Explore Your Options

As the **FFIEC's Cybersecurity Assessment Tool (CAT)** becomes a thing of the past, financial institutions are tasked with finding a suitable replacement. Currently, the top cybersecurity assessment frameworks include the following (click to visit):

NIST Cybersecurity Framework (CSF) 2.0

CISA Cybersecurity Performance Goals (CPG)

Cyber Risk Institute (CRI) Cyber Profile 2.1

Center for Internet Security (CIS) Critical Security Controls

Use this checklist as a guideline to evaluate each framework.

- ☐ **Based on a widely recognized cybersecurity framework** — This ensures alignment with industry best practices, promotes consistency, and builds credibility with regulators and auditors; e.g., the NIST Cybersecurity Framework.
- ☐ **Maintained and regularly updated by a reputable organization** — This keeps the framework current with emerging threats, regulatory changes, and evolving standards—ensuring long-term relevance.
- ☐ **Tailored to the specific challenges, regulatory expectations, and risk profiles of the financial industry** — The framework should reflect the high-security standards and compliance obligations unique to financial institutions, including their exposure to cyber threats and customer data sensitivity.
- ☐ **Supports structured assessment, tracking, and reporting of cybersecurity posture, including assessment-to-assessment comparison reports** — Financial institutions need the ability to evaluate their cybersecurity maturity over time, identify gaps, create an action plan for improvement, and demonstrate progress to stakeholders, including boards and regulators.
- ☐ **Flexible and customizable** — Each financial institution has its own size, complexity, and risk appetite—the framework should be flexible enough to accommodate these differences without compromising structure or rigor.

Make the Transition Smoother

Consider partnering with subject matter experts to assist with completion of the assessment and interpretation of the assessment results. Because each alternative framework differs significantly from the FFIEC CAT, implementation can be resource-intensive—requiring substantial time, effort, and expertise both initially and on an ongoing basis. Developing a prescriptive, results-driven action plan also hinges on accurately interpreting assessment results. Engaging experts can ease the implementation and maximize long-term impact. Additionally, having a partner that can transition the data from your previous CAT into the new format will save considerable time and effort. UFS is here to help! Our team of cybersecurity professionals can support you every step of the way. Learn more at ufstech.com