Cybersecurity Framework 2.0 Community Profiles

Date: April 23, 2024

This webinar is being recorded

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

nccoe.nist.gov

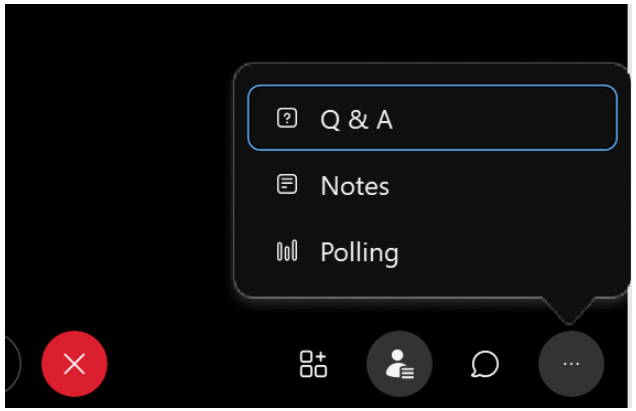
Agenda

Topic	Speaker
Welcome	Nakia Grayson, NIST
Introduction of NCCoE	Cheri Pascoe, NIST
NIST CSF 2.0 Overview	Nakia Grayson, NIST
Overview of Community Profiles	Julie Snyder, MITRE
Cyber Risk Institute (CRI) Profile	Emily Beam, CRI
Framework Resource Center	Nakia Grayson, NIST
Creating Community Profiles to Implement CSF 2.0	Julie Snyder, MITRE
Q&A	All

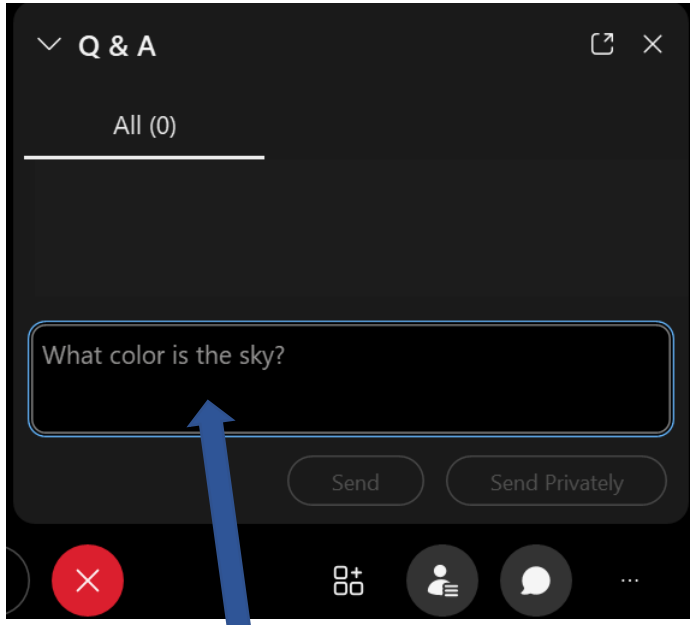
Submitting Questions

Please use the Q&A window to enter your questions.

We will do our best to answer all questions during the Q&A and will post responses to those we didn't have time to cover.

