WELCOME TO

From CAT to CSF: A Strategic Conversation for Financial Institutions

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

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.
  Original material is copyright © 2025 Tandem.

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

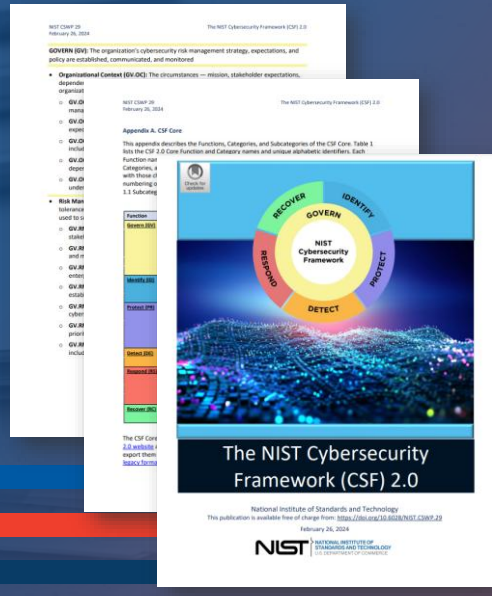
SESSION AGENDA

- NIST CSF Overview
- Interview with an Expert
  Daniel Eliot, NIST Applied Cybersecurity Division
- Wrap Up & Bonus Content
  How to Use Tandem to Complete the NIST CSF

