IT Security, Risk, & Enterprise Resiliency

Program/Strategy Updates

Brian Newman
Chief Legal Officer & General Counsel

Wendy Emanuelson
Director – IT Security & Risk

CITIZENS
PROPERTY INSURANCE CORPORATION

Citizens' Thread Landscape

Evaluating the Threat Landscape

Security is an iterative process – continuously asking and answering these four basic questions

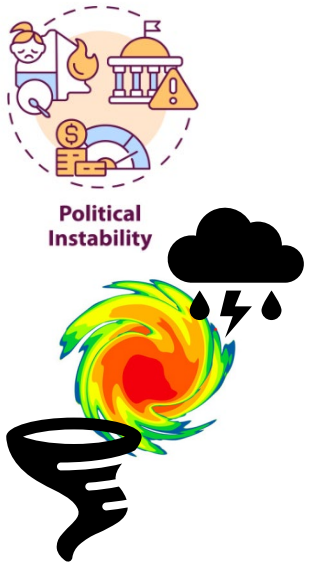
1. What makes us attractive to an attacker?

- Millions of Policyholders
- Large Reserves
- Government Agency / Political Connection
- Information

2. What are we trying to defend against?

- Cyber Criminals
- Insider Threats
- Vulnerabilities
- Vendors / Partners & Contractors

3. What is happening in our world?



4. What do we need to protect?

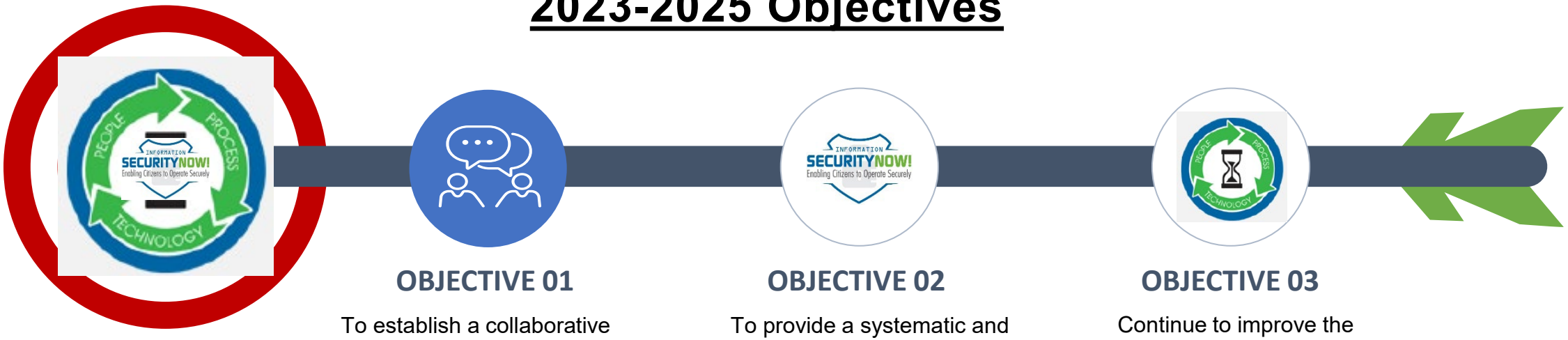
- Physical and Cloud Assets
- Software as a Service
- Data
- Business Operations

IT Security, Risk & Resiliency

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.

2023-2025 Objectives



OBJECTIVE 01

To establish a collaborative environment that leverages the expertise and capabilities of this multifunctional team to develop a comprehensive program that supports Citizen's overall strategy and enhances its resilience.

OBJECTIVE 02

To provide a systematic and proactive approach to identifying, assessing, mitigating, and managing IT risks and threats, while proactively safeguarding Citizens' critical assets and data from potential threats.

OBJECTIVE 03

Continue to improve the organization's resiliency and ability to respond to any unexpected adverse events that may impact the business.