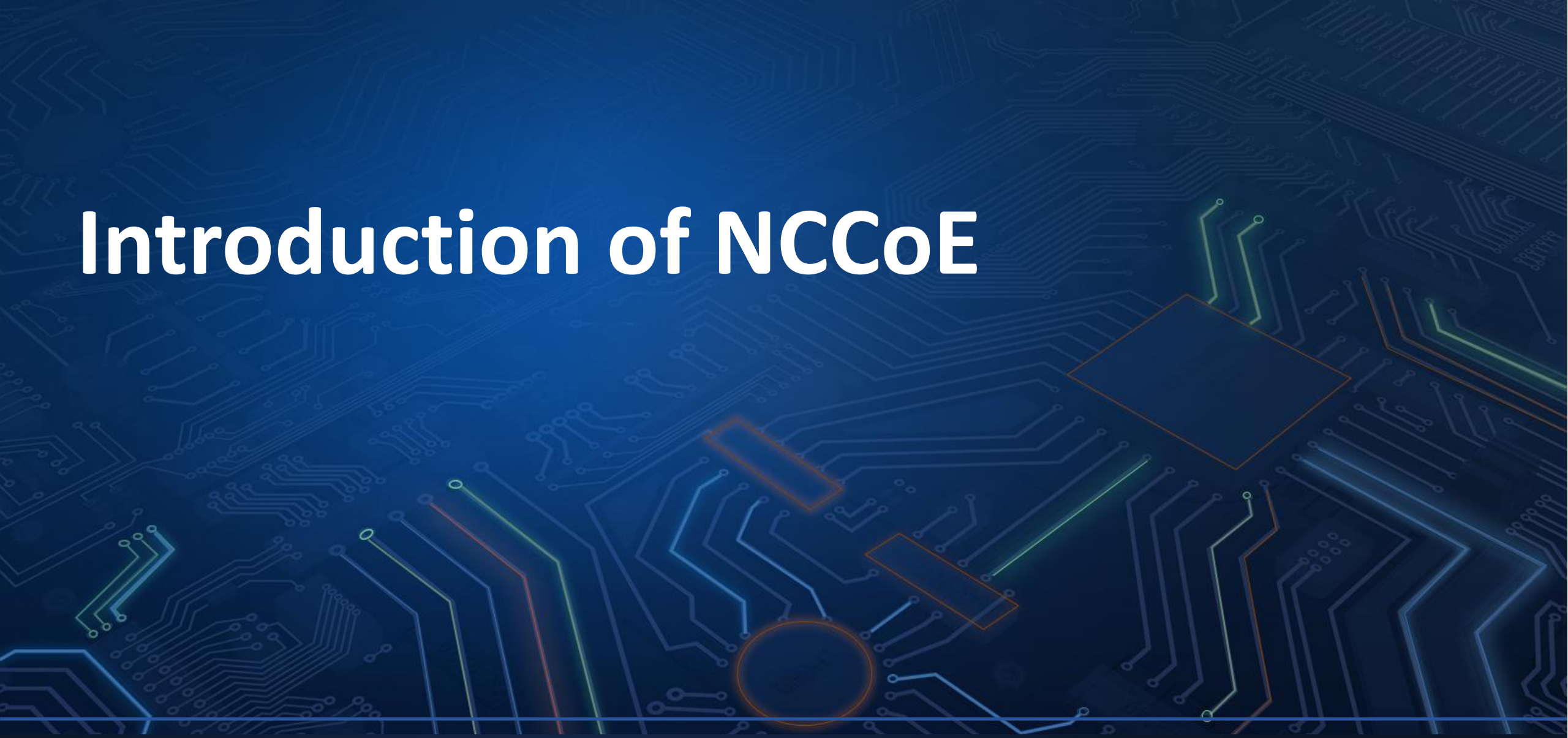


1. To open the Q&A panel, click on the ellipses at the bottom of the screen for 'More Panels' and click on Q&A.



2. Type your question in the text box and click Send

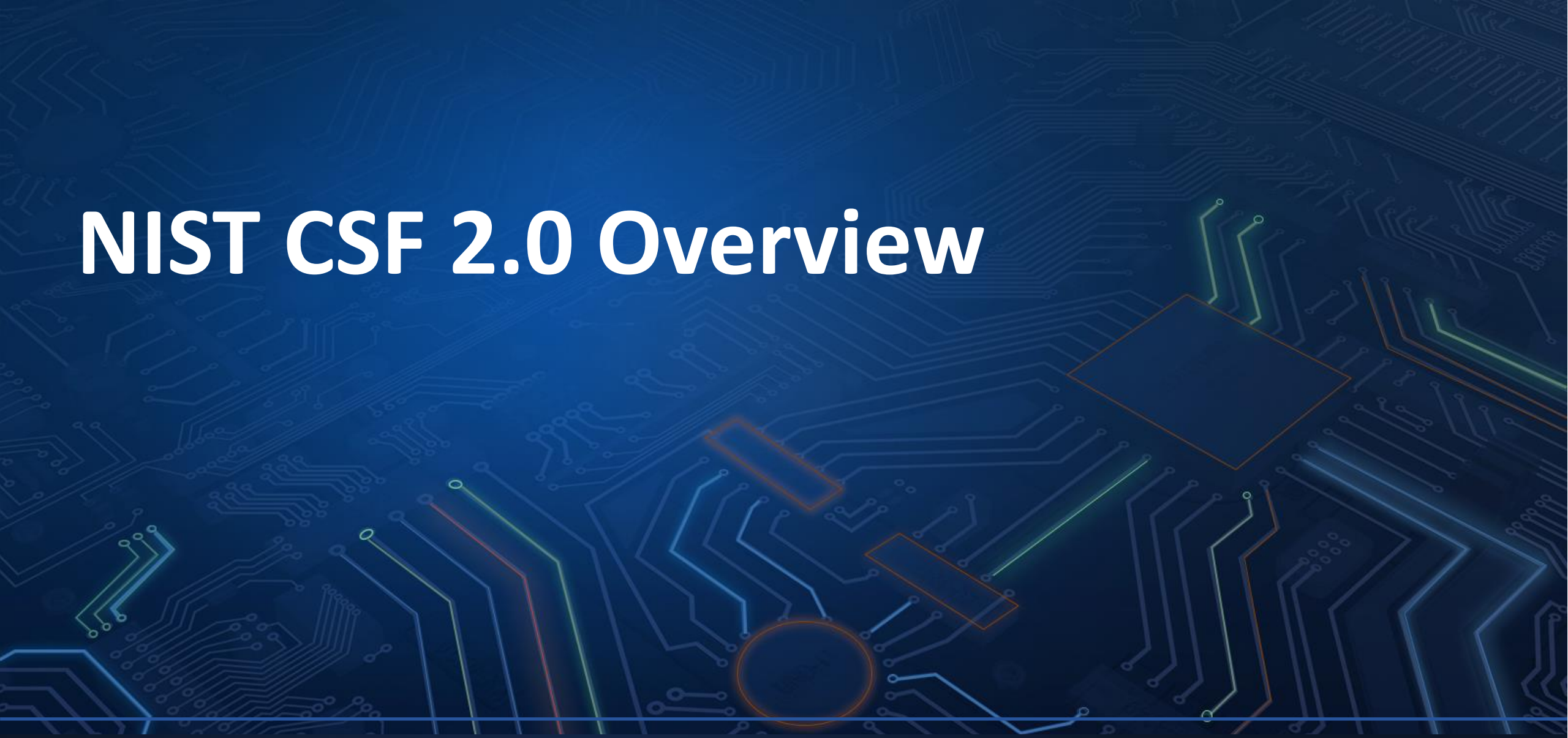
Introduction of NCCoE



NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

nccoe.nist.gov

NIST CSF 2.0 Overview



NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

nccoe.nist.gov

CSF 2.0 Overview

NIST has updated the widely used Cybersecurity Framework (CSF)—its landmark guidance document for reducing cybersecurity risk.

- Expanded scope beyond critical infrastructure
- Addition of a 6th Core Function “Govern”
- Increased emphasis on supply chain risk management
- Listened to feedback, made key updates, developed new resources and tools, and adjusted our guidance based on today’s cybersecurity environment.
- Formalized the term “Community Profiles”

CSF 2.0 Profiles

- **Organizational Profiles:** describes an organization's current and/or target cybersecurity posture in terms of the Core's outcomes
  - Used to understand, tailor, assess, prioritize, and communicate the Core's outcomes by considering an organization's mission objectives, stakeholder expectations, threat landscape, and requirements
  - **Current Profile:** specifies the Core outcomes that an organization is currently achieving (or attempting to achieve) and characterizes how or to what extent each outcome is being achieved
  - **Target Profile:** specifies the desired outcomes that an organization has selected and prioritized for achieving its cybersecurity risk management objectives

- **Community Profiles:** describes CSF outcomes to address shared interests and goals among multiple organizations

About Community Profiles

"A *Community Profile* is a baseline of CSF outcomes that is created and published to address shared interests and goals among a number of organizations. A Community Profile is typically developed for a particular sector, subsector, technology, threat type, or other use case. An organization can use a Community Profile as the basis for its own Target Profile. Examples of Community Profiles can be found on the NIST CSF website."

Overview of Community Profiles

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

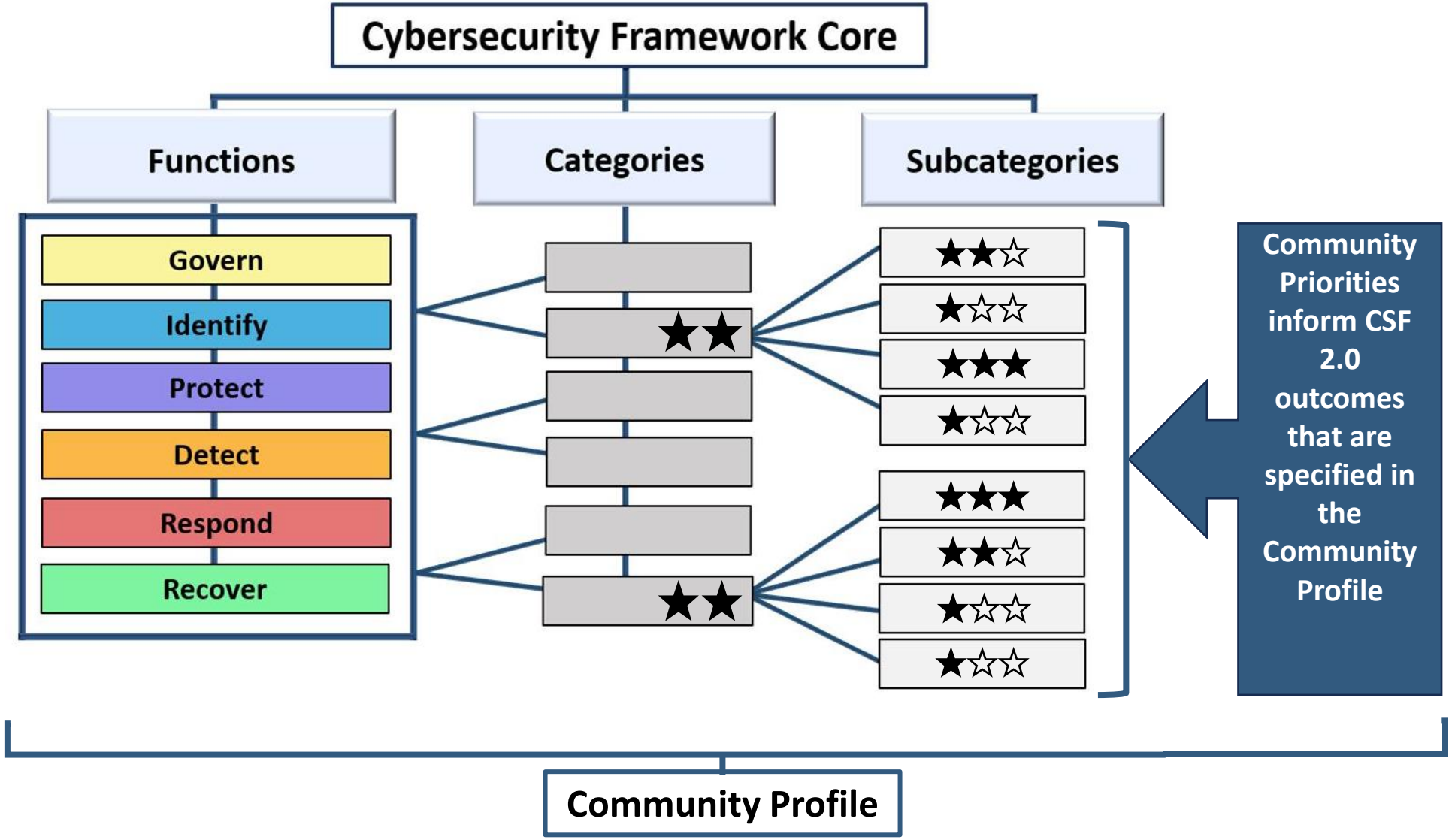
nccoe.nist.gov

Communities

Organizations that share a common context and an interest in their cybersecurity posture:

