Tandem®

A Board Member's Guide to Cybersecurity Assessments

How to understand your role, interpret assessment results, and oversee cybersecurity with confidence.

Introduction

A financial institution's Board of Directors plays an important role in overseeing cybersecurity risk. To fulfill those responsibilities, Board members need meaningful information about the institution's cybersecurity program.

Cybersecurity assessments are one of the primary tools management uses to provide that information. As financial institutions transition away from the FFIEC Cybersecurity Assessment Tool (CAT) and adopt new frameworks, the format and terminology of assessment reports may change. However, the Board's oversight responsibilities remain the same.

This guide explains the purpose of cybersecurity assessments, how to interpret assessment results, and what information Boards should expect to receive from management going forward.

About the FFIEC CAT Sunset

For a decade, many financial institutions used the FFIEC CAT to evaluate their cybersecurity preparedness. In 2024, the FFIEC announced the CAT would be sunset effective August 31, 2025.[1]

While the CAT would be going away, the need for cybersecurity assessments did not change. The FFIEC continues to encourage financial institutions to use a standardized approach to assessing cybersecurity preparedness.[2]

What has changed since the CAT sunset is how financial institutions conduct and report these cybersecurity assessments. Board members may now receive assessment reports that use different frameworks, different terminology, and different measurements than those used under the CAT.

That's where this guide comes in. The following sections explain the frameworks institutions are adopting, what assessment results mean, and how Board members can interpret the information presented to them.

---

[1] Federal Financial Institutions Examination Council, "FFIEC Cybersecurity Assessment Tool Sunset Statement," August 29, 2024

[2] Federal Financial Institutions Examination Council, "FFIEC Encourages Standardized Approach to Assessing Cybersecurity Preparedness," August 28, 2019

FFIEC CAT Timeline

2013

Executive Order 13636 initiated the development of cybersecurity resources by federal agencies.

2014

The FFIEC piloted a cybersecurity assessment at 500+ community financial institutions.

2015

In June, the FFIEC officially released the Cybersecurity Assessment Tool (CAT).

2017

In May, the FFIEC released its only update to the CAT to revise mappings and add a new answer option.

2024

In August, the FFIEC published a statement announcing the sunset of the CAT.

2025

On August 31, the CAT was officially sunset and removed from the FFIEC website.

What Frameworks are Financial Institutions Using?

In the sunset announcement, the FFIEC did not designate a single replacement framework for the CAT. Instead, it identified several cybersecurity resources financial institutions could use in their cybersecurity program, including:

- National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)
- Cybersecurity & Infrastructure Security Agency (CISA) Cybersecurity Performance Goals (CPGs)
- Cyber Risk Institute (CRI) Profile
- Center for Internet Security (CIS) Critical Security Controls