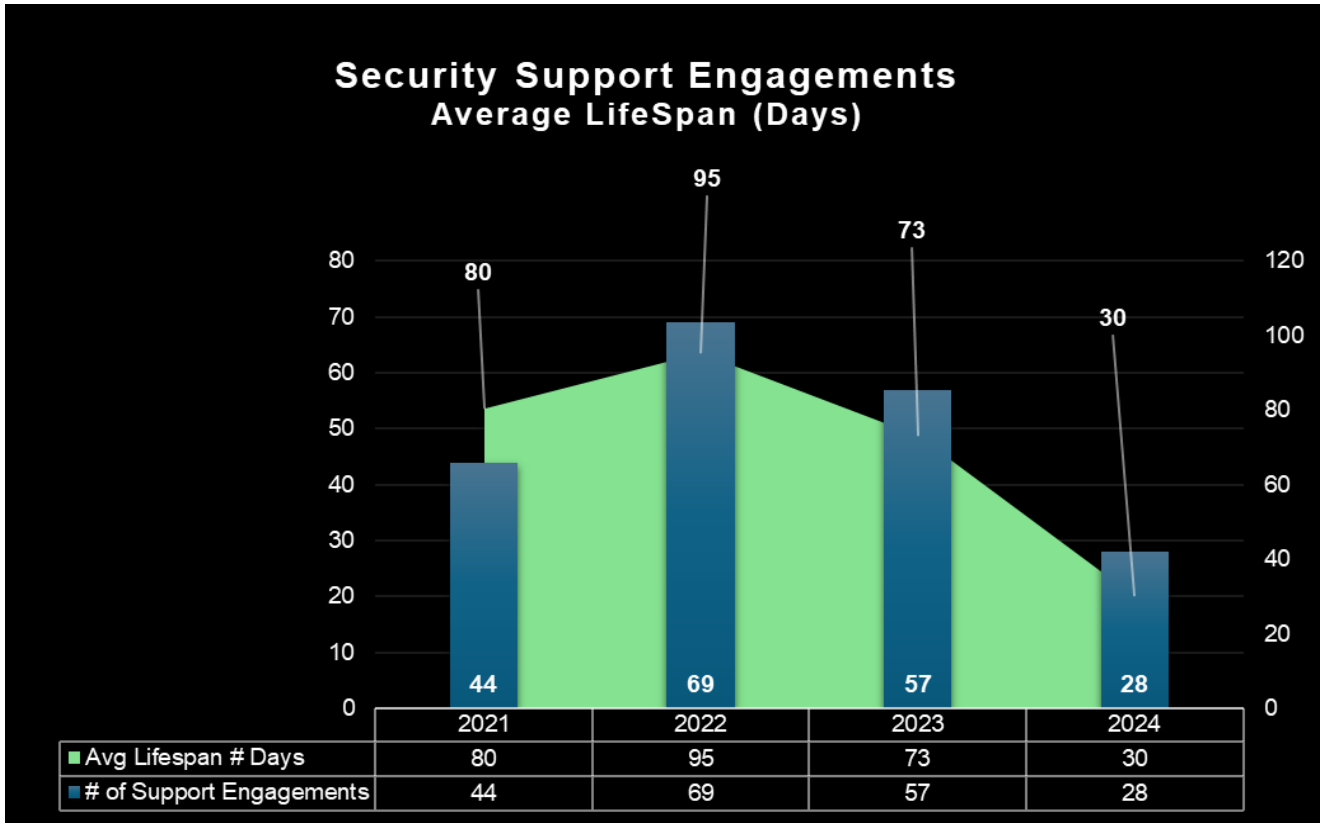
Objective 1

To establish a collaborative environment that leverages the expertise and capabilities of this multifunctional team to develop a comprehensive program that supports Citizen's overall strategy and enhances its resilience.

CITIZENS
PROPERTY INSURANCE CORPORATION

Supporting Secure Operations through Collaboration (KPI)

Objective 1: To establish a collaborative environment that leverages the expertise and capabilities of this multifunctional team to develop a comprehensive program that supports Citizen's overall strategy and enhances its resilience..



58.9% reduction 2023-2024
62.5% reduction 2021-2024

Security Support Engagements include:

- Contract Reviews
- Information Security Standards Assessment**
- PPM/LPM Project Support**
- Project Implementation Support**
- Questionnaire Review
- Resiliency Assessment – New**
- Resiliency Assessment – Follow up
- SOC Report/Complimentary User Entity Control Reviews(CUEC)**
- Solicitation Support**
- Other

***Can have above Average Lifespan and include artifact deliverables that are often used as audit evidence of compliance with governance or regulatory controls.*