- **Sectors/subsectors**
- **Technologies**
- **Other use cases**

Community Profiles

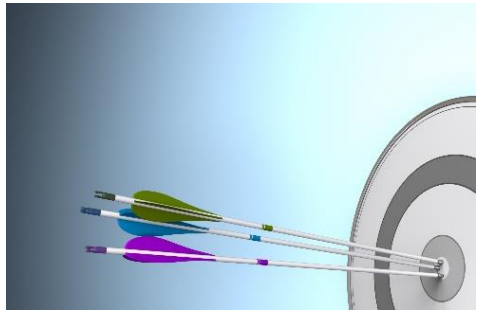


Benefits of Community Profiles

Use **shared taxonomy** for cybersecurity in the context of the community

Align requirements from multiple sources

Leverage expertise across the community



Encourage **common target** outcomes

Minimize the burden by working together

Communicate about cybersecurity risk

Examples of Community Profiles

- CSF 1.1 Profiles
  - eXtreme Fast Charging (XFC)
  - Genomic Data (draft)
  - Hybrid Satellite Networks (HSN)
  - Ransomware
- CSF 2.0 Profiles
  - CRI Profile for the Financial Sector
  - Incident Response

https://www.nccoe.nist.gov/framework-resource-center

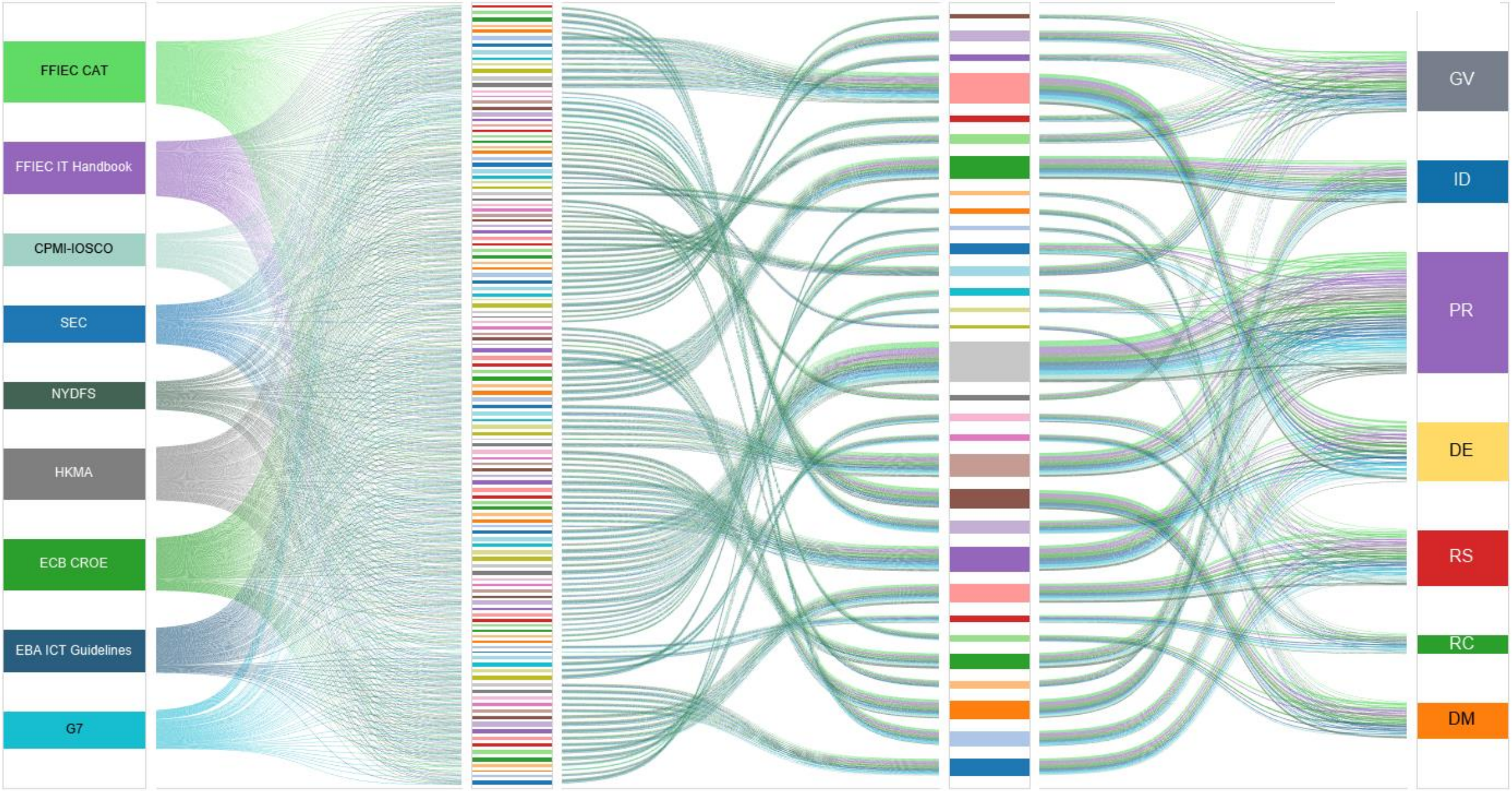
Cyber Risk Institute (CRI) Profile

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

nccoe.nist.gov

CYBER RISK INSTITUTE

Developing a CSF Profile for the Financial Services Sector

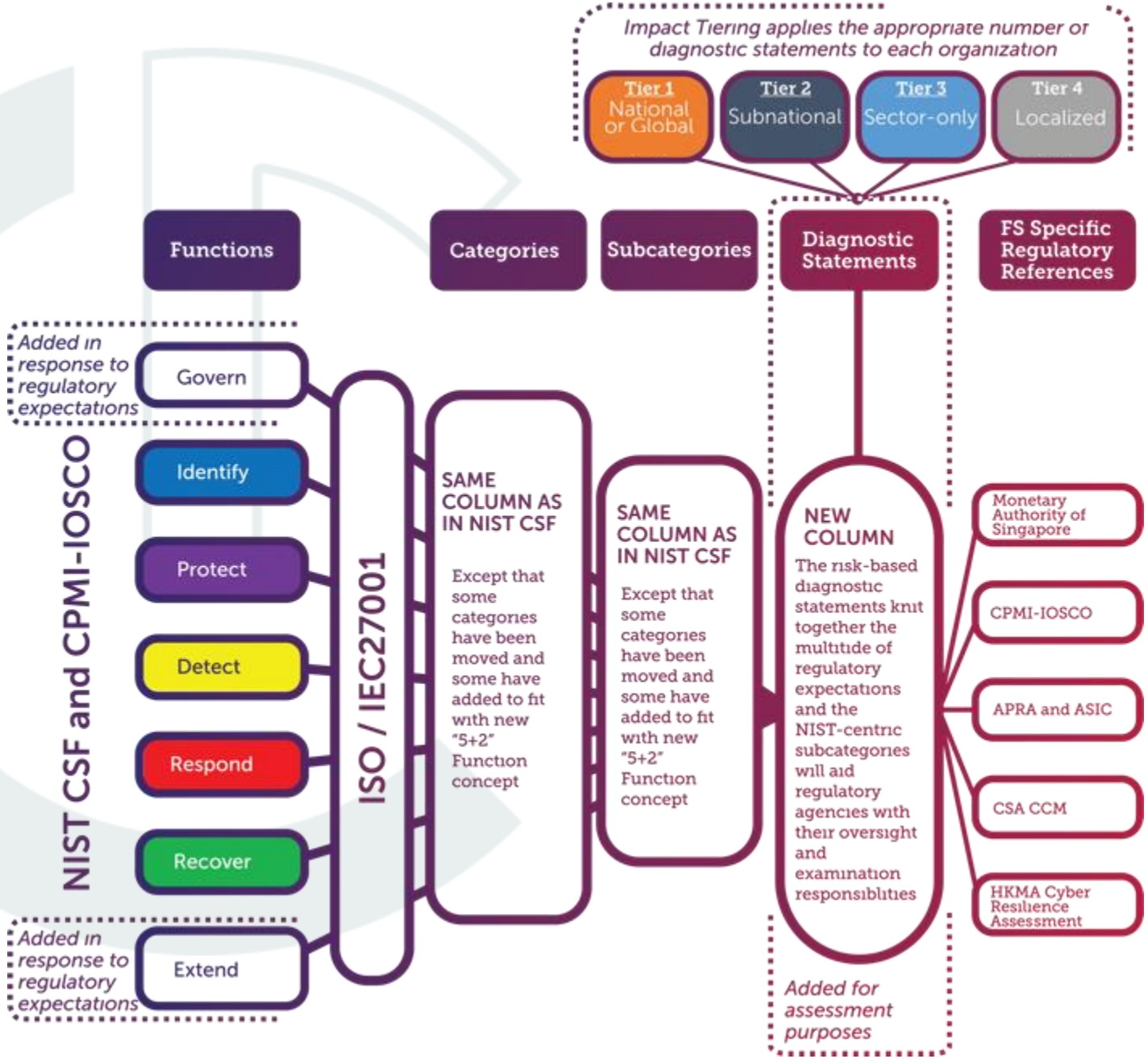

FFIEC CAT
FFIEC IT Handbook
CPMI-IOSCO
SEC
NYDFS
HKMA
ECB CROE
EBA ICT Guidelines
G7
GV
ID
PR
DE
RS
RC
DM

Developing the Profile

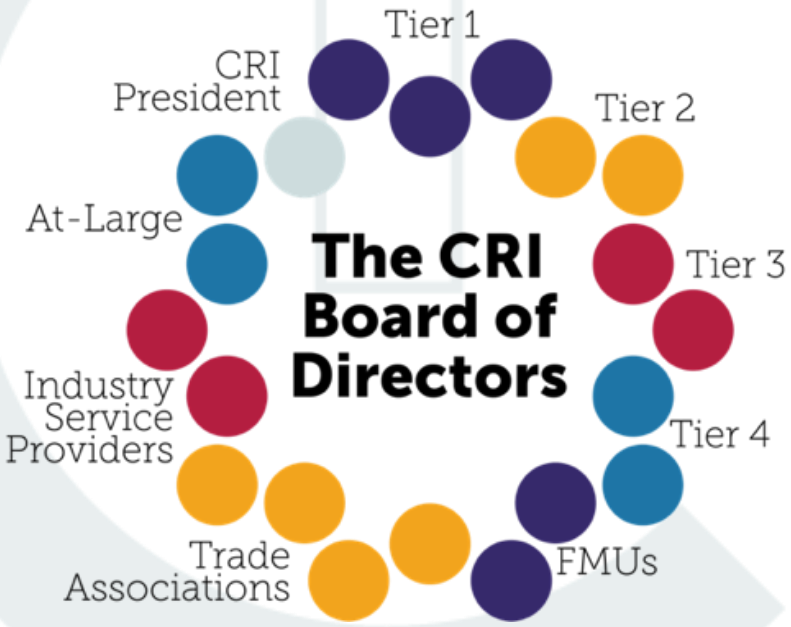
A Balancing Act: Crafting a Solution While Balancing Multiple Objectives

Profile Structure

- **The Profile expands upon the NIST CSF in three ways: additional functions, diagnostic statements, and an impact tiering questionnaire.**
  - **Diagnostic Statements**
    - Organized in a globally recognized, intuitive structure (NIST/ISO).
    - Distills numerous regulatory provisions into a single, granular control objective.
