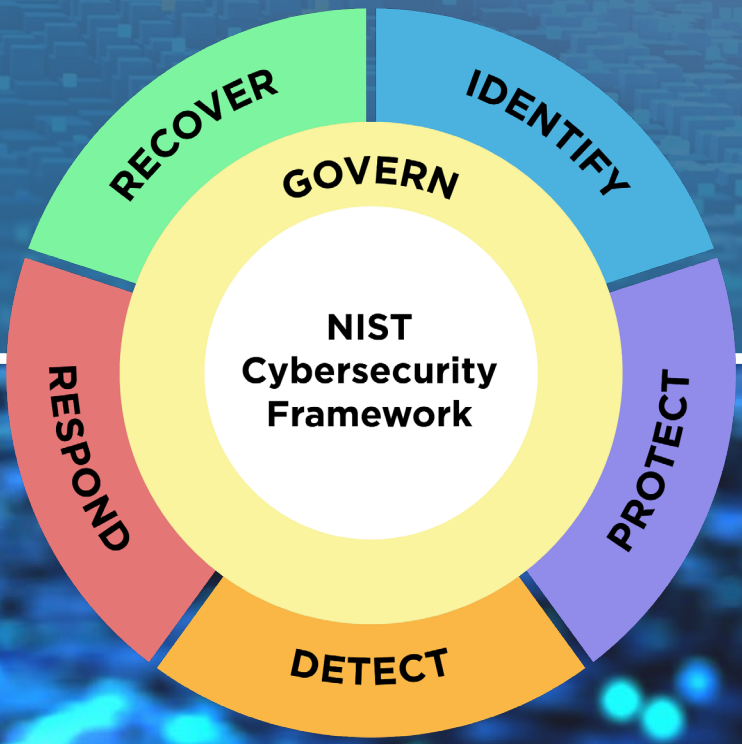
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

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 CSF 2.0:
RESOURCE & OVERVIEW GUIDE

WHAT IS THE CSF 2.0…AND POPULAR WAYS TO USE IT?

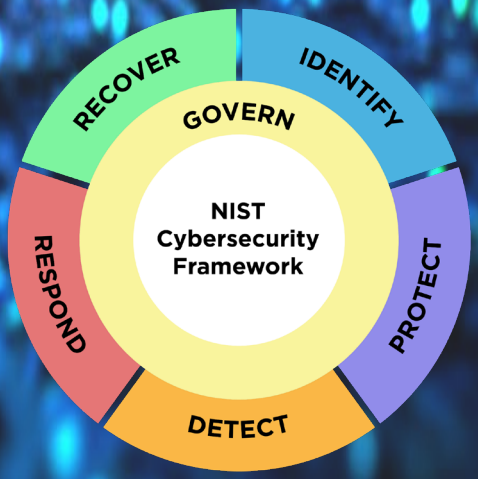
The NIST Cybersecurity Framework (CSF) 2.0 can help organizations manage and reduce their cybersecurity risks as they start or improve their cybersecurity program. The CSF outlines specific outcomes that organizations can achieve to address risk. Other NIST resources help explain specific actions that can be taken to achieve each outcome. *This guide is a supplement to the NIST CSF and is not intended to replace it.*

The CSF 2.0, along with NIST's supplementary resources, can be used by organizations to understand, assess, prioritize, and communicate cybersecurity risks; it is particularly useful for fostering internal and external communication across teams — as well as integrating with broader risk management strategies.

The CSF 2.0 is organized by six Functions — **Govern, Identify, Protect, Detect, Respond,** and **Recover.** Together, these Functions provide a comprehensive view for managing cybersecurity risk. This *Resource & Overview Guide* offers details about each Function to serve as potential starting points.

The CSF 2.0 is comprised of:

- **CSF Core** - A taxonomy of high-level cybersecurity outcomes that can help any organization manage its cybersecurity risks.
- **CSF Organizational Profiles** - A mechanism for describing an organization's current and/or target cybersecurity posture in terms of the CSF Core's outcomes.
- **CSF Tiers** - Can be applied to CSF Organizational Profiles to characterize the rigor of an organization's cybersecurity risk governance and management practices.



