

NIST Cybersecurity Framework 2.0 Overview & Updates

Bill Newhouse

Cybersecurity Engineer, NIST National Cybersecurity Center of Excellence
2024

CSF 2.0 Overview

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

Six Functions — **Govern, Identify, Protect, Detect, Respond, and Recover**. Together, they provide a comprehensive view for managing cybersecurity risk.

The Framework is also comprised of:

CSF Core

CSF Organizational Profiles

CSF Tiers



“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

How Did We Get Here?



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

CSF 2.0 | What Makes it Different?

- CSF 2.0 can help **all organizations** – not just those in critical infrastructure – manage and reduce risks.
- It 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.
- NIST’s suite of resources offers **practical and actionable suggestions** to help organizations immediately improve their cybersecurity posture (focus on *how* the CSF can be implemented).
- The CSF 2.0 is about a **suite of resources** that aims to help **all organizations** – not just those in critical infrastructure – manage and reduce risks.

TRAVELING THROUGH NIST’S CYBERSECURITY FRAMEWORK (CSF) 2.0 RESOURCES



Suite of Resources Snapshot



NIST Cybersecurity Framework 2.0: RESOURCE & OVERVIEW GUIDE

NIST Special Publication
NIST SP 1299
<https://doi.org/10.6028/NIST.SP.1299>
February 2024

NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide

NIST Special Publication
NIST SP 1299
February 2024

NIST Cybersecurity Framework 2.0: Quick-Start Guide for Creating and Using Organizational Profiles

NIST Special Publication
NIST SP 1299
February 2024

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

[View Quick Start Guide](#)

The below targeted guides will help you with specific topics.

- Quick Start | Small Business**
Resources specifically tailored to small businesses with modest or no cybersecurity plans currently in place.
[View Quick Start Guide](#)
- Quick Start | 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.
[View Quick Start Guide](#)
- Quick Start | Enterprise Risk Management**
How ERM practitioners can utilize the outcomes provided in the CSF 2.0 to improve organizational cybersecurity risk management.
[View Quick Start Guide](#)

The NIST Cybersecurity Framework (CSF) 2.0

National Institute of Standards and Technology
This publication is available free of charge from: <https://doi.org/10.6028/NIST.CSWP.29>
February 26, 2024

COMPUTER SECURITY RESOURCE CENTER

Cybersecurity and Privacy Reference Tool CPRT

Information Technology Laboratory

Projects: **CYBERSECURITY AND PRIVACY REFERENCE TOOL**

Search: [CSRC MENU](#)

Cybersecurity Framework 2.0 Draft, Version 2.0

Search:

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.
[Comparison Reports](#)

Download Informative Reference in the Core
Directly download all the Informative References for CSF 2.0
[Download \(zip\)](#) [Download \(json\)](#)

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 risks that may impede that mission.

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

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.

Learn About Our Global Impact: www.nist.gov/cyberframework

What is Next?



We hope that the CSF 2.0 suite of documents and tools will make a difference in managing and reducing cybersecurity risks.

NIST continues to encourage candid, constructive discussions and other engagements about organizations' experiences with the CSF .

Remember, cybersecurity risk management is always a journey – and the CSF 2.0 is a navigational guide that can help make that journey more successful.

See NIST's Suite of CSF 2.0 Resources: www.nist.gov/cyberframework

STAY IN TOUCH

CONTACT US



nist.gov/
cyberframework



@NISTcyber

Email us: cyberframework@nist.gov