JONATHAN GARNER & MORGAN MARET

A New Beginning for Cybersecurity Assessments

KEYS 2026 HORIZONS

Sign into Tandem to participate in this session.

1

DISCLAIMER

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

KEYS

2

Jonathan Garner
Support Assistant Manager
Tandem

Morgan Maret
Software Specialist
Tandem

KEYS

3

SESSION AGENDA

1. What is a Cybersecurity Assessment?
2. Choosing a Cybersecurity Framework
3. Cybersecurity Assessments in Tandem
4. Best Practices for Reporting to Stakeholders

KEYS

4

FFIEC CAT

KEYS

5

What is a Cybersecurity Assessment?

KEYS

6

CYBERSECURITY FRAMEWORKS

KEYS

7

FRAMEWORK

A structured set of guidelines, standards, best practices, goals, outcomes, or specific controls.

CONTROL

A security measure that an organization puts in place to prevent, detect, or respond to cybersecurity threats. For example, a policy, data encryption, or physically locking doors.

MAPPING

How controls from one cybersecurity framework logically align with those in another.

KEYS

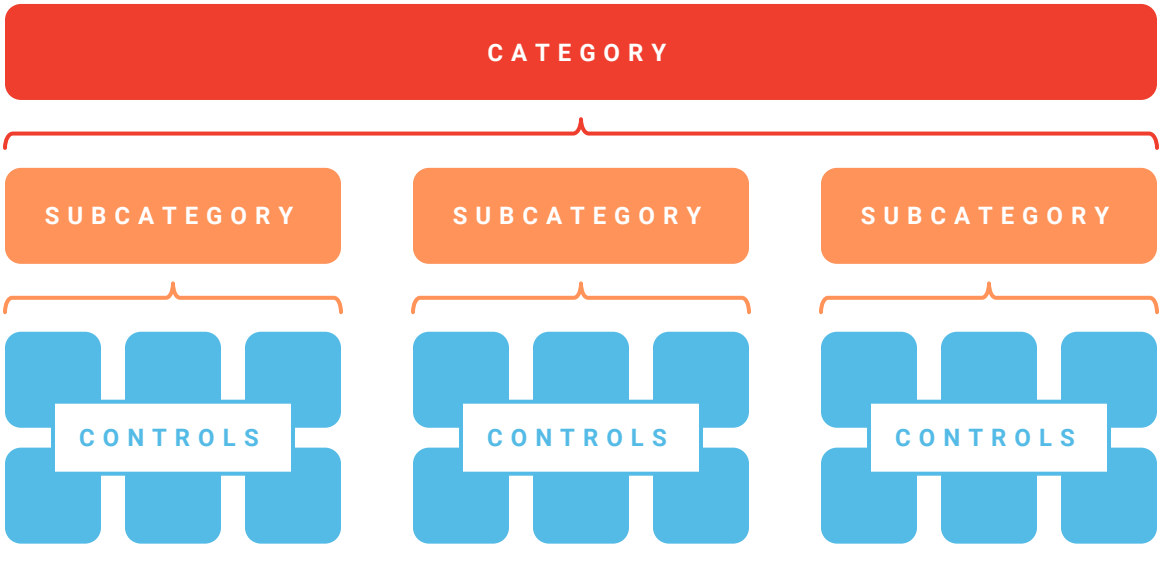
8

Choosing a Cybersecurity Framework

KEYS

9

FRAMEWORK STRUCTURE



KEYS

10

COMPARING FRAMEWORKS

NIST CSF

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

CISA CPGs

3.F Implement Multi-Factor Authentication
Add a critical, additional layer of security to protect assets accounts.

3.K Utilize Strong Encryption
Encryption is deployed to maintain confidentiality and integrity of sensitive data across the organization's network to protect from unauthorized access.

3.L Enable Email Security
Reduce risk from common email-based threats, such as spoofing, phishing, and interception.

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, tion, 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 tion algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.

KEYS

11

CONSIDER YOUR INSTITUTION'S PRIORITIES

1. Matches Size & Complexity
2. Easy to Understand
3. Simple to Implement
4. Cost Friendly
5. Familiar to Stakeholders
6. Easy to Report

KEYS

12

Q: What impacted the decision to use your current cybersecurity framework most?

