CONVERSATIONS
WITH THE ST. LOUIS FED

FEDERAL RESERVE BANK of ST. LOUIS
CENTRAL TO AMERICA'S ECONOMY®

May 14, 2018

1:30PM to 2:30PM CST

In Plain English:
Cybersecurity and IT Exam Expectations

Options to Join

Webinar and audio

- Click on the link: https://www.webcaster4.com/Webcast/Page/584/24606
- Choose to listen with your PC speakers

Webinar and phone

- Click on the link: https://www.webcaster4.com/Webcast/Page/584/24606
- Choose to listen with your phone
- Call in number: 888-625-5230
- Enter the participant code: 4229 1332#

Phone only

- Call in number: 888-625-5230
- Enter the participant code: 4229 1332#

Questions

- During the call, you can submit questions several ways.
  - **Via webinar chat:** You can submit a question via the **Ask Question** button in the webinar tool. Your question will only be seen by our presenters.
  - **Via email:** conversations@stls.frb.org.

CONVERSATIONS
WITH THE ST. LOUIS FED
FEDERAL RESERVE BANK of ST. LOUIS
CENTRAL TO AMERICA'S ECONOMY®

Todays Presenters

- **Allen North**
  Assistant Vice President
  Federal Reserve Bank of St. Louis

- **Matthew Case**
  Senior Examiner
  Federal Reserve Bank of St. Louis

- **Carey Sharp**
  Senior Examiner
  Federal Reserve Bank of St. Louis

CONVERSATIONS
WITH THE ST. LOUIS FED

FEDERAL RESERVE BANK of ST. LOUIS
CENTRAL TO AMERICA'S ECONOMY®

Disclaimer

The opinions expressed in the presentations are intended for informational purposes, and are not formal opinions of, nor binding on the Federal Reserve Bank of St. Louis or the Board of Governors of the Federal Reserve System.

What do we mean by Cybersecurity Posture?

- This term refers to the overall **cybersecurity strength** of an organization. We consider the *security status of the entire Information Technology (IT) "estate,"* with a primary focus on cyber risks.

- According to the National Institute of Standards and Technology (NIST), the cybersecurity posture of the organization is the *security status* of an enterprise's networks, information, and systems based on information assurance resources (e.g., people, hardware, software, policies) and capabilities in place to manage the defense of the enterprise and to react as the situation changes.

Educating the Board

It is often difficult to determine how to best educate a bank's board of directors about the bank's **network security**.

- Are the branch's front doors locked? That's easy to see.
- Are the network connections secure? That's harder to determine, especially for less technically-experienced individuals.

However, there is a way to do this in a manner that is both effective in measurement and communication.

This is done by determining the **cybersecurity posture of the bank's IT estate.**

