WELCOME TO

Replacing the FFIEC CAT: A Guide to Cybersecurity Frameworks

Alyssa Pugh, CISM, CRISC, Security+
GRC Content Manager
Tandem, LLC
apugh@tandem.app
LinkedIn.com/in/AlyssaPugh

Savannah Richardson, ITRF
GRC Content Analyst
Tandem, LLC
srichardson@tandem.app
LinkedIn.com/in/Savannah-Lee-Richardson

Tandem

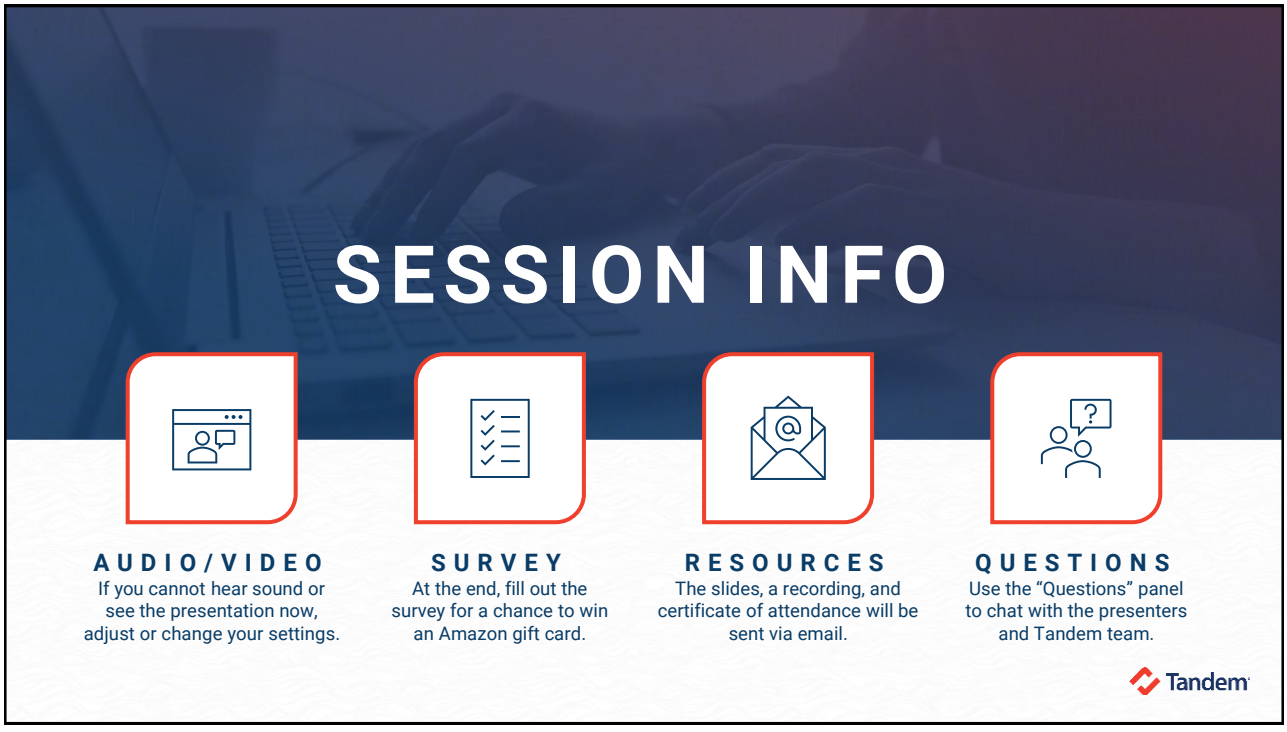
1

DISCLAIMER

- **This presentation is for information only.**
  Evaluate risks before acting on ideas from this session.
- **This presentation contains opinions of the presenters.**
  Opinions may not reflect the opinions of Tandem.
- **This presentation is proprietary.**
  Unauthorized release of this information is prohibited.

Tandem

2


SESSION INFO
AUDIO/VIDEO
If you cannot hear sound or see the presentation now, adjust or change your settings.
SURVEY
At the end, fill out the survey for a chance to win an Amazon gift card.
RESOURCES
The slides, a recording, and certificate of attendance will be sent via email.
QUESTIONS
Use the "Questions" panel to chat with the presenters and Tandem team.
Tandem

3


Audit Management
Business Continuity Plan
Compliance Management
Cybersecurity Assessment
Identity Theft Prevention
Incident Management
Internet Banking Security
Phishing
Policies
Risk Assessment
Vendor Management
Tandem®
A CoNetrix company
Tandem

4

POLL QUESTION

What type of organization do you currently work for?

Tandem

5

POLL QUESTION

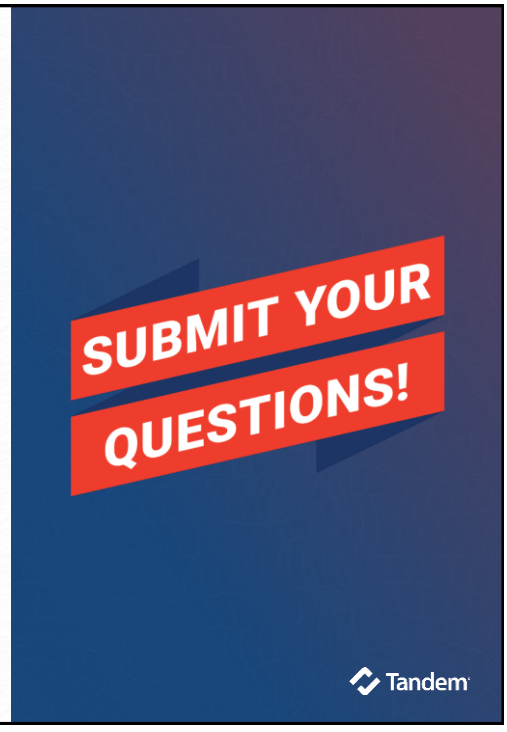
What is your organization's asset size?

Tandem

6

Session Topics

- Background
- Frameworks Overview
- Comparing Frameworks
- How to Pick a Framework
- Tandem Cybersecurity Assessment
- Wrap Up & Resources



7

Background

8

BACKGROUND

FEB 2013
Executive Order 13636

OCT 2016
FFIEC CAT FAQ

AUG 2024
FFIEC CAT Sunset Stmt.

