We'll get you there.

CPAs | CONSULTANTS | WEALTH ADVISORS

Preparing for the Sunset of the FFIEC CAT Framework

July 17, 2025

The information herein has been provided by CliftonLarsonAllen LLP for general information purposes only. The presentation and related materials, if any, do not implicate any client, advisory, fiduciary, or professional relationship between you and CliftonLarsonAllen LLP and neither CliftonLarsonAllen LLP nor any other person or entity is, in connection with the presentation and/or materials, engaged in rendering auditing, accounting, tax, legal, medical, investment, advisory, consulting, or any other professional service or advice. Neither the presentation nor the materials, if any, should be considered a substitute for your independent investigation and your sound technical business judgment. You or your entity, if applicable, should consult with a professional advisor familiar with your particular factual situation for advice or service concerning any specific matters.

CliftonLarsonAllen LLP is not licensed to practice law, nor does it practice law. The presentation and materials, if any, are for general guidance purposes and not a substitute for compliance obligations. The presentation and/or materials may not be applicable to, or suitable for, your specific circumstances or needs, and may require consultation with counsel, consultants, or advisors if any action is to be contemplated. You should contact your CliftonLarsonAllen LLP or other professional prior to taking any action based upon the information in the presentation or materials provided. CliftonLarsonAllen LLP assumes no obligation to inform you of any changes in laws or other factors that could affect the information contained herein.

Session CPE Requirements

- You need to attend 50 minutes to receive the full 1 CPE credit.
- There will be 4 polling questions throughout the presentation. You must respond to a minimum of 3 to receive the full 1 CPE credit.

Both requirements must be met to receive CPE credit

Polling *Question*

How optimistic are you on the economic conditions and the impact to your organization?

- 5 = Very confident
- 4 = Confident
- 3 = Neutral
- 2 = Somewhat confident
- 1 = Not at all confident

