

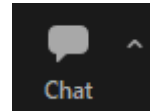
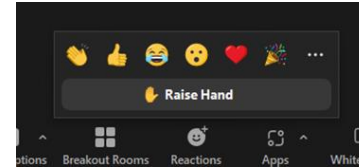
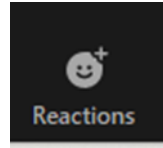
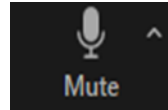
Journey to the National Institute of Standards & Technology Cybersecurity Framework 2.0



May 29, 2024

Housekeeping

- **Mute** when not speaking.
- If you do speak, share your name and agency.
- Raise your hand to speak.
- **Use the chat box to ask questions or to share links and information.**



Business Members

The Business Members Cyber Committee educates and shares knowledge and experience about recognizing and better managing the opportunities and risks associated with new technology.



Moderator

Scott Belcher
President and Chief Executive Officer
SFB Consulting, LLC
scottfbelcher@gmail.com



Panelists



Nakia Grayson

IT Security Specialist

National Institute of Standards
and Technology

Department of Commerce



Jeff Marron

IT Security Specialist

National Institute of Standards
and Technology

Department of Commerce



Amy Mahn

International Policy Specialist

National Institute of Standards
and Technology

Department of Commerce



Daniel Eliot

Lead for Small Business Engagement

National Institute of Standards
and Technology

Department of Commerce

Securing the Road Ahead with the Cybersecurity Framework 2.0

Amy Mahn, Nakia Grayson, Daniel Eliot, Jeff Marron

Applied Cybersecurity Division

May 2024

Agenda



- Introduction
- Brief Overview of CSF 2.0
- CSF Community Profiles
- Overview of the CSF 2.0 Small Business Quick Start Guide
- Additional CSF 2.0 Resources
- How to Get Involved

CSF 2.0 Overview

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

The Framework is comprised of:

CSF Core

CSF Organizational Profiles

CSF Tiers



Together, these six Functions provide a comprehensive view for managing cybersecurity risk.

How Did We Get Here?



Visit our CSF 2.0 Website: www.nist.gov/cyberframework

CSF 2.0 | What Makes it Different?

- Expanded scope beyond critical infrastructure. CSF 2.0 can help **all organizations** manage and reduce risks.
- Addition of a 6th Core Function “Govern.”
- Increased emphasis on supply chain risk management.
- Formalized the term “Community Profiles.”
- Improves on prior versions; we listened to your feedback, made key updates, **developed new resources and tools**, and adjusted our guidance based on today’s cybersecurity environment.

TRAVELING THROUGH NIST’S

CYBERSECURITY FRAMEWORK (CSF) 2.0 RESOURCES

CSF 2.0

For industry, government, and organizations
to reduce cybersecurity risks

IMPLEMENTATION EXAMPLES

Review action-oriented steps to help you achieve
various outcomes of the subcategories

QUICK START GUIDES

For organizations with specific common goals

MAPPINGS

See how NIST’s work interrelates and
shares themes

Quote from the NIST Director



“The CSF has been a vital tool for many organizations, helping them anticipate and deal with cybersecurity threats. CSF 2.0, which builds on previous versions, is not just about one document. It is about a suite of resources that can be customized and used individually or in combination over time as an organization’s cybersecurity needs change and capabilities evolve.”

~ **Laurie E. Locascio**

Under Secretary of Commerce for Standards and Technology
& NIST Director

Global Impact of CSF 2.0



- The CSF is used widely **internationally**.
- CSF versions 1.1 and 1.0 have been translated into 13 languages (*CSF 2.0 translations anticipated soon*).
- 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.
- The resources allow organizations to build cybersecurity frameworks and organize controls using the CSF Functions.