JUN 2015
FFIEC CAT v1.0

MAY 2017
FFIEC CAT v1.1

AUG 2019
FFIEC Guidance

https://tandem.app/blog/a-complete-history-of-the-ffiec-cat

Tandem

9

Federal Financial Institutions Examination Council

3501 Fairfax Drive • E-2035-C • Arlington, VA 22226-3550 • (703) 516-5588 • www.ffiec.gov

CAT Sunset Statement

The Federal Financial Institutions Examination Council (FFIEC),[1] on behalf of its members, is issuing this statement to communicate the agencies will sunset the Cybersecurity Assessment Tool (CAT)[2] on August 31, 2025.

The CAT was released in June 2015 as a voluntary assessment tool to help financial institutions identify their risks and determine their cybersecurity preparedness. While the fundamental security controls addressed throughout the maturity levels of the CAT are sound, several new and updated government and industry resources are available that financial institutions can leverage to better manage cybersecurity risks.

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. Supervised financial institutions can instead refer directly to these new government resources. CISA released Cross-Sector Cybersecurity Performance Goals in 2023 and is preparing to release Cybersecurity Performance Goals for the Financial Sector later this year. These resources were developed to help organizations of all sizes and sectors manage and reduce their cybersecurity risk in alignment with a whole-of-government approach to improve security and resilience. The FFIEC will discuss these resources during a banker webinar this Fall.

Supervised financial institutions may also consider use of industry-developed resources, such as the Cyber Risk Institute's (CRI) Cyber Profile, and the Center for Internet Security Critical Security Controls. These tools can be used in conjunction with other resources (e.g., frameworks, standards, guidelines, leading practices) to better address and inform management of continuously evolving cyber security risk. Supervised financial institutions should ensure that any self-assessment tool(s) they utilize support an effective control environment and are commensurate with their risk.

While the FFIEC does not endorse any particular tool, these standardized tools can assist financial institutions in their self-assessment activities. The tools are not examination programs and the FFIEC

[1] The FFIEC members are the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency (OCC), the Consumer Financial Protection Bureau (CFPB), the National Credit Union Administration (NCUA), and the State Liaison Committee. The FFIEC was established in March 1979 to prescribe uniform principles, standards, and report forms and to make recommendations to promote uniformity in supervisory matters. Issuance of this statement aligns with the FFIEC's mission of promoting consistency in supervisory matters.

[2] The National Credit Union Administration will continue to support and encourage credit unions to use the Automated Cybersecurity Examination Toolbox (NCUA ACET). Use of the NCUA ACET is voluntary and can be downloaded from the NCUA's website.

Board of Governors of the Federal Reserve System, Consumer Financial Protection Bureau, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, State Liaison Committee

https://www.ffiec.gov/sites/default/files/media/press-releases/2024/cat-sunset-statement-ffiec-letterhead.pdf

FFIEC CAT Sunset Statement

Sunset Date: August 31, 2025

Tandem

10

Frameworks Overview

Tandem

11

POLL QUESTION

What frameworks are you considering as a replacement for the FFIEC CAT?

Tandem

12

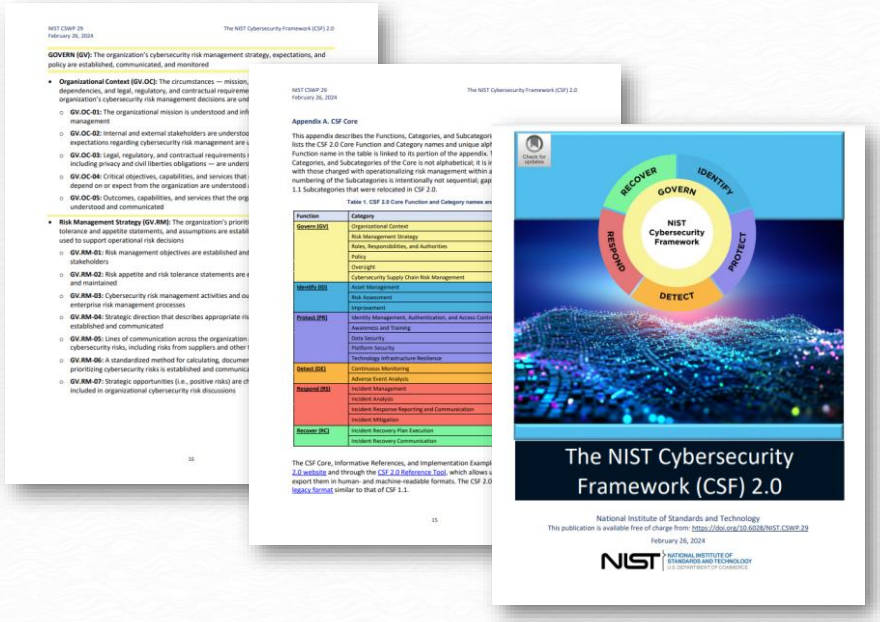
THE FRAMEWORKS

- NIST Cybersecurity Framework (CSF)
- CISA Cybersecurity Performance Goals (CPGs)
- Cyber Risk Institute (CRI) Profile
- Center for Internet Security (CIS) Controls
- Other Frameworks

Tandem

13

NIST CYBERSECURITY FRAMEWORK (CSF)



Tandem

14

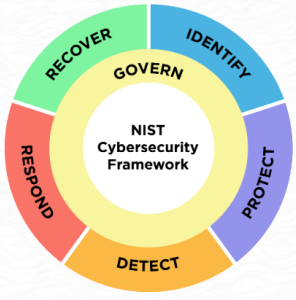
NIST CYBERSECURITY FRAMEWORK (CSF)

- **Author:** National Institute of Standards and Technology (Government Agency – Dept. of Commerce)
- **Published:** February 2014 | **Last Updated:** February 2024
- **In Response To:** Executive Order 13636
- **Target Audience:** Critical Infrastructure Sectors (including the Financial Sector)

https://www.nist.gov/cyberframework

15

NIST CYBERSECURITY FRAMEWORK (CSF)



"Outcomes"

Subcategory
PR.DS-11: Backups of data are created, protected, maintained, and tested