NIST CSF 2.0:
RESOURCE & OVERVIEW GUIDE

EXPLORE MORE CSF 2.0 RESOURCES

Informative References	**View and create mappings between CSF 2.0 and other documents.** Do you want to submit your mappings to NIST documents and have them displayed on our site? Please follow the link to the left or email olir@nist.gov if you have any questions.
Cybersecurity & Privacy Reference Tool (CPRT)	**Browse and download the CSF 2.0 Core & mapped content**. CPRT provides a centralized, standardized, and modernized mechanism for managing reference datasets (and offers a consistent format for accessing reference data from various NIST cybersecurity and privacy standards, guidelines, and frameworks).
Implementation Examples	View and download notional examples of concise, action-oriented steps to help achieve the outcomes of the CSF 2.0 Subcategories in addition to the guidance provided in the Informative References.
CSF 2.0 Reference Tool	Access human and machine-readable versions of the Core (in JSON and Excel). You can also view and export portions of the Core using key search terms.

Additional Resources Include:

Community Profiles and Profile templates (help organizations put the CSF into practice)

Search tools (simplify and streamline as you look for specific information)

Concept papers (learn more about various CSF topics)

FAQs (see what others are asking and get answers to top questions)

Explore the suite of NIST's CSF 2.0 Resource Repository

NIST CSF 2.0:
RESOURCE & OVERVIEW GUIDE

NAVIGATING NIST's CSF 2.0 QUICK START GUIDES (QSG)

QSG Type	Description	Explore
Small Business (SMB)	Provides SMBs, specifically those who have modest or no cybersecurity plans in place, with considerations to kick-start their cybersecurity risk management strategy.	See the QSG
Creating and Using Organizational Profiles	Provides all organizations with considerations for creating and using Current and/or Target Profiles to implement the CSF 2.0.	See the QSG
Using the CSF Tiers	Explains how any organization can apply the CSF Tiers to Organizational Profiles to characterize the rigor of its cybersecurity risk governance and management practices.	See the QSG
Draft Cybersecurity Supply Chain Risk Management (C-SCRM)	Helps all organizations to become smart acquirers and suppliers of technology products and services by improving their C-SCRM processes.	See the QSG
Draft Enterprise Risk Management (ERM) Practitioners	Details how Enterprise Risk Management practitioners can utilize the outcomes provided in CSF 2.0 to improve organizational cybersecurity risk management.	See the QSG

…and more to follow in the future.

See the current online QSG repository

NIST CSF 2.0: RESOURCE & OVERVIEW GUIDE

GOVERN

The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.

Understand and assess specific cybersecurity needs. Determine your organization's unique risks and needs. Discuss the current and predicted risk environment and the amount of risk your organization is willing to accept. Seek input and ideas from across the organization. Understand what has worked or not worked well in the past and discuss it openly.

Develop a tailored cybersecurity risk strategy. This should be based on your organization's specific cybersecurity objectives, the risk environment, and lessons learned from the past — and from others. Manage, update, and discuss the strategy at regular intervals. Roles and responsibilities should be clear.

Establish defined risk management policies. Policies should be approved by management and should be organization-wide, repeatable, and recurring, and should align with the current cybersecurity threat environment, risks (which will change over time), and mission objectives. Embed policies in company culture to help drive and inspire the ability to make informed decisions. Account for legal, regulatory, and contractual obligations.

Develop and communicate organizational cybersecurity practices. These must be straightforward and communicated regularly. They should reflect the application of risk management to changes in mission or business requirements, threats, and overall technical landscape. Document practices and share them with room for feedback and the agility to change course.

Establish and monitor cybersecurity supply chain risk management. Establish strategy, policy, and roles and responsibilities — including for overseeing suppliers, customers, and partners. Incorporate requirements into contracts. Involve partners and suppliers in planning, response, and recovery.

