FFIEC Cybersecurity Assessment Tool (CAT) Sunset: Alternative Frameworks and Strategies for 2025

The Federal Financial Institutions Examination Council (FFIEC) recently announced[1] the sunset of its Cybersecurity Assessment Tool (CAT), effective August 31, 2025. Financial institutions relying on the CAT should proactively explore alternative frameworks and tools to ensure a seamless transition while maintaining effective management of cybersecurity risks. Released in June 2015, the CAT helped institutions identify risks and assess cybersecurity preparedness. However, in the rapidly evolving cybersecurity landscape, nearly a decade without updates has left the tool outdated and misaligned with current standards.

Understanding the FFIEC's Decision to Sunset the CAT

Since 2016, the FFIEC has steadily aligned its resources and guidance with authoritative standards organizations, such as the National Institute of Standards and Technology (NIST). The CAT was last mentioned in the release notes of the 2016 *Information Security* booklet update[2]. However, subsequent booklets—including *Business Continuity Management* (2019), *Architecture, Infrastructure, and Operations* (2021), and *Development, Acquisition, and Maintenance* (2024)—omitted references to the CAT. Instead, NIST references have steadily increased, beginning with the *Architecture, Infrastructure, and Operations booklet* in 2021, which was the first to include a dedicated reference section for NIST standards. This progression reflected the FFIEC's ongoing commitment to aligning with authoritative standards organizations.

In a 2019 press release titled *FFIEC Encourages Standardized Approach to Assessing Cybersecurity Preparedness*[3], the FFIEC referenced the CAT but also encouraged financial institutions to adopt standardized tools, highlighting the NIST Cybersecurity Framework (CSF)[4], CIS Controls[5], and the FSSCC Cybersecurity Profile (now the CRI Profile)[6] as viable alternatives.

By 2022, momentum had further shifted toward NIST-aligned tools and frameworks. CISA released its Cross-Sector Cybersecurity Performance Goals (CPGs)[7], and in 2023, the Office of the Comptroller of the Currency (OCC) aligned its cybersecurity supervision work program[8] with the NIST CSF. Meanwhile, NIST released the first public draft of CSF 2.0. In 2024, this updated version of the CSF was finalized, accompanied by aligned updates from other entities: CISA announced plans to revise its CPGs, CIS Controls released Version 8.1, and the Cyber Risk Institute (CRI) published Version 2.0 of its Cyber Profile, a community-driven extension of the NIST CSF.

As both public and private sector organizations increasingly converged around the NIST CSF, the FFIEC faced a pivotal decision: update the CAT to align with the NIST CSF or retire the tool. Ultimately, the FFIEC chose the latter, issuing the following statement in its *CAT Sunset Statement*:

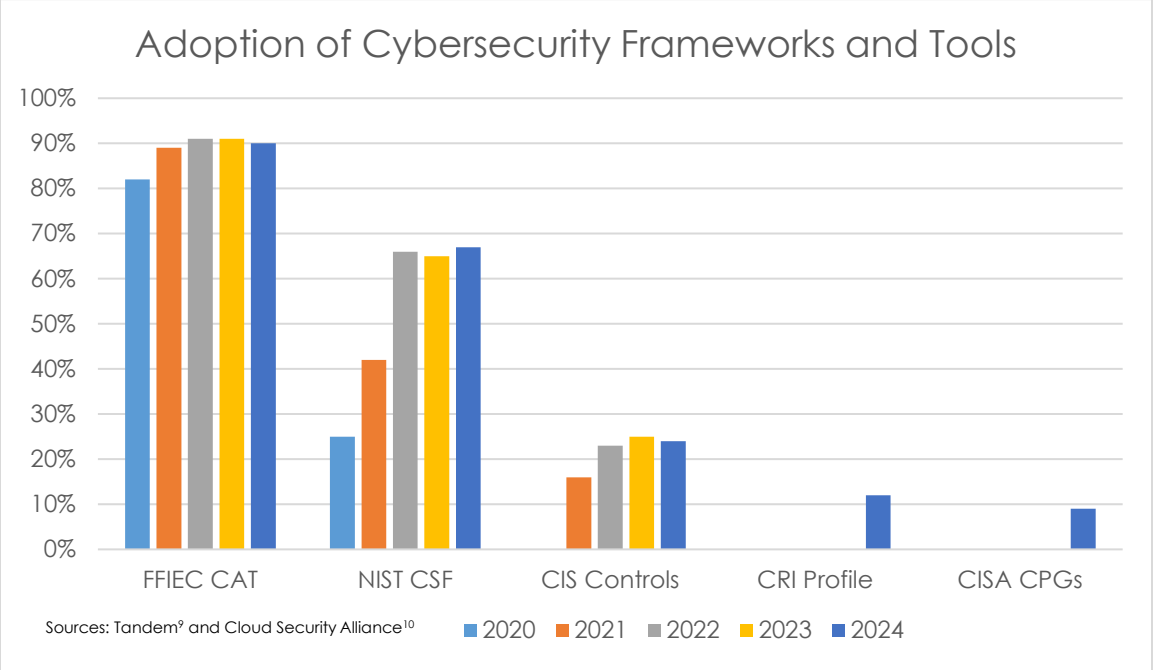
> "The FFIEC will remove the CAT from the FFIEC website on August 31, 2025. After much consideration, the FFIEC has determined not to update the CAT to reflect new government resources, including the National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0 and the Cybersecurity and Infrastructure Security Agency's (CISA) Cybersecurity Performance Goals."