1. Regulatory Expectations
2. Board or Executive Preference
3. Industry Norms or Peers
4. Other

KEYS

13

Q: What is your organization's priority when selecting a cybersecurity framework?

1. Size & Complexity Match
2. Familiarity
3. Simple Implementation
4. Other

KEYS

14

CISA CYBERSECURITY PERFORMANCE GOALS (CPGS)

Security Practices: 38	Built-In Consulting
Target Audience: Critical Infrastructure	Additional Resources
Focuses on Simplicity	Last Modified: December 2025, v2.0

KEYS

15

CENTER FOR INTERNET SECURITY (CIS) CONTROLS

Safeguards: Up to 153	Clear Growth Vision
Target Audience: Defense Contractors and Critical Infrastructure	OG: First developed in 2008
Implementation Groups	Last Modified: March 2025, v8.1.2

KEYS

16

CYBER RISK INSTITUTE (CRI) PROFILE

Diagnostic Statements: Up to 318	Four Tiers
Target Audience: Financial Services Sector	Small / Regional Sized FI's - Tier 4 Diagnostic Statements: 208
Deep Dive Framework	Last Modified: April 2025, v2.1

KEYS

17

NIST CYBERSECURITY FRAMEWORK (CSF)

Outcomes: 106	Very Popular Framework
Designed for All Organizations	Developed by the U.S. Government in 2014
Gold Standard	Last Modified: February 2024, v2.0

KEYS

18


TIME FOR OUR
Cybersecurity Framework Draft
KEYS

19


1. Examine Your 1st Round Pick
2. Complete your Draft
3. Discuss with Your Table
TANDEM.APP/QUIZ
KEYS

20

Framework	Controls	Groups	Fun Fact	Version
CISA CPGs	38	N/A	Details Cost, Impact, & Complexity	Dec. 2025, v2.0
CIS Controls	Up to 153	3	Clear Growth Vision	Mar. 2025, v8.1.2
CRI Profile	Up to 318	4	Dives Deep	Apr. 2025, v2.1
NIST CSF	106	N/A	Gold Standard	Feb. 2024, v2.0

KEYS

21

Q: Which framework did you draft first?

1 CISA CPGs

2 CIS Controls

3 CRI Profile

4 NIST CSF

KEYS

22

Q: How many cybersecurity frameworks does your institution use right now?

1 One

2 Two

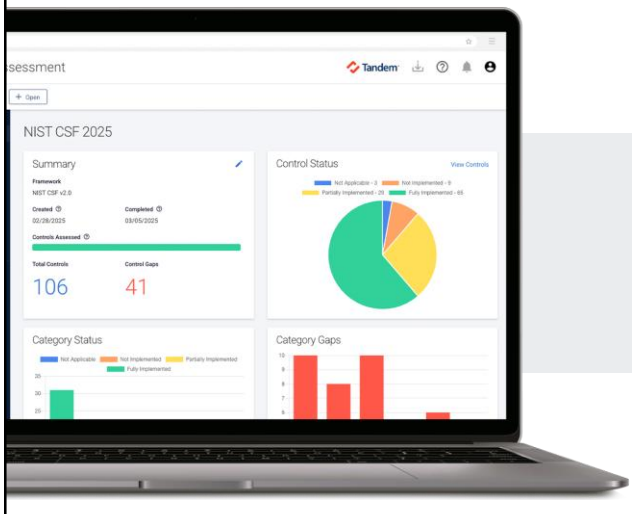
3 Three

4 4 or More

KEYS

23

KEYS



Tandem Cybersecurity Assessment Software

24

SESSION RECAP

1. Defined Cybersecurity Assessment
2. Evaluated 4 Frameworks and How to Choose a Cybersecurity Framework
3. Looked at Tandem Cybersecurity Assessment Pro
4. Viewed Sample Reports for Stakeholders

KEYS

25

KEYS

26

Fill out the survey to get your sticker!

KEYS

27

Thank You!

CONNECT WITH OUR SPEAKERS AT TANDEM.APP/AGENDA

KEYS

28