Citizens IT Risk & Security

IT Security Management - Overview

ISAC & Executive Leadership Team Meetings

Mitch Brockbank, Director – IT Risk & Security
Robert Sellers, VP/CTO

CITIZENS
PROPERTY INSURANCE CORPORATION

Comprehensive Validation & Assurance of the IT Security Program

Continuous Independent Audit:

- Auditor General (2015),
- Market Conduct (Office of Insurance Regulation-2016),
- Financial Statements (Dixon Hughes Goddman-2016)
- Internal Audits and Advisories (Office of Internal Audit-Continuous).

Identified issues are quickly corrected via formal risk mitigation programs.

Continuous Risk Management:

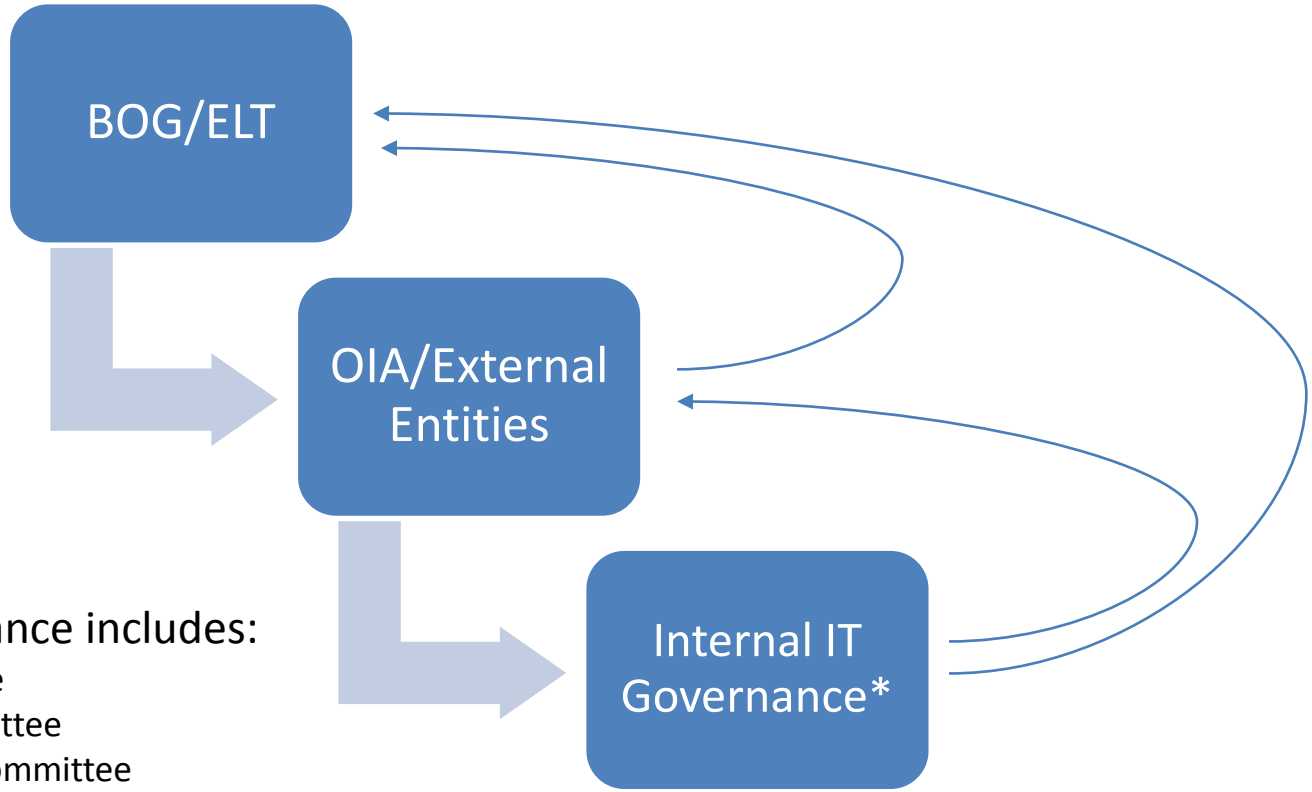
- 3rd Party External Vulnerability Scans (Qualys Corporation - Completed Monthly)
- 3rd Party External Penetration Tests (2015 Completed, Mid-2017 planned)
- Internal Security Team – (Continuous Operational Activities)
    - Internal Technology Vulnerability Scans and Monitoring
    - Internal and External System and Technology Risk Assessments

Benchmarking:

- Gartner ITScore – Information Security (2016 and 2017 Completed)
- FFIEC* Cybersecurity Benchmark (New Initiative)