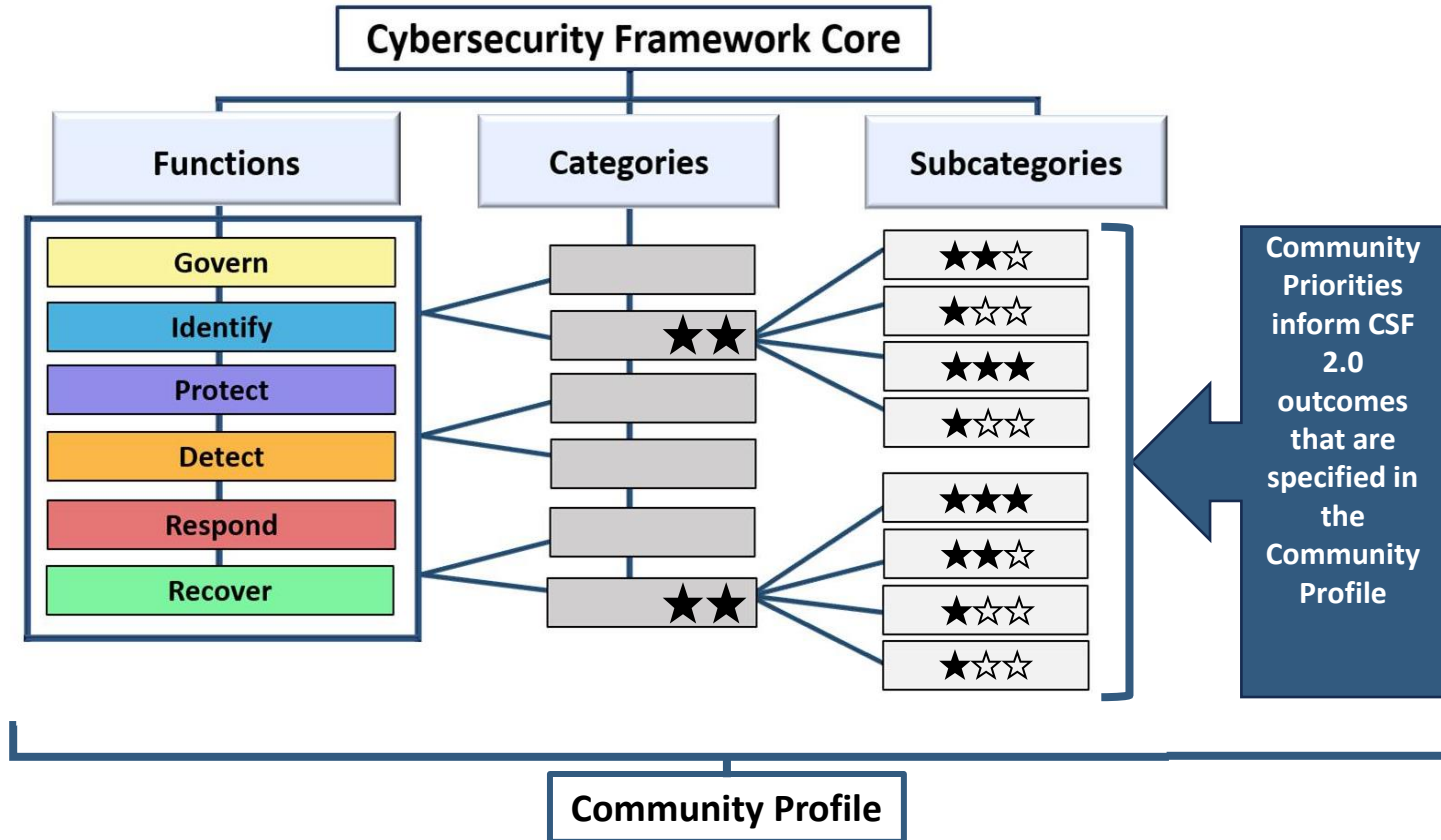


Overview of Community Profiles

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

Community Profiles



Benefits of Community Profiles



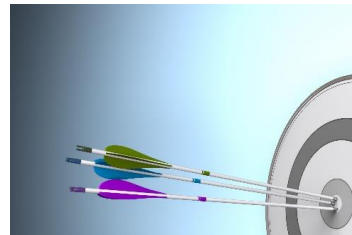
Use **shared taxonomy** for cybersecurity in the context of the community



