Journey to the NIST Cybersecurity Framework 2.0

Federal Advisory Committee on Insurance (FACI)
September 2023

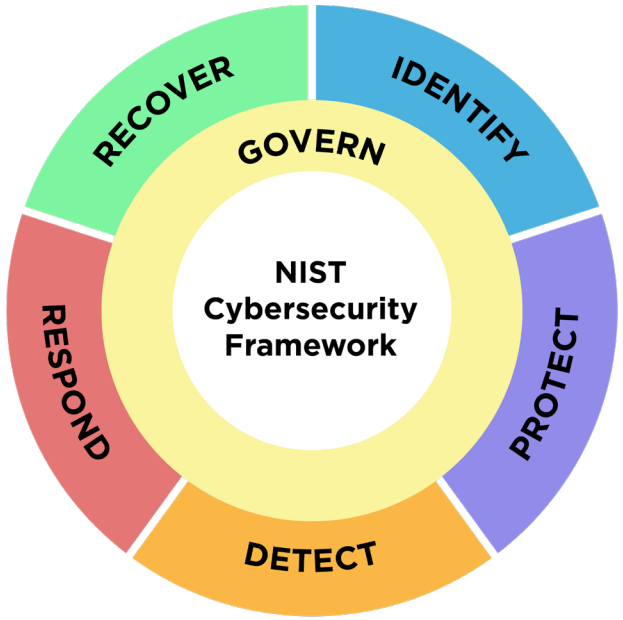
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

CSF Update | Journey to CSF 2.0

- **NIST is updating the Cybersecurity Framework** to address the evolving cybersecurity risk and standards landscape and make it easier for organizations to address risks. NIST is actively relying on and seeking diverse stakeholder feedback in the update process.

Ways to engage: www.nist.gov/cyberframework

JUST RELEASED | Draft CSF 2.0



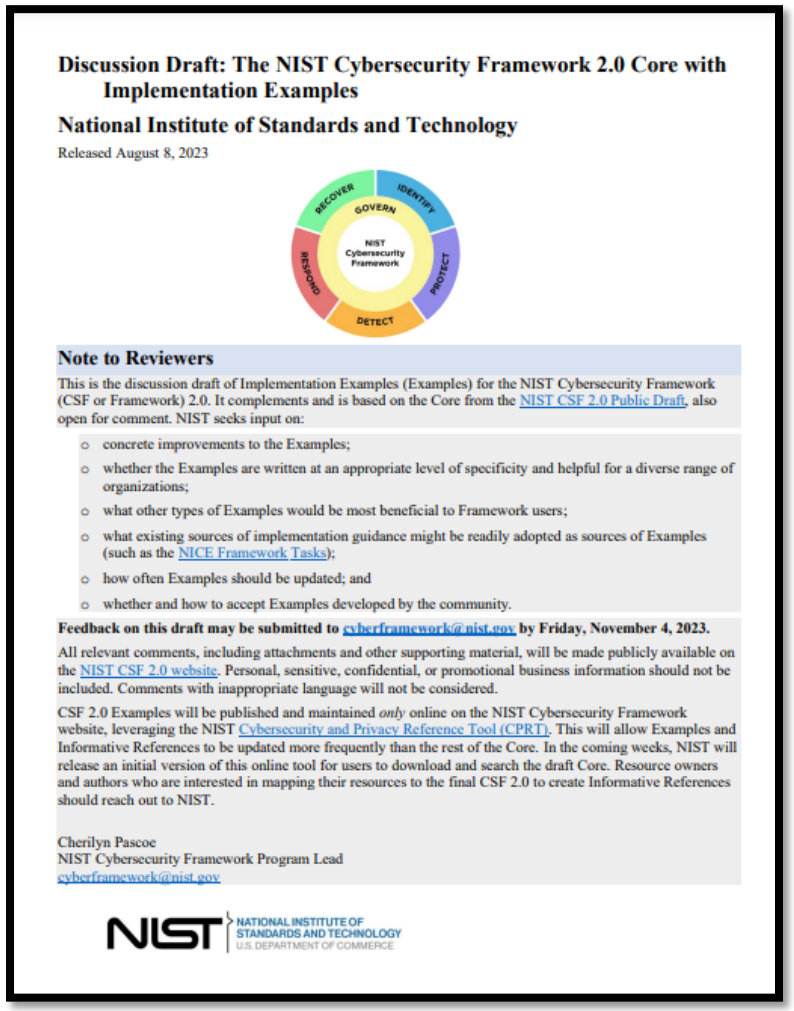
This newly released draft represents a major update to the CSF, which was first released in 2014.

Key Updates:

- Reflects changes in the cybersecurity landscape (risks, technologies, standard changes)
- Makes it easier to put the CSF into practice for all organizations through additional guidance on implementing the CSF
- An expanded scope beyond critical infrastructure.
- The addition of a sixth function, Govern.
- Additional coverage of supply chain security.

Comments on the Draft Core may be sent to cyberframework@nist.gov by November 4, 2023.