*FFIEC = Federal Financial Institutions Examination Council

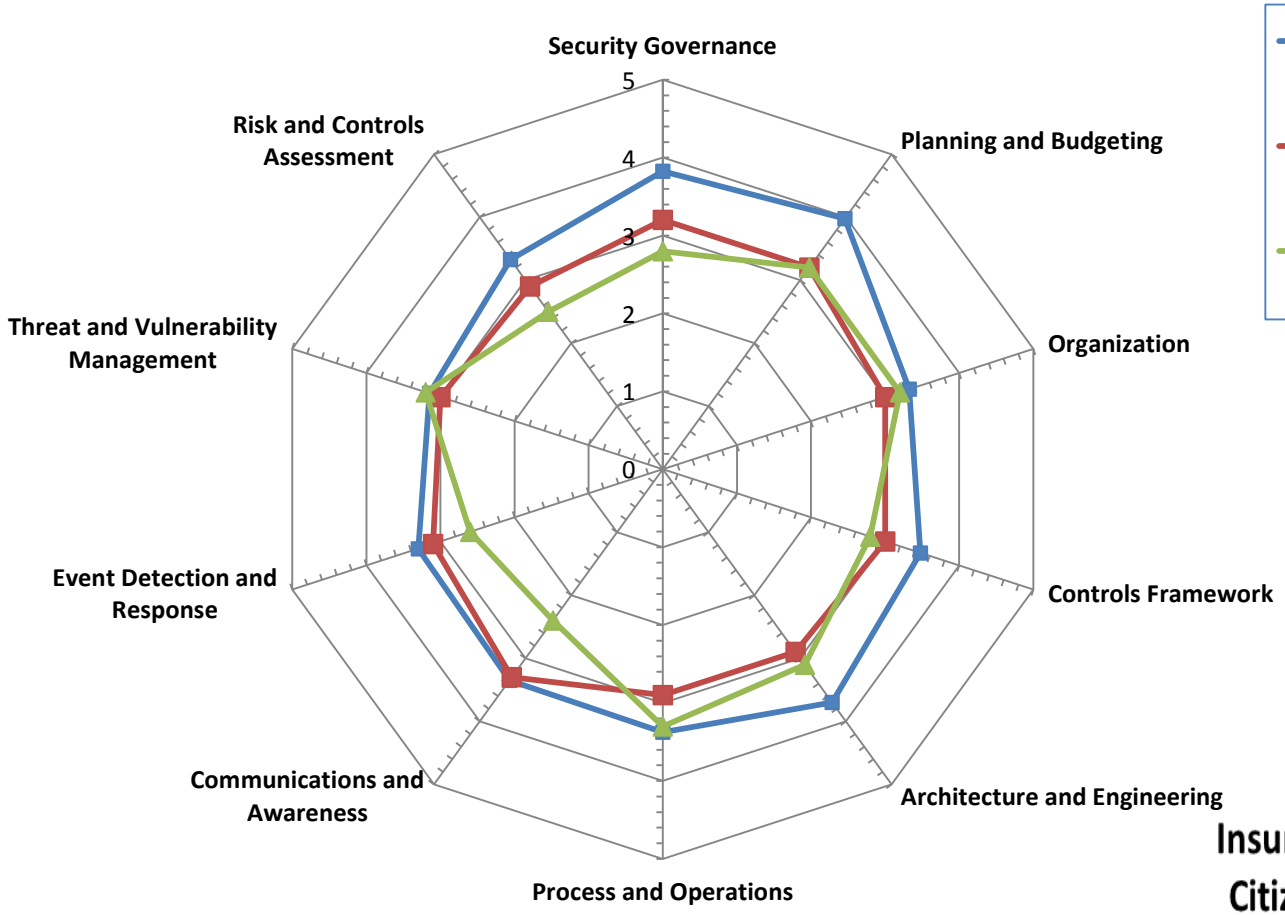
Governance/Oversight– Feedback Loops



*Internal IT Governance includes:

- IT Steering Committee
- IT Governance Committee
- IT Systems Security Committee
- IT Operational standards and processes

Gartner ITScore - Information Security



Insurance Benchmark = 3.0

Citizens' AVG (7/16) = 2.9

Citizens' Current AVG = 3.5

Gartner ITScore for Information Security

Benchmarks – IT Security Staff

Staff

IT Security – 13 FTE (+ 4 partial staff within other departments with specific security responsibilities)