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

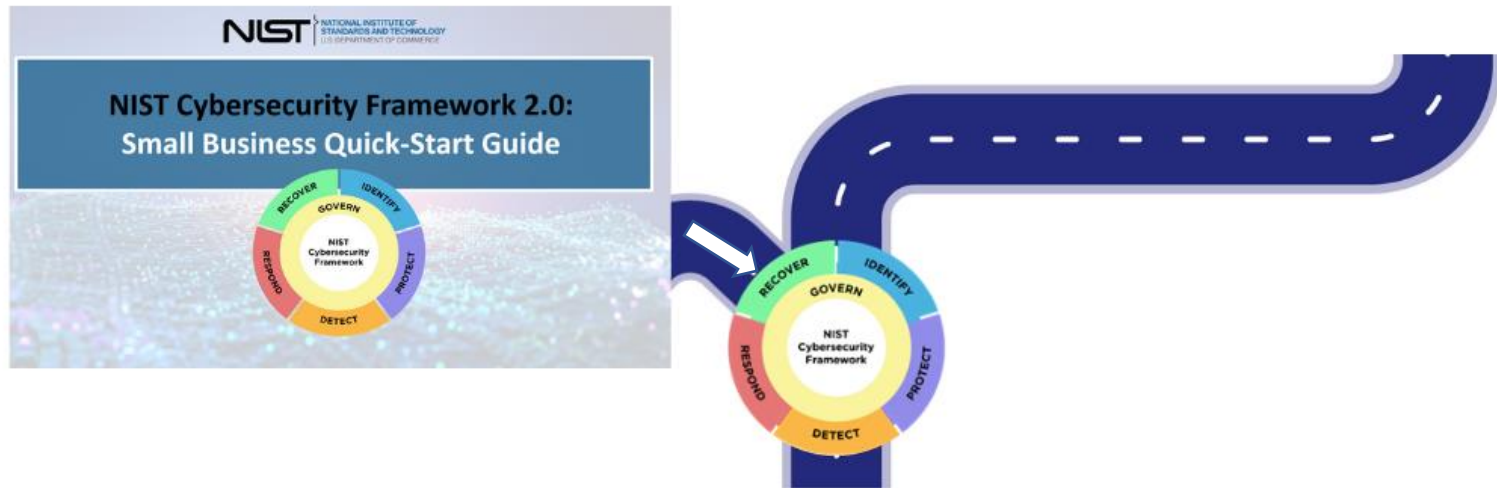
- CRI Profile for the Financial Sector
- Incident Response

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



Resources for CSF 2.0

NIST CSF 2.0 Small Business Quick Start Guide as an On-Ramp to the CSF 2.0 Journey



View full CSF 2.0 SMB Quick Start Guide: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf>

Creation of CSF 2.0 SMB QSG

- There was a clear desire for an actionable, accessible CSF resource for smaller entities.
- Not limited to only small businesses.
- Leveraging Implementation Examples as content for “Actions to Consider.”
- Focus on usability and readability.
- Focus on a limited number of high priority items that an under-resourced organization can implement.

GOVERN

The Govern Function helps you establish and monitor your business's cybersecurity risk management strategy, expectations, and policy.

Actions to Consider

Understand

- Understand how cybersecurity risk can thwart achievement of your business's mission. (IS-C-02)
- Understand your legal, regulatory, and contractual cybersecurity requirements. (IS-C-02)
- Understand who within your business will be responsible for developing and executing the cybersecurity strategy. (IS-C-02)

Assess

- Assess the potential impact of a total or partial loss of critical business assets and operations. (IS-C-04)
- Assess whether cybersecurity insurance is appropriate for your business. (IS-C-04)
- Assess cybersecurity risks posed by suppliers and other third parties before entering into formal relationships. (IS-C-06)

Prioritize

- Prioritize managing cybersecurity risks alongside other business risks. (IS-C-04)

Communicate

- Communicate leadership's support of a risk-aware, ethical, and continually improving culture. (IS-C-02)
- Communicate, authorize, and maintain policies for managing cybersecurity risks. (IS-C-02)

Getting Started with Cybersecurity Governance

You can use these tables to begin thinking about your cybersecurity governance strategy.