Implementing Controls

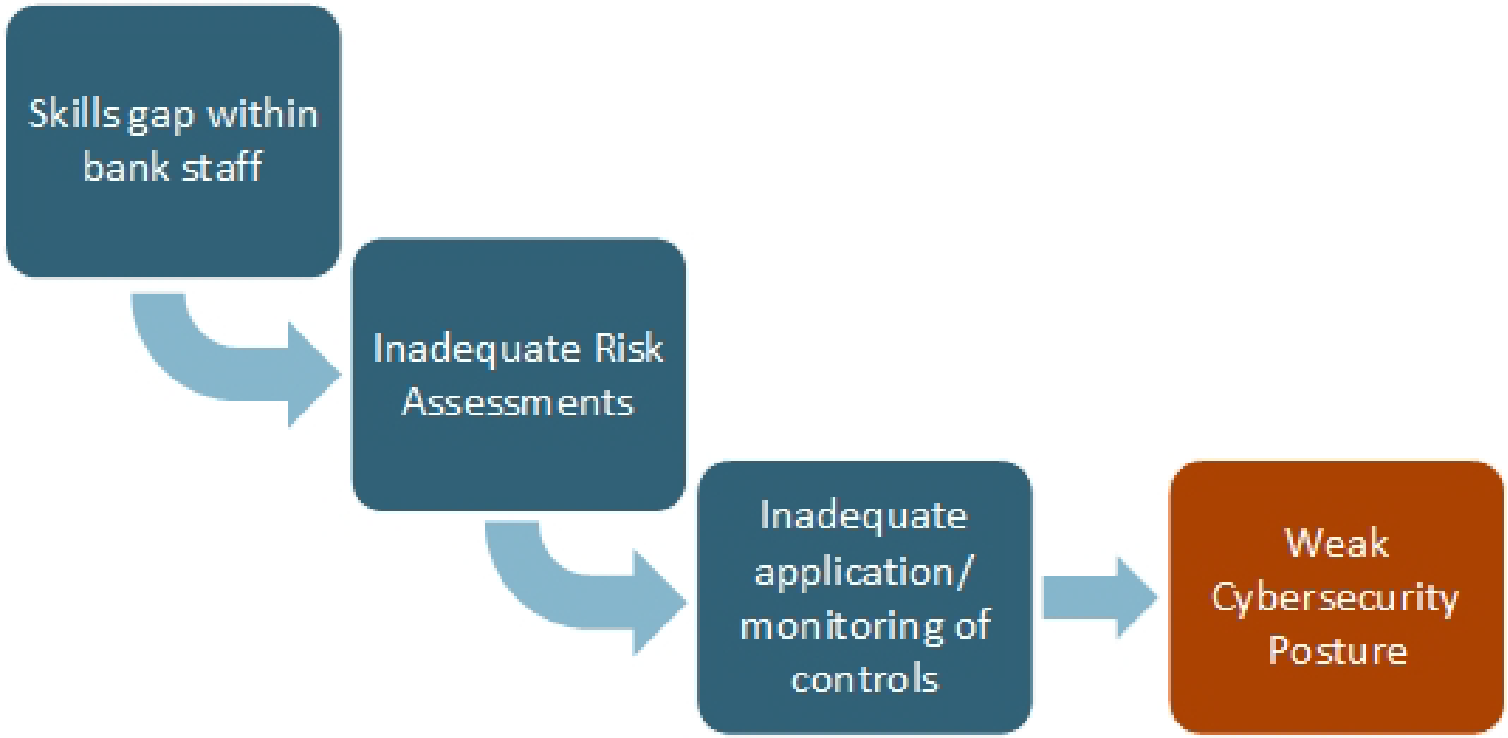
The best way to implement controls is through a quality control framework.

- No more guess work
- Built on secure architectural principles

However, we sometimes see an ad-hoc application of technical controls. This method is characterized by:

- IT individual's professional knowledge
- "Hot topic" of the day
- "Sky is falling" prioritization
- "Wait for the examiner to tell us"
- "If it's not cheap and easy, it must not be important"

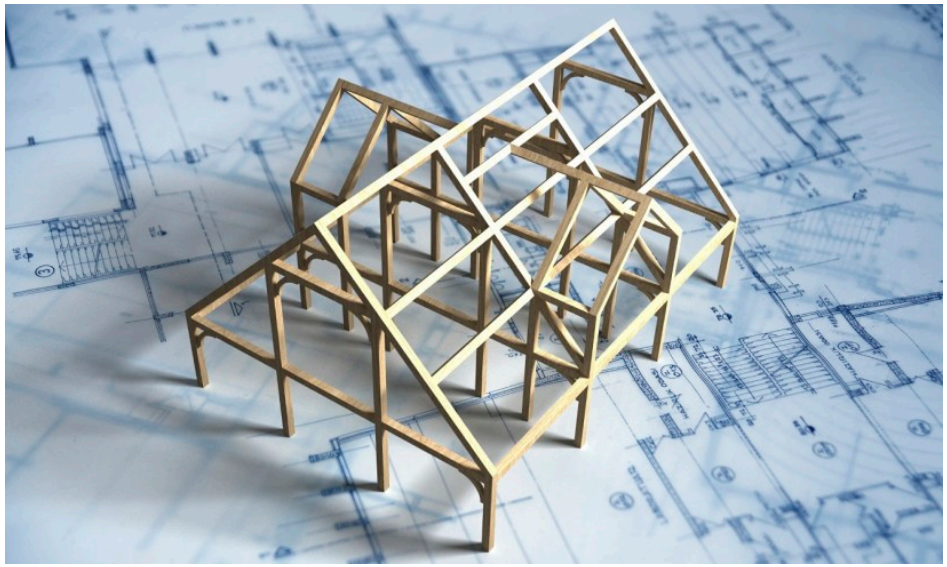
The Skills Gap Problem



Introducing Frameworks

What is a framework?