  - **Impact Tiering**
    - Nine questions based on global methodologies, reviewing transaction volume, and interconnectedness.
    - Measures an institution's impact on the global, national, and local economies.



Creation of the Cyber Risk Institute



Board of Directors
Sets strategic direction of CRI and provides financial oversight and counsel

Election Committee
Selects slate of CRI Board Directors and Operations Committee members

Standards Committee
Responsible for prioritizing cyber regs and standards for Profile integration

- **US Subcomte.**
- **International Subcomte.**

Profile Architecture Group
Considers and recommends strategic-level changes to the Profile's Design

Operations Committee
Identifies and evaluates partnering, licensing opportunities; and other ventures

Profile's Progression

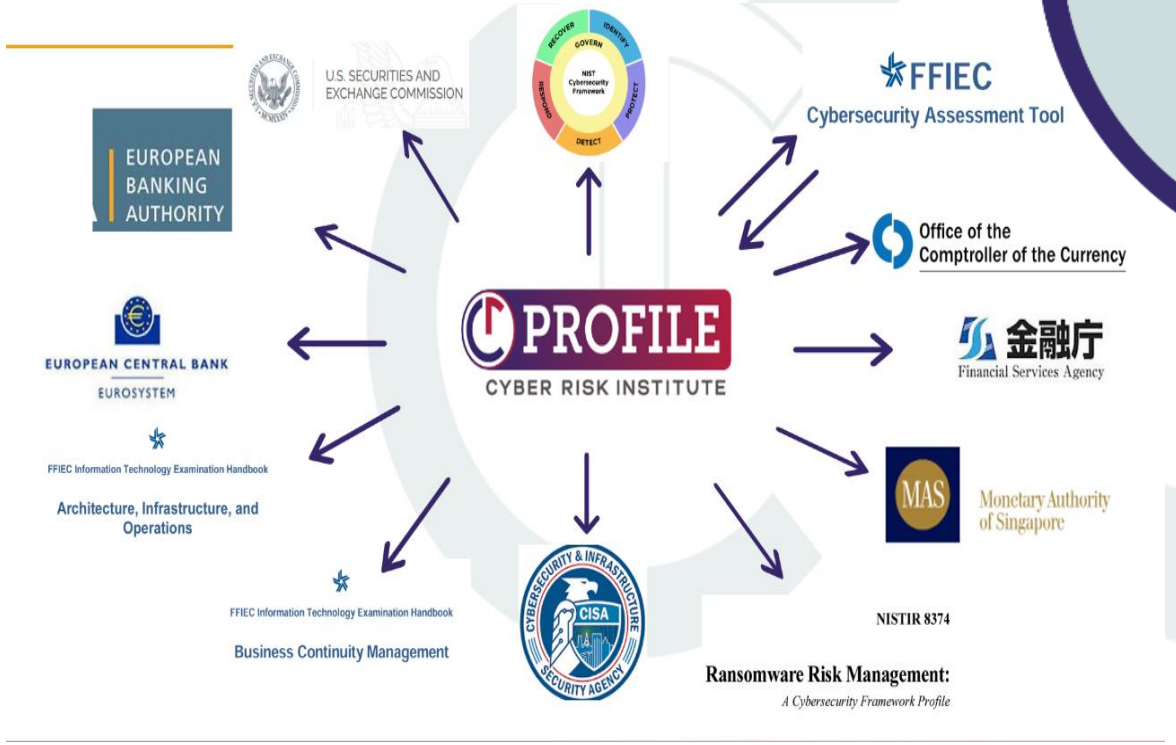
- FFIEC *IT Examination Handbook* booklets
- FINRA *Report on Cybersecurity Practices*
- FRB-OCC-FDIC *Advance Notice on Proposed Rulemaking on Enhanced Cyber Risk Management Standards*
- FTC *Start with Security A Guide for Business Lessons Learned from FTC Cases*
- Hong Kong-SFC *Circular to All Licensed Corporations on Cybersecurity*
- NAIC *Insurance Data Security Model Law*
- NFA *9070-NFA Compliance Rules 2-9 2-36 and 2-49 Information Systems Security Programs*
- SEC *OCIE s 2015 Cybersecurity Examination Initiative*
- SEC *Regulation S-P Regulation SDR Market Access Rule Regulation FD*
- Singapore-SAMA *Information Security Survey*
- South Africa Reserve Bank *IT Questionnaire*