CSF 2.0 Discussion Draft
Revised Core with Implementation Examples



Discussion Draft: The NIST Cybersecurity Framework 2.0 Core with Implementation Examples

National Institute of Standards and Technology

Released August 8, 2023

Note to Reviewers

This is the discussion draft of Implementation Examples (Examples) for the NIST Cybersecurity Framework (CSF or Framework) 2.0. It complements and is based on the Core from the NIST CSF 2.0 Public Draft, also open for comment. NIST seeks input on:

- concrete improvements to the Examples;
- whether the Examples are written at an appropriate level of specificity and helpful for a diverse range of organizations;
- what other types of Examples would be most beneficial to Framework users;
- what existing sources of implementation guidance might be readily adopted as sources of Examples (such as the NICE Framework Tasks);
- how often Examples should be updated; and
- whether and how to accept Examples developed by the community.

Feedback on this draft may be submitted to cyberframework@nist.gov by Friday, November 4, 2023.

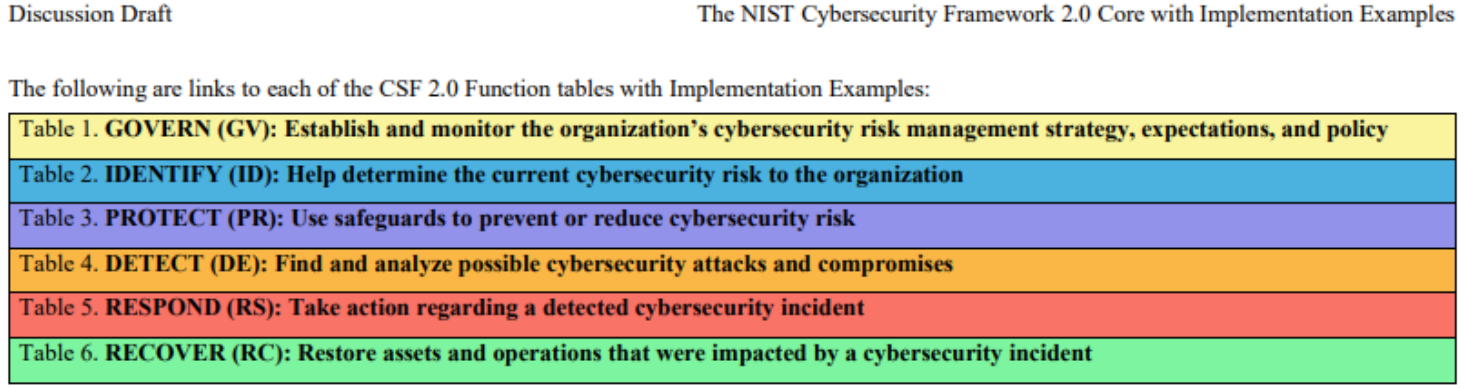
All relevant comments, including attachments and other supporting material, will be made publicly available on the NIST CSF 2.0 website. Personal, sensitive, confidential, or promotional business information should not be included. Comments with inappropriate language will not be considered.

CSF 2.0 Examples will be published and maintained *only* online on the NIST Cybersecurity Framework website, leveraging the NIST Cybersecurity and Privacy Reference Tool (CPRT). This will allow Examples and Informative References to be updated more frequently than the rest of the Core. In the coming weeks, NIST will release an initial version of this online tool for users to download and search the draft Core. Resource owners and authors who are interested in mapping their resources to the final CSF 2.0 to create Informative References should reach out to NIST.

Cherilyn Pascoe
NIST Cybersecurity Framework Program Lead
cyberframework@nist.gov

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

nist.gov/document/discussion-draft-nist-cybersecurity-framework-20-core-implementation-examples



Discussion Draft — The NIST Cybersecurity Framework 2.0 Core with Implementation Examples

The following are links to each of the CSF 2.0 Function tables with Implementation Examples:

Table 1. **GOVERN (GV): Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy**
Table 2. **IDENTIFY (ID): Help determine the current cybersecurity risk to the organization**
Table 3. **PROTECT (PR): Use safeguards to prevent or reduce cybersecurity risk**
Table 4. **DETECT (DE): Find and analyze possible cybersecurity attacks and compromises**
Table 5. **RESPOND (RS): Take action regarding a detected cybersecurity incident**
Table 6. **RECOVER (RC): Restore assets and operations that were impacted by a cybersecurity incident**

Comments on the Discussion Draft may be sent to cyberframework@nist.gov by November 4, 2023.

CSF 2.0 Next Steps

- **Public workshops and events**
  - Third and final CSF 2.0 Workshop → September 19-20 at the NIST NCCoE.
  - Find recordings of CSF Workshop #1 (August 2022) and #2 (February 2023) online.
- **Comment on drafts**
  - Provide comments on the Draft CSF 2.0 and the Discussion Draft by November 4, 2023 (all prior comments received can be found online).
- **Continuing to seek and develop CSF resources, success stories, and mappings to other frameworks and standards.**

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

STAY IN TOUCH

CONTACT US

NIST.gov

@NISTcyber