# CSF 2.0 Webinar Series

## Implementing CSF 2.0 — The Why, What, and How

*THE FIRST EVENT IN NIST'S MULTI-PART CSF 2.0 WEBINAR SERIES*


**Speakers:**

- Daniel Eliot, Lead for Small Business Engagement, Applied Cybersecurity Division, NIST
- Amy Mahn, International Policy Specialist, Applied Cybersecurity Division, NIST
- Stephen Quinn, Senior Computer Scientist and CSF Project Lead, Computer Security Division, NIST

NIST | NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

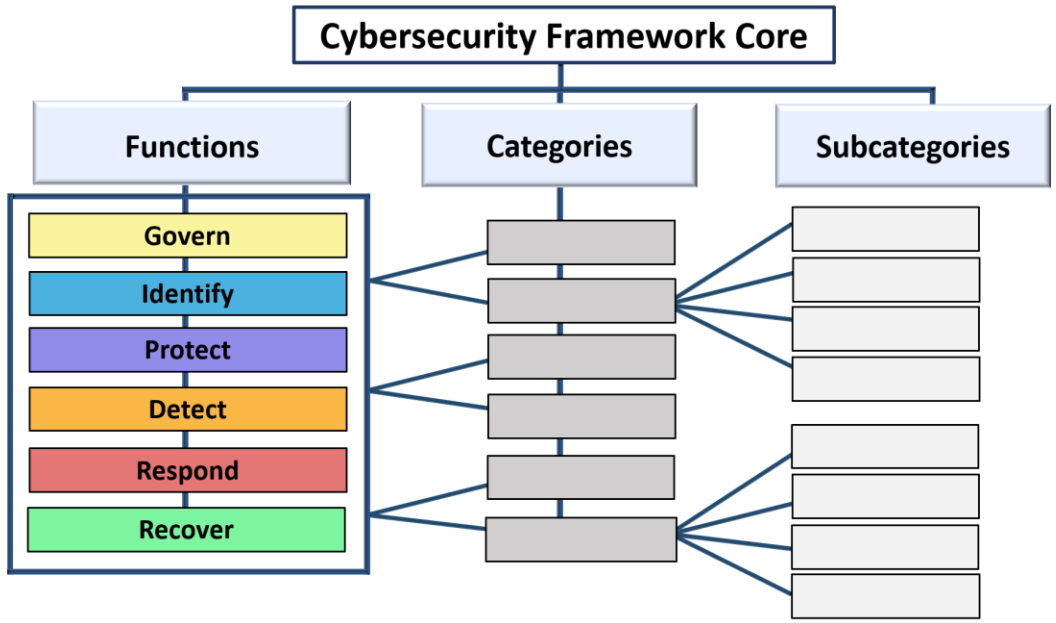
This webinar is being recorded

# Agenda


- Introduction
- Global impact of CSF 2.0
- **Why** organizations would want to upgrade to CSF 2.0
- **What** resources are available to assist with upgrading from CSF 1.1 to 2.0
- **How** organizations can begin to upgrade
- Call for public comments
- CSF 2.0 FAQs
- Audience Q&A

# NIST Cybersecurity Framework 2.0

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE




NIST.gov/cyberframework

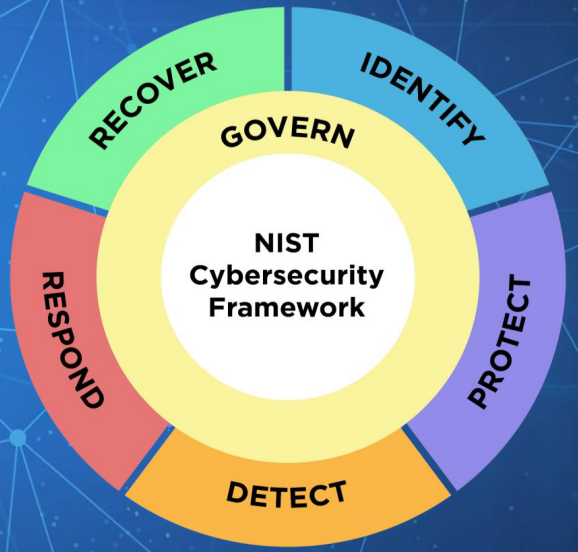
## How Did We Get Here?


