported by data to make risk-based decisions and reduce the probability of material impact."***

Enterprise Security & Risk Three Years Objectives

Objective	Description
Improve Citizens' Cyber Risk Culture	Foster a culture of secure employee behavior through continuous training; awareness campaigns; incident response drills; and by encouraging employees to partner with the security team to reduce risk to the organization.
Control access and distribution of sensitive data to reduce loss	Provide internal and external users, application owners, and IT administrative staff with secure, easy access to applications; solutions that require fewer and increasingly secure login credentials while protecting Citizens' data through our Identity and Access Management; and Data Loss Prevention programs.
Advance incident\threat Detection, Protection, and Response Practices	Manage the security operations, threat, vulnerability and incident response functions by building proper security data analytics platforms and playbooks to mitigate vulnerabilities based on risk while expediting the detection and response to specific threats to Citizens
Increase security analysis and protection of CPIC's apps and integrations	Collaborate across all areas of IT and business units to build processes and security testing platforms that leads to risk mitigation of vulnerabilities and security threats within Citizens' applications code base and integrations.
Mature IT Governance, Risk and Compliance	Mature Citizens' IT GRC program to provide self-service capabilities to the business, empowering risk and controls owners to take control of their risks; promote accountability for unhandled issues; and delivering assurance that controls are performing effectively.
Optimize Citizens' Cloud Security Platforms & Architecture	Continue to deliver controls that are aligned with Citizens' technology architecture and that are designed to progressively mitigate risk and protect the Confidentiality, Integrity and Availability (CIA Tirage) of Citizens' assets and services.

Enterprise and Security Objectives Mapping

Mission: **"*Educate and empower our workforce to make informed cyber-risk decisions that are supported by proper security controls.*"**
Vision: ***"Maintain cyber hygiene control assurance supported by data to make risk-based decisions and reduce the probability of material impact."***

Recommended Ransomware Controls by U.S. Inter-Agency Advisory	Citizens' Security Strategic Objective
Backups	Control Access and Distribution of Sensitive Information Enterprise Resiliency Strategies (DR/BC)
Risk Analysis	Mature IT Governance, Risk & Compliance
Staff Training	Improve Citizens' Cyber Risk Culture
Vulnerability Patching	Advance incident, threat and vulnerability Detection, Protection, and Response practices
Application Whitelisting	Control Access and Distribution of Sensitive Information
Incident Response	Advance incident, threat and vulnerability Detection, Protection, and Response practices
Business Continuity	Enterprise Resiliency Strategies (DR/BC)
Penetration Testing	Advance incident, threat and vulnerability Detection, Protection, and Response practices

- These recommended controls are directly mapped to CIS 20 Critical Security Controls (Citizens' foundational controls framework).
- Analysis show that applying CIS 20 Controls mitigate more than 75% of techniques used in Ransomware attacks.

APPENDIX
Terminology

Common Security Cybersecurity Terminology

Term	Definition
ACCESS MANAGEMENT (AM)	Is the oversight of who can access what resource based on their role and need to know basis.
CIS CONTROLS (CIS 20, 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
CLOUD SECURITY	The strategies and policies used to protect data applications and cloud system apps.
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.
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.
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 stakeholders.
PHISHING	The method of obtaining user information through fraudulent communications targeted directly at individuals.
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	A form of malware used to threaten victims by blocking, publishing, or corrupting their data unless the ransom is paid.
RED TEAMs	They are internal "attackers" part of the security team 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 confirmed attempt or actual unauthorized access, use, disclosure, modification, or destruction of information.
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

September 8, 2021

CITIZENS
PROPERTY INSURANCE CORPORATION

Enterprise Resiliency

What is 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
- The 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

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 34 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 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 Communications
- Corporate Communications

Human Resources
- HR Strategic Services & Communications

Enterprise Operations
- IT Security & Risk
- ITSD – IT Shared Services
- ITSD – IT Operations
- ITSD – IT Infrastructure
- ITSD – Information Management
- Vendor Management Office
- Implementation & Analysis

1 – 2 Days

Financial Services
- Business Analysis

Human Resources
- Facilities Management

8 – 24 Hours

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

Enterprise Operations
- Application Development
- Enterprise Architecture & IT Strategy
- Persona Lines Underwriting Services
- Product Development
- Commercial Lines Underwriting Services

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

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

Legal
- Purchasing

2 – 3 Days

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

Human Resource
- HRIM (HR Information Management)

Enterprise Operations
- Market Services

3 Days – 1 Week

Human Resource
- Learning & Development

Legal
- Records Management
- Privacy
- Legal Services/Insurance

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

1 – 2 Weeks

Legal Services
- Claims & Litigation

Enterprise Operations
- Enterprise Services - Quality Improvement

>2 Weeks

Legal
- Ethics/Compliance

Office of Inspector General
- OIG - Investigations

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

Enterprise Operations
- Enterprise Programs

Enterprise Resiliency Governance

2021 Program Governance and Progress

- Enterprise Resiliency Program is operational with continuous improvements from lessons learned through regular exercises and actual events
- Enterprise Resiliency & IT Security Advisory Committee
  - Quarterly meetings for oversight and support for ongoing resiliency and IT security program activities. Senior leaders and Enterprise Risk representation
- Crisis Management Team Redbook Updates
- Program Updates/Activities
  - Enterprise Resiliency & IT Security Advisory Committee
  - Crisis Management & Response Planning
  - Business Continuity Plans
  - Business Continuity Exercises
  - Resiliency State Assessment
  - Business Impact Analysis (Q3/Q4)