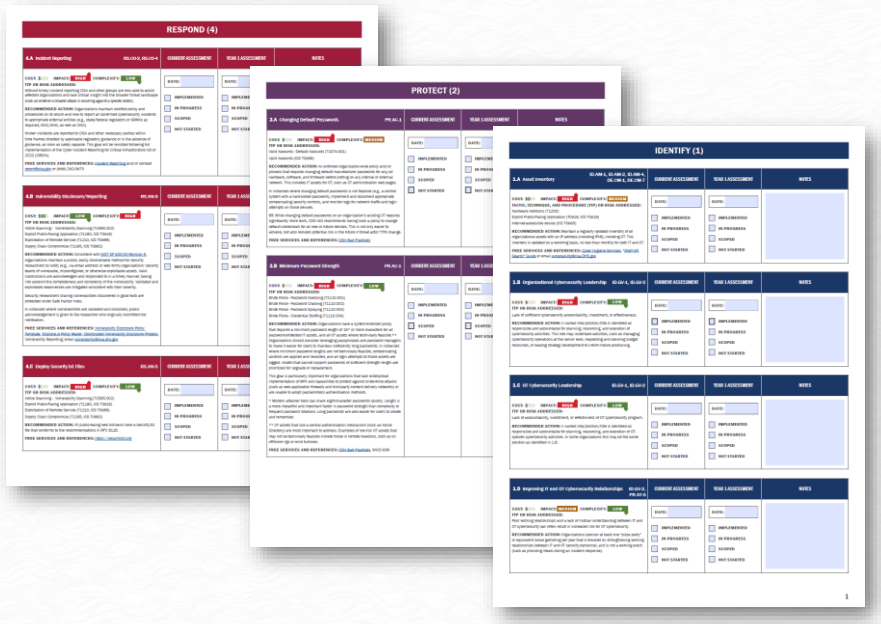
Implementation Examples
Ex1: Continuously back up critical data in near-real-time, and back up other data frequently at agreed-upon schedules
Ex2: Test backups and restores for all types of data sources at least annually
Ex3: Securely store some backups offline and offsite so that an incident or disaster will not damage them
Ex4: Enforce geographic separation and geolocation restrictions for data backup storage

https://csrc.nist.gov/Projects/cybersecurity-framework/Filters#/csf/filters

Tandem

16

CISA CYBERSECURITY PERFORMANCE GOALS (CPGS)



Tandem

17

CISA CYBERSECURITY PERFORMANCE GOALS (CPGS)

- **Author:** Cybersecurity and Infrastructure Security Agency (Government Agency – Dept. of Homeland Security)
- **Published:** October 2022 | **Last Updated:** February 2023
- **In Response To:** July 2021 National Security Memorandum
- **Target Audience:** Critical Infrastructure

https://www.cisa.gov/cross-sector-cybersecurity-performance-goals-cpgs

18

CISA CYBERSECURITY PERFORMANCE GOALS (CPGS)

Simplicity

1.A Asset Inventory — ID.AM-1, ID.AM-2, ID.AM-4, DE.CM-1, DE.CM-7

COST: $$$$ **IMPACT:** HIGH **COMPLEXITY:** MEDIUM

Built-In Consulting

TACTIC, TECHNIQUE, AND PROCEDURE (TTP) OR RISK ADDRESSED:

Hardware Additions (T1200)

Exploit Public-Facing Application (T0819, ICS T0819)

Internet-accessible device (ICS T0883)

RECOMMENDED ACTION: Maintain a regularly updated inventory of all organizational assets with an IP address (including IPv6), including OT. This inventory is updated on a recurring basis, no less than monthly for both IT and OT.

FREE SERVICES AND REFERENCES: Cyber Hygiene Services, "Stuff Off Search" Guide or email vulnerability@cisa.DHS.gov

Helpful Guidance

Tandem

19

CISA FINANCIAL SECTOR-SPECIFIC GOALS (SSGs)

Financial Sector-Specific Goals

Available Now:

- Cross-Sector CPGs
- Chemical Sector SSGs
- Energy Sector (Distribution and Distributed Energy Resources) SSGs
- Healthcare SSGs
- Information Technology SSGs

Coming Soon:

- Financial Services SSGs (Winter 2025)

https://www.cisa.gov/cross-sector-cybersecurity-performance-goals

Tandem

20

CRI PROFILE

PROFILE
CYBER RISK INSTITUTE

CRI Profile ver. 2.0 Assessment

				Target Assessment Level -->				Tier-4
Outline Id	Profile Subcategory	Profile Id	CRI Profile v2.0 Diagnostic Statement	Tier-1	Tier-2	Tier-3	Tier-4	Assessment Rating
003.001	**GOVERN** / Organizational Context / Organizational Mission	GV.OC-01.01	**GV.OC-01.01:** Technology and cybersecurity strategies, architectures, and programs are formally governed to align with and support the organization's mission, objectives, priorities, tactical initiatives, and risk profile.	Yes	Yes	Yes	Yes	To Be Assessed
004.002	**GOVERN** / Organizational Context / Stakeholder Risk Management Expectations	GV.OC-02.01	**GV.OC-02.01:** The organization's obligation to its customers, employees, and stakeholders to maintain safety and soundness, while balancing size and complexity, is reflected in the organization's risk management strategy and framework, its risk appetite and risk tolerance statements, and in a risk-aware culture.	Yes	Yes	Yes	Yes	To Be Assessed
004.003	**GOVERN** / Organizational Context / Stakeholder Risk Management Expectations	GV.OC-02.02	**GV.OC-02.02:** Technology and cybersecurity risk management strategies identify and communicate the organization's role within the financial services sector as a component of critical infrastructure.	Yes	No	No	No	Not Applicable

Tandem

21

CRI PROFILE

- **Author:** Cyber Risk Institute (Non-Profit Organization)
- **Formerly Known As:** FSSCC Cybersecurity Profile
- **Published:** October 2018 | **Last Updated:** February 2024
- **In Response To:** Industry Cybersecurity Needs
- **Target Audience:** Financial Institutions

https://cyberriskinstitute.org/the-profile/

22

CRI PROFILE

PR.AA-03.02: Decisions to authorize user access to devices and other assets are made with consideration of:
(1) Business need for the access;
(2) The type of data being accessed (e.g., customer PII, public data);
(3) The risk of the transaction (e.g., internal-to-internal, external-to-internal);
(4) The organization's level of trust for the accessing agent (e.g., external application, internal user); and
(5) The potential for harm.

Diagnostic Statements

EXTEND / Procurement Planning and Due Diligence / Prospective Third Party Due Diligence	EX.DD-02.01	**EX.DD-02.01:** The organization implements procedures, and allocates sufficient resources with the requisite knowledge and experience, to conduct third party due diligence and risk assessment consistent with the procurement plan and commensurate with level of risk, criticality, and complexity of each third-party relationship.
EXTEND / Procurement Planning and Due Diligence / Prospective Third Party Due Diligence	EX.DD-02.02	**EX.DD-02.02:** The organization reviews and evaluates the proposed business arrangement, to include the proposed fee structures, incentives, and penalties, proposed staff resources, viability of proposed approaches, and business terms, to ensure that products or services are being obtained at competitive and reasonable costs and terms.