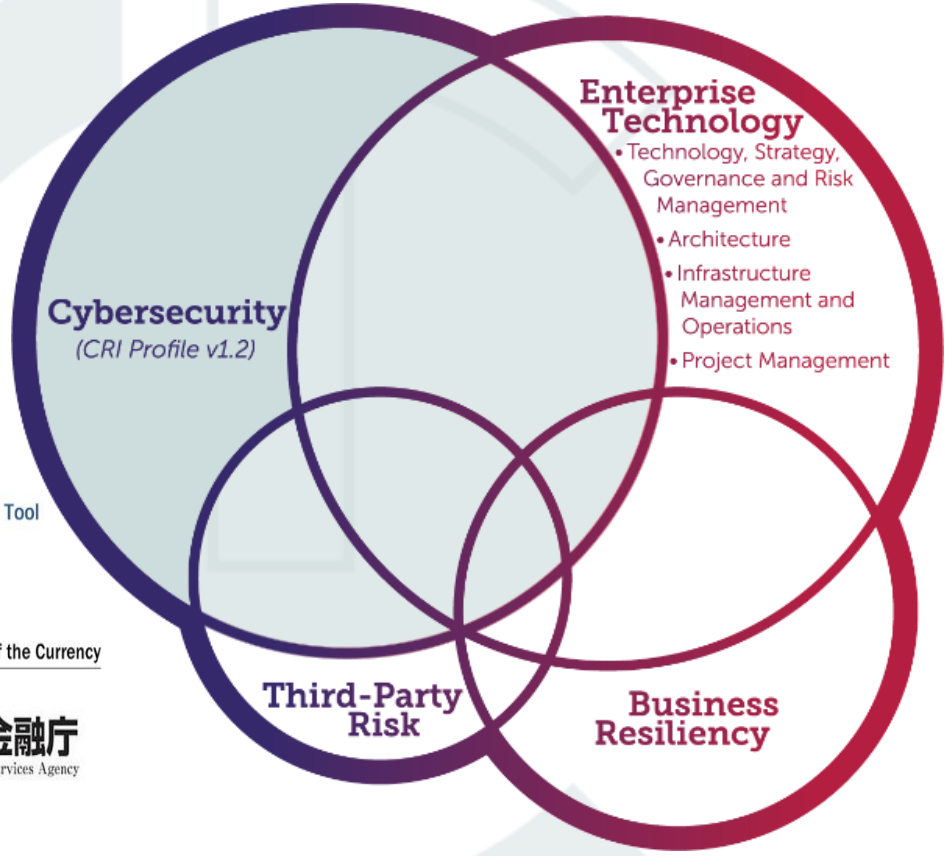
- National Association of Insurance Commissioners (NAIC) IT Handbook Mappings
- Additional Informational References from NIST ISO COBIT among others

- European Central Bank s *Cyber resilience oversight expectations for financial market infrastructures*
- European Banking Authority s (EBA) *EBA Guidelines on ICT and security risk management*
- Bidirectional mappings to the FFIEC Cybersecurity Assessment Tool (CAT)
- FFIEC *Business Continuity Management* Bookle
- New York State Department of Financial Services (NYDFS) 23 NYCRR Part 500 *Cybersecurity Requirements for Financial Services Companies*

- FFIEC Handbook on Architecture Infrastructure & Operations
- Monetary Authority of Singapore
- Hong Kong Monetary Authority
- Third Party Risk Management
- Maturity Overlay
- Revised Impact Tiering

Maintaining & Enhancing the Profile

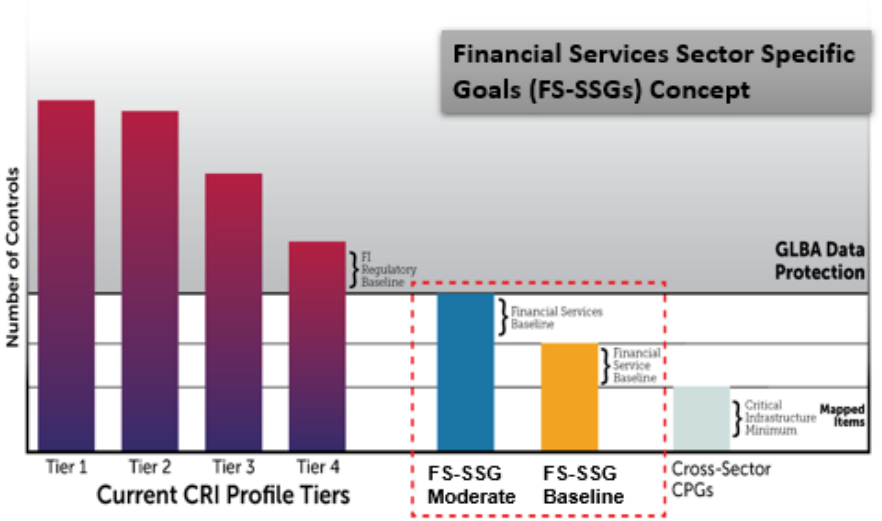




CRI Profile Subject Tag	Diagnostic Statements per Tag
#risk_management	90
#policy_management	58
#supply_chain_management	53
#third_party_risk_management	53
#critical_infrastructure	51
#resilience	51
#security_logging_monitoring_and_alerting	50
#incident_management	47
#review_assessment,_and_testing	40
#mission_and_strategy	36
#asset_management	31
#disaster_recovery	31
#threat_management	31
#data_protection	29
#vulnerability_management	28
#risk_oversight	26
#due_diligence	25
#enterprise_risk_management	25
#business_impact_analysis	24
#identity_and_access_management	23
#infrastructure_security	23
#information_sharing	22
#architecture	21
#board_or_committee_oversight	21
#staffing_and_resource_management	21

Stakeholder Engagement

Regulatory bodies in the US, Europe, and the Asia Pacific have recognized the Profile, giving it a truly global reach.



Affiliate

Affiliate Membership permits Profile licensing for commercial offerings.