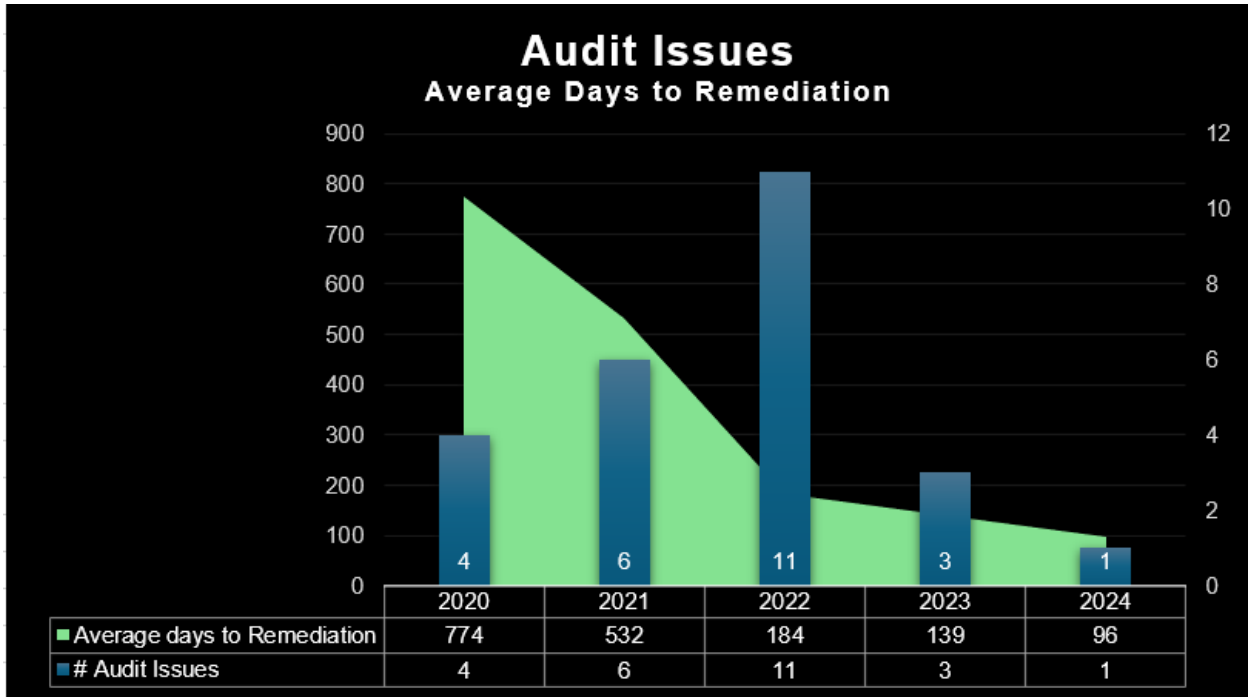
Objective 2

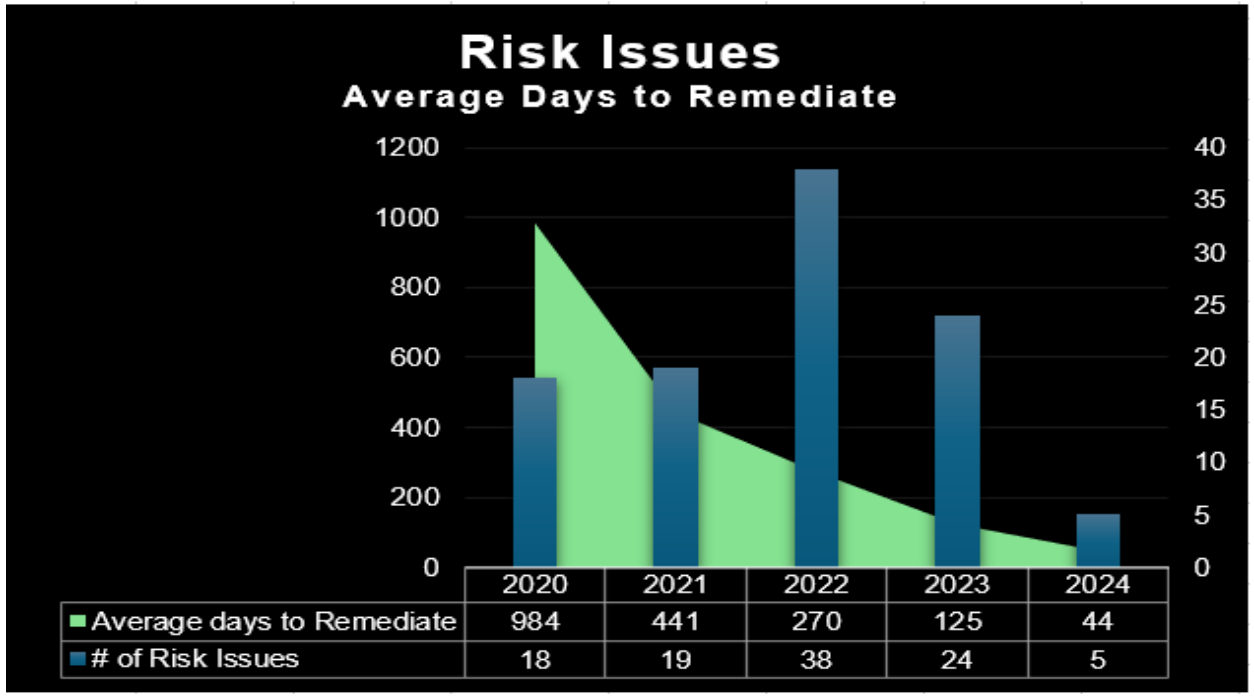
To provide a systematic and proactive approach to identifying, assessing, mitigating, and managing IT risks and threats, while proactively safeguarding Citizens' critical assets and data from potential threats.

CITIZENS
PROPERTY INSURANCE CORPORATION

Key Performance Indicators (KPI)

Objective 2: To provide a systematic and proactive approach to identifying, assessing, mitigating, and managing IT risks and threats, while proactively safeguarding Citizens' critical assets and data from potential threats.