*NIST's subject matter experts have collaborated with stakeholders in industry, academia, government, and international forums to develop the CSF. Thousands of detailed comments and suggestions from users around the world have helped shape the CSF you see today.*

***Helping organizations of all sizes and sectors improve their cybersecurity posture***

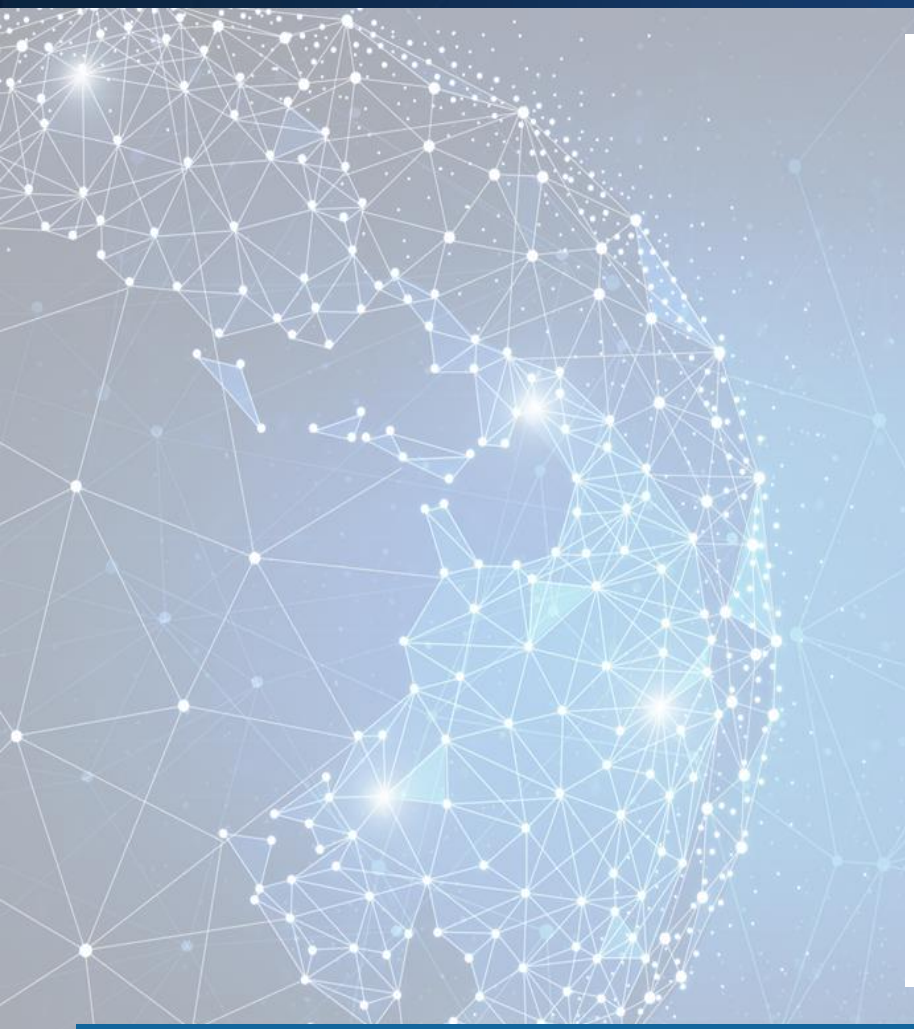
Most downloaded document of all NIST technical pubs in 2024!

# Global Impact of CSF 2.0



# Global Impact of CSF 2.0

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE



**Translations of CSF resources help expand the use of our cybersecurity and privacy resources globally and help improve U.S. company engagement in global markets.**

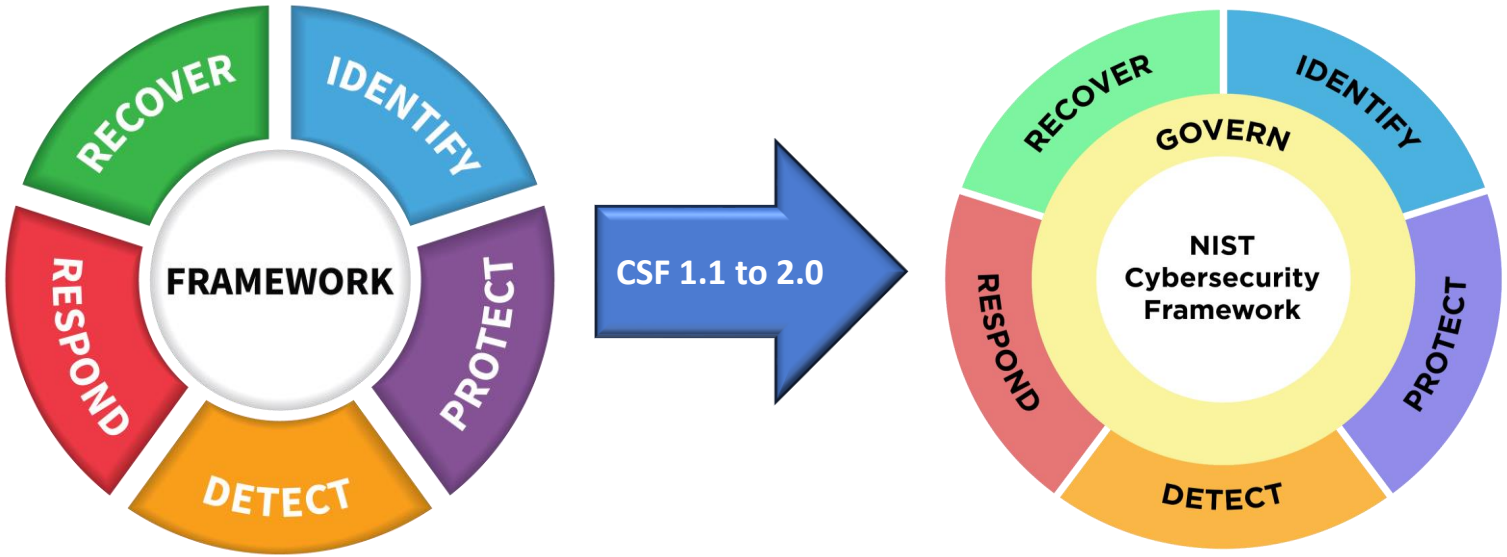
- The CSF is used widely internationally.
- CSF 2.0 resources have been translated into 9 different languages so far.
- The resources allow organizations to build cybersecurity frameworks and organize controls using the CSF Functions.
- NIST's work with the International Organization for Standardization (ISO), in conjunction with the International Electrotechnical Commission (IEC), over the last 11 years has been expansive.
- NIST encourages international participation at all stages in the development and evolution of its cybersecurity and privacy programs and resources.