Setting Organizational Context	Documenting Cybersecurity Requirements
Our business mission statement	List your legal requirements
What cybersecurity risks may present us with achieving this mission?	List your regulatory requirements
	List your contractual requirements

Technical Deep Dive: Update Cybersecurity Risk to Enterprise Risk Management and Governance Context

Questions to Consider

- As our business grows, how often are we reviewing our cybersecurity strategy?
- Do we need to update our existing staff, our talent, or engage an external partner to help us establish and manage our cybersecurity plan?
- Do we have acceptable use policies for our business and for employees/external devices accessing business resources? Have employees been educated on these policies?

Related Resources

- Security Small and Medium-Sized Supply Chain Resource Handbook
- Choosing a Vendor/Service Provider

[View all NIST CSF 2.0 Resources Here](#)

IDENTIFY

The Identify Function helps you determine the current cybersecurity risk to the business.

Actions to Consider

Understand

- Understand what assets your business relies upon by creating and maintaining an inventory of hardware, software, systems, and services. (IS-0A-01)

Assess

- Assess your assets' (off and/or physical) potential vulnerabilities. (IS-0A-02)
- Assess the effectiveness of the business's cybersecurity program to identify areas that need improvement. (IS-0A-02)

Prioritize

- Prioritize inventories and classifying your business data. (IS-0A-01)
- Prioritize documenting internal and external cybersecurity threats and associated responses using a risk register. (IS-0A-01)

Communicate

- Communicate cybersecurity plans, policies, and best practices to all staff and relevant third parties. (IS-0A-02)
- Communicate to staff the importance of identifying needed improvements to cybersecurity risk management processes, procedures, and activities. (IS-0A-02)

Getting Started with Identifying Current Cybersecurity Risk to the Business

Before you can protect your assets, you need to identify them. Then you can determine the appropriate level of protection for each asset based upon its sensitivity and criticality to your business mission. You can use this sample table to get started on your information technology (IT) asset inventory. As your business matures, you might consider using an automated asset inventory solution or a managed security service provider to help you manage all of your business assets.

Software/hardware/service	Asset's official use or owner	Identify associated data to access this asset?	Is multi-factor authentication required to access this asset?	Risk to the business if we lose access to this asset?

Technical Deep Dive: Integrating Cybersecurity and Enterprise Risk Management

Questions to Consider

- What are our most critical business assets (info, hardware, software, systems, facilities, services, people, etc.) we need to protect?
- What are the elements and primary risks associated with each asset?
- What technologies or services are approved for use to accomplish this work? Are these services or technologies secure and approved for use?

Related Resources

- NIST Risk Register Template
- Take Stock: Assess What Security Information You Have
- Evaluating Your Operational Resilience and Cybersecurity Practices

[View all NIST CSF 2.0 Resources Here](#)

PROTECT

The Protect Function supports your ability to use safeguards to prevent or reduce cybersecurity risks.

Actions to Consider

Understand

- Understand what information resources (info) you own or have access to. Protect sensitive information assets to only those employees who need it to do their jobs. (IS-0P-01)

Assess

- Assess the timeliness, quality, and frequency of your company's cybersecurity training for employees. (IS-0P-02)

Prioritize

- Prioritize requiring multi-factor authentication on all accounts that offer it and consider using password managers to help you and your staff generate and protect strong passwords. (IS-0P-01)
- Prioritize changing default manufacturer passwords. (IS-0P-01)
- Prioritize regularly updating and patching software and operating systems. Enable automatic updates to help you remember. (IS-0P-02)
- Prioritize regularly backing up your data and testing your backups. (IS-0P-03)
- Prioritize configuring your laptops and laptops to enable full-disk encryption to protect data. (IS-0P-03)

Communicate

- Communicate to your staff how to recognize common attacks, report attacks or suspicious activity, and perform basic cyber hygiene tasks. (IS-0P-02)

Getting Started with Protecting Your Business

Building multi-factor authentication (MFA) is one of the fastest, cheapest ways you can protect your data. Start with accounts that you can find the most common information. Use this checklist to get you a head start. Not every account you can use will be on this longer list.

