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

NIST Cybersecurity Framework 2.0: Quick-Start Guide for Using the CSF Tiers

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

NIST Special Publication
NIST SP 1302 ipd (Initial Public Draft)
The public comment period for this draft ends May 3, 2024.
Please send your comments to cyberframework@nist.gov.
https://doi.org/10.6028/NIST.SP.1302.ipd
February 2024

NIST CSF 2.0: USING THE CSF TIERS

A QUICK START GUIDE

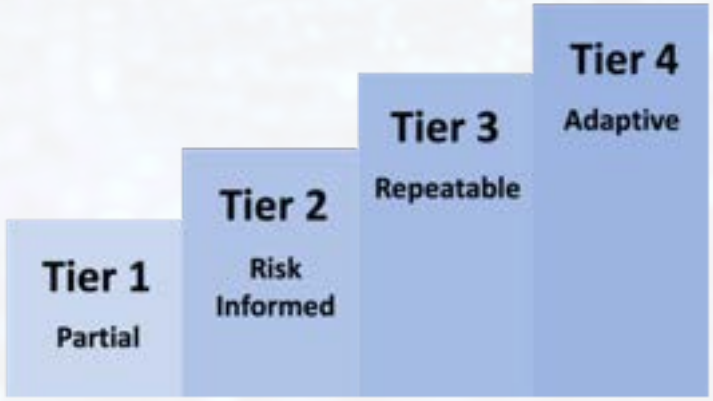
CSF Tiers

CSF Tiers can be applied to CSF Organizational Profiles to characterize the rigor of an organization's cybersecurity risk governance and management outcomes. This can help provide context on how an organization views cybersecurity risks and the processes in place to manage those risks. The Tiers can also be valuable when reviewing processes and practices to determine needed improvements and monitor progress made through those improvements.

Appendix B of the CSF contains a notional illustration of the CSF Tiers. In that illustration, each Tier has separate descriptions for Cybersecurity Risk Governance (corresponding to the Govern Function) and Cybersecurity Risk Management (for the other five CSF Functions: Identity, Protect, Detect, Respond, and Recover).

The Tiers capture an organization's outcomes over a range: Partial (Tier 1), Risk Informed (Tier 2), Repeatable (Tier 3), and Adaptive (Tier 4). They reflect a progression from informal, ad hoc responses to approaches that are agile, risk-informed, and continuously improving.

An organization wanting to use the CSF Tiers can reuse the notional descriptions from Appendix B of the CSF, or they can customize those descriptions, create new ones, or use a set of descriptions they already have in place.



Selecting Tiers

Selecting the CSF Tiers that your organization should be meeting in its cybersecurity risk governance and management activities is generally performed by organization leadership.

Here are tips for selecting Tiers:

- Selecting Tiers overall or at the Function or Category level will provide a better sense of the organization's current cybersecurity risk management practices than selecting Tiers at the Subcategory level.
- You can use one of the two Tier components (governance or management descriptions) if you want to focus on a subset of the CSF Functions. For example, if your scope is governance only, you can omit the Cybersecurity Risk Management descriptions.
- When selecting Tiers, consider the following aspects of the organization:
    - current risk management practices
    - threat environment
    - legal and regulatory requirements
    - information sharing practices
    - business and mission objectives
    - supply chain requirements
    - organizational constraints, including resources
- Ensure that the Tiers being selected help to meet organizational goals, are feasible to implement, and reduce cybersecurity risks to critical assets and resources to levels that are acceptable to the organization.
- Progression to higher Tiers is encouraged when needed to address risks or mandates.

NIST CSF 2.0: USING THE CSF TIERS

A QUICK START GUIDE

APPLYING TIERS TO PROFILES

Applying Tiers to Profiles

Once your organization's Tier selections have been made, you can use them to help inform your Current and Target Profiles.

For example, if leadership has determined that your organization should be at Tier 2 (Risk Informed) for the Identify and Protect Functions, then your Current Profile would reflect how well the Tier 2 Cybersecurity Risk Management characteristics are currently being achieved for each CSF Category within those two Functions. Similarly, the Target Profile would reflect any improvements to Identity and Protect outcomes needed to fully achieve the Tier 2 description. The table excerpt below shows the relevant part of the Tier 2 description.

Tiers should be used to **guide and inform** an organization's cybersecurity risk governance and management methodologies rather than take their place.

Tier	Cybersecurity Risk Governance	Cybersecurity Risk Management
Tier 1: Partial	…	…
Tier 2: Risk Informed	…	There is an awareness of cybersecurity risks at the organizational level, but an organization-wide approach to managing cybersecurity risks has not been established. Consideration of cybersecurity in organizational objectives and programs may occur at some but not all levels of the organization. Cyber risk assessment of organizational and external assets occurs but is not typically repeatable or reoccurring. Cybersecurity information is shared within the organization on an informal basis. The organization is aware of the cybersecurity risks associated with its suppliers and the products and services it acquires and uses, but does not act consistently or formally in response to those risks.
Tier 3: Repeatable	…	…
Tier 4: Adaptive	…	…

Additional Resources

- *Quick-Start Guide for Creating and Using Organizational Profiles* (includes taking CSF Tiers into account in Current and Target Profiles)
- Organizational Profile notional template
- *A Guide to Creating CSF 2.0 Community Profiles* (includes using CSF Tiers to inform the development of Community Profiles)