"Extended" Emphasis

Target Assessment Level -->				Tier-4
Tier-1	Tier-2	Tier-3	Tier-4	Assessment Rating
Yes	Yes	Yes	Yes	To Be Assessed

Four Tiers

Tier 1 – National/Super-National Impact
Tier 2 – Subnational Impact
Tier 3 – Sector Impact
Tier 4 – Localized Impact

Tandem

23

CRI PROFILE

GV.RM-05.02

The organization establishes minimum requirements for its third-parties that include how the organizations will communicate and coordinate in times of emergency, including:

1. Joint maintenance of contingency plans;
2. Responsibilities for responding to incidents, including forensic investigations;
3. Planning and testing strategies that address severe events in order to identify single points of failure that would cause wide-scale disruption; and
4. Incorporating the potential impact of an incident into their BCM process and ensure resilience capabilities are in place.

ID.RA-03.02

The organization solicits and considers threat intelligence received from the organization's stakeholders, service and utility providers, and other industry and security organizations.

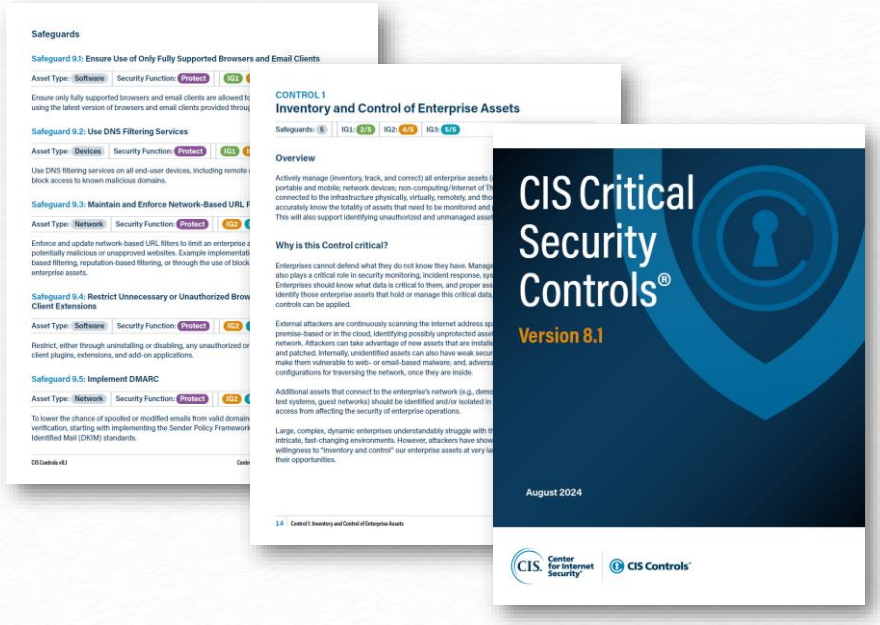
PR.PS-01.02

The organization's systems are configured to provide only essential capabilities to implement the principle of least functionality.

Tandem

24

CIS CONTROLS



Tandem

25

CIS CONTROLS

- **Author:** Center for Internet Security (Non-Profit Organization)
- **Formerly Known As:** SANS Top 20, Consensus Audit Guidelines (CAG)
- **Published:** February 2009 | **Last Updated:** June 2024
- **In Response To:** DoD Contractor Data Breaches
- **Target Audience:** Defense Contractors / Critical Infrastructure

https://www.cisecurity.org/controls

26

CIS CONTROLS

Implementation Groups

Widely Adopted

https://tandem.app/state-of-cybersecurity-report

Highly Supported

Tandem

27

Q: Do I have to use one of these four frameworks?

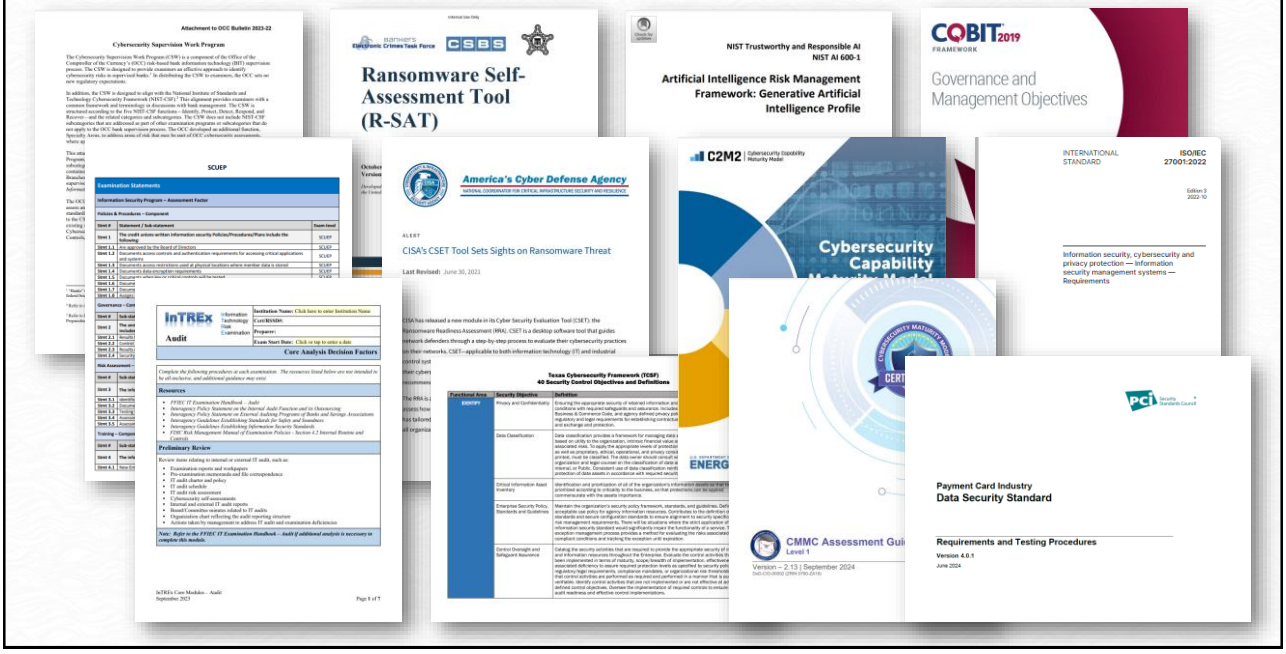
A: Not necessarily. The FFIEC encourages a standardized approach to assessing cybersecurity preparedness. While the sunset statement listed four possible options for this, "supervised financial institutions may also consider use of industry developed resources," as long as the frameworks "support an effective control environment and are commensurate with [the institution's] risk."

https://www.ffiec.gov/news/press-releases/2024/an-09-29
https://www.ffiec.gov/news/press-releases/2019/pr-08-28

Tandem

28

OTHER FRAMEWORKS



29

POLL QUESTION

How many cybersecurity frameworks are you currently using?