**CSF 2.0 Translations:** nist.gov/cyberframework/translations
**Learn About Our Global Impact**: nist.gov/cybersecurity/international-cybersecurity-and-privacy-resources

# What Makes CSF 2.0 Different?

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

- Incorporates an entirely new function to address **Governance.**
- **Integrates Supply Chain** throughout the existing functions, categories, subcategories, and new resources.
- Modifies categories & subcategories to **address specific threats and technology** shifts.
- Shifts focus to how organizations can **more rapidly implement and improve their cybersecurity posture**.
- Less about a single document and more about a **suite of resources** that aims to provide flexible, leading-edge inputs to consumers.




**Resources Showing Differences Between CSF 1.1 and CSF 2.0:**

NIST Cybersecurity Framework 2.0 Reference Tool- https://csrc.nist.gov/extensions/nudp/services/json/csf/download?olirids=all

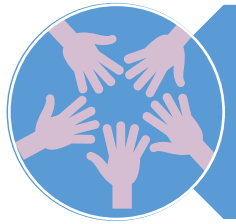
From the CSF 2.0 Tool page - https://csrc.nist.gov/Projects/cybersecurity-framework/Filters#/csf/filters

The Crosswalk from the OLIR catalog with more detail - https://csrc.nist.gov/csrc/media/Projects/olir/documents/submissions/CSFv1.1_to_CSFv2.0_CROSSWALK_20240220.xlsx

**View all CSF 2.0 FAQS:** https://www.nist.gov/faqs

# Key CSF 2.0 Updates Reflecting the Evolving Threat Landscape of the Last Decade

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE



## Supply Chain

- GV.SC-01, -02, -03, -04, -05, -06, -07, -08, -09, -10, DE.CM-06

## Shared & Virtualized Environments (e.g., cloud)

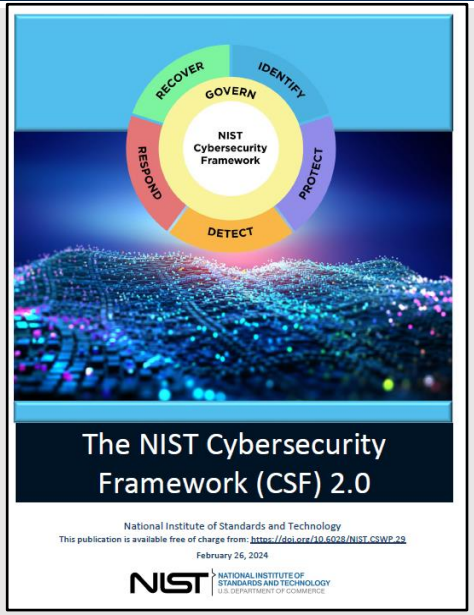
- ID.AM-08, PR.AA-04, PR.DS-10, PR.PS-02, -03, PR.IR-01, DE.CM-03, -06


## Software Flaws

- GV.SC-09, ID.AM-08, ID.RA-09, PR.PS-02, PR.PS-06

# A Suite of Resources

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE






## CSF 2.0 Quick Start Guides


**Available Guides:**

- CSF 2.0 Overview
- Organizational Profiles
- Community Profiles
- Small Business
- Cybersecurity SCRM
- Tiers
- Enterprise Risk Management
- Cybersecurity, ERM and Workforce Management

**Resource and Overview Guide**
Understand the basics and learn about the many available helpful CSF 2.0 resources
Download

**CSF 2.0 Organizational Profiles**
Guidance for organizations, with considerations for creating and using spreadsheets called *Profiles*, to implement the CSF 2.0.
Download

**CSF 2.0 Community Profiles**
This guide provides considerations for creating and using Community Profiles to implement the CSF 2.0 and support the needs of organizations in communities that share common priorities.
Download

**Small Business**
Resources specifically tailored to small businesses

**Cybersecurity Supply Chain Risk Management**
Helps organizations become smarter acquirers and suppliers of technology

## Cybersecurity and Privacy Reference Tool CPRT

### NIST Cybersecurity Framework, Version 2.0

Search: Enter exact match phrase...