Account	MFA Enabled (Y/N)
Banking Accounts	
Accounting and Tax Accounts	
Microsoft Accounts	
Google, Microsoft, Apple ID Accounts	
Amazon Accounts	
Payment Manager	
Employer Accounts	

Technical Deep Dive: NIST Digital Identity Dashboards

Questions to Consider

- Are we restricting access and privileges only to those who need it? Are we removing access when they no longer need it?
- How are we securely controlling and distributing data and data storage devices in our work environment?
- Do employees possess the knowledge and skills to perform their jobs with security as they're required?

Related Resources

- Cybersecurity Training Resources
- Multi-Factor Authentication
- Protecting Your Accounts from Phishing

[View all NIST CSF 2.0 Resources Here](#)

DETECT

The Detect Function provides outcomes that help you find and analyze possible cybersecurity attacks and compromises.

Actions to Consider

Understand

- Understand how to identify common indicators of a cybersecurity incident. (IS-0D-01)

Assess

- Assess your computing technologies and external services for deviations from expected or typical behavior. (IS-0D-01)
- Assess your physical environment for signs of tampering or suspicious activity. (IS-0D-01)

Prioritize

- Prioritize installing and maintaining antivirus and anti-malware software on all business devices—including servers, desktops and laptops. (IS-0D-01)
- Prioritize engaging a service provider to monitor computers and networks for suspicious activity if you don't have the resources to do it internally. (IS-0D-01)

Communicate

- Communicate with your authorized incident responder such as an MSP about the relevant details from the incident to help them analyze and mitigate it. (IS-0D-01)

Getting Started with Detecting Incidents

Some common indicators of a cybersecurity incident are:

- Loss of usual access to data, applications, or services
- Unusually sluggish network
- Antivirus software alerts when it detects that a host is infected with malware
- Multiple failed login attempts
- An email administrator notes many bounced emails with suspicious content
- A network administrator notices an unusual decrease in typical network traffic flows

Technical Deep Dive: NIST Computer Security Incident Handling Guide

Questions to Consider

- Do devices that are used for our business, whether business-owned or employee-owned, have antivirus software installed?
- Do employees know how to detect possible cybersecurity attacks and how to report them?
- How do our business monitoring logs and alerts to detect potential cyber incidents?

Related Resources

- Network Protection and Response
- Security of Physical Systems
- Cybersecurity Training Resources

[View all NIST CSF 2.0 Resources Here](#)

RESPOND

The Respond Function supports your ability to take action regarding a detected cybersecurity incident.

Actions to Consider

Understand

- Understand what your incident response plan is and who has authority and responsibility for implementing various aspects of the plan. (IS-0R-01)

Assess

- Assess your ability to respond to a cybersecurity incident. (IS-0R-01)
- Assess the incident's dependence to security, what happened, and its root causes. (IS-0R-01, IS-0R-02)

Prioritize

- Prioritize taking steps to contain and evaluate the incident to prevent further damage. (IS-0R-01)

Communicate

- Communicate a confirmed cybersecurity incident with all internal and external stakeholders (e.g., customers, business partners, law enforcement agencies, regulatory bodies) as required by law, regulations, contracts, or policies. (IS-0R-01)

Getting Started with an Incident Response Plan

Before an incident occurs, you need to be ready with a basic response plan. This will help your business respond to a cybersecurity incident.

- A business changes:** Someone who is responsible for developing an incident response plan is called an incident responder.
- Who to call:** List all of the individuals who may be part of your incident response efforts, including their contact information, responsibilities, and authority.
- What/When/How to report:** Set your business's communication/escalation responsibilities as required by law, regulations, contracts, or policies.

Technical Deep Dive: NIST Computer Security Incident Handling Guide

Questions to Consider

- Do we have a cybersecurity incident response plan? If so, how have we practiced it to see if it works?
- Do we know who the key internal and external stakeholders and decision makers are who will work if we have a detected cybersecurity incident?