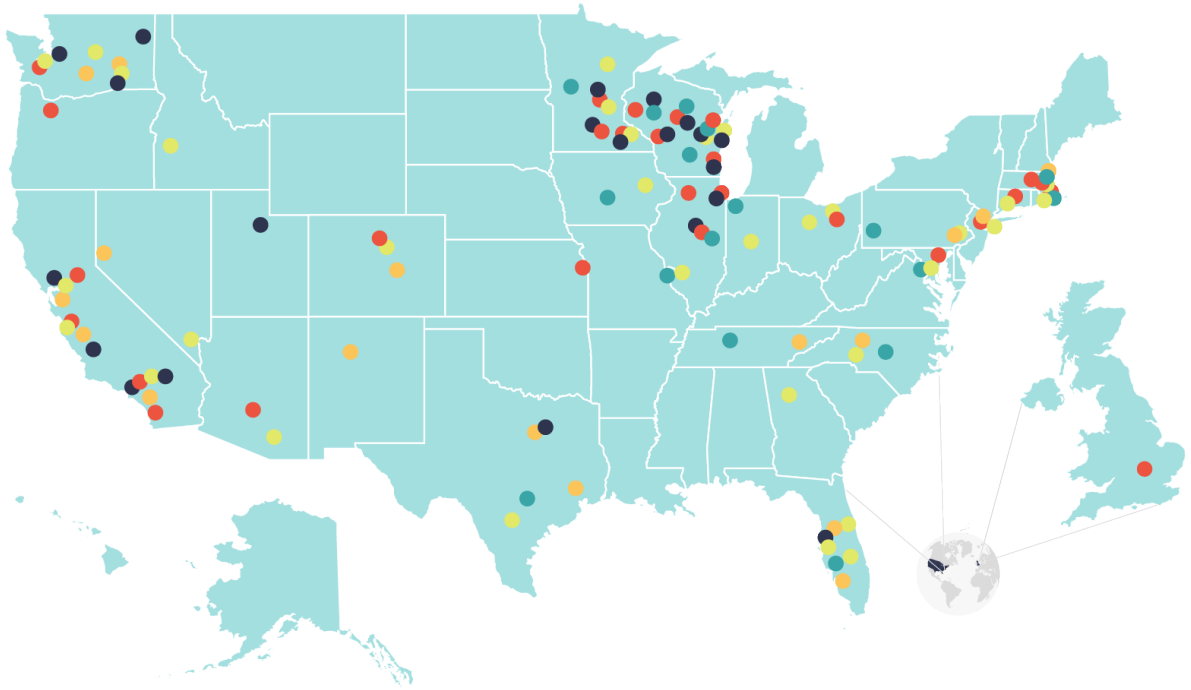
National and International Reach

9,000
NEARLY 9,000 PEOPLE

130+
LOCATIONS

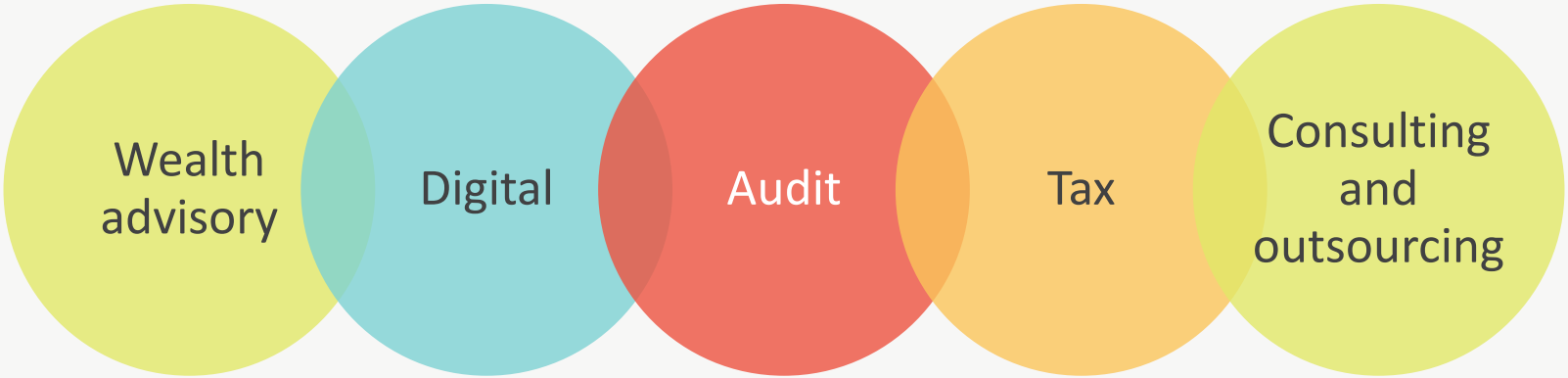
AN INDEPENDENT
NETWORK MEMBER OF

CLA Global



CLA (CliftonLarsonAllen LLP) is an independent network member of CLA Global. See CLAglobal.com/disclaimer.

Helping You is Our Passion.



Speakers

Randy Romes
Principal - Cybersecurity

Tim Dively
Digital Growth Manager

Learning Objectives

1. Recall the implications of the FFIEC CAT framework sunsetting and the urgency of adopting a new cybersecurity framework.
2. Identify alternative frameworks and their suitability for different institution sizes and complexities.
3. Identify practical steps and strategies for transitioning to a new cybersecurity framework before the effective date.
4. Discuss the impact of doing nothing and the risks associated with non-compliance and outdated cybersecurity measures.
5. Recall how to reduce the impact of the transition on your institution and provide a smooth adoption process.