Percent of IT – 7.4%

Benchmark* – 7.1%

IT Security Team

>30 professional Security certifications

>100 years combined Security experience

*Gartner "IT Key Metrics Data 2017: Key IT Security Measures: by Industry"

Current IT Security Program/Activities

IT Security Strategy* (3 year plan)

Defined Information Security Management Program
Annual Activities (Approved by Citizens IT Security Steering Committee)

- Risk Assessments of Systems, Technologies and Processes
- Compliance Assessments
- Security Awareness Programs
- External Penetration Testing of Systems and Technology
- Internal Vulnerability Scans and Monitoring Programs
- Program Governance
- Benchmarking
- Annual Review/Planning (Continuous Improvement
  - Based on a Plan, Do, Check, Act (PDCA) Methodology

Credentialing – AIM project, Team Initiatives 2016-17

- Focus on user access and credentialing improvements across Citizens Systems

IT Security Risk Assessment Activities

Enterprise and IT Department Programs

- Risk Assessments and Project/Systems Consulting

Industry and Citizens Specific Information Security Threats - Identification and Management

- Assessments
- Citizens IT and Organization Risk Tolerance Levels
- IT Risk Heat Map
- Risk Mitigations Activities – time based and appropriate levels based on risk levels

Citizens' Critical Security Controls Risk & Compliance Initiative (Underway)

- Identifying Citizens' 20 Critical Security Controls based on *"Best Practices"* (Center for Internet Security - Critical Security Controls)
- Perform Gap Analysis/Prioritization and Activity Assignments
- Track Remediation Efforts

Other IT Security Assessments in Flight

- Federal Financial Institutions Examination Council – Cybersecurity Assessment Tool Benchmark (New Initiative)

Program Successes/Outcomes

- Cross-Functional IT Systems Security Committee in place and providing regular guidance and prioritization. (IT Security Team re-staffed after significant Jacksonville consolidation turnover)

- Increased Organizational Maturity in IT Security
  - Currently Above Industry Benchmark (Gartner ITScore)

- Ongoing Awareness/Alert Messages
  - Regular Security Now! Blasts – Weekly
  - Privacy Notifications
  - Annual and on-demand Training Programs
  - Employee Recommendations – example - Password Reset Process Improvements

- Very Low Malware/Phishing/Ransomware Impacts
  - Attributed to increased awareness and system detection/prevention.

- Integrated Security consulting activities with Enterprise and Departmental initiatives and projects
  - Primary Goal is to identify and mitigate security risks early.

- Enterprise Data Incident Response Plan – Exercised in 2016 and a 2017 Exercise Planned.

Assuring Continued Success of IT Security

- Board awareness and support.
- Executive engagement on IT Security and Risk Initiatives.
- Well defined IT Security Strategy and IT Security Operational Plan with an agreed upon and communicated implementation plan.
- Complementary Internal Organizational Partnerships/Initiatives (Compliance Champion Network, Internal Audit – Management Advisories, Privacy Program, Vendor Management Office – Claims IA Program, Agency Management).
- Ongoing Independent Audits and Internal Controls Framework.
- External Engagement/Awareness – Financial Services-Information Sharing and Analysis Center, JAX Cybersecurity Council, Infragard, ISACA.
- Elevated Internal Staff Engagement and Awareness of Information Security and Privacy Requirements and Responsibilities

Recent Events of 5/12/2017 through 5/15/2017 – Global Ransomware

On Friday, 5/12/2017, reports in the news media and in security forums from around the world indicated a new attack (Ransomware) impacting thousands of organizations.

This incident and associated attack methodology resulted in computer systems around the world becoming infected and encrypting an organizations data. Access to the compromised data can only be accomplished through either payment of the "ransom" or restoration of data from backups, if available.

Impact to Citizens Property Insurance Corporation.

- **Citizens' alerting processes notified the appropriate IT security staff and IT management of the event, at which time staff began a standard re-assessment of our preventative posture and defenses in depth that are in place for this particular type of attack.**

Citizens primary preventative methods for this particular event included:

- **Regular system patching activity for Citizens technology equipment and software.**
  - **This specific vulnerability was previously patched at Citizens in March 2017 during routine patching activities. Additional patches provided by Microsoft on Saturday for this particular vulnerability for older system were immediately applied in our environment.**
- **Endpoint (PC's, Servers, Networks) Anti-malware protection, scanning and alerting processes and procedures.**
- **External and internal email protection systems.**
- **Organizational security awareness training and continuing staff education regarding these types of threats and appropriate behaviors.**
- **Regular system and file backup processes for recovery purposes, if required.**

As of this time, Citizens has not experienced any negative impacts from this event.