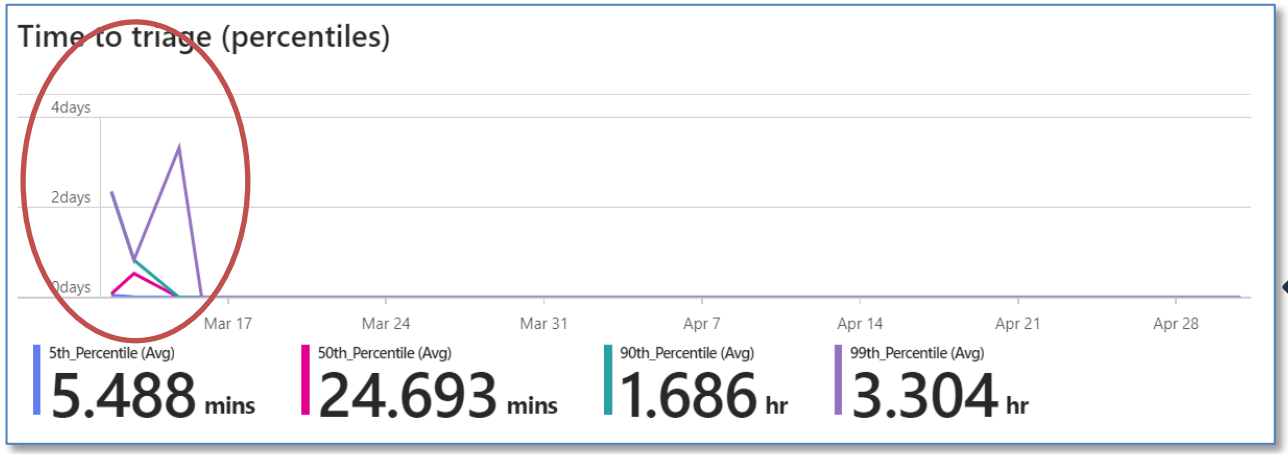


30.9% reduction 2023-2024
87.6% reduction 2020-2024

64.8% reduction 2023-2024
95.5% reduction 2020-2024

Managed Detection and Response Vendor Switch

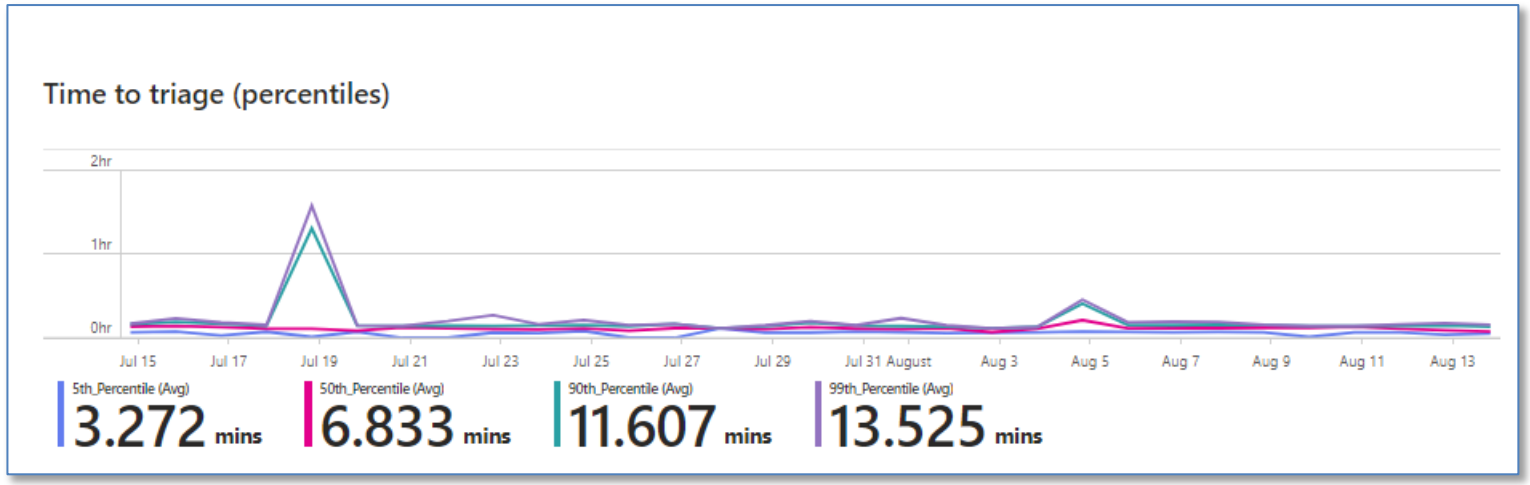
Objective 2: To provide a systematic and proactive approach to identifying, assessing, mitigating, and managing IT risks and threats, while proactively safeguarding Citizens' critical assets and data from potential threats.



Since switching to Ontinue, we've seen a large decrease in response time. Shown is Time to Triage.

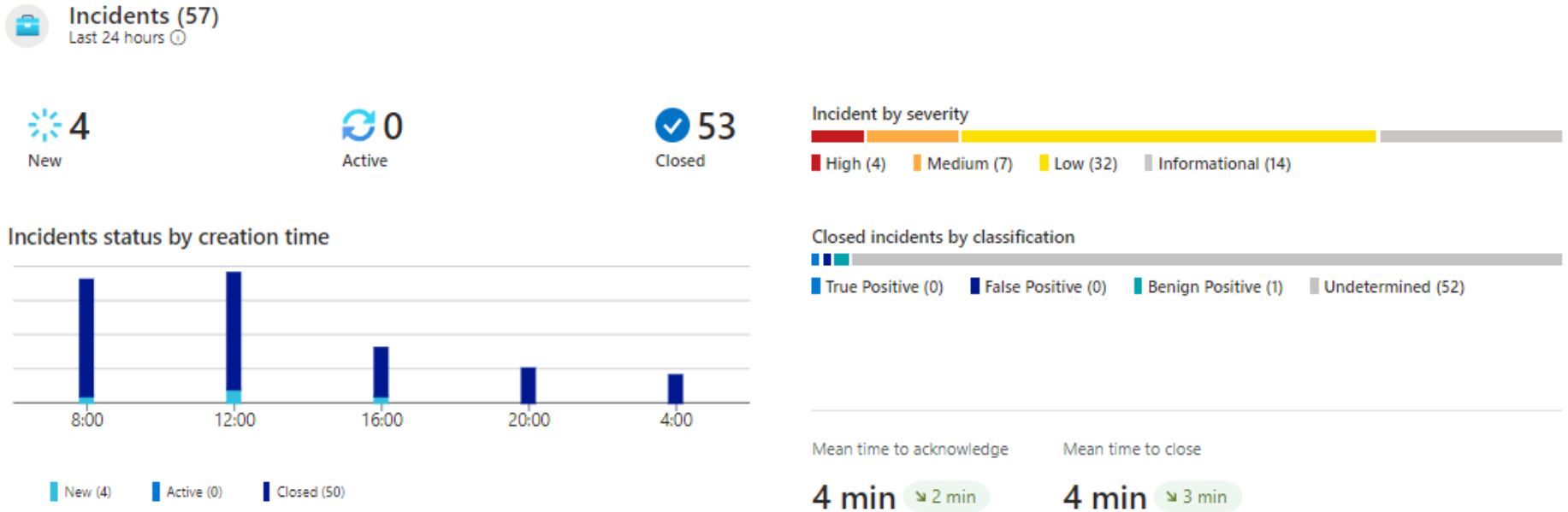
** The graph and numbers at the bottom are heavily skewed by activity prior to the start of Ontinue. It might look like there's no data after Mar 16; it's there, just in minutes instead of days.*