Implement continuous oversight and checkpoints. Analyze risks at regular intervals and monitor them continuously (just as you would with financial risks).

IDENTIFY

The organization's current cybersecurity risks are understood.

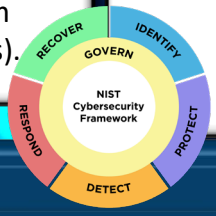
Identify critical business processes and assets. Consider which of your organization's activities absolutely must continue to be viable. For example, this could be maintaining a website to retrieve payments, securely protecting customer/patient information, or ensuring that the information critical to your organization remains accessible and accurate.

Maintain inventories of hardware, software, services, and systems. Know what computers and software your organization uses — including services provided by suppliers — because these are frequently the entry points of malicious actors. This inventory could be as simple as a spreadsheet. Consider including owned, leased, and employees' personal devices and apps.

Document information flows. Consider what type of information your organization collects and uses (and where the data are located and how they are used), especially when contracts and external partners are involved.

Identify threats, vulnerabilities, and risk to assets. Informed by knowledge of internal and external threats, risks should be identified, assessed, and documented. Examples of ways to document them include risk registers – repositories of risk information, including data about risks over time. Ensure risk responses are identified, prioritized, and executed, and that results are monitored.

Lessons learned are used to identify improvements. When conducting day-to-day business operations, it is important to identify ways to further refine or enhance performance, including opportunities to better manage and reduce cybersecurity risks. This requires purposeful effort by your organization at all levels. If there is an incident, assess what happened. Prepare an after-action report that documents the incident, the response, recovery actions taken, and lessons learned.



NIST CSF 2.0: RESOURCE & OVERVIEW GUIDE

PROTECT

Safeguards to manage the organization's cybersecurity risks are used.

Manage access. Create unique accounts for employees and ensure users only have access to necessary resources. Authenticate users before they are granted access to information, computers, and applications. Manage and track physical access to facilities/devices.

Train users. Regularly train employees to ensure they are aware of cybersecurity policies and procedures and that they have the knowledge and skills to perform general and specific tasks; explain how to recognize common attacks and report suspicious activity. Certain roles may require extra training.

Protect and monitor your devices. Consider using endpoint security products. Apply uniform configurations to devices and control changes to device configurations. Disable services or features that don't support mission functions. Configure systems and services to generate log records. Ensure devices are disposed of securely.

Protect sensitive data. Ensure sensitive stored or transmitted data are protected by encryption. Consider utilizing integrity checking so only approved changes are made to data. Securely delete and/or destroy data when no longer needed or required.

Manage and maintain software. Regularly update operating systems and applications; enable automatic updates. Replace end-of-life software with supported versions. Consider using software tools to scan devices for additional vulnerabilities and remediate them.

Conduct regular backups. Back up data at agreed-upon schedules or use built-in backup capabilities; software and cloud solutions can automate this process. Keep at least one frequently backed-up set of data offline to protect it against ransomware. Test to ensure that backed-up data can be successfully restored to systems.

DETECT

Possible cybersecurity attacks and compromises are found and analyzed.

Monitor networks, systems, and facilities continuously to find potentially adverse events. Develop and test processes and procedures for detecting indicators of a cybersecurity incident on the network and in the physical environment. Collect log information from multiple organizational sources to assist in detecting unauthorized activity.

Determine and analyze the estimated impact and scope of adverse events. If a cybersecurity event is detected, your organization should work quickly and thoroughly to understand the impact of the incident. Understanding details regarding any cybersecurity incidents will help inform the response.

Provide information on adverse events to authorized staff and tools. When adverse events are detected, provide information about the event internally to authorized personnel to ensure appropriate incident response actions are taken.

NIST CSF 2.0: RESOURCE & OVERVIEW GUIDE

RESPOND

Actions regarding a detected cybersecurity incident are taken.

Execute an incident response plan once an incident is declared, in coordination with relevant third parties. To properly execute an incident response plan, ensure everyone knows their responsibilities; this includes understanding any requirements (e.g., regulatory, legal reporting, and information sharing).

