NIST Cybersecurity Framework 2.0
Overview & Updates

Stephen Quinn
Information Technology Laboratory
November 2024

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

Executive Order 13636 – Improving Critical Infrastructure Cybersecurity

February 12, 2013

"It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties"

Executive Order 13636

Cybersecurity Enhancement Act of 2014

December 18, 2014

Amends the National Institute of Standards and Technology Act (15 U.S.C. 272(c)) to say:

*"…on an ongoing basis, facilitate and support the development of a **voluntary**, **consensus-based**, **industry-led** set of standards, guidelines, best practices, methodologies, procedures, and processes to cost-effectively reduce cyber risks to critical infrastructure"*

Public Law No: 113-274

Cybersecurity Framework Authorities

How Did We Get Here?

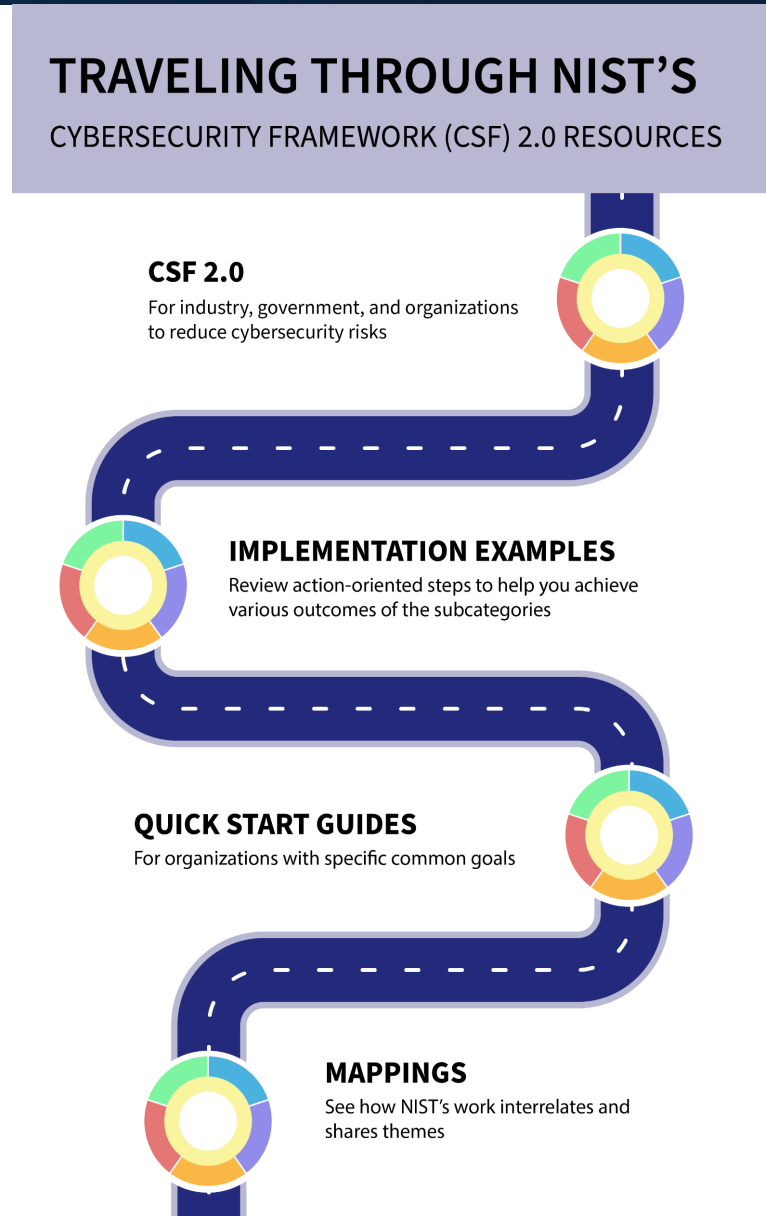
NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

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

Why Upgrade to CSF 2.0 from 1.1?