CPRT / Version 2.0 / All

Export

**GOVERN (GV)**

The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored
> Show all GV References

| Category | Subcategory | Implementation Examples |
|---|---|---|
| **Organizational Context (GV.OC):** The circumstances - mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements - surrounding the organization's cybersecurity risk management decisions are understood<br>> Show all GV.OC References | **GV.OC-01:** The organizational mission is understood and informs cybersecurity risk management<br>> Show all GV.OC-01 References | **Ex1**: Share the organization's mission (e.g., through vision and mission statements, marketing, and service strategies) to provide a basis for identifying risks that may impede that mission |
| | **GV.OC-02:** Internal and external stakeh... and their needs and expectations rega... management are understood and cons...<br>> Show all GV.OC-02 References | |
| | **GV.OC-03:** Legal, regulatory, and contr... regarding cybersecurity - including pri... obligations - are understood and mana...<br>> Show all GV.OC-03 References | |

## CSF 2.0 Informative References

Informative References help inform how an organization may achieve the Core's outcomes. Given the diversity of use cases this page allows the user to choose how to best consume Informative References.

**Download CSF 2.0 Informative Reference in the Core**

**Directly download all the Informative References for CSF 2.0**
For users that want all informative references.
Download English (xlsx)

**Select Informative References to be included with the Core**
For users that want to select specific informative references.
Browse

Download Translations (xlsx) +

**CSF 2.0 Implementation Examples**
Implementation Examples offer potential ways to achieve each outcome
Download (xlsx)
Download (pdf)

**Informative Reference Catalog**
Browse and download specific informative references
Catalog

**Compare Informative References**
Generate, view and download Comparison Reports between CSF 2.0 Informative References
Comparison Reports

## NIST Cybersecurity Framework (CSF) 2.0 Reference Tool

Search: Enter exact match phrase... Filter Export

Collapse All/Expand All

**Function**
**GOVERN (GV)**: Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy

**Category**
**Organizational Context (GV.OC)**: The circumstances - mission, stakeholder expectations, and legal, regulatory, and contractual requirements - surrounding the organization's cybersecurity risk management decisions are understood (formerly ID.BE)

**Subcategory**
**GV.OC-01**: The organizational mission is understood and informs cybersecurity risk management (formerly ID.BE-02, ID.BE-03)
**Implementation Examples**
**Ex1**: Share the organization's mission (e.g., through vision and mission statements, marketing, and service strategies) to provide a basis for identifying

**Cybersecurity Framework 1.1 to 2.0 Core Transition Changes Spreadsheet:**
https://www.nist.gov/document/csf-11-csf-20-core-transition-changes

# Where to Begin

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

- ✓ Compare your current implementation of CSF 1.1 with CSF 2.0.
- ✓ Develop a step-by-step transition plan, prioritizing critical updates.
- ✓ Engage stakeholders across the organization to ensure buy-in and collaboration.
- ✓ Leverage available resources and tools to streamline the process.

# Understanding Your Current and Target Cybersecurity Posture

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

**Create Organizational Profile**

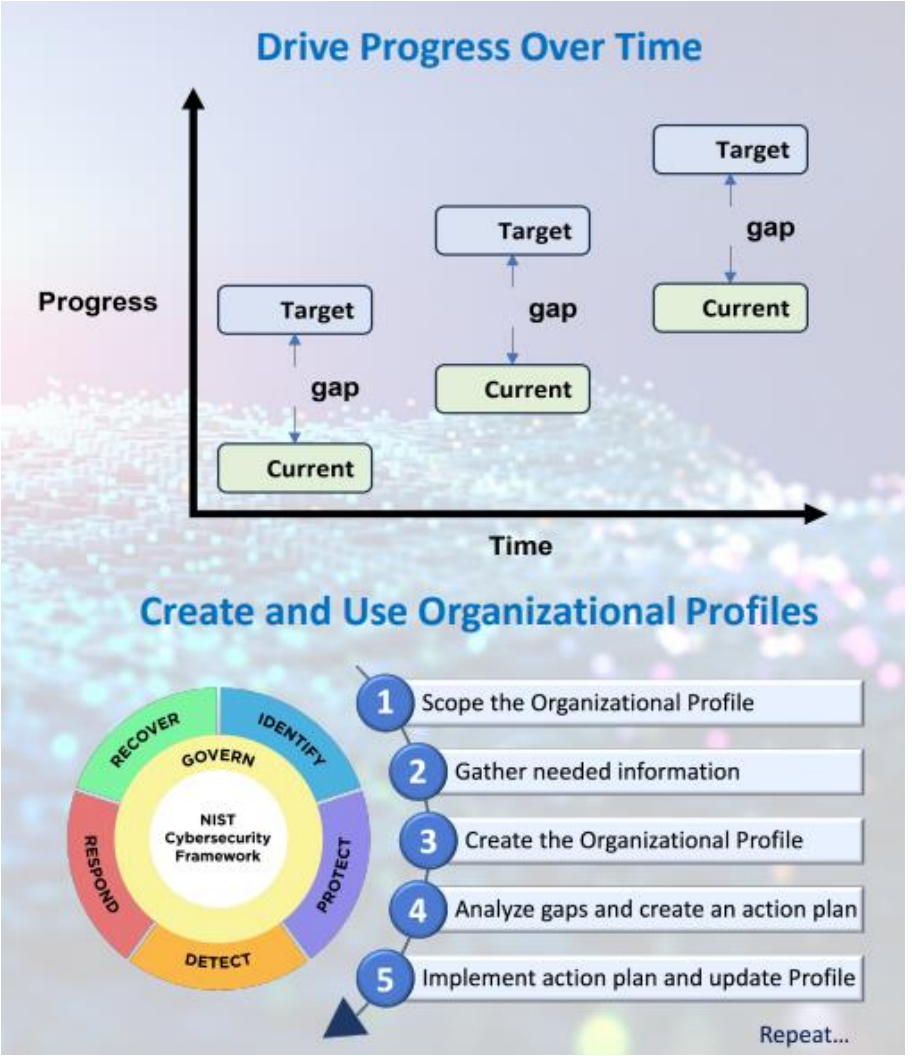
- CSF 2.0 Organizational Profiles Quick Start Guide: https://doi.org/10.6028/NIST.SP.1301