This decision underscores the FFIEC's recognition of the widespread industry adoption of NIST-aligned tools, ensuring that financial institutions can leverage the most current and robust resources to manage cybersecurity risk effectively.

Exploring Alternative Frameworks and Tools Adopted by Financial Institutions

The FFIEC noted the following resources as alternatives to the CAT in their statement:

- NIST Cybersecurity Framework 2.0
- CISA Cybersecurity Performance Goals (Financial Sector-Specific Goals slated for Winter 2025 release)
- Cyber Risk Institute Cyber Profile
- Center for Internet Security Controls



Data from Tandem and the Cloud Security Alliance reveals that the NIST CSF has emerged as the most widely adopted alternative to the CAT, experiencing a significant rise in adoption since 2020. By 2024, adoption rates for alternative frameworks and tools were as follows: NIST CSF (67%), CIS Controls (24%), CRI Profile (12%), and CISA CPGs (9%). These figures highlight the NIST CSF's growing prominence as the preferred industry standard.

Choosing the Right Cybersecurity Framework for Your Financial Institution

Selecting the right cybersecurity framework is a critical decision for financial institutions navigating the complex landscape of cyber threats. One question we often hear from our clients is, "Which framework is the best fit for our organization?" Here's how we approach answering this critical question.

Start with the Fundamentals

The FFIEC does not endorse specific cybersecurity tools or frameworks, leaving the choice up to each organization. Instead, it provides institutions the flexibility to choose a framework that aligns with their unique goals, objectives, and the ever-changing nature of cybersecurity risks.

We advise our clients to begin with a NIST CSF maturity assessment. This serves as a foundational step to:

- **Define a target maturity level:** Establishing a clear vision of where the organization wants to be in terms of cybersecurity capabilities.
- **Assess the current maturity level:** Identifying the organization's present state to pinpoint gaps between current and desired cybersecurity practices.

Expanding Beyond the NIST CSF

Once an organization achieves its target maturity level with the NIST CSF, it can explore additional frameworks to complement and expand its cybersecurity program. A particularly relevant option for financial institutions is the CRI Profile, which is a tailored extension of the NIST CSF designed specifically for the financial sector. The CIS Controls and CISA CPGs are also valuable tools for financial institutions. Both frameworks group their controls using the NIST CSF functions and have freely available mappings online. These frameworks can serve as valuable references or evaluation criteria for the NIST CSF, and organizations may opt to implement them as standalone frameworks.

The Bottom Line

Selecting the right cybersecurity framework isn't about finding a one-size-fits-all solution. It's about choosing a framework—or combination of frameworks—that empowers an organization to proactively manage cyber risks, enhance resilience, and meet regulatory expectations.

Starting with the NIST CSF provides a strong foundation. From there, financial institutions can strategically integrate complementary tools like the CRI Profile, CIS Controls, or CISA CPGs. Together, these resources help build a strong, adaptable cybersecurity program that not only addresses a dynamic threat landscape but also aligns with industry best practices.

References

[1] https://www.ffiec.gov/press/pdf/CAT_Sunset_Statement_FFIEC_Letterhead.pdf

[2] https://ithandbook.ffiec.gov/whats-new

[3] https://www.ffiec.gov/press/pr082819.htm

[4] https://www.nist.gov/cyberframework

[5] https://www.cisecurity.org/controls/v8-1

[6] https://cyberriskinstitute.org/the-profile/

[7] https://www.cisa.gov/cybersecurity-performance-goals-cpgs

[8] https://www.occ.gov/news-issuances/bulletins/2023/bulletin-2023-22.html

[9] https://tandem.app/state-of-cybersecurity-report

[10] https://cloudsecurityalliance.org/artifacts/cyber-resiliency-in-the-financial-industry-2024-survey-report