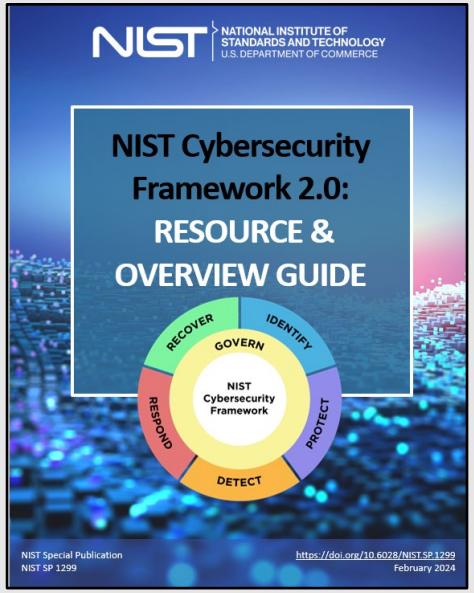
NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

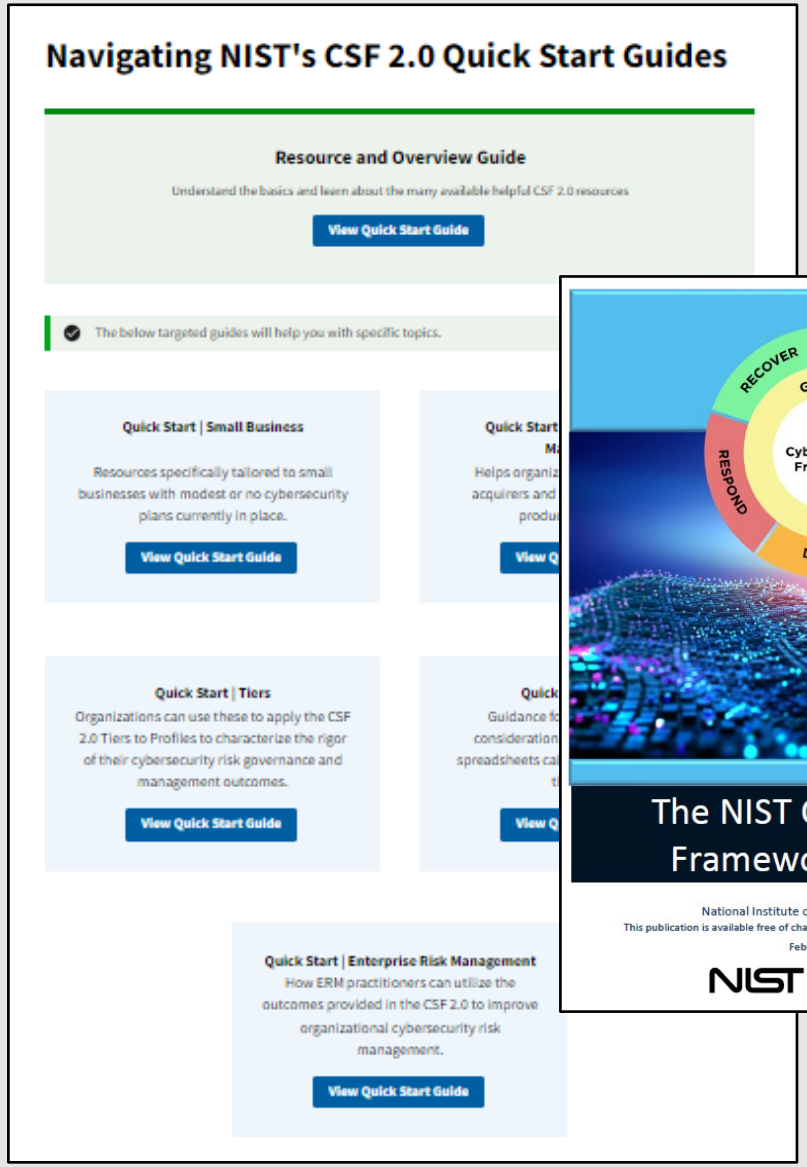
- CSF 2.0 is a wide-ranging resource, not just a document.
- A focus on cybersecurity supply chain and risk management (CSRM, SCRM, and ERM)
- Dynamic informative references and implementation examples
- Greatly enhanced with the addition of Govern Function
- To keep pace with the current technology windows