Categorize and prioritize incidents and escalate or elevate as needed. Analyze what has been taking place, determine the root cause of the incident, and prioritize which incidents require attention first from your organization. Communicate this prioritization to your team and ensure everyone understands who information should be communicated to regarding a prioritized incident when it occurs.

Collect incident data and preserve its integrity and provenance. Collecting information in a safe manner will help in your organization's response to an incident. Ensure that data are still secure after the incident to maintain your organization's reputation and trust from stakeholders. Storing this information in a safe manner can also help inform updated and future response plans to be even more effective.

Notify internal and external stakeholders of any incidents and share incident information with them — following policies set by your organization. Securely share information consistent with response plans and information-sharing agreements. Notify business partners and customers of incidents in accordance with contractual requirements.

Contain and eradicate incidents. Executing a developed and tested response plan will help your organization contain the effects of an incident and eradicate it. Meaningful coordination and communication with stakeholders can result in a more effective response and mitigation of the incident.

RECOVER

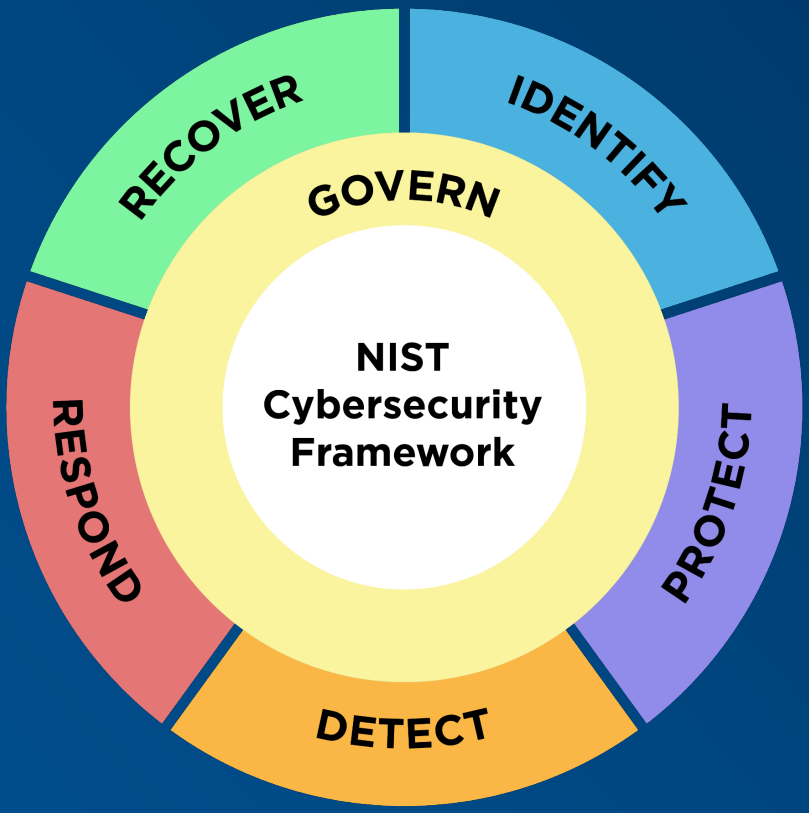
Assets and operations affected by a cybersecurity incident are restored.

Understand roles and responsibilities. Understand who, within and outside your business, has recovery responsibilities. Know who has access and authority to make decisions to carry out your response efforts on behalf of the business.

Execute your recovery plan. Ensure operational availability of affected systems and services; and prioritize and perform recovery tasks.

Double-check your work. It is important to ensure the integrity of backups and other recovery assets before using them to resume regular business operations.

Communicate with internal and external stakeholders. Carefully account for what, how, and when information will be shared with various stakeholders so that all interested parties receive the information they need, but no inappropriate information is shared. Communicate to your staff any lessons learned and revisions to processes, procedures, and technologies (following policies already set by the organization). This is a good time to train, or retrain, staff on cybersecurity best practices.



U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology