CSF 2.0 2024 UPDATE

The Cybersecurity Framework (CSF) 2.0 is designed to help organizations of all sizes and sectors
— including industry, government, academia, and nonprofit — to manage and reduce their
cybersecurity risks. It is useful regardless of the maturity level and technical sophistication of an
organization's cybersecurity programs. Nevertheless, the CSF does not embrace a one-size-fits-
all approach. Each organization has both common and unique risks, as well as varying risk
appetites and tolerances, specific missions, and objectives to achieve those missions. By
necessity, the way organizations implement the CSF will vary.

Cybersecurity Framework (CSF) Overview

This document is version 2.0 of the NIST Cybersecurity Framework (Framework or CSF). It
includes the following components:

• CSF Core, the nucleus of the CSF, which is a taxonomy of high-level cybersecurity
outcomes that can help any organization manage its cybersecurity risks. The CSF Core
components are a hierarchy of Functions, Categories, and Subcategories that detail each
outcome. These outcomes can be understood by a broad audience, including executives, managers, and practitioners, regardless of their cybersecurity expertise.
Because the outcomes are sector-, country-, and technology-neutral, they provide an
organization with the flexibility needed to address its unique risks, technologies, and

mission considerations.

• CSF Organizational Profiles, which are a mechanism for describing an organization’s
current and/or target cybersecurity posture in terms of the CSF Core’s outcomes.

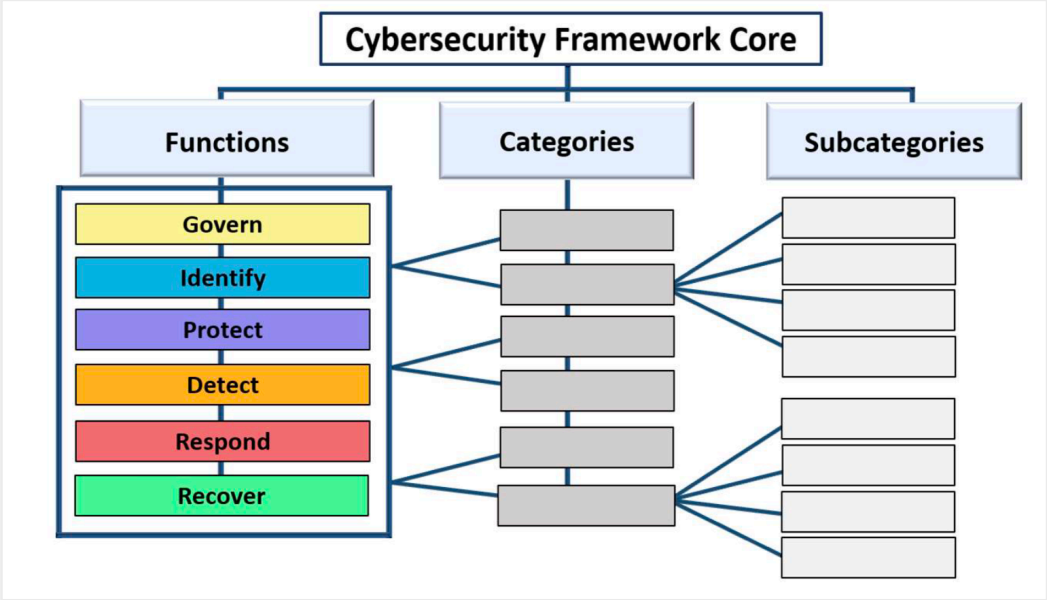
• CSF Tiers, which can be applied to CSF Organizational Profiles to characterize the rigor of
an organization’s cybersecurity risk governance and management practices. Tiers can
also provide context for how an organization views cybersecurity risks and the processes
in place to manage those risks.

An organization can use the CSF Core, Profiles, and Tiers with the supplementary resources to
understand, assess, prioritize, and communicate cybersecurity risks.

• Understand and Assess: Describe the current or target cybersecurity posture of part or
all of an organization, determine gaps, and assess progress toward addressing those
gaps.

• Prioritize: Identify, organize, and prioritize actions for managing cybersecurity risks that
align with the organization’s mission, legal and regulatory requirements, and risk
management and governance expectations.

• Communicate: Provide a common language for communicating inside and outside the
organization about cybersecurity risks, capabilities, needs, and expectations.



GOVERN (GV) — The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.

IDENTIFY (ID) — The organization's current cybersecurity risks are understood. Understanding the organization's assets (e.g., data, hardware, software, systems,
facilities, services, people), suppliers, and related cybersecurity risks enables an
organization to prioritize its efforts consistent with its risk management strategy and the
mission needs identified under GOVERN.

PROTECT (PR) — Safeguards to manage the organization's cybersecurity risks are used.

DETECT (DE) — Possible cybersecurity attacks and compromises are found and analyzed.

RESPOND (RS) — Actions regarding a detected cybersecurity incident are taken. RESPOND
supports the ability to contain the effects of cybersecurity incidents.

RECOVER (RC) — Assets and operations affected by a cybersecurity incident are restored.

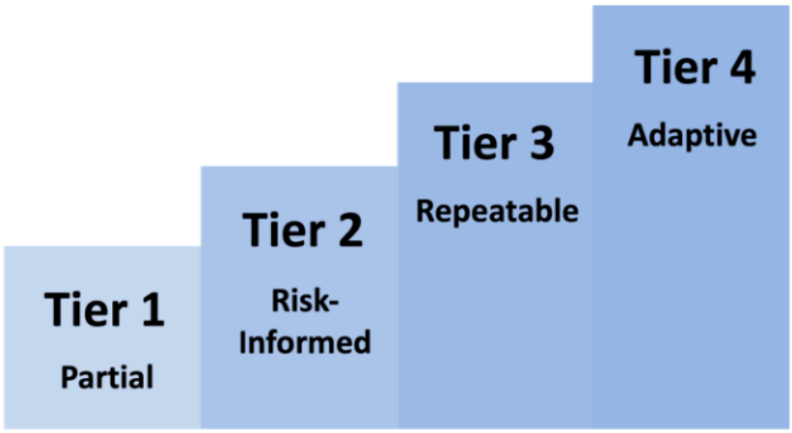


Fig. 4. CSF Tiers for cybersecurity risk governance and management

Fig. 5. Using the CSF to improve risk management communication

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

REFER EXCEL SHEET