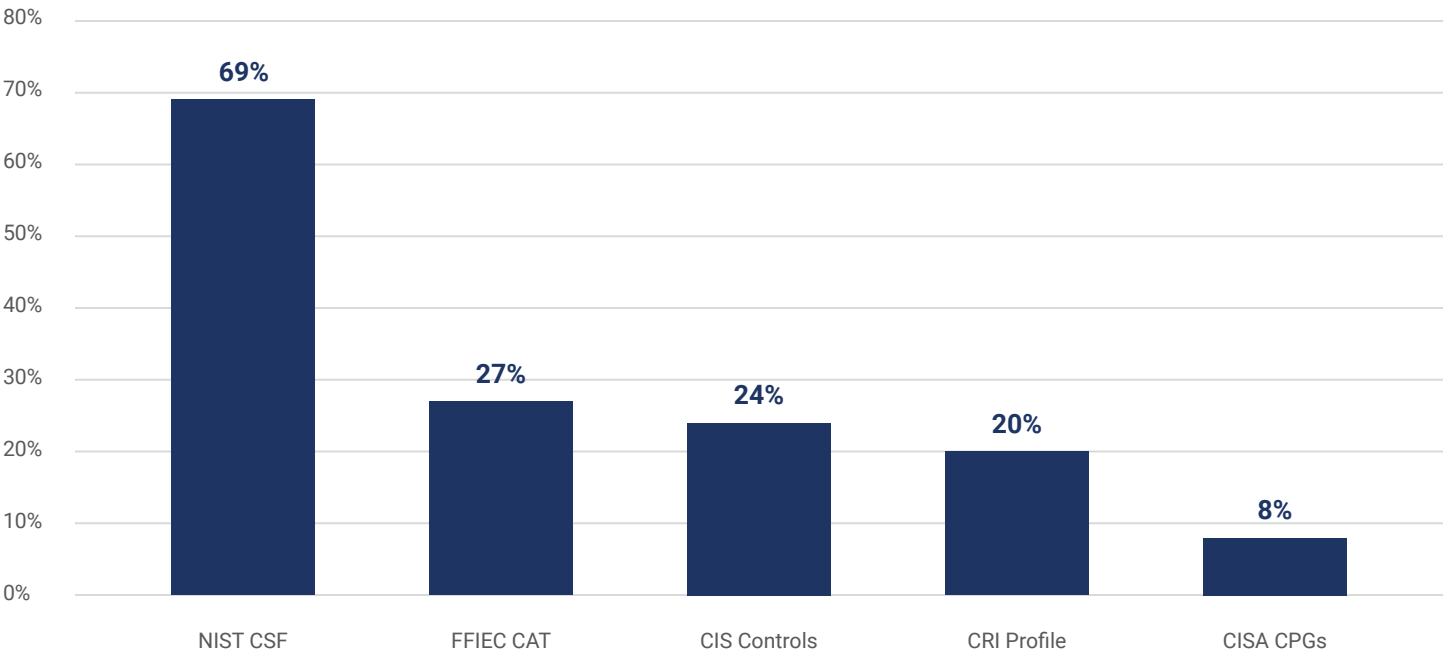
While these frameworks differ in structure and terminology, they all serve the same purpose: helping institutions evaluate cybersecurity controls, identify opportunities for improvement, and communicate results with the Board of Directors.

Some institutions are still using the CAT while they transition to another framework or have considered continuing to use the CAT indefinitely. While this approach may preserve familiarity, the CAT no longer receives updates from the FFIEC and the Conference of State Bank Supervisors (CSBS) has described it as "inadequate" as a standalone tool.[3]

Financial institutions can select the framework that best fits their size, complexity, and risk environment.

As a result, many financial institutions have chosen to transition to frameworks that continue to receive active development, ongoing maintenance, broad industry adoption, and recognition from regulators.

2026 CYBERSECURITY FRAMEWORK ADOPTION



Source: *2026 Tandem Cybersecurity GRC Survey (n=306). Respondents could select more than one framework, so percentages total more than 100%.*

[3] Conference of State Bank Supervisors, "FFIEC CAT Sunset Frequently Asked Questions," September 18, 2024

The Board's Role in Cybersecurity Assessments

The Board of Directors plays an important oversight role in the financial institution's cybersecurity program. Use the following questions to discuss what the assessment indicates about the institution's cybersecurity posture and whether management is taking appropriate steps to address identified gaps and risks.

FRAMEWORK SELECTION

Objective: Understand why management selected this framework

- [ ] Which framework is the institution using?
- [ ] Is the framework appropriate for the institution's size, complexity, and risk profile?
- [ ] How does the framework align with regulatory expectations?
- [ ] Has management evaluated alternative or supplemental frameworks?

OVERALL RESULTS

Objective: Understand the institution's overall performance against the selected framework.

- [ ] How did the institution perform overall?
- [ ] What do the results indicate about the institution's cybersecurity posture?
- [ ] Does management believe the results accurately reflect the institution's cybersecurity program?

RISK COVERAGE

Objective: Understand whether the assessment addresses the institution's most significant cybersecurity risks.

- [ ] What are the institution's most significant cybersecurity risks?
- [ ] Did the assessment evaluate controls related to those risks?
- [ ] Were any significant areas excluded from the assessment?

GAP ANALYSIS

Objective: Understand any weaknesses that could expose the institution to heightened risk.

- [ ] What gaps were identified by the assessment?
- [ ] Which gaps present the greatest risk to the institution?
- [ ] Which gaps are management's highest priorities for remediation?

PEER COMPARISON

Objective: Understand how the institution's cybersecurity program compares with similar organizations.

- [ ] How do our results compare with peer institutions?
- [ ] Are there areas where we appear significantly ahead of or behind our peers?
- [ ] Do the differences reflect our risk profile and strategy, or potential weaknesses?