Related Resources

- Incident Response Plan Basics
- US Cyber Incident Coordination Center
- Data Breach Response: A Guide for Business
- Best Practices for Incident Response and Reporting of Cyber Incidents

Contact	Phone
Business leader	
Technical Contact	
State	
Federal	
NGO	
Bank	
Insurance	

[View all NIST CSF 2.0 Resources Here](#)

RECOVER

The Recover Function involves activities to restore assets and operations that were impacted by a cybersecurity incident.

Actions to Consider

Understand

- Understand who within and outside your business has recovery responsibilities. (IS-0R-02)

Assess

- Assess what happened by preparing an after-action report—on your own or in consultation with a stakeholder—that documents the incident, the response and recovery actions taken, and lessons learned. (IS-0R-02)
- Assess the integrity of your backup data and sources before using them for restoration. (IS-0R-03)

Prioritize

- Prioritize your recovery activities based on organizational needs, resources, and month impacts. (IS-0R-02)

Communicate

- Communicate regularly and accurately with internal and external stakeholders.
- Communicate and document completion of the incident and resumption of normal activities. (IS-0R-02)

Getting Started with a Recovery Playbook

A playbook typically includes the following critical elements:

- A list of formal recovery processes
- Documentation of the catalogs of organizational resources (e.g., people, facilities, technical components, external services)
- Documentation of systems that process and store organizational information, particularly key assets. This will help inform the order of restoration priority
- A list of personnel who will be responsible for defining and implementing recovery plans
- A comprehensive recovery communications plan

Technical Deep Dive: NIST Guide for Cybersecurity Event Response

Questions to Consider

- What are our lessons learned? How can we minimize the chances of a cybersecurity incident happening in the future?
- How are our legal, regulatory, and contractual obligations for communicating to internal and external stakeholders about a cybersecurity incident?
- How do we ensure that the recovery steps we are taking are not introducing new vulnerabilities to our business?

Related Resources

- Continuity of Training Resources
- Security of IT Systems: Recovery Plan
- Business and Recovery Resources

[View all NIST CSF 2.0 Resources Here](#)

GOVERN



The Govern Function helps you establish and monitor your business's cybersecurity risk management strategy, expectations, and policy.

Actions to Consider

Understand

- Understand how cybersecurity risks can disrupt achievement of your business's mission. (GV.OC-01)
- Understand your legal, regulatory, and contractual cybersecurity requirements. (GV.OC-03)
- Understand who within your business will be responsible for developing and executing the cybersecurity strategy. (GV.RR-02)

Assess

- Assess the potential impact of a total or partial loss of critical business assets and operations. (GV.OC-04)
- Assess whether cybersecurity insurance is appropriate for your business. (GV.RM-04)
- Assess cybersecurity risks posed by suppliers and other third parties before entering into formal relationships. (GV.SC-06)

Prioritize

- Prioritize managing cybersecurity risks alongside other business risks. (GV.RM-03)

Communicate

- Communicate leadership's support of a risk-aware, ethical, and continually improving culture. (GV.RR-01)
- Communicate, enforce, and maintain policies for managing cybersecurity risks. (GV.PO-01)

Getting Started with Cybersecurity Governance

You can use these tables to begin thinking about your cybersecurity governance strategy.

Setting Organizational Context		Documenting Cybersecurity Requirements	
Our business mission statement:		List your legal requirements:	
What cybersecurity risks may prevent us from achieving this mission?		List your regulatory requirements:	
		List your contractual requirements:	

Technical Deep Dive: [Staging Cybersecurity Risks for Enterprise Risk Management and Governance Oversight](#)

Questions to Consider

- As our business grows, how often are we reviewing our cybersecurity strategy?
- Do we need to upskill our existing staff, hire talent, or engage an external partner to help us establish and manage our cybersecurity plan?
- Do we have acceptable use policies in place for business and for employee-owned devices accessing business resources? Have employees been educated on these policies?