Tandem

30

KEY TAKEAWAY

There are a lot of good cybersecurity frameworks out there. Whichever you choose, you're taking a step in the right direction.

SUBMIT YOUR QUESTIONS!

Tandem

31

Comparing Frameworks

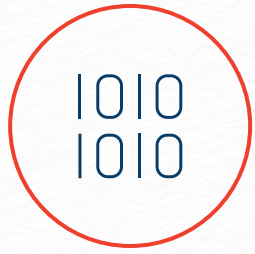
Tandem

32

COMPARING FRAMEWORKS

Training

Authentication



Encryption

Tandem

33

COMPARING FRAMEWORKS: TRAINING

NIST CSF

PR.AT-01
Personnel are provided awareness and training so they possess the knowledge and skills to perform general tasks with security risks in mind.

PR.AT-02
Individuals in specialized roles are provided awareness and training so they possess the knowledge and skills to perform relevant tasks with security risks in mind.

CISA CPGs

2.I Basic Cybersecurity Training
At least annual trainings for all organizational employees and contractors that cover basic security concepts, such as phishing, business email compromise, basic operational security, password security, etc., as well as foster an internal culture of security and cyber awareness.

New employees receive initial cybersecurity training within 10 days of onboarding and recurring training on at least an annual basis.

2.J OT Cybersecurity Training
In addition to basic cybersecurity training, personnel who maintain or secure OT as part of their regular duties receive OT-specific cybersecurity training on at least an annual basis.

CRI PROFILE

PR.AT-01.01
All personnel receive cybersecurity awareness training upon hire and on a regular basis.

PR.AT-01.02
Cybersecurity awareness training includes, at a minimum, awareness of and competencies for data protection, personal data handling, compliance obligations, working with third parties, detecting cyber risks, and how to report any unusual activity or incidents.

PR.AT-01.03
Cybersecurity awareness training is updated on a regular basis to reflect risks and threats identified by the organization, the organization's security policies and standards, applicable laws and regulations, and changes in individual responsibilities.

PR.AT-01.04
As new technology is deployed or undergoes change that also requires changes in practices, all impacted personnel (e.g., end-users, developers, operators, etc.) are trained on the new system and any accompanying technology and cybersecurity risks.

PR.AT-02.01
Mechanisms are in place to ensure that the personnel working with cybersecurity and technology (e.g., developers, DBAs, network admins, etc.) maintain current knowledge and skills related to changing threats, countermeasures, new tools, best practices, and their job responsibilities.

PR.AT-02.02
High-risk groups, such as those with elevated privileges or in sensitive business functions (including privileged users, senior executives, cybersecurity personnel and third-party stakeholders), receive cybersecurity situational awareness training for their roles and responsibilities.

PR.AT-02.03
All personnel (employee and third party) are made aware of and are trained for their role and operational steps in response and recovery plans.

PR.AT-02.04
The organization maintains and enhances the skills and knowledge of the in-house staff performing incident management and forensic investigation activities.

PR.AT-02.05
All third party staff receive cybersecurity awareness and job training sufficient for them to perform their duties and maintain organizational security.

PR.AT-02.06
The organization has established and maintains a cybersecurity awareness program through which the organization's customers are kept aware of new threats and vulnerabilities, basic cybersecurity hygiene practices, and their role in cybersecurity, as appropriate.

PR.AT-02.07
The organization's governing body (e.g., the Board or one of its committees) and senior management receive cybersecurity situational awareness training to include appropriate skills and knowledge to:
1. Evaluate and manage cyber risks;
2. Promote a culture that recognizes that staff at all levels have important responsibilities in ensuring the organization's cyber resilience; and
3. Lead by example.

PR.AT-02.08
Where the organization's governing authority (e.g., the Board or one of its committees) does not have adequate cybersecurity expertise, they should have direct access to the senior officer responsible for cybersecurity and independent sources of expertise to discuss cybersecurity-related matters.

CIS CONTROLS

CIS Control 14
Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.

CIS Control 14.1
Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.

CIS Control 14.2
Train workforce members to recognize social engineering attacks, such as phishing, business email compromise (BEC), pretexting, and tailgating.

CIS Control 14.3
Train workforce members on authentication best practices. Example topics include MFA, password composition, and credential management.

CIS Control 14.4
Train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive data. This also includes training workforce members on clear screen and desk best practices, such as locking their screen when they step away from their enterprise asset, erasing physical and virtual whiteboards at the end of meetings, and storing data and assets securely.

CIS Control 14.5
Train workforce members to be aware of causes for unintentional data exposure. Example topics include mis-delivery of sensitive data, losing a portable end-user device, or publishing data to unintended audiences.

CIS Control 14.6
Train workforce members to be able to recognize a potential incident and be able to report such an incident.

CIS Control 14.7
Train workforce to understand how to verify and report out-of-date software patches or any failures in automated processes and tools. Part of this training should include notifying IT personnel of any failures in automated processes and tools.

CIS Control 14.8
Train workforce members on the dangers of connecting to and transmitting data over insecure networks for enterprise activities. If the enterprise has remote workers, training must include guidance to ensure that all users securely configure their home network infrastructure.

CIS Control 14.9
Conduct role-specific security awareness and skills training. Example implementations include secure system administration courses for IT professionals, OWASP® Top 10 vulnerability awareness and prevention training for web application developers, and advanced social engineering awareness training for high-profile roles.