** This is current average Time to triage (percentiles) the difference from days to hours*



Security Information and Event Management (SIEM) System

Objective 2: To provide a systematic and proactive approach to identifying, assessing, mitigating, and managing IT risks and threats, while proactively safeguarding Citizens' critical assets and data from potential threats.

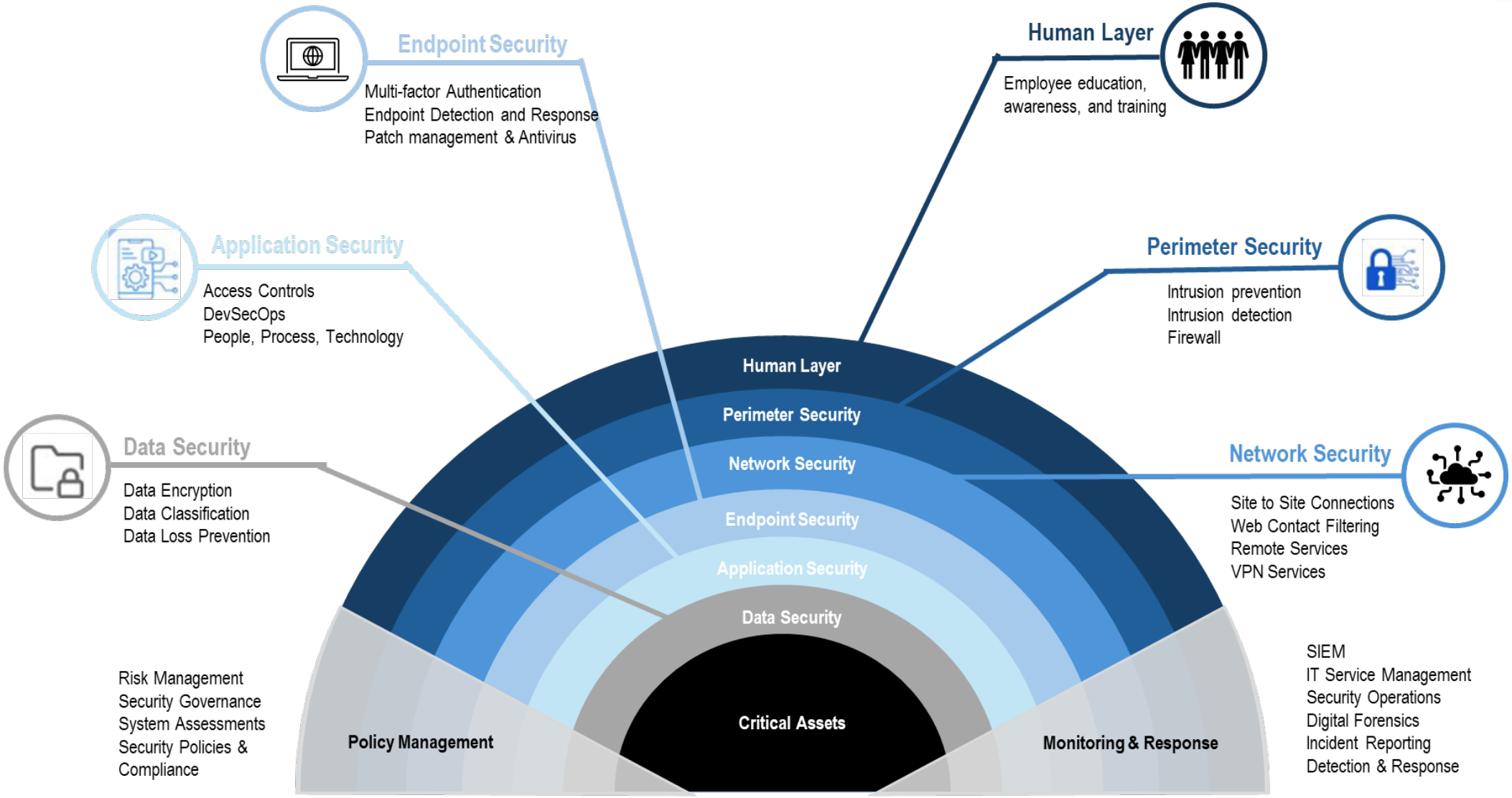


Beyond what you would expect of a capable SIEM tool:

- Monitoring and Alerting
- Log Querying
- Security Operations Metrics

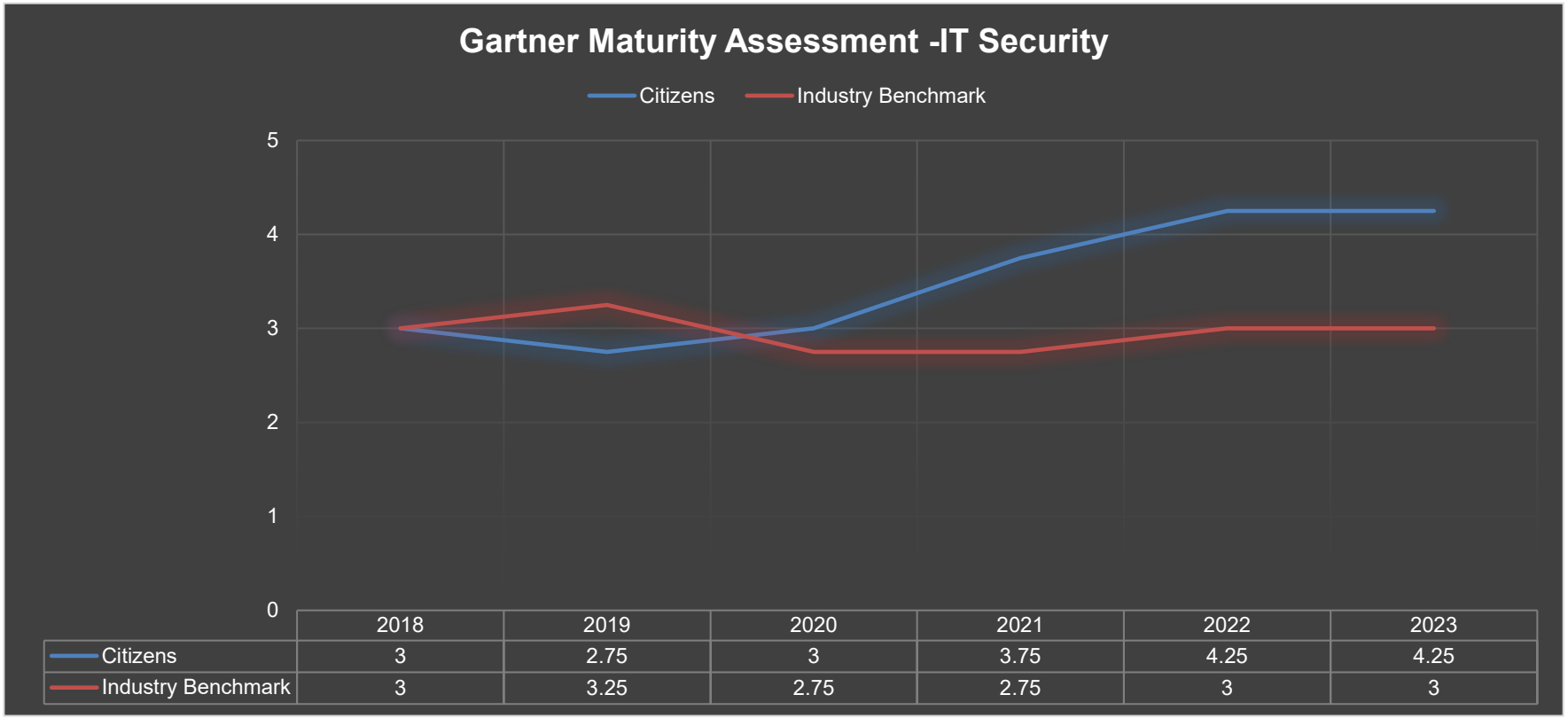
Sentinel also provides seamless integration into all other Microsoft and Azure products allowing for easy pathways into activities we have ongoing such as: Insider Risk, User Behavior Analysis, Data Loss Prevention (DLP), File Integrity Monitoring, Threat Hunting, etc.

Citizens Security Layers



Gartner Annual Security Assessment

Objective 2: To provide a systematic and proactive approach to identifying, assessing, mitigating, and managing IT risks and threats, while proactively safeguarding Citizens' critical assets and data from potential threats.



	2018	2019	2020	2021	2022	2023
Citizens	3	2.75	3	3.75	4.25	4.25
Industry Benchmark	3	3.25	2.75	2.75	3	3

IT Score for Security and Risk Management (SRM) measures performance across seven objectives and 30 key management activities.

See Appendix for a listing of the seven objectives and 30 key management activities that are measured in this assessment.

Objective 3

Continue to improve the organization's resiliency and ability to respond to any unexpected adverse events that may impact the business.

CITIZENS
PROPERTY INSURANCE CORPORATION

Resiliency Planning Lifecycle

Objective 3: Continue to improve the organization's resiliency and ability to respond to any unexpected adverse events that may impact the business

BIA/TIA

Perform Business Impact and Technical Impact assessments to identify criticality of people, processes, and technology, to the business.

BC/DR planning

Based on the criticality determined in the BIA/TIA, develop business continuity and IT disaster recovery plans to meet the recovery objective.

Training

Train staff to ensure they know their role in the recovery of the business process and/or technology and how to perform the tasks.

Exercise

Exercise the BC or DR plan to ensure tasks are accurate and usable while achieving the Recovery Time (RTO) and Recovery Point Objectives (RPO). This can be performed in various ways.