Related Resources

- [Securing Small and Medium-Sized Supply Chains Resource Handbook](#)
- [Choosing A Vendor/Service Provider](#)

[View all NIST CSF 2.0 Resources Here](#)



Additional CSF 2.0 Resources

CSF 2.0 Resource Library

An official website of the United States government [Here's how you know](#)

NIST Search NIST Menu

CYBERSECURITY FRAMEWORK

Helping organizations to better understand and improve their management of cybersecurity risk

CSF 2.0 Resource Center

- Download (PDF)
- Quick Start Guides
- Profiles
- Informative References
- FAQs
- Translations
- CSF 2.0 Tool

News and Events

Related Programs

Ways to Engage

Cybersecurity @ NIST

CSF 1.1 Archive

CONNECT WITH US

BIG NEWS | The NIST CSF 2.0 has been released, along with other supplementary resources!

CSF 2.0

For industry, government, and organizations to reduce cybersecurity risks

[Read the Document](#)

CSF 2.0 Profiles

Templates and useful resources for creating and using both CSF profiles

[See the Profiles](#)

Quick Start Guides

For users with specific common goals

[View the Quick Start Guides](#)

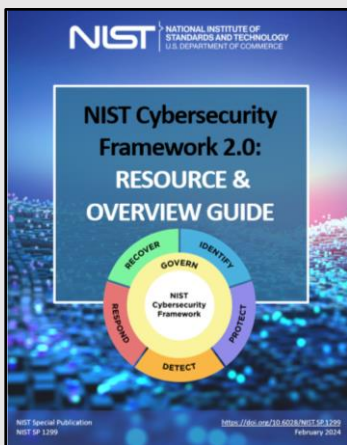
Informative References (Mappings)

See how NIST's resources overlap and share themes

[See the Mappings](#)

View the CSF 2.0 Resource Library: <https://nist.gov/cyberframework>

Explore Other CSF 2.0 Resources



Navigating NIST's CSF 2.0 Quick Start Guides

Resource and Overview Guide

Understand the basics and learn about the many available helpful CSF 2.0 resources

[Download](#)

The below targeted guides will help you with specific topics.

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 with modest or no cybersecurity plans currently in place.

[Download](#)

C-SCRM

Helps organizations become smarter acquirers and suppliers of technology products and services.

[Download](#)

Tiers

Organizations can use these to apply the CSF 2.0 Tiers to Profiles to characterize the rigor of their cybersecurity risk governance and management outcomes.

[Download](#)

Enterprise Risk Management

How ERM practitioners can utilize the outcomes provided in the CSF 2.0 to improve organizational cybersecurity risk management.

[Download](#)

NIST Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER

Search CSRC CSRC MENU

PROJECTS **CYBERSECURITY AND PRIVACY REFERENCE TOOL**

Cybersecurity and Privacy Reference Tool CPRT

f t in

The NIST Cybersecurity Framework 2.0 Draft, Version 2.0

Search:

CPRT / Version 2.0
[Expand Entire Reference Dataset](#)

Functions

- GV GOVERN**
Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy
- ID IDENTIFY**
Help determine the current cybersecurity risk to the organization
- PR PROTECT**
Use safeguards to prevent or reduce cybersecurity risk
- DE DETECT**
Find and analyze possible cybersecurity attacks and compromises
- RS RESPOND**
Take action regarding a detected cybersecurity incident
- RC RECOVER**

NIST Cybersecurity Framework (CSF) 2.0 Reference Tool

Search:

Function
GOVERN (GV): Establish and monitor the organization's cybersecurity risk management strategy.

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

Subcategory
OL-OC-01: The organizational mission is understood and informs cybersecurity risk management (Formerly ID.BE-01, 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 risks that may impede that mission

Subcategory
OL-OC-02: Internal and external stakeholders are determined, and their needs and expectations regarding cybersecurity risk management are understood

CYBERSECURITY FRAMEWORK

Informative References

CSF 2.0 Informative Reference Catalog
See what documents have been mapped to the CSF 2.0 Document.
[Catalog](#)

Compare CSF 2.0 Informative References
Generate Comparison Reports between CSF 2.0 Informative References you've selected.
[Compare Reports](#)