FFIEC CAT History

FFIEC History

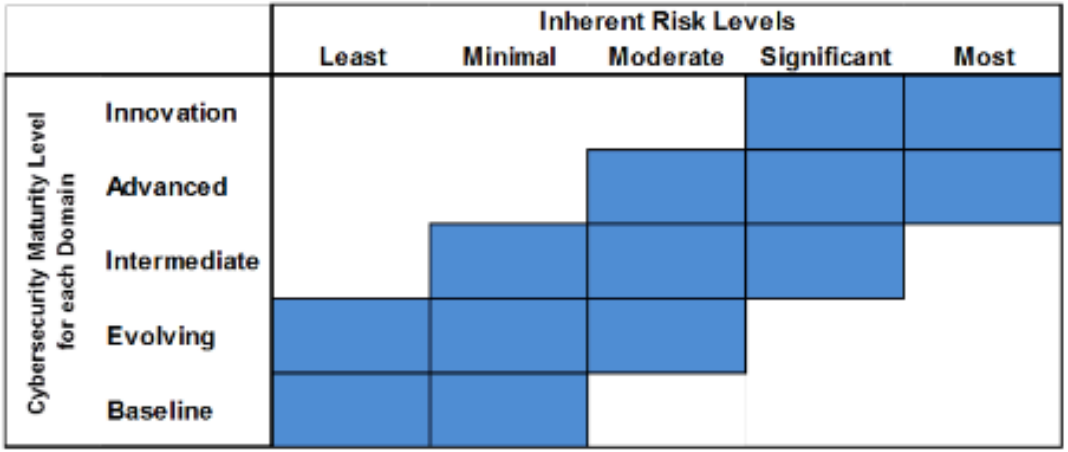
- The FFIEC Cybersecurity Assessment Tool was introduced in 2015 to assist financial institutions in identifying cybersecurity risks and readiness.
- The tool evaluates cybersecurity maturity across different domains, ensuring alignment with regulatory requirements for financial institutions. A total of 494 questions were included within the assessment.
- Financial institutions were required to address questions to determine inherent risk profiles (least, minimal, moderate, significant and most)
- Desired level of cyber-maturity levels included the following:
  - Baseline
  - Evolving
  - Intermediate
  - Advanced
  - Innovative

Defining a Maturity Target

The FFIEC provided a general chart which shows the intersection of the Inherent Risk Level obtained using this Risk Profile and the Cybersecurity Maturity Levels.

For example - if the results of completing the Inherent Risk Profile indicated "Moderate" - then the institution should strive to have a Cybersecurity Maturity of "Evolving", "Intermediate" or "Advanced"

The Inherent Risk Results Tab calculates what your Cybersecurity Maturity Level is expected to be.



Polling *Question*

Have you started to prepare for the sunsetting of the FFIEC CAT framework?