Gap Analysis

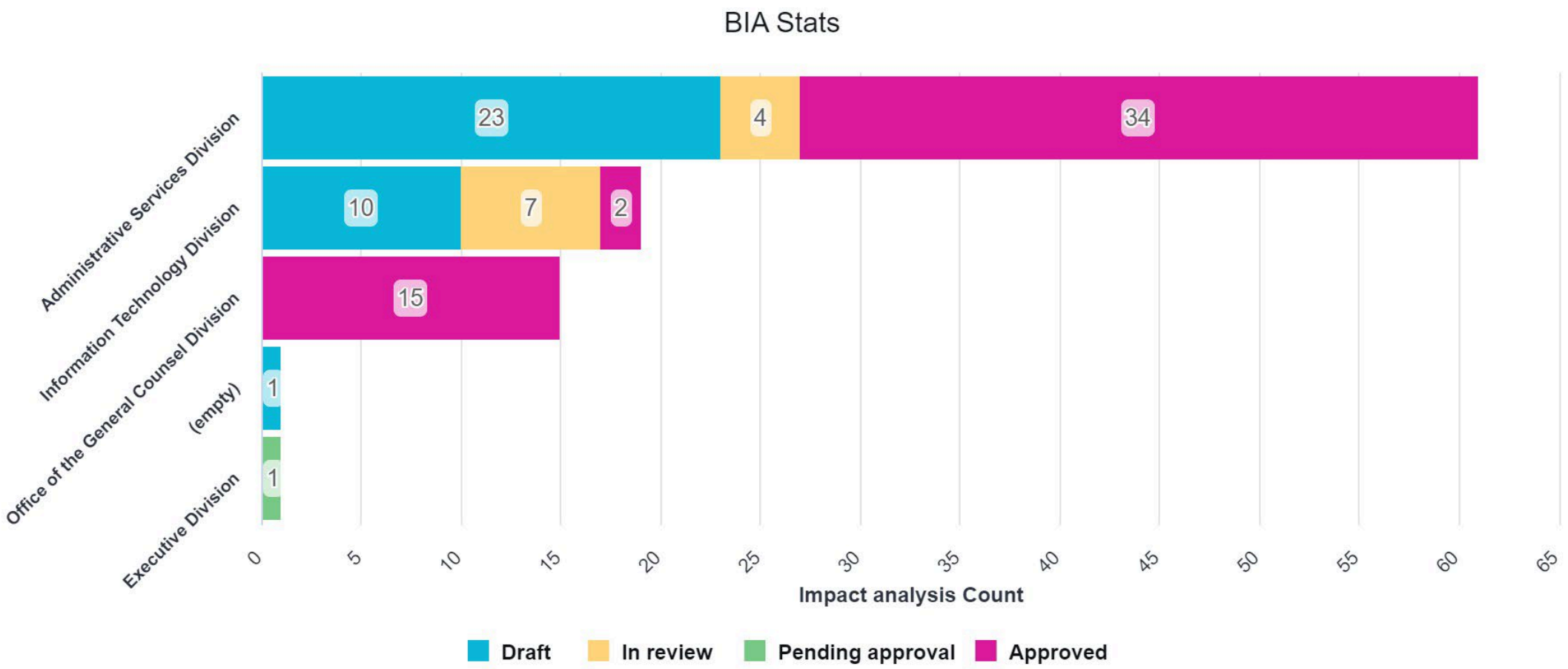
Perform a GAP analysis based on what was the committed RTO and RPO against the actual RTO and RPO.

Update Plans

Develop options, if needed, to the recovery strategy and provide a cost benefit analysis of the options based on the gap analysis and exercise feedback.

Enterprise Resiliency Updates

Objective 3: Continue to improve the organization's resiliency and ability to respond to any unexpected adverse events that may impact the business



Appendix

Citizens One-Page Security, Risk, & Enterprise Resiliency Strategic Plan

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, and Enterprise Resiliency encompasses all the ways in which we identify, treat and monitor risk while protecting our information assets and digital platforms, 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 and frequency of Attacks (i.e., Ransomware, Malware)
- Advancement of Technology (i.e., Cloud, Artificial Intelligence)
- Strengthen Citizens' Resiliency

Current Challenges

- **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.
- **Resiliency:** Influencing a paradigm shift of how Citizens' personnel understand and strategically apply resiliency best practices (to everything they do) to mitigate and minimize the impacts of disruptive events to enterprise business processes and to maintain continuity of operations.

Strategic Objectives (What?)

Strategic Objectives and Focus Areas

Objective 1: To establish a collaborative environment that leverages the expertise and capabilities this multi functional team to develop a comprehensive program that supports Citizen's overall strategy and enhances its resilience.

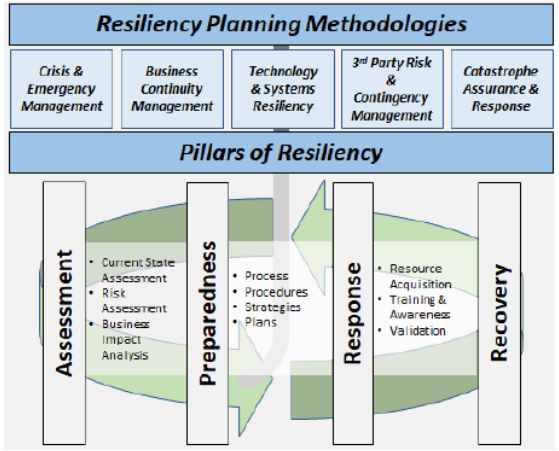
Objective 2: To provide a systematic and proactive approach to identifying, assessing, mitigating, and managing IT risks and threats, while proactively safeguarding Citizens' critical assets and data from potential threats.