**Organizational Profiles can be categorized as:**

- **A Current Profile** that specifies the CSF outcomes an organization is currently achieving and characterizes how or to what extent each outcome is being achieved.

- **A Target Profile** that specifies the desired CSF outcomes an organization has selected and prioritized for achieving its cybersecurity risk management objectives.

**Analyze the gaps, then create an action plan**



# Sample Page from the CSF 2.0 Organizational Profiles Quick Start Guide

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

## NIST CSF 2.0: CREATING AND USING ORGANIZATIONAL PROFILES

### A QUICK START GUIDE

### CREATE THE ORGANIZATIONAL PROFILE – PART 2

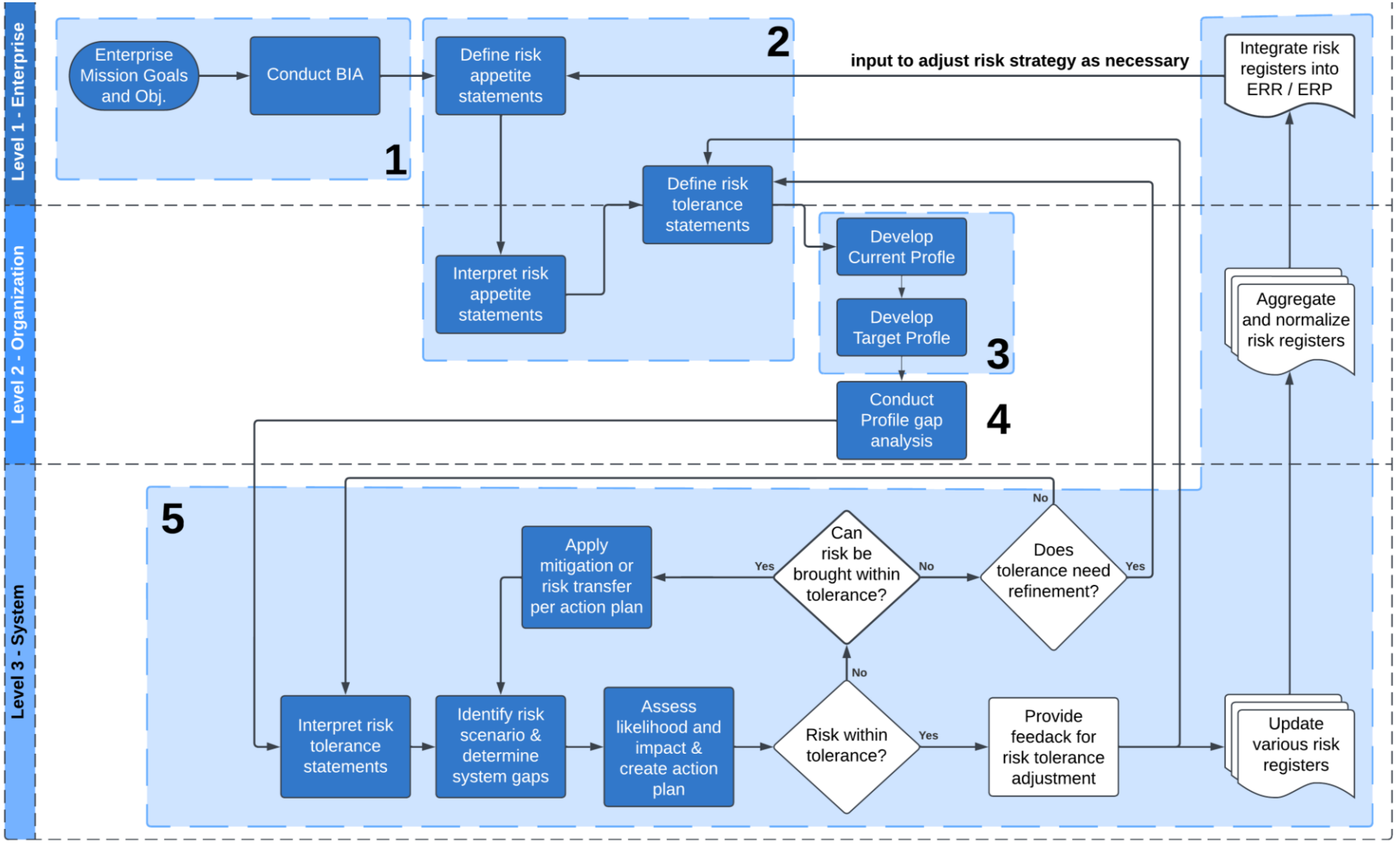
**The table below shows a notional example of a single row from an Organizational Profile.** This is meant for illustrative purposes only. Here are some tips drawn from the example:

- Add and remove columns from the Organizational Profile template to suite your needs. The CSF encourages users to record whatever information is significant and to use whatever format they prefer.
- The columns do not have to be the same for the Current Profile and the Target Profile.
- Include Informative References to understand differences between Practices and Goals. This example shows SP 800-53 controls in the square brackets.


| CSF Outcomes | | Current Profile | | | Target Profile | |
|---|---|---|---|---|---|---|
| **Identifier** | **Description** | **Practices** | **Status** | **Rating** | **Priority** | **Goals** |
| PR.PS-01 | Configuration management practices are established and applied | Policy: Configuration Management policy version 1.4, last updated 10/14/22. Defines the configuration change control policy [**CM-1**].<br>Procedures: System owners and technology managers informally implement configuration management practices. Change control processes are not consistently followed. The CIO specifies configuration baselines [**CM-2**] for the IT platforms and applications most widely used within the organization, but baseline use is not monitored or enforced consistently across the organization. | Configuration management is partially implemented within the organization. Some systems do not follow available baselines and other systems do not have baselines, so they may have weak configurations that make them more susceptible to misuse and compromise. Unauthorized changes may go undetected. Some changes are not tested or tracked. | 3 *out of 5* | High | Policy: The Configuration Management policy requires configuration baselines to be specified, used, enforced, and maintained for all commodity technologies used by the organization. The policy requires change control processes to be followed for all technologies within the organization [**CM-1**].<br>Procedures: Each division of the organization has a configuration management plan [**CM-9**], as well as maintains, implements, and enforces configuration baselines [**CM-2**] and settings [**CM-6**] for their systems. Baselines are applied to all systems before production release. All systems are continuously monitored for unexpected configuration changes, and tickets are automatically generated when deviations from baselines occur. Designated parties review change requests and corresponding impact analyses [**CM-4**] and approve or deny each [**CM-3**]. |

# Cybersecurity Framework steps in Support of CSRM Integration

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE




https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8286C-upd1.pdf (Figure 8)

# Implementation and Assessment

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

A recommended approach for developing action plans is to use the NIST CSF 2.0 Reference Tool to follow the references from your Target Profile's pertinent Subcategories to the associated informative references, such as SP 800-53.

## CSF 2.0 Informative References

Relationships between the Core and various best practices, including standards, guidelines, regulations, and other resources.