- A framework can be defined as a basic structure underlying a system, concept, or text.[1]



[1] https://www.google.com/search?q=define+framework

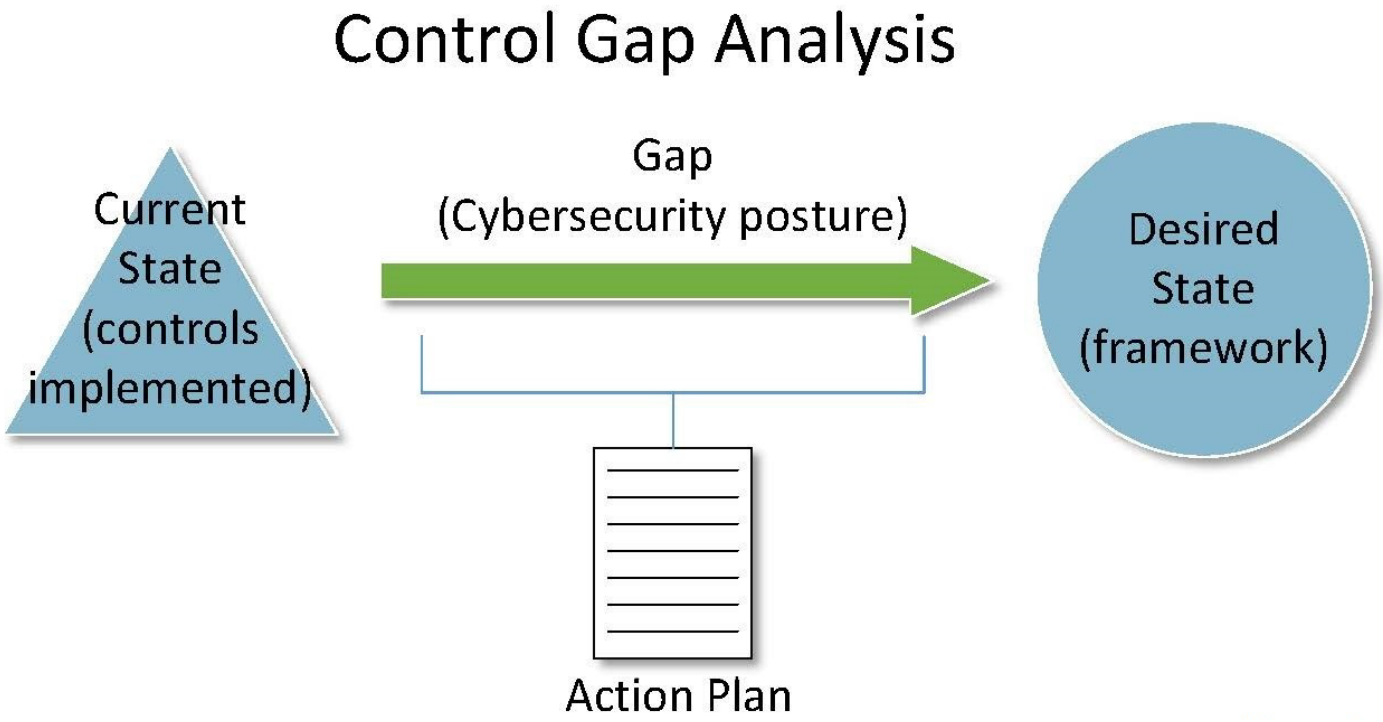
Introducing Frameworks

Frameworks provide a starting point and a number of benefits for information security/cybersecurity. Specifically, the use of frameworks can:

- Help management identify gaps in the bank's control structure which may not be covered by a critical control.
- Provide a measured approach to determine a bank's control implementation against their chosen cybersecurity framework.
- Assist the board in identifying the areas where resources need to be applied to achieve a stronger cybersecurity posture.
- Provide a means to to educate the Board on the cybersecurity posture of their bank in a way that is understandable regardless of the directors' experience in information technology.