REMEDIATION PLANNING

Objective: Understand how management plans to address identified gaps.

- What remediation plans have been established?
- What resources are needed to address significant findings?
- What is the expected timeline for remediation?
- How will progress be reported to the Board of Directors?

PROGRESS OVER TIME

Objective: Understand whether the institution's cybersecurity program is improving.

- What improvements have been made since the last assessment?
- Which previously identified gaps have been resolved?
- Have any new gaps or concerns emerged?
- Is the institution making measurable progress over time?

Documents Directors Should Expect to Receive

As institutions transition away from the FFIEC CAT to different assessment frameworks, the reporting format and terminology may change. Regardless of the framework used, the Board of Directors should typically receive:

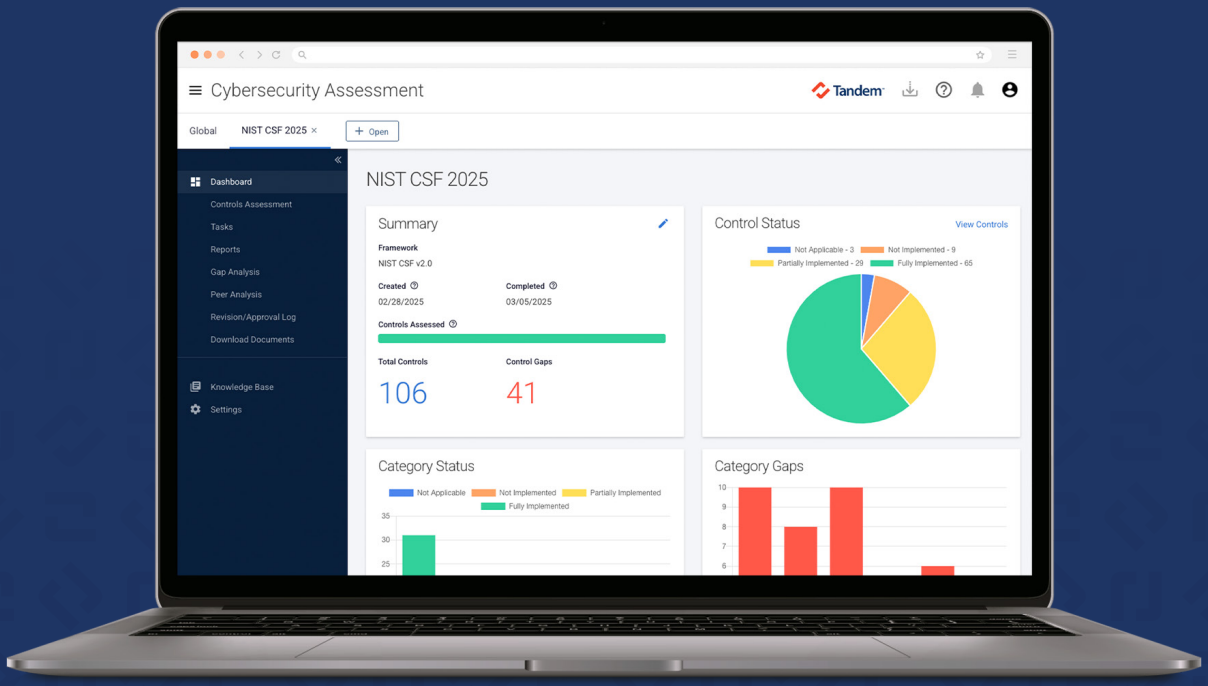
Cybersecurity Assessment Executive Overview
A summary of results, significant gaps, peer comparisons (if available), remediation activities, and progress over time.

Information Security Risk Assessment
An inventory of the institution's significant information security and cybersecurity risks and related risk exposure.

Supporting Documentation (as appropriate)
Other relevant control evidence and cybersecurity program documentation (e.g., vendor management, incident response, audit reports, etc.).

Tandem Cybersecurity Assessment

Turn cybersecurity assessments into reporting that supports Board oversight and examination readiness.



Trusted by more than 1,300 U.S. financial institutions, Tandem Cybersecurity Assessment supports the frameworks referenced in the FFIEC CAT sunset statement and generates executive-level reporting on cybersecurity controls, identified gaps, and remediation efforts. Sign up for free and get started today.

TANDEM.APP/CYBERSECURITY