- Yes
- No
- Looking for some guidance on next steps

Reasons for Sunsetting

Evolving cybersecurity landscape

Need for flexibility

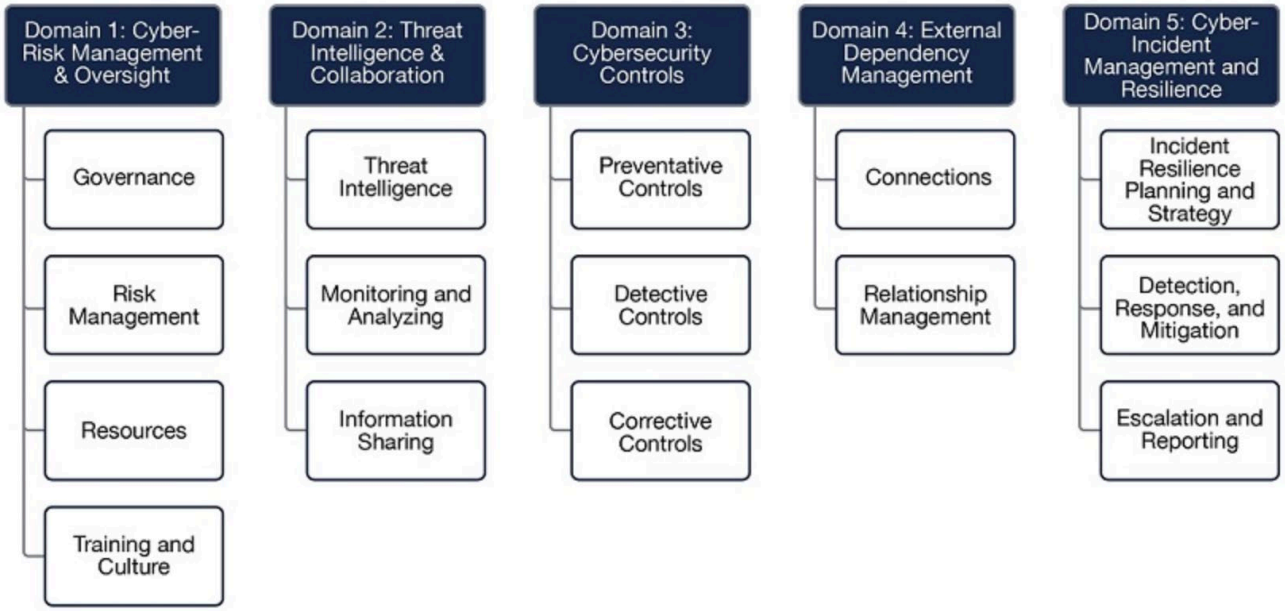
Comprehensive frameworks

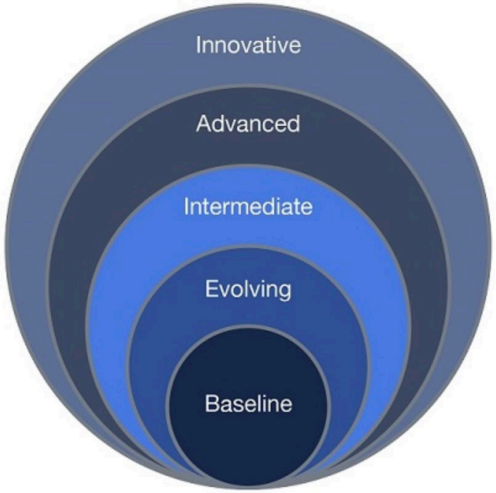
Lessons Learned and Recommended Practice Observations From FFIEC CAT Framework?

14

Alternative Frameworks to Consider

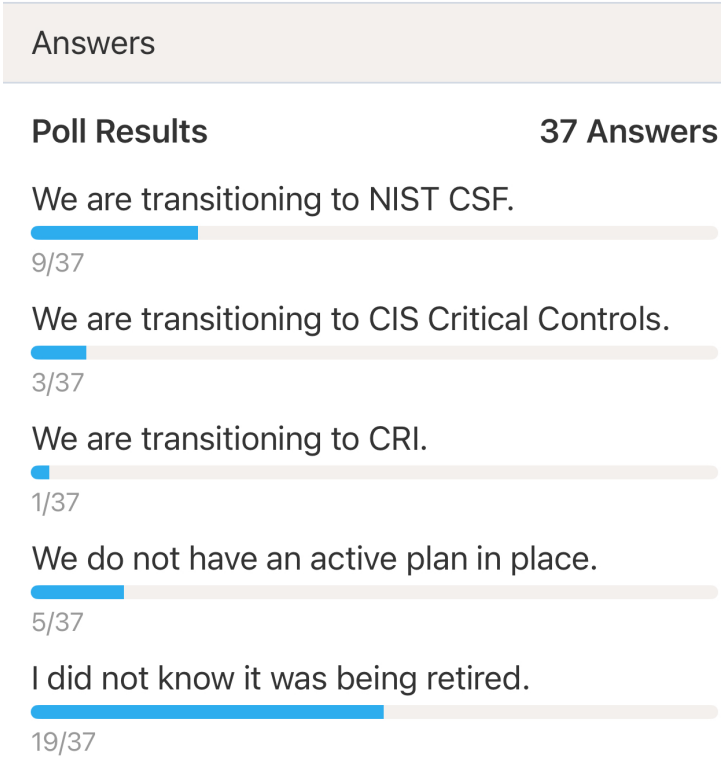
Risk and Maturity Frameworks





Risk and Maturity Frameworks

- FFIEC ACET is retired…
- How is your institution planning to address the retirement of the ACET cyber risk evaluation and communication tool?



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

Available Tools and Frameworks

- NIST Cybersecurity framework (CSF)*
- Cyber Security and Infrastructure Security Agency Cybersecurity performance goals (CISA)*
- Cyber Risk Institute (CRI)*
- Center for Internet Security (CIS)*
- NCUA's Automated Cybersecurity Evaluation Toolbox (ACET)*

*Refer to appendix at the end of presentation

Framework Overview

NIST - The first version was published in 2014 and was developed as result of an executive order. The NIST Cybersecurity Framework offers a flexible approach tailored to different organizational needs for managing cybersecurity risks. The framework emphasizes five core functions (Identify, Protect, Detect, Respond and Recover).

CISA - CISA provides resources and frameworks aimed at strengthening the security of critical infrastructure sectors across industries (federal government, SLTT governments, industry, small and medium businesses, educational institutions). Cross sector cybersecurity performance goals for financial services is to be released in winter 2025.

CIS Controls - They have been around for 25 years and was developed by experts in government agencies, private sector innovative labs and top security institutions. They have developed several benchmarks for securing organization's IT environments that are globally recognized. They evaluate cyber hygiene using 18 critical control areas.