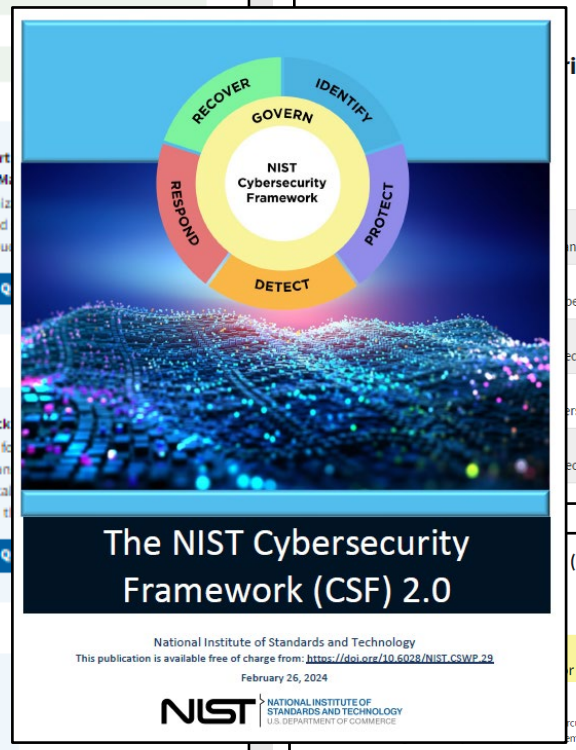


Suite of Resources Snapshot

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







October 2024 Resource Expansion

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

NIST CSF 2.0 NEWS & UPDATES

WHAT'S NEW. WHAT'S COMING.

It's Cybersecurity Awareness Month and we're celebrating by sharing NIST Cybersecurity Framework (CSF) updates! Since the launch of the CSF 2.0 in February, 2024, a lot has been happening...

QUICK START GUIDES (QSG)
We've released three new final versions of QSGs to help you with specific topics and understanding the basics.

NEW TRANSITION SPREADSHEET
Use our Category and Subcategory transition explanations from CSF 1.1 to CSF 2.0.

MORE TRANSLATIONS
The CSF has been translated into several different languages (with more to come).

UPADATED FAQs
Learn the answers to the most common questions being asked about the CSF.

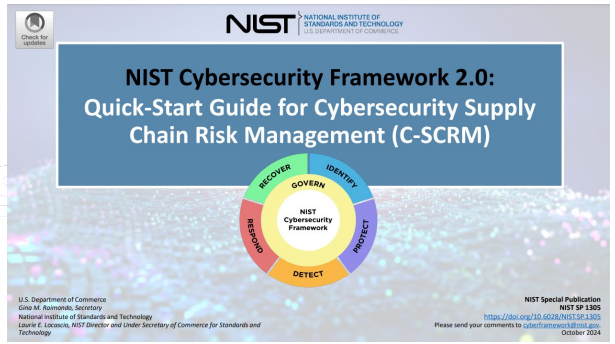
NEW VIDEOS
Learn the basics, see clips from our experts, and see our new CSF overview video.

EVENTS & ANNOUNCEMENTS
See the latest CSF updates and find out what events we have coming up.

STAY CONNECTED WITH US!