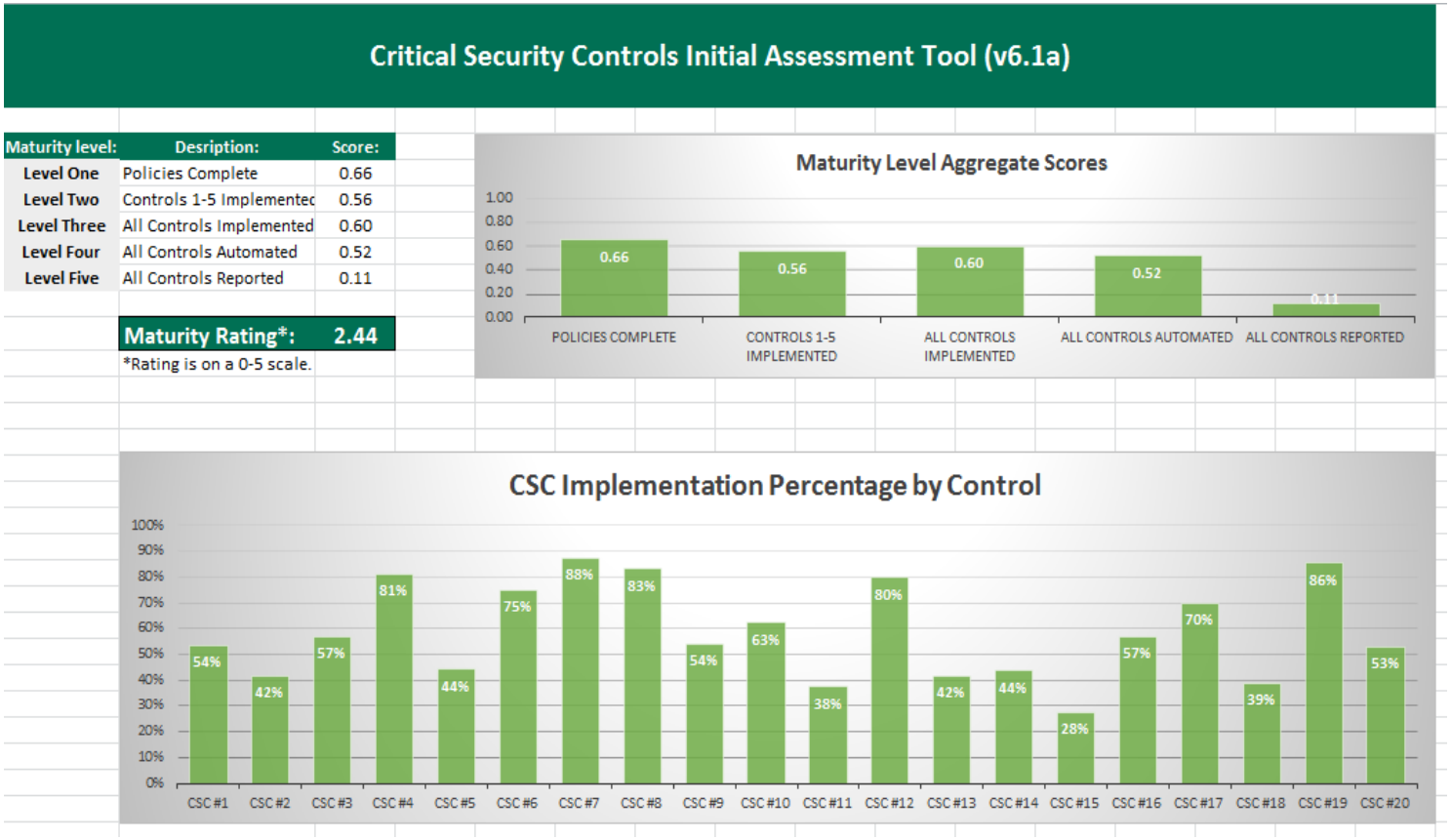
Introducing Frameworks

Back to **cybersecurity posture**



Introducing Frameworks

- Metrics and reporting



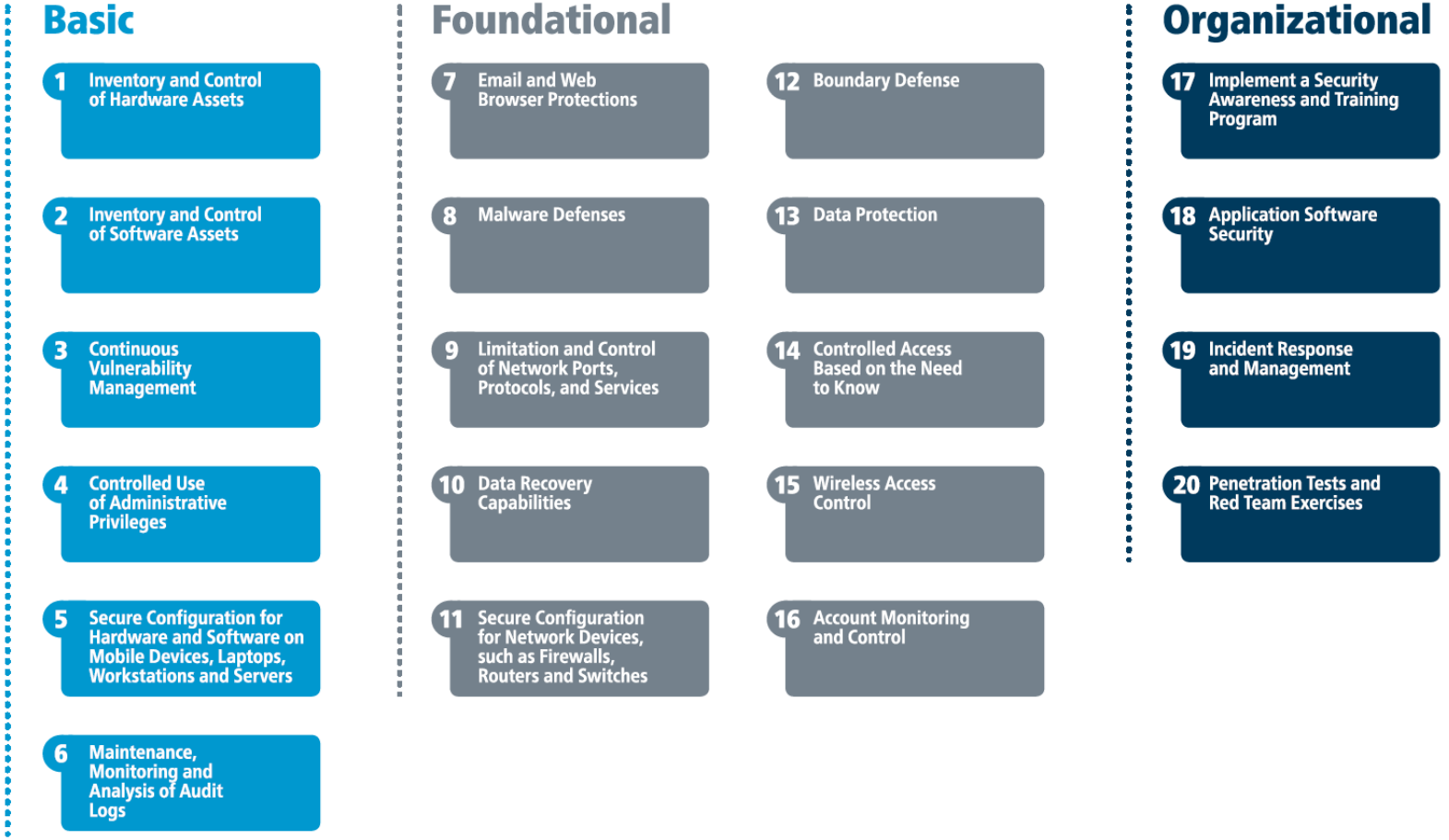
CIS Top 20 Controls™

Center for Internet Security (CIS) – Top 20 Controls

- Digestible for any size bank
- Prioritized, practical, and actionable
- Align with and map to all of the major compliance frameworks (e.g., NIST, ISO series, PCI, FFIEC, etc.)
- What are the core, foundational, steps I can take to get most of my security value?

CIS Controls™

How are the Controls™ structured?



