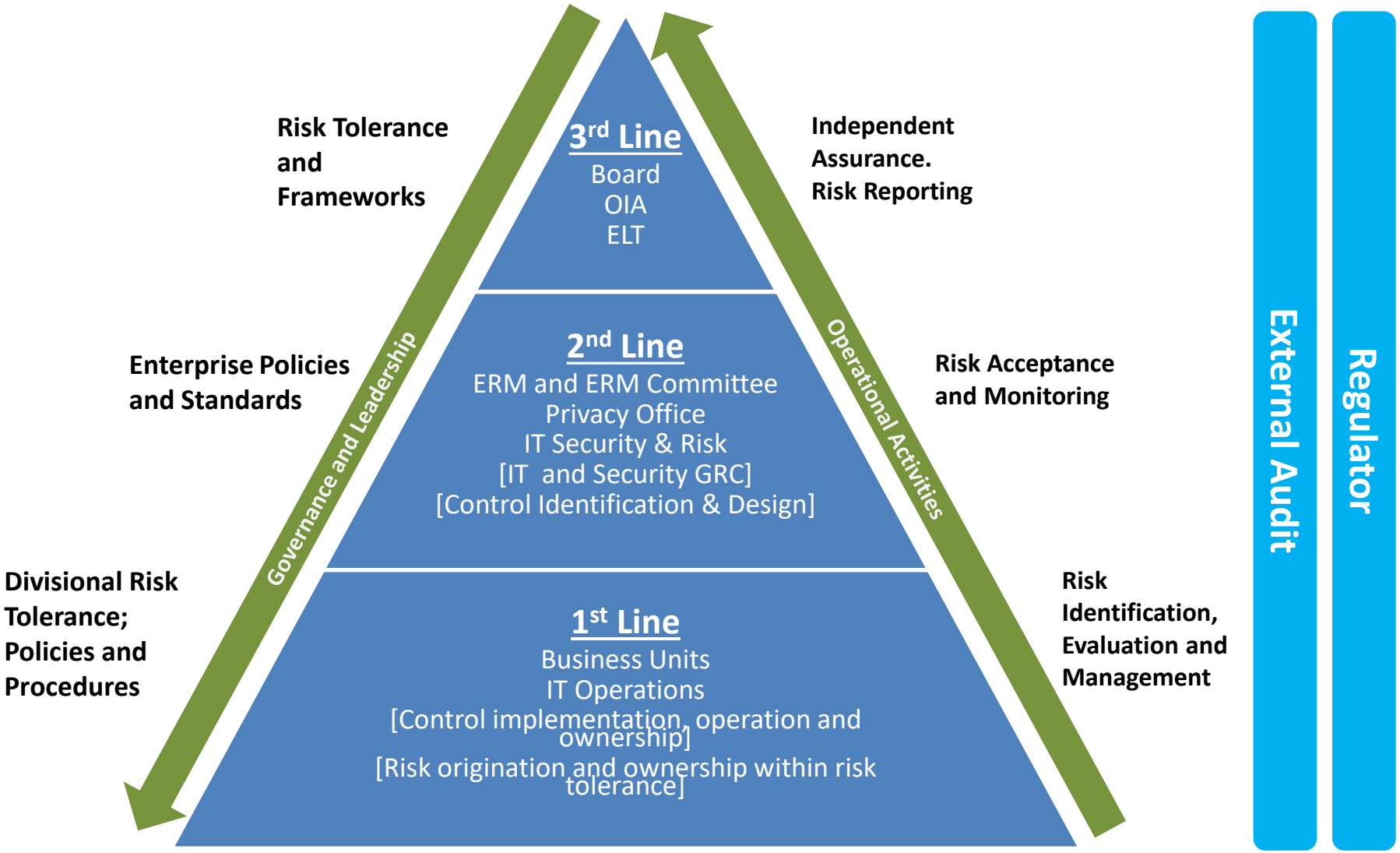
Security Strategy Update

Robert Sellers
VP and CTO

March 12, 2019

CITIZENS
PROPERTY INSURANCE CORPORATION

IT Security & Risk
The Three Lines of Defense



IT Security & Risk Strategy Update

IT Security and Risk Position Statement

The IT Security & Risk department purpose is to **influence and support** all Citizens' business units, so they can produce desired business outcomes successfully without taking on undue technology and cybersecurity risk.

Background information on activities related to 2019 IT Security Strategy update

- Initiated the planned IT security strategy plan revision process in 3rd Qtr. 2018.
- Developed Strategy has been brought through appropriate IT governance processes for review and acceptance by senior IT leadership and the CIO. Citizens' Senior Leadership, including the ELT level IT Steering Committee (ITSC) have been briefed on the updated 2019 IT Security Strategy and key IT Security projects and roadmaps.
- Prioritized IT Security Program and Project activities have commenced, utilizing Citizens' Enterprise portfolio and planning processes.

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

Identity & Access Management Vision

The ideal Identity and Access Management solution will provide Citizens with process and technology capabilities that enables internal and external users, application owners, and IT administrative staff with:

- **Secure, easier access to applications;**
- **Solutions that require fewer and more secure login credentials;**
- **The ability to collaborate across and beyond Citizens';**
- **Improved identity governance, security and auditing in order to minimize the exposure of Citizens information assets.**

As a result, security risk to Citizens will be reduced by providing the right access, to the right people in a consistent and quick manner.

2 Year Program Roadmap with multiple, phased deliverables

Key Objectives of the IAM Initiative and 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.