CRI - The CRI Profile v2.1 tailors risk management for financial institutions by incorporating elements from multiple security frameworks. Tier levels have been outlined, and selection is based on overall complexity.

Making an Informed Decision

Assessment of Frameworks

- Organizations must conduct a thorough assessment of available cybersecurity frameworks to determine their suitability for specific needs.

Comparison Criteria

- Comparing different frameworks involves evaluating various criteria such as effectiveness, cost, and compliance with regulations.

Strategic Alignment

- The chosen framework should align with the organization's strategic objectives to ensure effective cybersecurity management.

Practical Next Steps in Adapting to Change

No Framework Doesn’t Mean No Responsibility

Adjusting Your Programs: What Can You Do Now?

Broader Trends to Consider

Actionable Next Steps

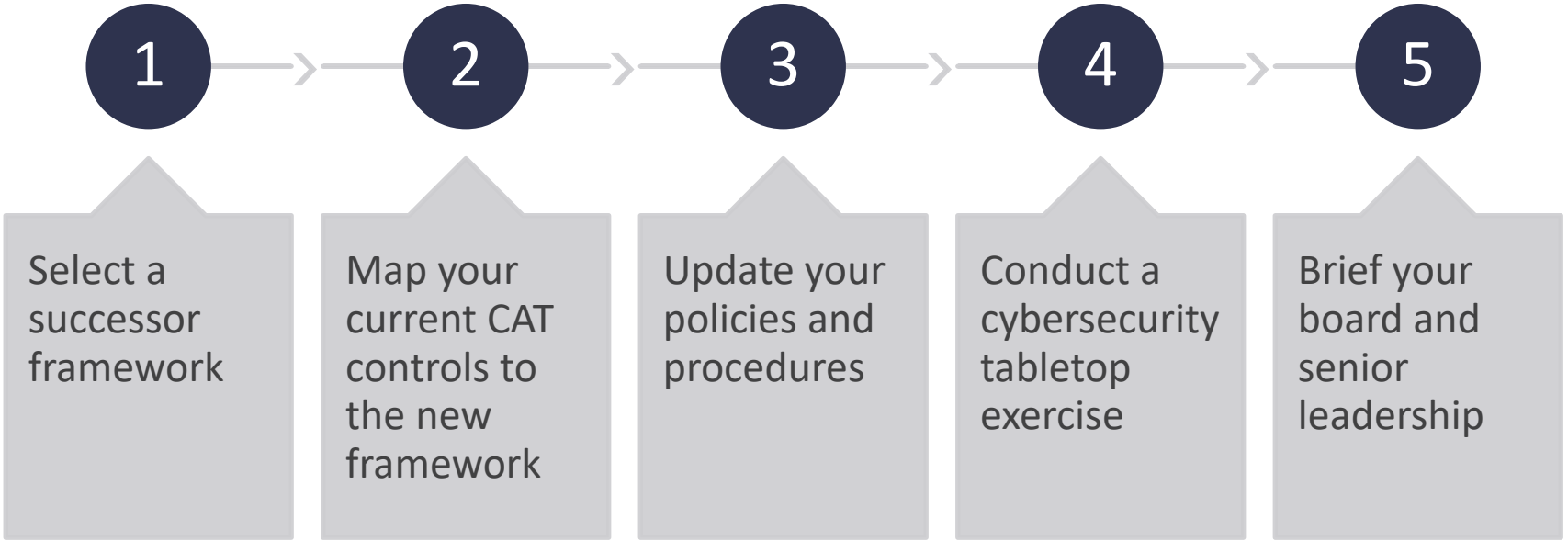
Polling *Question*

Did you find the information in this CLA webinar helpful to you and your organization or business?

- Yes
- No

Next Steps

Collaborative roadmap development focusing on removing key barriers to growth and accelerating scale.



What Is the Cost of Doing Nothing?

- Regulatory compliance risk
- Decreased examiner confidence
- Security gaps and outdated controls
- Operational inefficiencies
- Board and stakeholder perception risks
- Delayed strategic planning

Polling *Question*

I’d like someone from CLA to contact me to discuss the following services:

- Transitioning from FFIEC CAT framework
- M365 controls and configuration review
- Overall digital strategy
- Nothing at this time

Thank you!