Tandem

34

COMPARING FRAMEWORKS: AUTHENTICATION

NIST CSF

PR.AA-03
Users, services, and hardware are authenticated

CISA CPGs

2.B Minimum Password Strength
Organizations have a system-enforced policy that requires a minimum password length of 15 or more characters for all password-protected IT assets, and all OT assets where technically feasible. Organizations should consider leveraging passphrases and password managers to make it easier for users to maintain sufficiently long passwords. In instances where minimum password lengths are not technically feasible, compensating controls are applied and recorded, and all login attempts to those assets are logged. Assets that cannot support passwords of sufficient strength length are prioritized for upgrade or replacement.

2.H Phishing-Resistant MFA
Organizations implement MFA for access to assets using the strongest available method for that asset.

CRI PROFILE

PR.AA-01.01
Identities and credentials are actively managed or automated for authorized devices and users (e.g., removal of default and factory passwords, password strength requirements, automatic revocation of credentials under defined conditions, regular asset owner access review, etc.).

PR.AA-02.01
The organization authenticates identity, validates the authorization level of a user before granting access to its systems, limits the use of an account to a single individual, and attributes activities to the user in logs and transactions.

PR.AA-03.01
Based on the risk level of a user access or a specific transaction, the organization defines and implements authentication requirements, which may include multi-factor or out-of-band authentication, and may adopt other real-time risk prevention or mitigation tactics.

PR.AA-04.01
Access credential and authorization mechanisms for internal systems and across security perimeters (e.g., leveraging directory services, directory synchronization, single sign-on, federated access, credential mapping, etc.) are designed to maintain security, integrity, and authenticity.

PR.AA-05.02
The organization institutes controls over privileged system access by strictly limiting and closely managing staff and services with elevated system entitlements (e.g., multi-factor authentication, dual accounts, privilege and time constraints, etc.)

PR.AA-05.03
The organization institutes controls over service account (i.e., accounts used by systems to access other systems) lifecycles to ensure strict security over creation, use, and termination; access credentials (e.g., no embedded passwords in code); frequent reviews of account ownership; visibility for unauthorized use; and hardening against malicious insider use.

CIS CONTROLS

CIS Control 4.10
Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts.

CIS Control 5.2
Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using Multi-Factor Authentication (MFA) and a 14-character password for accounts not using MFA.

CIS Control 6.6
Establish and maintain an inventory of the enterprise's authentication and authorization systems, including those hosted on-site or at a remote service provider. Review and update the inventory, at a minimum, annually, or more frequently.

CIS Control 7.5
Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans.

CIS Control 12.7
Require users to authenticate to enterprise-managed VPN and authentication services prior to accessing enterprise resources on end-user devices.

CIS Control 13.9
Deploy port-level access control. Port-level access control utilizes 802.1x, or similar network access control protocols, such as certificates, and may incorporate user and/or device authentication.

CIS Control 16.11
Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.

Tandem

35

COMPARING FRAMEWORKS: ENCRYPTION

NIST CSF

PR.DS-01
The confidentiality, integrity, and availability of data-at-rest are protected

PR.DS-02
The confidentiality, integrity, and availability of data-in-transit are protected

PR.DS-04
The confidentiality, integrity, and availability of data-in-use are protected

CISA CPGs

2.K Strong and Agile Encryption
Properly configured and up-to-date transport layer security (TLS) is utilized to protect data in transit, when technically feasible. Organizations should also plan to identify any use of outdated or weak encryption, update these to sufficiently strong algorithms, and consider managing implications of post-quantum cryptography.

CRI PROFILE

PR.DS-01.01
Data-at-rest is protected commensurate with the criticality and sensitivity of the information and in alignment with the data classification and protection policy (e.g., through the use of encryption, authentication, access control, segregation, masking, tokenization, and file integrity monitoring).

PR.DS-01.03
The organization defines and implements controls for the protection and use of removable media (e.g., access/use restrictions, encryption, malware scanning, data loss prevention, etc.)

PR.DS-02.01
Data-in-transit is protected commensurate with the criticality and sensitivity of the information and in alignment with the data classification and protection policy (e.g., through the use of encryption, authentication, access control, masking, tokenization, and alternate transit paths).

PR.DS-10.01
Data-in-use is protected commensurate with the criticality and sensitivity of the information and in alignment with the data classification and protection policy (e.g., through the use of encryption, authentication, access control, masking, tokenization, visual shielding, memory integrity monitoring, etc.)

PR.PS-01.05
Acceptable encryption standards, methods, and management practices are established in accordance with defined industry standards.

PR.PS-01.06
The organization employs defined encryption methods and management practices commensurate with the criticality of the information being protected and the inherent risk of the technical environment where used.

PR.PS-01.08
End-user mobile or personal computing devices accessing the organization's network employ mechanisms to protect network, application, and data integrity, such as "Mobile Device Management (MDM)" and "Mobile Application Management (MAM)" technologies, device fingerprinting, storage containerization and encryption, integrity scanning, automated patch application, remote wipe, and data leakage protections.

PR.IR-01.05
Remote access is carefully controlled (e.g., restricted to defined systems, access is actively managed (e.g., session timeouts, logging, forced disconnect, etc.), and encrypted connections with multi-factor authentication are used).

CIS CONTROLS

CIS Control 3.6
Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.

CIS Control 3.9
Encrypt data on removable media.

CIS Control 3.10
Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).

CIS Control 3.11
Encrypt sensitive data at rest on servers, applications, and databases. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.

CIS Control 11.3
Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements.

CIS Control 15.4
Ensure service provider contracts include security requirements. Example requirements may include minimum security program requirements, security incident and/or data breach notification and response, data encryption requirements, and data disposal commitments. These security requirements must be consistent with the enterprise's service provider management policy. Review service provider contracts annually to ensure contracts are not missing security requirements.

CIS Control 16.11
Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.

Tandem

36

Overlap is not equal.

Tandem

37

POLL QUESTION

When do you plan to transition to another framework?

Tandem

38

KEY TAKEAWAY

Similar structures and goals don't mean identical controls or requirements.

SUBMIT YOUR QUESTIONS!