https://www.nist.gov/informative-references

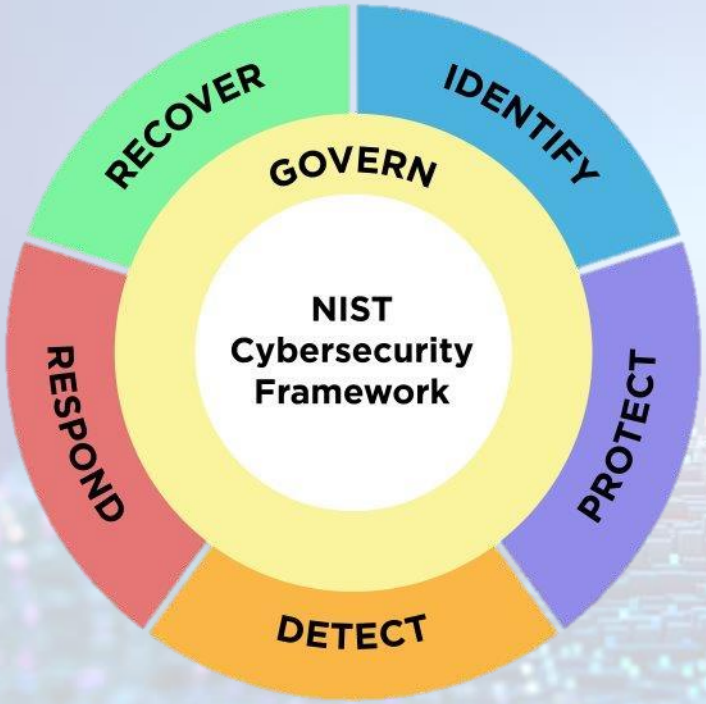
## Additional NIST Resources

- NIST IR 8286B, Prioritizing Cybersecurity Risk for Enterprise Risk Management
- NIST IR 8286D, Using Business Impact Analysis to Inform Risk Prioritization and Response
- NIST SP 800-37 Revision 2, Risk Management Framework for Information Systems & Organizations
- NIST SP 800-53 Revision 5, Security and Privacy Controls for Information Systems & Organizations
- NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments

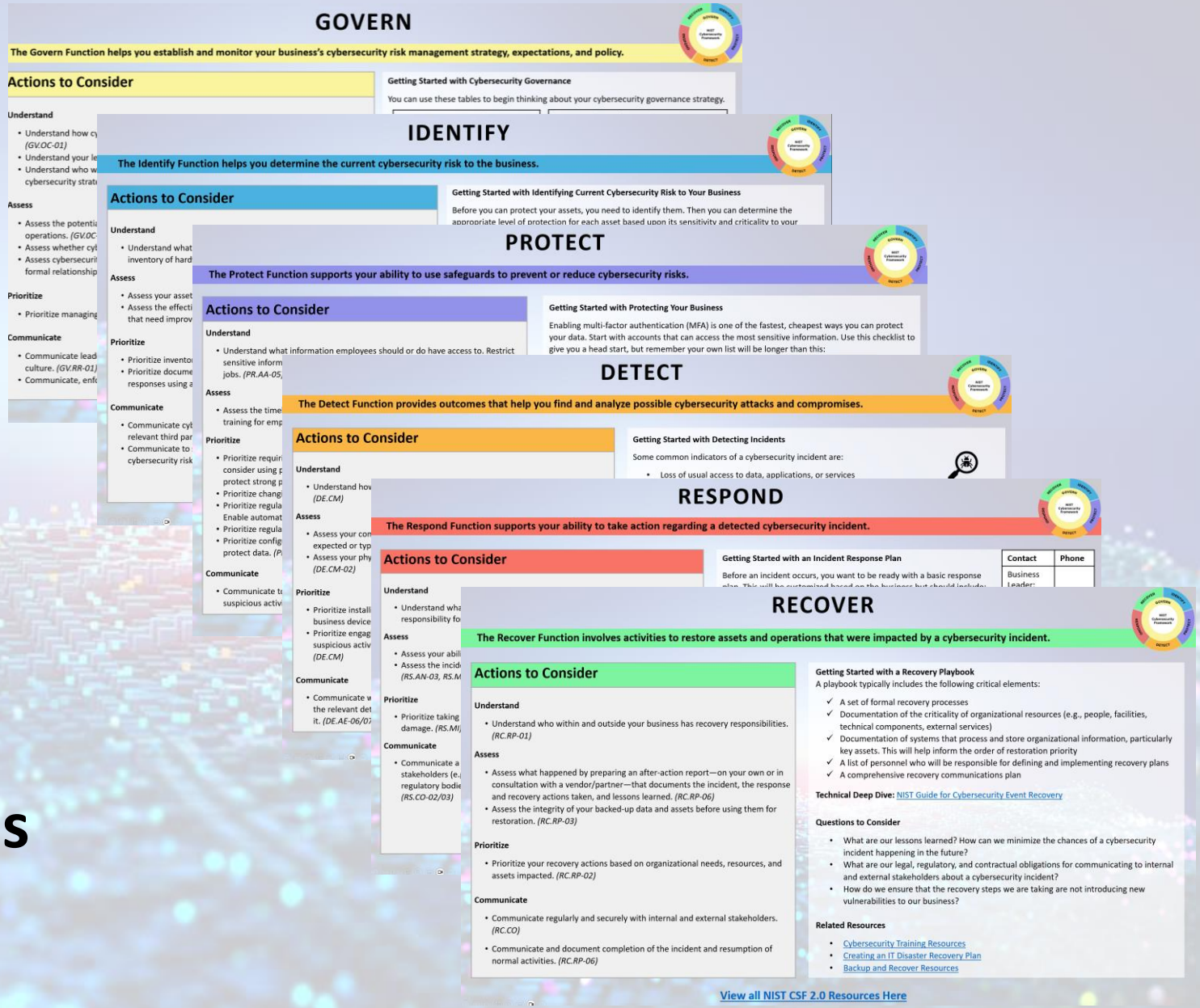
## Implementation Examples

| Subcategory | Implementation Example |
|---|---|
| GV.SC-04: Suppliers are known and prioritized by criticality | Ex1: Develop criteria for supplier criticality based on, for example, the sensitivity of data processed or possessed by suppliers, the degree of access to the organization's systems, and the importance of the products or services to the organization's mission |
| | Ex2: Keep a record of all suppliers, and prioritize suppliers based on the criticality criteria |