Randy Romes
randy.romes@CLAconnect.com

Tim Dively
tim.dively@CLAconnect.com

Scan here for a
complimentary
30-minute listening session

CLAconnect.com

CPAs | CONSULTANTS | WEALTH ADVISORS

Appendix

NIST

Flexible Risk Management

- The NIST Cybersecurity Framework offers a flexible approach tailored to different organizational needs for managing cybersecurity risks.

Core Functions

- The framework emphasizes five core functions:
  - Identify – understand assets, data and risks
  - Protect – safeguard systems and services
  - Detect – discover cybersecurity events quickly
  - Respond – take action to contain and mitigate
  - Recover – restore capabilities and operations

Incident Management

- Effective incident management is critical, focusing on timely detection and recovery from cybersecurity incidents to minimize impact.

CISA

Identify Critical Assets

- Identifying critical assets is a key component of the CISA Cybersecurity Framework, helping organizations focus their defense efforts on the most important areas.

Detecting Threats

- The framework emphasizes the importance of detecting threats in a timely manner to prevent potential damage and maintain security.

Effective Response

- Responding effectively to identified threats is crucial for mitigating risks and protecting organizational assets.

Continuous Monitoring

- Continuous monitoring and improvement of security measures are essential to ensure defense against evolving cyber risks.

CIS Controls (v8.1)

Critical Security Controls

- The CIS framework includes 18 critical security controls that are essential for enhancing an organization's security posture.

Three Implementation Groups (IG)

- These controls are organized into three groups:
  - IG1- An IG1 enterprise is small to medium-sized with limited IT and cybersecurity expertise to dedicate toward protecting IT assets and personnel.
  - IG2 - An IG2 enterprise employs individuals responsible for managing and protecting IT infrastructure. These enterprises support multiple departments with differing risk profiles based on job function and mission
  - IG3I - An IG3 enterprise employs security experts that specialize in the different facets of cybersecurity (e.g., risk management, penetration testing, application security). IG3 assets and data contain sensitive information or functions that are subject to regulatory and compliance oversight

Identifying Vulnerabilities

- The framework assists organizations in identifying vulnerabilities within their systems to prevent potential security breaches.

Continuous Monitoring

- Organizations implementing the framework can continuously monitor their security systems to stay protected against evolving threats.

CRI Profile (v2.1)

Guidance for Organizations

- CRI offers essential guidance to organizations aiming to strengthen their cybersecurity measures effectively.

Core Functions

- The CRI profile includes a maturity model assessment for peer benchmarking and is designed to counter dynamic and evolving threats. The CRI profile is divided into seven core functions — govern, identify, protect, detect, respond, recover, and extend — which meet the regulatory expectations for the financial services sector. The framework developed by CRI helps organizations create robust systems to effectively respond to evolving cybersecurity threats.

Tier Approach

- The framework is designed into distinct tiers and levels, providing a clear structure for evaluating cybersecurity maturity.
  - Tier 1: National/Super-National Impact – These institutions are designated most critical by one or more global regulatory agencies and/or bodies. This category assumes the gross cyber risk exposure of an institution or service categorized as Tier 1 would have the most potential adverse impact to the overall stability of a national economy, and potentially, the global market.
  - Tier 2: Subnational Impact – These institutions provide mission critical services with millions of customer accounts. This category assumes the gross cyber risk exposure of an institution or service would have the potential for a substantial adverse impact to the financial services sector and subnational regional economy but does not rise to the level of Tier 1.
  - Tier 3: Sector Impact – These institutions have a high degree of interconnectedness, with certain institutions acting as key nodes within, and for, the sector. The nature of the services that these institutions provide to the sector plays a significant role in determining their criticality.
  - Tier 4: Localized Impact – These institutions have a limited impact on the overall financial services sector and national economy. Typical characteristics include: (a) institutions with a local presence and less than 1 million customers (e.g., community banks, state banks) and (b) providers of low criticality services.

Additional Resources

- NIST - https://www.nist.gov/cyberframework
- CISA - https://www.cisa.gov/news-events/news/cybersecurity-performance-goals-sector-specific-goals
- CIS - https://www.cisecurity.org/controls
- CRI - https://cyberriskinstitute.org/the-profile/