Basic Cyber Hygiene

#1– Inventory and Control of Hardware Assets

Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

- You can't secure what you don't know you have!
- Inventory and control plays a critical role in planning and executing system backup, incident response, and recovery.

Basic Cyber Hygiene

#2 – Inventory and Control of Software Assets

Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

- Again… you can't secure what you don't know you have!
- Builds upon Control #1 (hardware) and focuses on what software is ALLOWED to run in the environment.

Basic Cyber Hygiene

#3 – Continuous Vulnerability Management

Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.

- Scan… Patch… Rescan
- Financial Services *Information Sharing and Analysis Center* (FS ISAC) or similar organization can be a resource for the latest threats.

Basic Cyber Hygiene

#4 – Controlled use of administrative privileges

The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

- Super Users have the “keys to the kingdom”
- Administrators are targets

Basic Cyber Hygiene

#5 – Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

- Beware of default settings
- Continuous management required

Basic Cyber Hygiene

#6 – Maintenance, Monitoring, and Analysis of Audit Logs

Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

- Timing of logs is everything
- Security Information and Event Management (SIEM)

Foundational & Organizational

CIS Controls 7-16 (Foundational)

7) Email and Web Browser Protections
8) Malware Defenses
9) Limitation and Control of Network Ports, Protocols, and Services
10) Data Recovery Capabilities
11) Secure Configurations for Network Devices, such as Firewalls, Routers, and Switches
12) Boundary Defense
13) Data Protection
14) Controlled Access Based on the Need to Know
15) Wireless Access Control
16) Account Monitoring and Control

CIS Controls 17-20 (Organizational)

17) Implement a Security Awareness and Training Program
18) Application Software Security
19) Incident Response and Management
20) Penetration Tests and Red Team Exercises

Drive Security Across the Enterprise

The **five critical tenets** of an effective cyber defense system as reflected in the CIS Controls™ are:

1. *Offense Informs Defense*: Use knowledge of actual attacks that have compromised systems to provide the foundation to continually learn from these events to build effective, practical defenses. **Include only those controls that can be shown to stop known real-world attacks.**

2. *Prioritization*: **Invest first in controls that will provide the greatest risk reduction and protection** against the most dangerous threat actors and that can be feasibly implemented in your computing environment.

Drive Security Across the Enterprise

3. *Measurements and metrics*: **Establish common metrics to provide a shared language for executives, IT specialists, auditors, and security officials** to measure the effectiveness of security measures within an organization so that required adjustments can be identified and implemented quickly.

4. *Continuous diagnostics and mitigation*: Carry out **continuous measurement to test and validate** the effectiveness of current security measures and to help drive the priority of next steps.

5. *Automation*: **Automate defenses** so that organizations can achieve **reliable, scalable**, and continuous measurements of their adherence to the controls and related metrics.

Common Examination Findings

The most common findings* in the Eighth District over the last few years as they correlate to the Controls™ :

- Hardware/Software (1 & 2)
- Patch Management (3)
- Excessive Privileges (4 & 14)
- Configurations (5 & 11)
- Wireless (15)
- Business Continuity Planning/ Disaster Response (10)

*Matters Requiring Attention (MRAs)

Examiner Expectations

- Hardware and Software Inventory
  - Know what's connected
  - Know what's in production
- Vulnerability Management
  - Scanning on a regular frequency
  - Automated patching
- Admin Privileges
  - Need to know
  - Change all default passwords
- Configurations
  - Utilize hardening guidelines from industry sources
- Log Monitoring
  - SIEM (or third-party monitoring)
  - Cross-pollination with incident response discipline

Frameworks and Examinations

- What does the future hold for examination techniques?

- How does the use and adoption of a security framework align bank and regulatory expectations?

Frameworks drive priorities. Priorities drive strategies. Strategies drive budgets.

References

CIS Controls™

https://www.cisecurity.org/controls/

NIST Cybersecurity Framework

https://www.nist.gov/cyberframework

FFIEC IT Examination Handbooks

https://ithandbook.ffiec.gov/

Questions

- **Via webinar chat:** You can submit a question via the **Ask Question** button in the webinar tool. Your question will only be seen by our presenters.
- **Via email:** conversations@stls.frb.org..