- Follow us on X: @NISTcyber
- Email us: cyberframework@nist.gov
- Visit our page: nist.gov/cyberframework
- Subscribe to get email updates

October 2024



National Institute of Standards and Technology (Instituto Nacional de Estándares y Tecnología)
Esta publicación está disponible de forma gratuita en: https://doi.org/10.6028/NIST.CSWP.29.spa
Febrero 26, 2024

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

	A	B	C	D	E	F	G	H	I	J
1	CSF 1.1 Identifier	CSF 1.1 Description	CSF 1.1 SORT-ID	Relocation	Noteworthy Modifications	CSF 2.0 Identifier	CSF 2.0 Description	New in CSF 2.0	CSF 2.0 SORT-ID	Implementation Examples
4	ID.BE-2	The organization's place in critical infrastructure and its industry sector is identified and communicated	v11-011	Y (incorporated into)	Clarified the original wording	GV.OC-01	The organizational mission is understood and informs cybersecurity risk management	N	v20-003	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
5	ID.BE-3	Priorities for organizational mission, objectives, and activities are established and communicated	v11-012	Y (incorporated into)	Clarified the original wording	GV.OC-01	The organizational mission is understood and informs cybersecurity risk management	N	v20-003	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
6	ID.GV-2	Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	v11-017	Y (incorporated into)	Changed scope to include all stakeholder needs and expectations for cybersecurity, not just roles and responsibilities	GV.OC-02	Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered	N	v20-004	Ex1: Identify relevant internal stakeholders and their cybersecurity-related expectations (e.g., performance and risk expectations of officers, directors, and advisors; cultural expectations of employees) Ex2: Identify relevant external stakeholders and their cybersecurity-related expectations (e.g., privacy expectations of customers, business expectations of partnerships, compliance expectations of regulators, ethics expectations of society)

How It's Being Used

- CSF 2.0 Profile for the Financial Services Sector
- Consortium For Certified Service Centers member self-attestation for adherence to CSF 2.0
- Cybersecurity Forum for Independent and Executive Branch Regulators selects CSF 2.0 as the basis for their regulatory activities.
- Incorporation of CSF 2.0 into training curricula and clinics

The CSF 2.0 is the most downloaded NIST publication within the NIST library database

- Through September 17, the CSF has been downloaded more than **625,000** times.
- Since August 14, a series of new Quick Start Guides have been downloaded more than **144,000** times.

"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

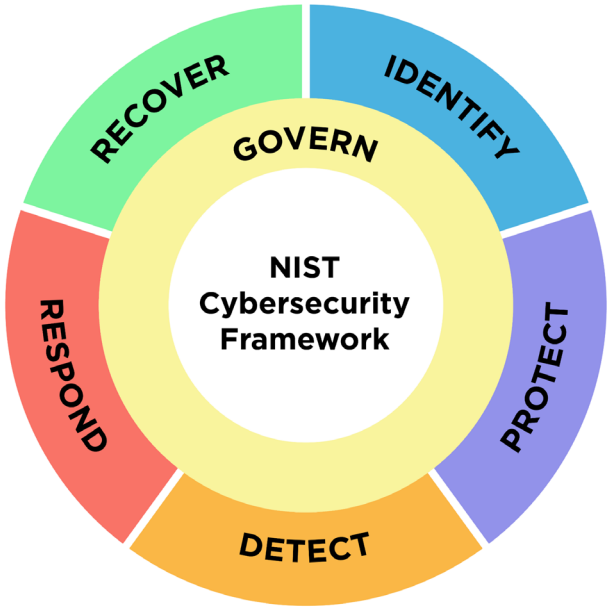
Global Impact of CSF 2.0

- The CSF is used widely internationally.
- CSF 2.0 has been translated into Spanish, Portuguese, and Korean, with 8 more expected fall 2024.
- Quick Start Guides are being translated into French, Spanish, Portuguese, and Japanese, with more to come.
- Other translations and uses by additional government and industry known to be taking place.
- At least 43% total CSF downloads are from outside the U.S.

https://www.nist.gov/cyberframework/csf-11-archive/translations

What's Next?

- Collecting and documenting CSF 2.0 use cases
- Additional translations and resources
- Community Profiles
- CSF 2.0 webinars and self-paced modules
- NIST continues to encourage candid, constructive discussions and other engagements about organizations' experiences with the CSF.



Website: https://www.nist.gov/cyberframework
Email: cyberframework@nist.gov

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