Innovator

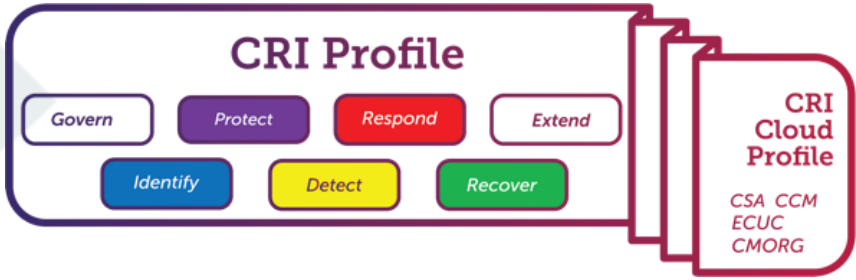
Innovator Membership permits Profile licensing for commercial offerings, AND

BASIC

- Invites to select events

PREMIUM

- Attendance to CRI Member-only events
- Enhanced marketing opportunites

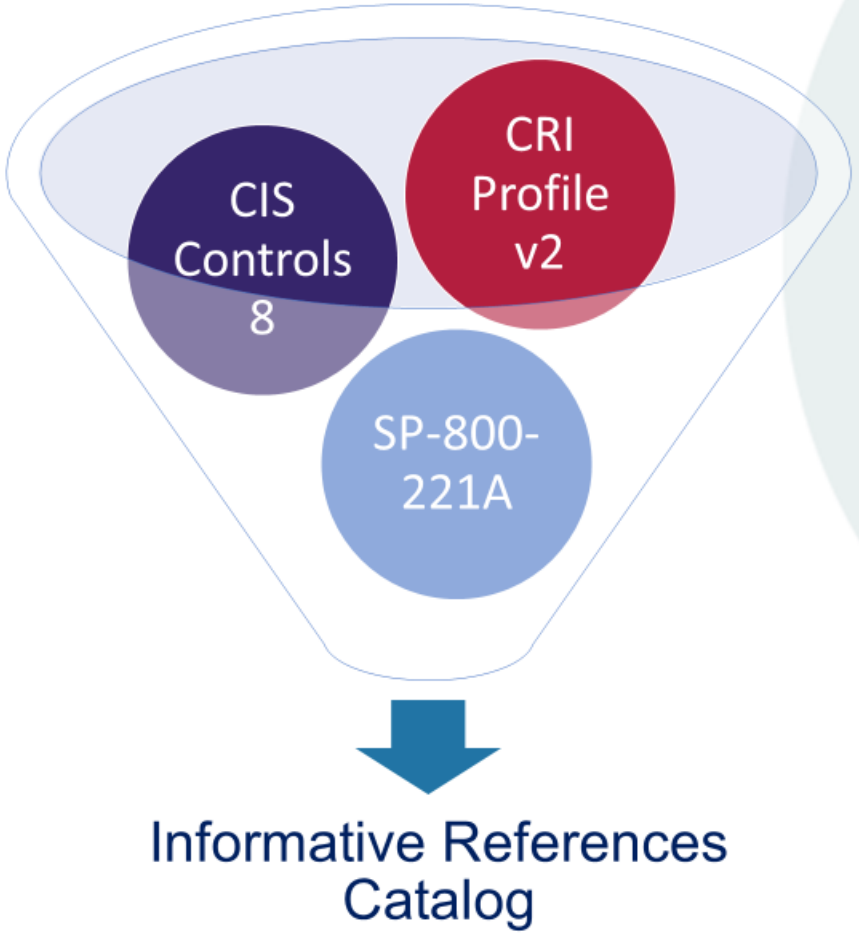


CRI Current Production Pipeline

	February	March	April	May	June	July
Profile v2.0 & Guidebook v2.0	NIST CSF v2.0 Issued **Published**					
Profile v2.1	In Development	In Development	In Development	In Development	In Development	In Development
Profile v2.0 Maturity	In Development	In Development	In Development	In Development	In Development	In Development
Cloud Profile v2.0	Government Review	Government Review	Government Review	Government & Sector Review		
Cloud Profile Shared Responsibility Checklist	Member Review	Government Review	Government Review	Government & Sector Review		
Cloud Profile Guidebook v2.0	Member Review	Government Review	Government Review	Government & Sector Review		
Financial Services Sector Specific Goals (FS-SSGs)	Government Review	Government Review	Government Review			

CRI Included as Informative Reference in NIST OLIR Program

Mappings between documents in a standardized template to identify relationships



	A	B	C	D	E
1	 NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE The NIST Cybersecurity Framework 2.0 www.nist.gov/cyberframework				
2	**Function**	**Category**	**Subcategory**	**Implementation Examples**	**Informative References**
42	**IDENTIFY (ID)**: The organization's current cybersecurity risks are understood				**CRI Profile Version 2.0: ID**
43		**Asset Management (ID.AM)**: Assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy			**CRI Profile Version 2.0: ID.AM** **Information and Communications Technology (ICT) Risk Outcomes: MA.RI-1**
44			**ID.AM-01**: Inventories of hardware managed by the organization are maintained	**1st**: 1st Party Risk **Ex1**: Maintain inventories for all types of hardware, including IT, IoT, OT, and mobile devices **Ex2**: Constantly monitor networks to detect new hardware and automatically update inventories	**CIS Controls: 1.1** **CRI Profile Version 2.0: ID.AM-01** **CRI Profile Version 2.0: ID.AM-01.01** **Information and Communications Technology (ICT) Risk Outcomes: MA.RI-1**

Profile Included in NIST Mapping Tools

Cybersecurity & Privacy Reference Tool

NIST | Search CSRC | ≡ CSRC MENU

Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER

PROJECTS | CYBERSECURITY AND PRIVACY REFERENCE TOOL

Cybersecurity and Privacy Reference Tool CPRT

GV.SC-05 Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties

› Show all GV.SC-05 References

GV.SC-06 Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships

OLIR Informative Reference Name: CRI-Profile-Version-2.0-to-Cybersecurity-Framework-v2.0

GV.SC-06 Assertions
From: CRI Profile Version 2.0
To: NIST Cybersecurity Framework 2.0

Framework Element	Framework Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Group Identifier	Comments	Strength of Relationship
GV.SC-06	Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships	Functional	intersects with	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.				8

Close

Hide all GV.SC-06 References
- OLIR
  - + CIS Controls v8.0 to GV.SC-06
  - – CRI Profile v2.0 to GV.SC-06
    - GV.SC-06 ↔ EX.DD
    - GV.SC-06 ↔ EX.DD-01
    - GV.SC-06 ↔ EX.DD-02
    - GV.SC-06 ↔ EX.DD-01.01
    - GV.SC-06 ↔ EX.DD-01.02
    - GV.SC-06 ↔ EX.DD-01.03
    - GV.SC-06 ↔ EX.DD-02.01
    - GV.SC-06 ↔ EX.DD-02.02
    - GV.SC-06 ↔ EX.DD-02.03
    - GV.SC-06 ↔ EX.DD-02.04
  - + CSF v1.1 to GV.SC-06
  - + SP 800-221A to GV.SC-06

Derived Relationship Mapping Tool

Generate Report

Focal Document: Cybersecurity Framework v2.0

*Informative Reference 1: CRI-Profile-Version-2.0-to-Cybersecurity-Framewo
*Informative Reference 2: CIS-Controls-8.0-to-Cybersecurity-Framework-v2.
Informative Reference 3:
Informative Reference 4:

Function: DETECT (DE), GOVERN (GV), IDENTIFY (ID), PROTECT (PR), RECOVER (RC)
Category: GV.OC, GV.RM, GV.RR, GV.PO, GV.OV
Subcategory:

Rationale: ☐ Functional ☐ Semantic ☐ Syntactic
Relationship: ☐ equal ☐ intersects with ☐ not related to ☐ subset of ☐ superset of
Strength: N/A, 0, 1, 3

Generate | Reset

CSF v2	CSF v2 Statement	Source Document	Source id	Reference Document Element Description	Rationale	Relationship	Strength
DE.CM-06	External service provider activities and services are monitored to find potentially adverse events	CISv8.0-CSFv2.0	15.2	Establish and Maintain a Service Provider Management Policy	Semantic	intersects with	
		CISv8.0-CSFv2.0	15.6	Monitor Service Providers	Semantic	intersects with	
		CRI-Profile-v2.0-CSF-v2.0	DE.CM-06.01	The organization reviews, documents, authorizes, and monitors all third-party connections, data transfer mechanisms, and Application Programming Interfaces (APIs).	Functional	intersects with	8
		CRI-Profile-v2.0-CSF-v2.0	DE.CM-06.02	The organization implements an explicit approval and logging process and sets up automated alerts to monitor and prevent any unauthorized access to a critical system by a third-party service provider.	Functional	intersects with	8
		CRI-Profile-v2.0-CSF-v2.0	DE.CM-06	External service provider activities and services are monitored to find potentially adverse events	Semantic	subset of	9

