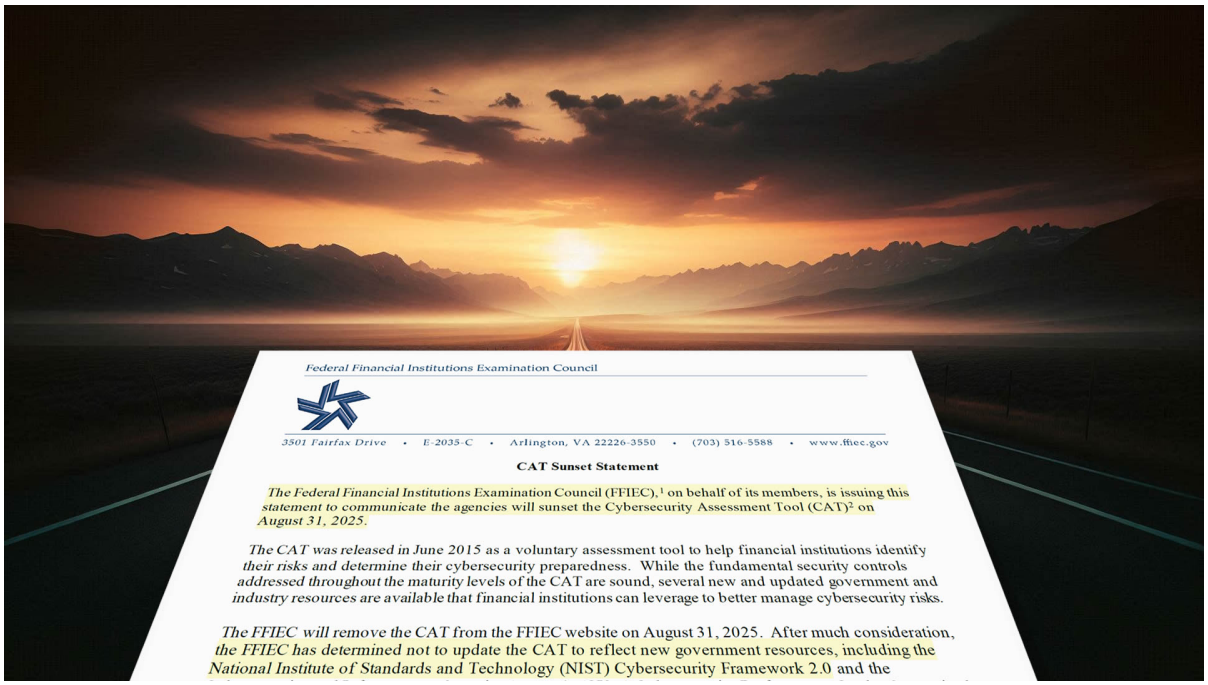


The FFIEC is retiring its Cybersecurity Assessment Tool (CAT) by August 31, 2025, and recommends that financial institutions transition to the **NIST Cybersecurity Framework 2.0 (CSF 2.0)** as an alternative. This shift is driven by the need for more updated and comprehensive cybersecurity frameworks as threats evolve. **Time is running out for supervised financial institutions to transition to deploy and assess cybersecurity according to NIST CSF 2.0.**

Why the change?

The FFIEC determined that the CAT, while helpful, wasn't being updated to reflect newer government resources like NIST CSF 2.0 and CISA's (U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency) Cybersecurity Performance Goals. NIST CSF 2.0 offers a more comprehensive and up-to-date framework for managing cybersecurity risks (in IT, OT, and IoT), encompassing a wider range of controls and aligning with other government resources.

Transitioning to NIST CSF 2.0

Financial institutions will need to conduct gap analyses, map existing assessments to NIST CSF 2.0, develop NIST CSF 2.0 implementation roadmaps, and engage internal and external stakeholders (including its supply chain) to ensure a smooth transition.

Preparing for the transition to NIST CSF 2.0

The organizational scope of applicability of NIST CSF 2.0 is quite broad. Recently release in February 2024, this new framework is not just for Information Technology - it is equally applicable and relevant for all Operations Technology, mobile devices, and IoT.

Financial institutions can't properly deploy or assess cybersecurity according to NIST CSF 2.0 without first understanding how to do the job. Since NIST CSF 2.0 requires proof of training and competence for specialized roles in its own desired outcome objective described in CSF 2.0 PR.AT-02, institutions supervised by the FFIEC need to quickly train and certify top management (116 of CSF 2.0's recommended implementation actions are explicitly for cybersecurity risk program governance) in NIST CSF 2.0 in particular, regardless of existing cybersecurity competence and skills.

Roles requiring provable CSF 2.0 competence and skills (to comply with CSF 2.0 PR.AT-02) CSF 2.0 training and competence include:

- Chief Information Officers (CIO)
- Chief Information Security Officers (CISO)
- Chief Security Officers (CSO)
- Security Analysts
- Chief Technology Officers (CTO)
- Chief Audit Executives (CAE)
- Chief Risk Officers (CRO)
- Compliance managers
- Chief Compliance Officers (COO)
- Compliance Analysts
- Chief Privacy Officers (CPO)
- Data Protection Officers (DPO)
- Internal auditors
- IT managers
- Security Operations (SecOps) team members

Getting NIST CSF 2.0 training and proof of competence (professional certification)

A quick Google search shows the training and certification programs currently available for NIST: https://www.google.com/search?q=nist+csf+2.0+lead+lead+auditor.

Certified Information Security provides NIST CSF 2.0 Lead Implementer and NIST CSF 2.0 Lead Auditor training and certification. Live classes are open for registration at locations throughout the US and Caribbean, and all live classes are simulcast for hybrid presentation supporting budget-friendly remote attendance. Learn more at https://www.certifiedinfosec.com/event-calendar.

Certified Information Security provides NIST CSF 2.0 Lead Implementer and NIST CSF 2.0 Lead Auditor training and certification. Live classes are open for registration at locations throughout the US and Caribbean, and all live classes are simulcast for hybrid presentation supporting budget-friendly remote attendance. Learn more.

NIST CSF 2.0 professional credentials

- NIST CSF 2.0 Lead Implementer
- NIST CSF 2.0 Lead Auditor