Tandem

39

How to Pick a Framework

Tandem

40

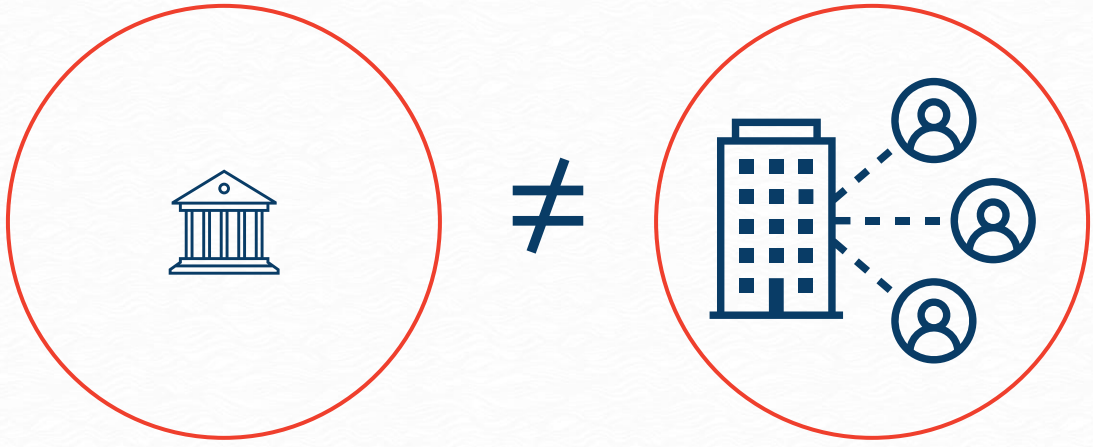
THE BEST CYBERSECURITY FRAMEWORK

- Matches Size & Complexity
- Cost Friendly
- Easy to Understand
- Familiar to Stakeholders
- Easy to Implement
- Easy to Report

Tandem

41

SIZE & COMPLEXITY



Tandem

42

EASY TO UNDERSTAND

1 Clear Language

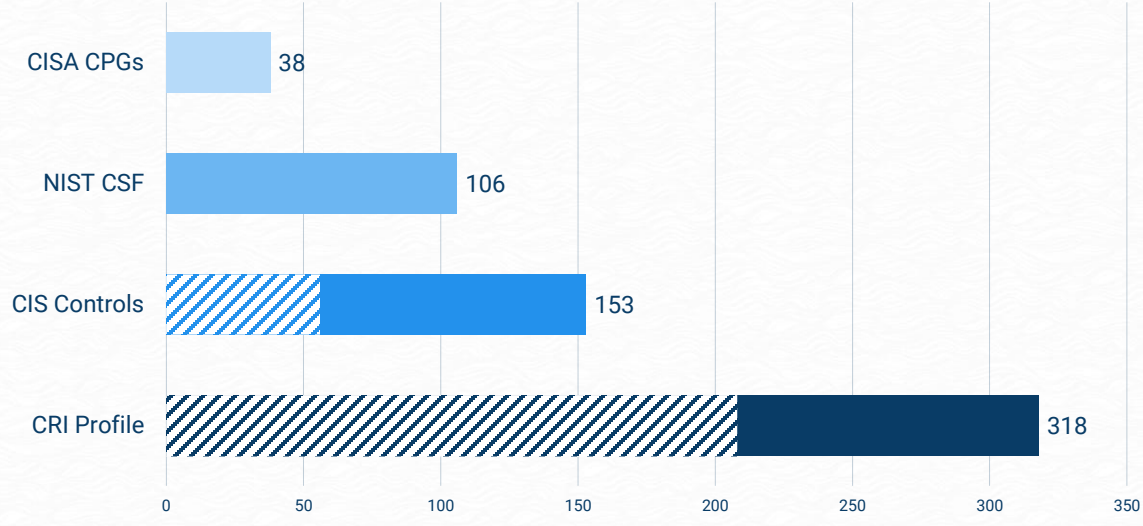
2 Actionable Steps

3 Prioritized Structure

Tandem

43

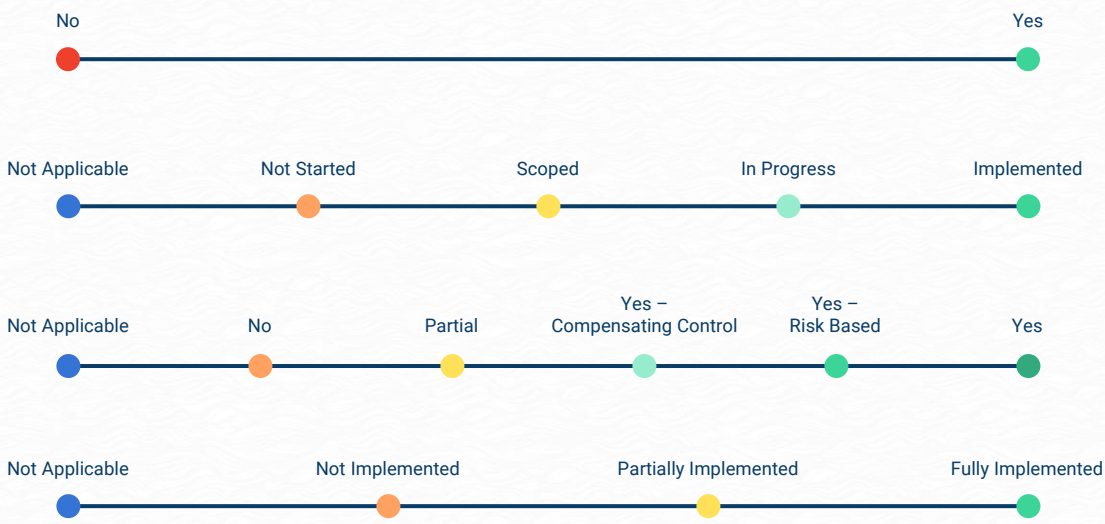
EASY TO IMPLEMENT | LENGTH



Tandem

44

EASY TO IMPLEMENT | FLEXIBILITY



Tandem

45

COST FRIENDLY

Control Costs

Time Costs

Vendor Costs

Tandem

46

POLL QUESTION

Will a vendor be helping you with your cybersecurity assessments?