Download Informative Reference in the Core
Weekly download of all the Informative References for CSF 2.0
[Download \(all\)](#) [Download \(url\)](#)

Resources

Quick Links	Contact Information
CSF 2.0 Website: https://www.nist.gov/cyberframework	cyberframework@nist.gov
CSF 2.0 FAQs: https://www.nist.gov/faqs	
Framework Resource Center-Community Profiles: https://www.nccoe.nist.gov/framework-resource-center	framework-profiles@nist.gov
Guide to Creating Community Profiles: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.32.ipd.pdf	
CSF 2.0 Small Business Quick Start Guide: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf	smallbizsecurity@nist.gov
CSF 2.0 Cybersecurity Supply Chain Risk Management (C-SCRM) Quick Start Guide: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf	scrm-nist@nist.gov
National Online Informative References Program (OLIR)-Mappings: https://csrc.nist.gov/projects/olir & https://csrc.nist.gov/Projects/olir/derived-relationship-mapping#	olir@nist.gov
Cybersecurity and Privacy Reference Tool (CPRT): https://csrc.nist.gov/Projects/cprt	cpirt@nist.gov
NIST International Cybersecurity and Privacy Resources: https://www.nist.gov/cybersecurity/international-cybersecurity-and-privacy-resources	intl-cyber-privacy@nist.gov

How to Get Involved

How to Get Involved

- **Join the NCCoE CSF 2.0 Community Profiles Community of Interest:**
<https://www.nccoe.nist.gov/framework-resource-center>
- **Join a Small Business Cybersecurity Community of Interest:**
<https://www.nist.gov/itl/smallbusinesscyber/get-engaged>
- **Submit resources.** These can include Profiles, Translations, Mappings, and more.
- **Sign up for CSF email alerts:**
<https://public.govdelivery.com/accounts/USNIST/subscriber/new>
- **Send us a note:** cyberframework@nist.gov



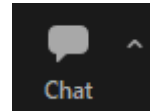
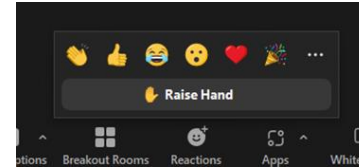
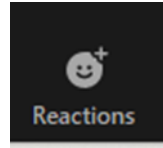
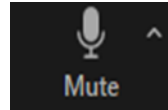
Thank You for Joining Us Today!

FOR FURTHER INFORMATION AND/OR QUESTIONS ABOUT THE CYBERSECURITY FRAMEWORK:

cyberframework@nist.gov

Questions

- **Mute** when not speaking.
- If you do speak, share your name and agency.
- Raise your hand to speak.
- **Use the chat box to ask questions** or to share links and information.



Resources

Quick Links	Contact Information
CSF 2.0 Website: https://www.nist.gov/cyberframework	cyberframework@nist.gov
CSF 2.0 FAQs: https://www.nist.gov/faqs	
Framework Resource Center-Community Profiles: https://www.nccoe.nist.gov/framework-resource-center	framework-profiles@nist.gov
Guide to Creating Community Profiles: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.32.ipd.pdf	
CSF 2.0 Small Business Quick Start Guide: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf	smallbizsecurity@nist.gov
CSF 2.0 Cybersecurity Supply Chain Risk Management (C-SCRM) Quick Start Guide: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf	scrm-nist@nist.gov
National Online Informative References Program (OLIR)-Mappings: https://csrc.nist.gov/projects/olir & https://csrc.nist.gov/Projects/olir/derived-relationship-mapping#	olir@nist.gov
Cybersecurity and Privacy Reference Tool (CPRT): https://csrc.nist.gov/Projects/cprt	cpert@nist.gov
NIST International Cybersecurity and Privacy Resources: https://www.nist.gov/cybersecurity/international-cybersecurity-and-privacy-resources	intl-cyber-privacy@nist.gov

APTA Security Standards

<https://www.apta.com/research-technical-resources/standards/security/>



PT ISAC

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION



Thanks for attending

phanson@apta.com

703-505-2523

Polly Hanson

Senior Director Security, Risk and
Emergency Management

American Public Transportation Association