Business Continuity Plans

2021 Maintenance Schedule – 19 Continuity Plans

- Claims
- Communications, Legislative & External Affairs
- Consumer Policy Services
- Enterprise Operations (4)
- Financial Services (5)
- Human Resources (3)
- Legal Services (2)
- Office of Internal Audit
- Office of Inspector General

2021 Business Continuity Plan Maintenance Schedule

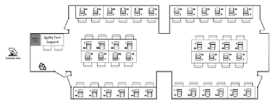
Division/Department/Business Unit	2021 Maintenance Calendar											
	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Claims												
Claims												
Communications, Legislative & External Affairs												
Communications, Legislative & External Affairs												
Consumer and Policy Services												
Consumer & Policy Services												
Enterprise Operations												
Information Technology												
Enterprise Services												
Purchasing												
Underwriting Services												
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												
Legal Services												
Claims Legal Services												
Legal Services TLH												
Office of Inspector General												
Office of Inspector General												
Office of Internal Audit												
Office of Internal Audit												

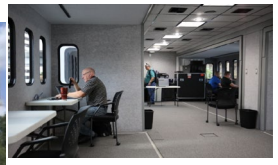
Legend: Complete, In Process, Pending

Business Continuity Validation

Claims Strike Zone Exercise

- ERO and Claims CAT Operations successfully conducted a remote recovery exercise with Agility Recovery Solutions on June 17 & 18
- Achieved objectives expected by Claims which Validated technology capabilities between the CSV and Agility's MRC (Mobile Recovery Center)
- Several Mail Operations alternative processing strategies implemented were validated





Business Continuity Exercises

- 19 Table-top Exercises Scheduled
  - 2021 Scenario: Cyber Security Incident

2021 Proposed Business Continuity Exercise Schedule

	2021 Target Time Frame											
Division/Department/Business Unit	**Jan**	**Feb**	**Mar**	**Apr**	**May**	**Jun**	**Jul**	**Aug**	**Sep**	**Oct**	**Nov**	**Dec**
Claims												
Claims							7/27					
Communications, Legislative & External Affairs												
Communications, Legislative & External Affairs								8/4				
Consumer & Policy Services												
Consumer & Policy Services								8/10				
Enterprise Operations												
Information Technology										10/4		
Enterprise Services								8/4				
Purchasing								8/11				
Underwriting Services									9/13			
Financial Services												
Accounting Operations - Jacksonville								8/25				
Actuarial Services							7/29					
Financial Services - Tallahassee									9/16			
Corporate Analytics								8/11				
Treasury & Investment									9/1			
Human Resources												
Human Resources Division									9/22			
Human Resources Total Rewards									9/29			
Facilities Management							7/1					
Legal Services												
Claims Legal Services		2/4										
Legal Services TLH									9/20			
Office of Internal Auditor												
Office of the Internal Auditor	1/20											
Office of Inspector General												
Office of Inspector General									9/15			

IT Resiliency & Disaster Recovery Posture

- Continuous improvement in DR strategy for technical infrastructure changes/ improvements
- Backup and Recovery / Replication Enhancements ongoing
  - Recovery Time Objectives and Recovery Point Objectives for business requirements per BIA, new/enhanced technology and services
  - Disaster Recovery - Cloud Infrastructure strategy planning in progress
- Failover Tests Completed for 2020
  - Citizens Insurance Suite (CIS) – July 2020
  - Telephony Failover & Survivability – December 2020
  - Business Processes validated at Winter Haven (DR) and CSX (production) sites
- 2021 Ongoing Activities
  - CIS, Voluntary, CAIS, DoX, and Liferay External Exercise completed successfully with OIA observation team (April 2021)
  - Pending Exercise – Telephony Survivability (December 2021)
- Ongoing Unit Testing and health checks of new and existing technology

IT Resiliency Readiness State 2021		
Functional Area	**Components**	**Readiness**
Storage	EMC/Infinidat/Networker/Replication	
Systems Engineering	VM Ware/System Start up/Citrix	
Telecommunications	Telephony Infrastructure	
Networking	Routers/Firewalls/VPN	
Data Center Operations	Power, Connectivity, Cooling	
Citizens Office Locations	Office Space, Power, Connectivity	

Enterprise CAT Assurance and Response

- Annual Assurance process completed (130+ checklist items)
  - Field Service Vehicles, Claims Service Vehicle and Satellite services ready
  - Technology Monitoring ongoing
  - Catastrophe Response Center testing completed
  - Strike Zone capabilities validated with Agility Recovery Solution, Mobile Recovery Center
  - Systems Validated and Ready
- Response Ready, COVID-19
  - Virtual Onboarding for Storm Response
  - Validated Catastrophe Response Centers for CDC guidelines
  - Technical validation of Remote Work capabilities for Independent Adjusters
    - Citrix
    - Softphones
    - Virtual Conferencing

#	Category/Assurance Item	Category Count	Status Readiness			Percent Ready
			Red	Yellow	Green	
**	Cumulative CAT Prep Assurance Totals/Percentage	137	0	2	135	✓ 99%