**https://www.nist.gov/document/csf-20-implementation-examples-xlsx**




# CSF 2.0 Small Business Quick Start Guide




nist.gov/itl/smallbusinesscyber/nist-cybersecurity-framework-0

# CSF Frequently Asked Questions

| |
|---|
| Why are there gaps in the CSF Subcategory enumeration? |
| How does an organization go about implementing the CSF 2.0? |
| Does NIST provide certification for CSF implementation or products? |
| Is the CSF aligned with international cybersecurity initiatives and standards? (nist.gov/informative-references) |

# Links Referenced

| NIST Resource Library | NIST.gov/cyberframework |
|---|---|
| **Global Impact of CSF 2.0** | • CSF 2.0 Translations: nist.gov/cyberframework/translations<br>• NIST International Cybersecurity and Privacy Resources: nist.gov/cybersecurity/international-cybersecurity-and-privacy-resources |
| **CSF 1.1 to 2.0 Changes** | • NIST Cybersecurity Framework 2.0 Reference Tool- csrc.nist.gov/extensions/nudp/services/json/csf/download?olirids=all<br>• From the CSF 2.0 Tool page - csrc.nist.gov/Projects/cybersecurity-framework/Filters#/csf/filters<br>• The Crosswalk from the OLIR catalog with more detail - csrc.nist.gov/csrc/media/Projects/olir/documents/submissions/CSFv1.1_to_CSFv2.0_CROSSWALK_20240220.xlsx |
| **Understanding Your Current and Target Cybersecurity Posture** | • CSF 2.0 Organizational Profiles Quick Start Guide: https://doi.org/10.6028/NIST.SP.1301 |
| **Staging Cybersecurity Risks for Enterprise Risk Management and Governance Oversight** | • NIST IR 8286C, nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8286C-upd1.pdf |
| **Implementation and Assessment** | • CSF 2.0 Informative References: nist.gov/informative-references<br>• NIST IR 8286B, Prioritizing Cybersecurity Risk for Enterprise Risk Management csrc.nist.gov/pubs/ir/8286/b/final<br>• NIST IR 8286D, Using Business Impact Analysis to Inform Risk Prioritization and Response csrc.nist.gov/pubs/ir/8286/d/upd1/final<br>• NIST SP 800-37 Revision 2, Risk Management Framework for Information Systems & Organizations csrc.nist.gov/pubs/sp/800/37/r2/final<br>• NIST SP 800-53 Revision 5, Security and Privacy Controls for Information Systems & Organizations csrc.nist.gov/pubs/sp/800/53/r5/upd1/final<br>• NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments csrc.nist.gov/pubs/sp/800/30/r1/final |
| **Small Business Resources** | • CSF 2.0 Small Business Quick Start Guide: nist.gov/itl/smallbusinesscyber/nist-cybersecurity-framework-0 |
| **Frequently Asked Questions** | • CSF 2.0 FAQs: nist.gov/cyberframework/faqs |

# Seeking Public Comment

**Open for public comment through April 14, 2025.**

- NIST IR 8286,Rev. 1: *Integrating Cybersecurity and Enterprise Risk Management* https://csrc.nist.gov/pubs/ir/8286/r1/ipd

- NIST IR 8286A, Rev. 1: *Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management* https://csrc.nist.gov/pubs/ir/8286/a/r1/ipd

- NIST IR 8286C, Rev. 1: *Staging Cybersecurity Risks for Enterprise Risk Management and Governance Oversight* https://csrc.nist.gov/pubs/ir/8286/c/r1/ipd

**Draft Quick Start Guide**

- NIST SP 1308: CSF 2.0 Cybersecurity, Enterprise Risk Management, and Workforce Management Quick Start Guide. Comments due: April 25, 2025. https://doi.org/10.6028/NIST.SP.1308.ipd

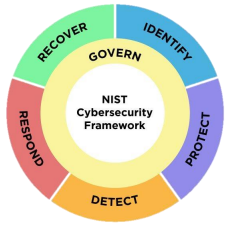
**Draft Mappings**

- Mapping of SP-800-37-Rev-2-to-Cybersecurity-Framework-v2.0 https://csrc.nist.gov/projects/olir/informative-reference-catalog/details?referenceId=149#/

- Mapping of NICE-v1.0.0-to-CSF-v2.0 https://csrc.nist.gov/projects/olir/informative-reference-catalog/details?referenceId=151#/

# Questions?

*This webinar has been recorded.*
*Slides have been posted to the event page.*
*A recording will be posted in the coming weeks, once it is available.*




**Email the CSF Team:** cyberframework@nist.gov

**Visit the CSF 2.0 Resource Library:** nist.gov/cyberframework

**View all upcoming events at:**

*nist.gov/cyberframework/events*