Objective 3: Continue to improve the organization's resiliency and ability to respond to any unexpected adverse events that may impact the business.

Strategy Execution Approach (How?)

IT Security & Risk Guiding Principles

- **Protect Confidentiality, Integrity and Availability (CIA Triad):** Deliver controls that are designed to progressively mitigate risk and protect data.
- **Enable Risk Based Decisions:** Provide transparency around cyber security risk to educate and enable risk-based decision making.
- **Partner with Stakeholders:** Partner with stakeholders to protect against cybersecurity threats while promoting accountability and risk ownership.
- **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.



What We Do

Security Operations

- IT Security Operations Communications and Support
- IT Security Network and Systems Event Monitoring
- Threat and Vulnerability Management
- Baseline Compliance Scans
- IT Security Incident Response
- IT Security Awareness and Education
- IT Security Design and Implementation
- Systems Development Life Cycle
- New Software and Firewall Request Analysis
- Subject Matter Expert Support on Citizens' Initiatives
  - Information Security Standards Assessments (ISSA)
- Security Tool Administration
- Citizens Information Security Incident Response Planning

Enterprise Resiliency

- Crisis Management
- Business Continuity
- IT Recovery
  - DR Planning & Exercises
- CAT Assurance and Response
- Business Impact Analysis
- Subject Matter Expert Support on Citizens' Initiatives
  - Resiliency Assessments

Governance, Risk, & Compliance (GRC)

- Citizens IT Risk Identification, Management & Remediation
- Risk Assessment of Citizens' Technology Infrastructure and Applications
- Assist and advise on development of Remediation Plans
- Third Party Risk Management
- Citizens' IT Programs and Functions Regulatory Compliance Review
- IT Controls Evaluation and Improvement
- Audit Entities Liaison Support toward Value-added Audit Outcomes.
- Subject Matter Expert Support on Citizens' Initiatives
  - Information Security Standards Assessments (ISSA)

Application Security Architecture

- IT Security Applications Administration
- Liaison with:
  - Application Development,
  - Systems Analysts,
  - Release Managers, and
  - Enterprise Architects
- Identify, design and apply security controls for applications
- Review Secure Code Practices
- Develop Security Champions

Security Solution Architecture

- Provides technical guidance to IT security teams.
- Primary technical point of contact for complex enterprise projects and provides technical security guidance and solutions.
- Works collaboratively with key stakeholders to design, develop, document and implement security integrated solutions.
- Evaluates process improvements through automation, technical process efficiency using new and existing technology and security controls that benefits the entire enterprise.

Objective 2 Accomplishments

Objective 2: Identifying threats and proactively safeguarding Citizens' critical assets and data from potential threats.

Facilitated closure of 5 findings related to 4 internal audit projects and 4 findings/observations related to 2 external audit projects.

Collaborated with IT groups and other to respond to over 300 requests for evidence and information related to 2 external audit projects.

Moved to an Annual Penetration Testing Model and completed engagements in 2023 and 2024.

Incorporated 3rd Party External Scanning Service to better measure efforts to improve security posture.

Maintained low number of local admins through proactive monitoring, significantly reducing risk of malware spread.

Multi-Factor Authentication (MFA) now required on > 95% of user accounts to use our systems remotely.

YTD Average of 514 phishing reports per month, averaging 8 incidents involving user clicks per month.

Facilitated closure of 52 risk issues related to security controls and penetration test findings.

42 security assessments (ISSA) or resiliency reviews (IRA) completed, 9 contract reviews. 10 Solicitation and project implementation support engagements Completed.

Consulted in 77 engagements throughout the organization.

Refreshed guidelines and guardrails to ensure alignment with business needs by means of updates and enhancements made to over 30 policy, standards and questionnaire documents.

Established Baselines for all Supported Windows OS and process for continuous monitoring of compliance including quarterly reporting to IT leadership.

Maintained at least 93% compliance with monthly server patching and over 88% compliance for workstations.

Gartner Annual Security Assessment

Objective 2: Systematically and proactively identifying, evaluating, mitigating, and managing IT risks.

Engage and Support Stakeholders	Manage the Function	Assess and Manage Risk	Protect the Infrastructure	Manage Operations	Deliver Assurance	Manage People and Workforce Strategy
Interact with CEO and Board	Develop Strategy	Define and Conduct Risk Assessments	Secure Network Edges	Discover and Remediate Vulnerabilities	Support Privacy	Conduct Workforce Planning
Foster Collaborative Risk Relationships	Plan Budget	Develop Controls	Secure the Endpoints	Manage Security Events	Manage Compliance	Recruit Talent
Enable Business Decisions	Organize Structure	Manage Third-Party Risk	Secure Applications	Respond to Security Incidents	Support Audit	Develop Skills
Drive Ownership and Accountability	Design Architecture	Monitor Risks	Secure Data	Identify and Track Threats	Assess Digital Transformation	Manage Behavior and Culture
	Manage Policy					
	Measure Performance					