Tandem

7

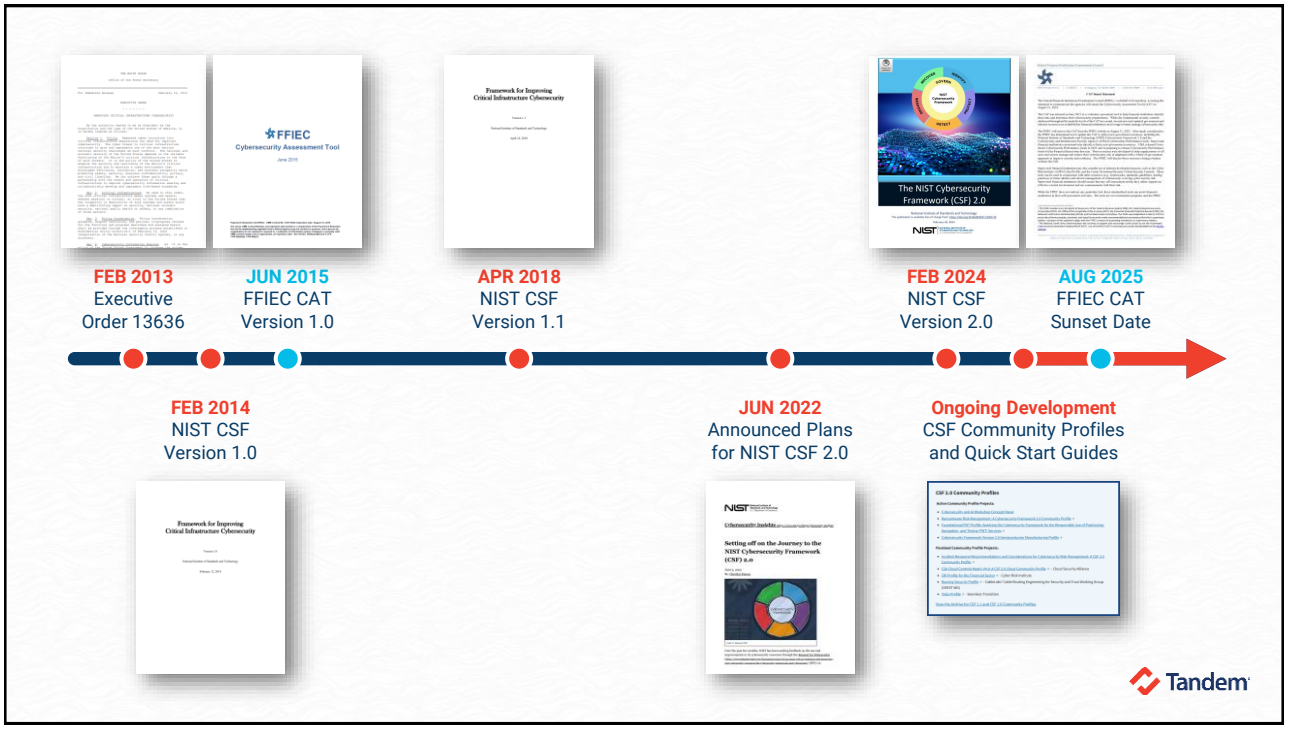
NIST Cybersecurity Framework Overview



https://nist.gov/cyberframework

Tandem

8



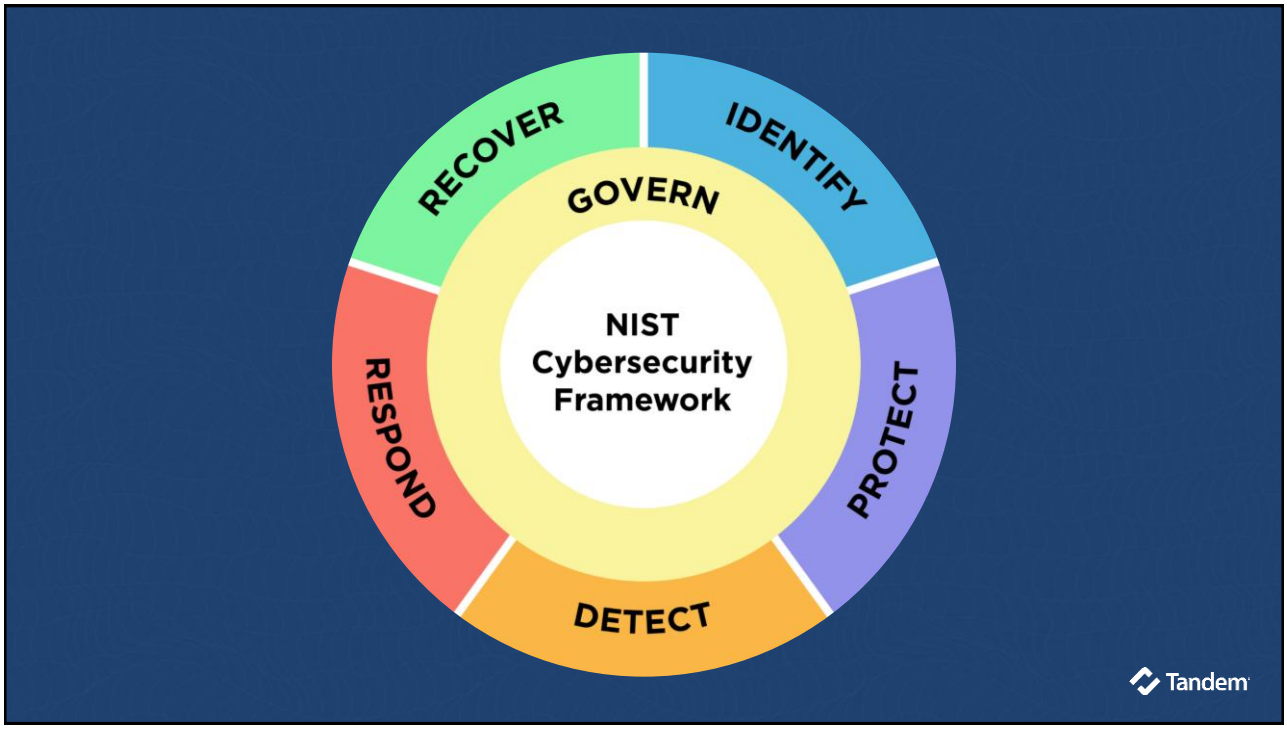
9

POLL QUESTION

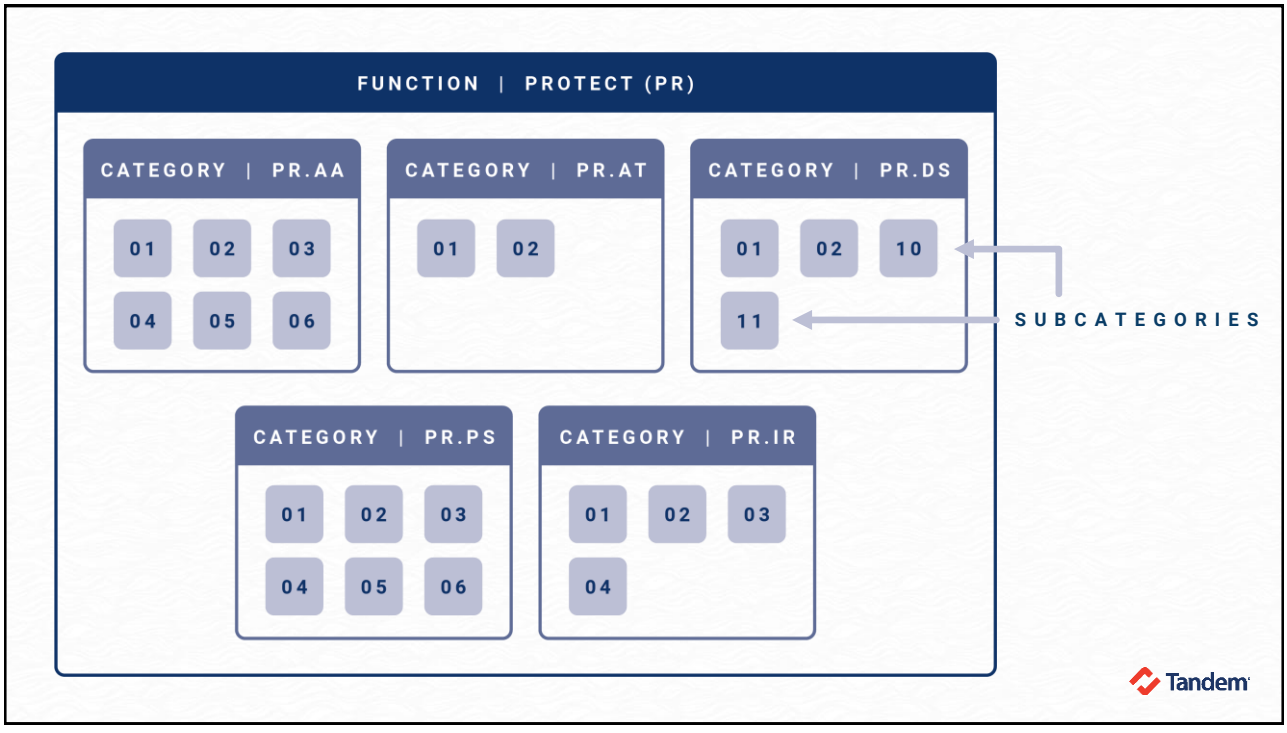
Does your organization use the NIST CSF?

Tandem

10


RECOVER
IDENTIFY
GOVERN
NIST
Cybersecurity
Framework
PROTECT
RESPOND
DETECT
Tandem

11


FUNCTION | PROTECT (PR)
CATEGORY | PR.AA
01
02
03
04
05
06
CATEGORY | PR.AT
01
02
CATEGORY | PR.DS
01
02
10
11
SUBCATEGORIES
CATEGORY | PR.PS
01
02
03
04
05
06
CATEGORY | PR.IR
01
02
03
04
Tandem

12

NIST CSF OUTCOME	FFIEC CAT DECLARATIVE STATEMENTS
PR.DS-11 Backups of data are created, protected, maintained, and tested.	• **Baseline:** A formal backup and recovery plan exists for all critical business lines. • **Baseline:** The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident. • **Evolving:** Information backups are tested periodically to verify they are accessible and readable. • **Intermediate:** The enterprise network is segmented in multiple, separate trust/security zones with defense-in-depth strategies (e.g., logical network segmentation, hard backups, air-gapping) to mitigate attacks. • **Innovative:** The technology infrastructure has been engineered to limit the effects of a cyber attack on the production environment from migrating to the backup environment (e.g., air-gapped environment and processes).

Tandem

13

> "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. […] 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."

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

Tandem

14

Function

PROTECT (PR): Safeguards to manage the organization's cybersecurity risks are used

Category

Data Security (PR.DS): Data are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information

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

15

KEY TAKEAWAY

The CSF is a flexible framework created and supported by NIST. Its outcome-focused approach makes it a strong foundation for other frameworks and a solid option for financial institutions.