Framework Resource Center

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

nccoe.nist.gov

Framework Resource Center

The Framework Resource Center at the NCCoE serves as a repository of Community Profiles and additional guidance to help communities work together to apply CSF 2.0, including Community Profile efforts that integrate multiple NIST frameworks (e.g., NIST Privacy Framework).

https://www.nccoe.nist.gov/framework-resource-center

Available Resources

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Check for updates

NIST Cybersecurity White Paper
NIST CSWP 32 ipd

NIST Cybersecurity Framework 2.0: A Guide to Creating Community Profiles

Initial Public Draft

Cherilyn Pascoe
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Julie Nethery Snyder
The MITRE Corporation

Karen Scarfone
Scarfone Cybersecurity

This publication is available free of charge from:
https://doi.org/10.6028/NIST.CSWP.32.ipd

February 26, 2024

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

SECURITY GUIDANCE | OUR APPROACH | NEWS & INSIGHTS | GET INVOLVED | SEARCH

Examples of Community Profiles

Community Profiles provide a way for communities, (i.e., group of organizations that share a common context and an interest in their cybersecurity posture) to describe a consensus point of view about cybersecurity risk management. The NCCoE Framework Resource Center provides examples of Community Profiles and other resources to help communities understand and develop Community Profiles.

- CSF 2.0 Community Profiles
- CSF 1.1 Community Profiles
- CSF 1.0 Community Profiles

More Resources

NIST has developed additional guidance to support implementation of CSF Community Profiles.

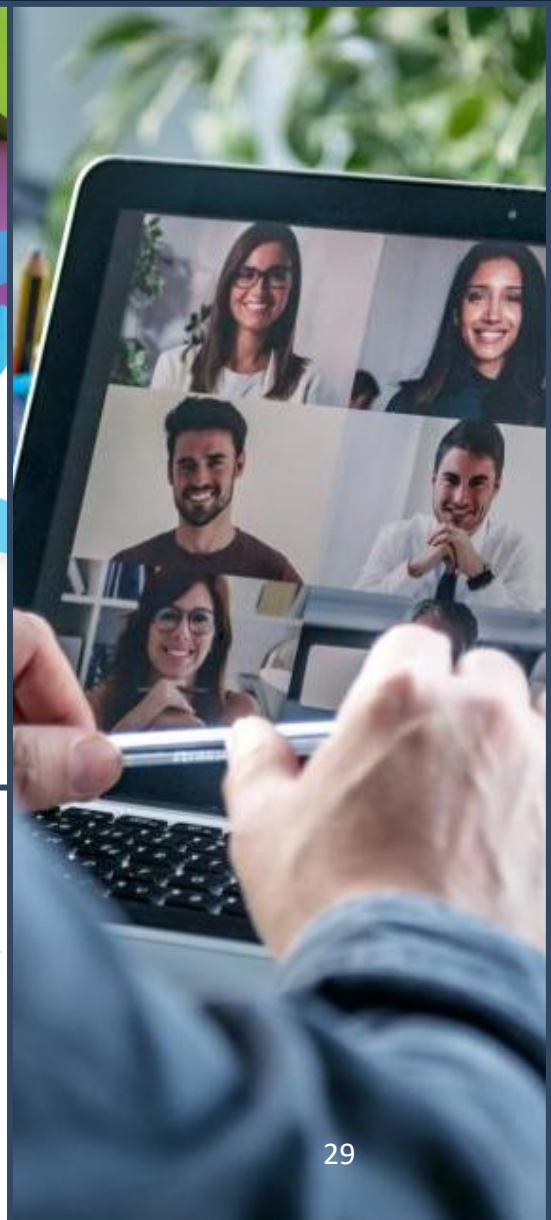
CSF 2.0

- NIST Cybersecurity Framework
- NIST CSF 2.0 Quick Start Guides

Understanding and Using CSF Mappings

Cybersecurity and Privacy Reference Tool (CPRT). The CPRT provides a centralized, standardized, and modernized mechanism for managing reference datasets and offers a consistent format for accessing reference data from various NIST cybersecurity and privacy standards, guidelines, and Frameworks (.xlsx and JSON).

OLIR Mapping from CSF v2.0 to CSF v1.1. This spreadsheet maps functions, categories, and subcategories that were added or reorganized in CSF v2.0 to their closest counterpart in CSF v1.1.



Creating Community Profiles to Implement CSF 2.0

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

nccoe.nist.gov

A Guide to Creating Community Profiles

NIST Cybersecurity White Paper (CSWP) 32

NIST Cybersecurity Framework 2.0: A Guide to Creating Community Profiles
Initial Public Draft

Cherilyn Pascoe
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Julie Nethery Snyder
The MITRE Corporation

Karen Scarfone
Scarfone Cybersecurity

February 26, 2024

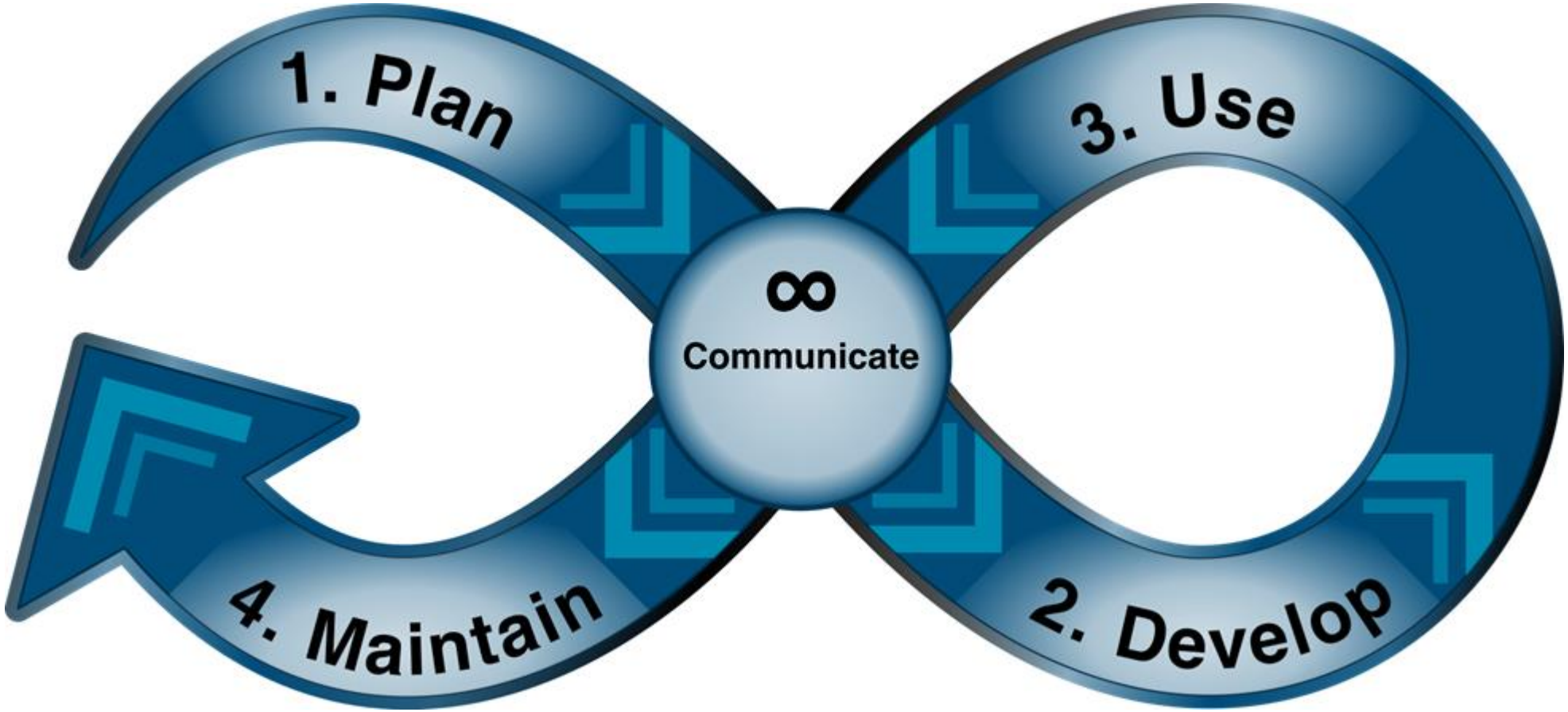
- Describes Community Profiles
- Provides a template and guidance for developing Community Profiles
- Offers a Community Profiles Lifecycle