Tandem

47

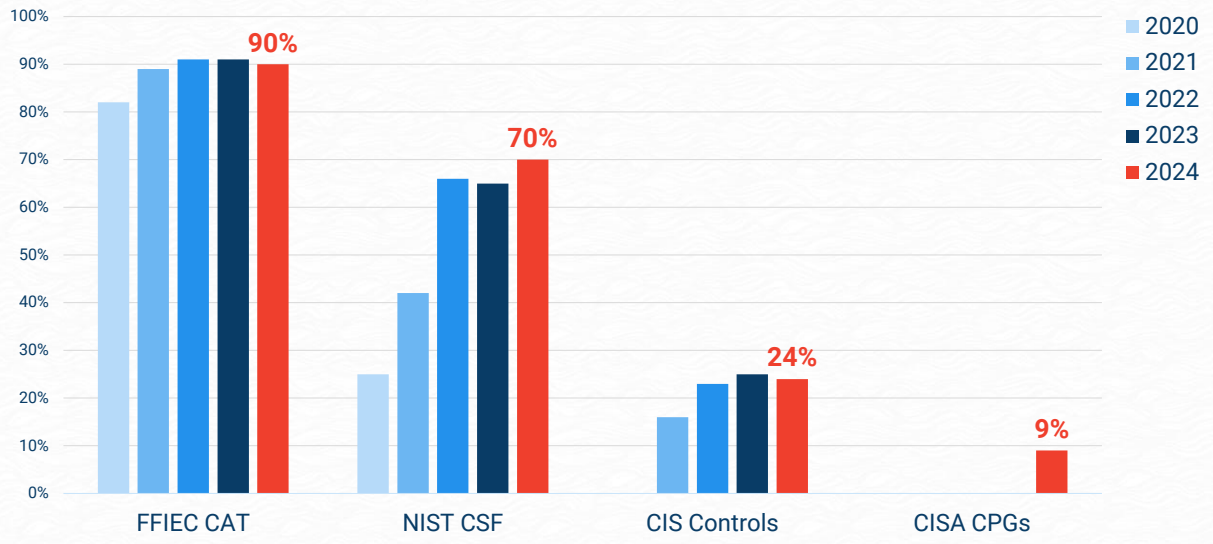
FAMILIAR TO STAKEHOLDERS

- Information Technology (IT)
- External Auditors
- Board of Directors
- Regulators
- Senior Leadership
- Vendors (e.g., MSP, consultants, etc.)

Tandem

48

FAMILIAR TO STAKEHOLDERS



https://tandem.app/state-of-cybersecurity-report

Tandem

49

The more familiar a framework is, the smoother the adoption process.

Tandem

50

EASY TO REPORT

Summary Reports

Executive-Level Data

Charts & Graphs

Tandem

51

KEY TAKEAWAY

The best framework is the one that fits. Choose what works for your team, your size, and your goals, and makes your life a little easier along the way.

SUBMIT YOUR QUESTIONS!

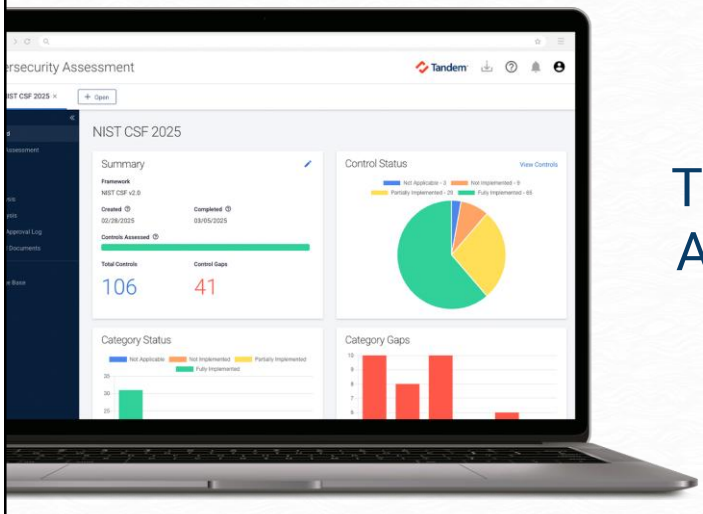
Tandem

52

Tandem Cybersecurity Assessment

Tandem

53



EARLY RELEASE

Tandem Cybersecurity Assessment Software

Tandem.App/Cybersecurity

54

TANDEM CYBERSECURITY ASSESSMENT

FREE

- Enable frameworks
- Create assessments
- Compare with peers
- Review dashboards and reports
- Send reminders with tasks

SIGN UP
Tandem.App/Cybersecurity

PRO

- Copy assessments
- Upload file attachments
- Edit and Read Only access
- Filter peer results
- Create custom documents
  (Coming soon!)

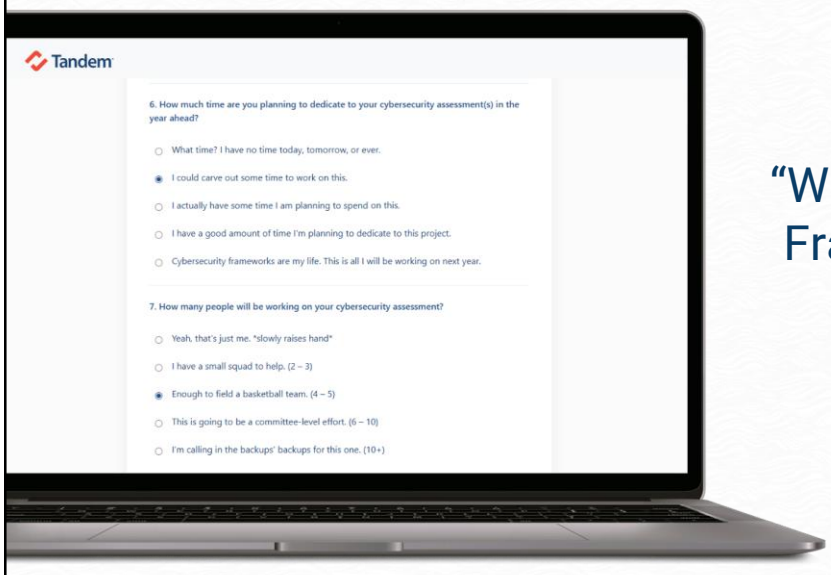
SPECIAL PRICING
Request a quote and sign before May 1st

55

Wrap Up & Resources

56

CYBERSECURITY FRAMEWORK QUIZ



FREE RESOURCE

"Which Cybersecurity Framework Should I Choose?" Quiz

Tandem.App/Quiz

Tandem

57

58

THANKS FOR JOINING

Replacing the FFIEC CAT: A Guide to Cybersecurity Frameworks

Alyssa Pugh, CISM, CRISC, Security+
GRC Content Manager
Tandem, LLC
apugh@tandem.app
LinkedIn.com/in/AlyssaPugh

Savannah Richardson, ITRF
GRC Content Analyst
Tandem, LLC
srichardson@tandem.app
LinkedIn.com/in/Savannah-Lee-Richardson

- ☑ *Remember to complete the survey!*
- ☑ *Sign up for free: Tandem.App/Cybersecurity*
- ☑ *Take the quiz: Tandem.App/Quiz*

Tandem

59