Tandem

16

Interview with an Expert

Tandem

17

Daniel Eliot
Applied Cybersecurity Division
National Institute of Standards & Technology

Daniel Eliot works within the Applied Cybersecurity Division of the National Institute of Standards and Technology (NIST), part of the U.S. Department of Commerce. Daniel helps lead the NIST Cybersecurity Framework (CSF) 2.0 project, working to expand the portfolio of CSF 2.0 resources and regularly promoting adoption and use of the CSF more broadly. Daniel also serves as the lead for small business engagement, working across NIST's cybersecurity and privacy program to advise and support development of cybersecurity resources, communication materials, and collateral tailored for use by small businesses and their resource partners. Prior to joining NIST, Daniel held cybersecurity roles at MITRE Corporation's Center for Securing the Homeland, the National Cybersecurity Alliance, and the University of Delaware's Office of Economic Innovation and Partnerships.

LinkedIn.com/in/Daniel-Eliot

Tandem

18

DISCUSSION TOPIC

Understanding the NIST CSF

Tandem

19

DISCUSSION TOPIC

Supply Chain Risk Management
(GV.SC)

Tandem

20

DISCUSSION TOPIC

Positive Cybersecurity Risk
(GV.RM-07)

"Strategic opportunities (i.e., positive risks) are characterized and are included in organizational cybersecurity risk discussions."

Tandem

21

DISCUSSION TOPIC

Secure Software Development
(PR.PS-06)

"Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle."

Tandem

22

DISCUSSION TOPIC

Data and Metadata Inventory
(ID.AM-07)

"Inventories of data and corresponding metadata for designated data types are maintained."

Tandem

23

DISCUSSION TOPIC

Implementing the NIST CSF

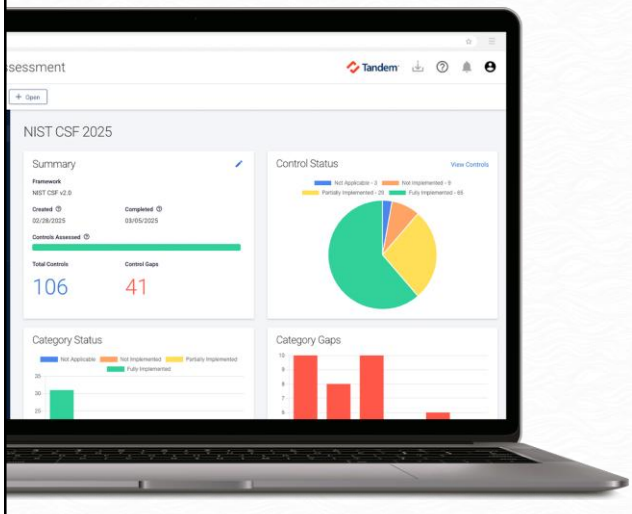
Tandem

24

Wrap Up & Bonus Content

Tandem

25



LEARN MORE

Tandem Cybersecurity Assessment Software

Tandem.App/Cybersecurity

26

27

FURTHER READING

NIST RESOURCES

- NIST Cybersecurity Framework
- NIST Cybersecurity Framework (PDF)
- NIST CSF Informative Reference Tool
- NIST CSF Quick Start Guides
- NIST CSF Profiles

The slides, recording, and certificate of attendance will be sent after the session.

ADDITIONAL RESOURCES

- FFIEC Cybersecurity Assessment Tool Sunset Statement
- Tandem Cybersecurity Assessment Product
- Tandem Quiz: Which Cybersecurity Framework is the Best Fit for You?
- Tandem Blog: What is a Cybersecurity Control Self-Assessment
- Tandem Blog: Difference Between Risk Assessments and Cybersecurity Control Self-Assessments
- Tandem Blog: Frequently Asked Questions about the NIST Cybersecurity Framework (CSF)
- Tandem Blog: What Framework Do I Replace the FFEIC CAT With?

Tandem

28

Fill out the survey for a chance to win.

Tandem

29

LEARN MORE

Tandem Partner Program

Tandem.App/Partner

Tandem

30

THANKS FOR JOINING

From CAT to CSF: A Strategic Conversation for Financial Institutions

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

☑ *Remember to complete the survey*

Tandem

31