This publication is available free of charge from:
https://doi.org/10.6028/NIST.CSWP.32.ipd

Sample Template

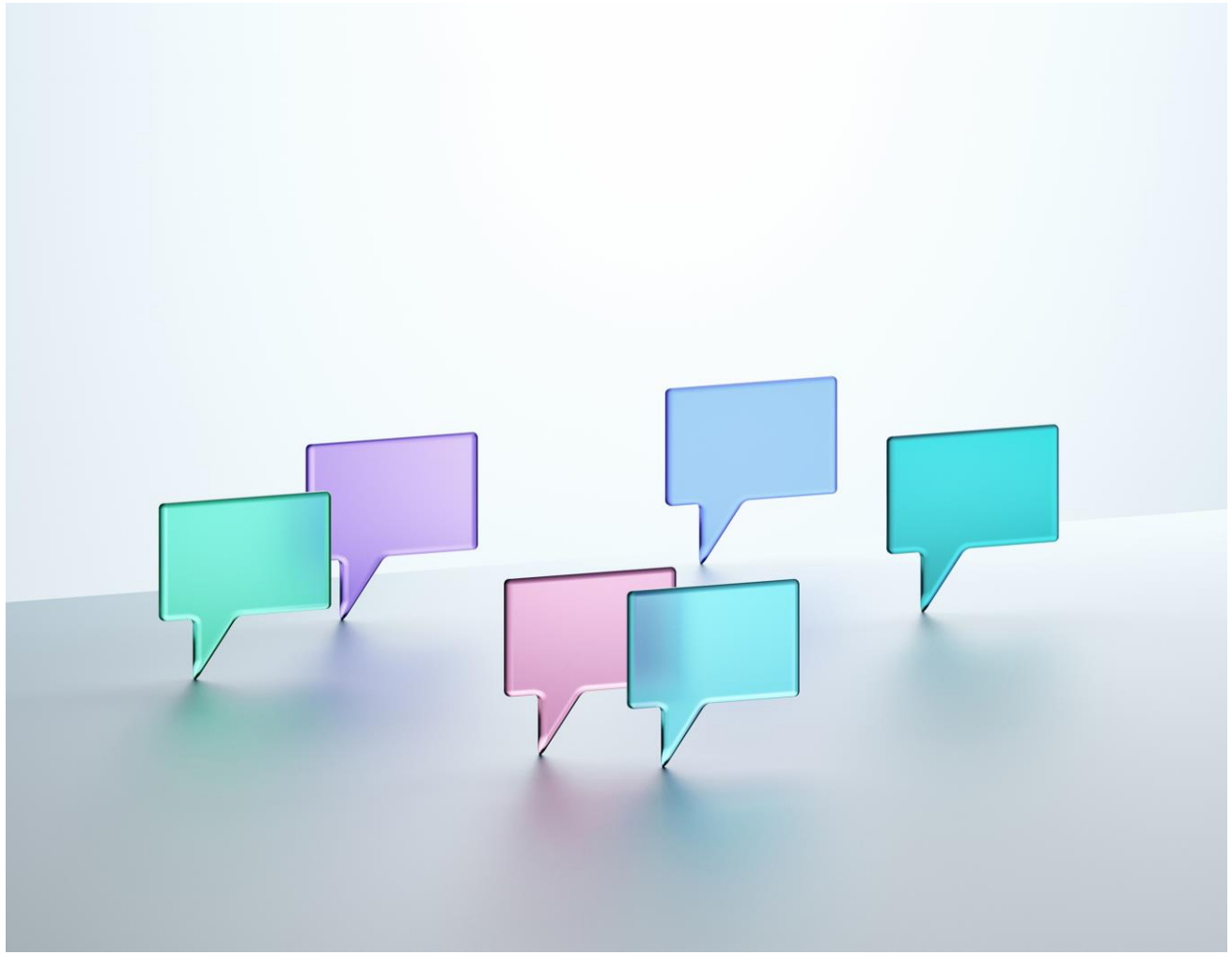
CSF 2.0 Outcome		Priority	Rationale	Informative References / Mappings
ID.AM-01	Inventories of hardware managed by the organization are maintained			
ID.AM-02	Inventories of software, services, and systems managed by the organization are maintained			

Community Profile Lifecycle



The Community Profile Lifecycle offers a structured approach for developing and maintaining Community Profiles.

Please Share Your Feedback!



Open for public comment through May 3, 2024!

Please email all draft comments to framework-profiles@nist.gov.

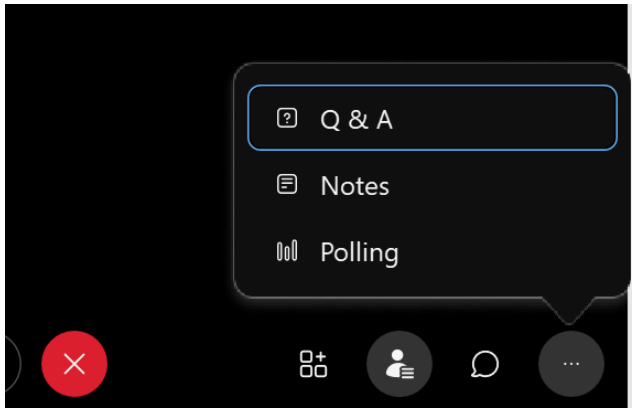
We encourage you to submit all feedback using the comment template found on our project page.

Q&A

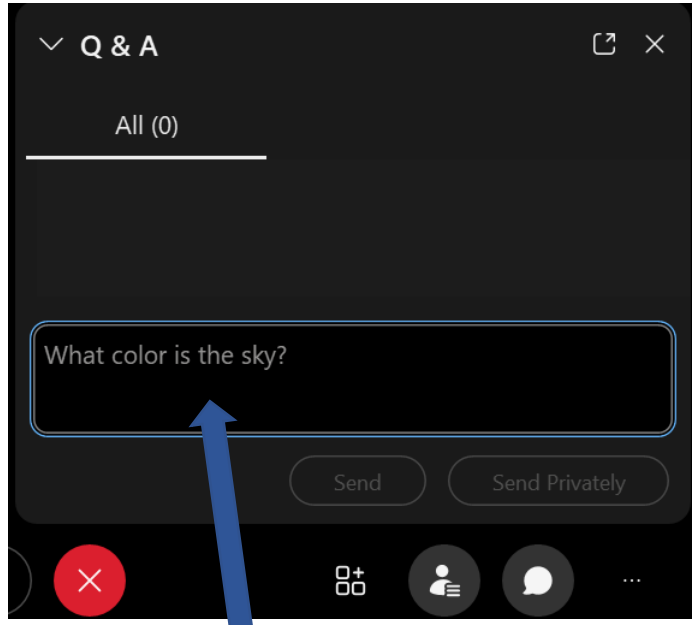
Submitting Questions

Please use the Q&A window to enter your questions.

We will do our best to answer all questions during the Q&A and will post responses to those we didn't have time to cover



1. To open the Q&A panel, click on the ellipses at the bottom of the screen for 'More Panels' and click on Q&A.



2. Type your question in the text box and click Send

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Framework Resource Center at NCCoE

https://www.nccoe.nist.gov/framework-resource-center

framework-profiles@nist.gov

nccoe.nist.gov

@NISTcyber