Identity and Access Management Update

Robert Sellers
VP and CTO

September 10, 2019

CITIZENS
PROPERTY INSURANCE CORPORATION

Identity and Access Management Program Update

The ISAC was briefed in March of 2019 on the 2019 IT Security Strategy. This is a briefing on one of the objectives of the strategy – An improved Citizens' Identity and Access Management (IAM) capability.

- Citizens is implementing an enterprise-wide strategy to consolidate and centralize user identity and access management processes and technology capabilities.
- The Identity and Access Management program commenced in May, utilizing Citizens' Enterprise portfolio and planning processes.
- We have engaged Gartner Consulting Services to conduct a Gap Analysis and to develop with Citizens an IAM Strategy and Program Roadmap to assist us in building a strong foundation for the multi-year IAM program.
- We will implement further organization wide improvements based upon our work with Gartner to better manage user identities and permissions throughout all stages of the user identity and access management lifecycle.
- **Specific improvements already identified by our team have been vetted and are being addressed now and through the remainder of 2019 as part of this program and other IT initiatives such as our Cloud Foundations and Office 365 programs.**

Identity and Access Management Program Update

Program Roadmap:

- Cross functional team is working with Gartner Consulting Services to fully discover and understand the current and proposed Citizens IAM landscape
- Goal – Development of a well-planned IAM Implementation that is tailored to the current and future needs of Citizens
- The successful 12-week session with Gartner Consulting Services from June 27th to September 27th will result in:
  - The evaluation of current IAM governance and provisioning processes
  - The evaluation of existing IAM technology stack
  - The evaluation of existing organizational requirements
  - A Gap analysis report that details the requirements for an improved IAM program
  - Delivery of an improved and validated IAM Strategy
  - Implementation roadmap for a multi-phased IAM program
  - Budget requirements for resources, hardware and software required for rollout during remainder of 2019 and the overall program timeline

Key Objectives of the IAM Program

Business Objectives Driving IAM

Reduce Cybersecurity Risk

- Streamline the provisioning and de-provisioning of users and better manage user and systems identity access privileges to reduce the risk of unauthorized access.

Ensure Regulatory Compliance

- Improve visibility to compliance through better analytic capabilities
- Reduce risk of non-compliance by reducing the number of known risk items. For example, removing manual processing and workflows related to IAM through process automations.

Enhance User Experience and Productivity

- Improve service-levels and business user satisfaction pertaining to on-boarding, off-boarding, and other provisioning requests.
- Avoid delays in users' ability to access the resources they need and have permission to access.

Improve Operational Efficiency

- Remove process inefficiencies such as manual processes and approvals that cause delays in providing user access.

Facilitate Digital Innovation

- Streamline the IAM system to quickly and securely integrate with or implement cloud platforms, applications and other services.

IT Security & Risk Strategic Goals

IT Security & Risk Three Years Goals

Goal	Description
Identity & Access Management Program	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; the ability to collaborate across and beyond CPIC; and improved security and auditing in order to minimize the exposure of Citizens information assets
Incident Response Center	Partner with a Managed Security Services Provider to establish a co-managed Incident Response Center (IRC) that will use a security incident and event manager that combines security information (logs) and security event functions into one security management system for analysis and visualization into the environment
Cloud Security & Privacy Readiness Framework	Develop a Cloud & Privacy Framework that enables the proper level of governance, preparedness, collaboration, deployment, continuous monitoring and proper response to Security, Risk and Compliance threats and requirements
Adopt DevSecOps for Application Security	Collaborate with Service & Delivery to develop a strategy and governance that leads to more secure code design and development which will help teams create secure code and reduce the number of vulnerabilities by building continuous, sustainable and proactive security practices embedded within CPIC's SDLC
Mature Data and System Protection	Data is a valuable asset at Citizens which moves through several states and systems throughout its lifecycle. Accounting for the security of the data during each of these states is a reliable way to ensure the confidentiality, availability and integrity of the data
Third Party IT Security Risk Management	Partners\vendors are a significant source of potential security risk, to which Citizens has the responsibility to ensure that vendors are managed and operating at the same level of security standards as our company does. We achieve this by adopting a Third-Party Security Minimum Requirements Standard for vendors
IT Governance, Risk and Compliance Program	Mature Citizens' IT GRC program to break silos and build processes by providing a clear, integrated process and a single point of reference for the organization. The program will provide a "single version of the truth" available to employees, management, auditors and regulatory bodies
Develop T-Shaped Cybersecurity & Risk Professionals	Grow T-Shaped professionals that are Equipped and Empowered to continuously Evolve and adapt as the fields of Technology and Cybersecurity as well as CPIC needs change, leading to more efficient Cyber Risk Identification and Treatment by engaging all nine divisions through proper venues and Citizens' processes