The NIST Cybersecurity Framework (CSF) 2.0

National Institute of Standards and Technology
https://doi.org/10.6028/NIST.CSWP.29
February 26, 2024

“Ideally, the CSF will be used to address cybersecurity risks alongside other risks of the enterprise, including those that are financial, privacy, supply chain, reputational, technological, or physical in nature. ” -p5

“The CSF describes desired outcomes [...] Outcomes are mapped directly to a list of potential security controls for immediate consideration to mitigate cybersecurity risks.” -p5

CSF Core

About CSF Core

- taxonomy of high-level cybersecurity outcomes that can help any organization manage its cybersecurity risks
- components detail each outcome
  - Functions
  - Categories
  - Subcategories

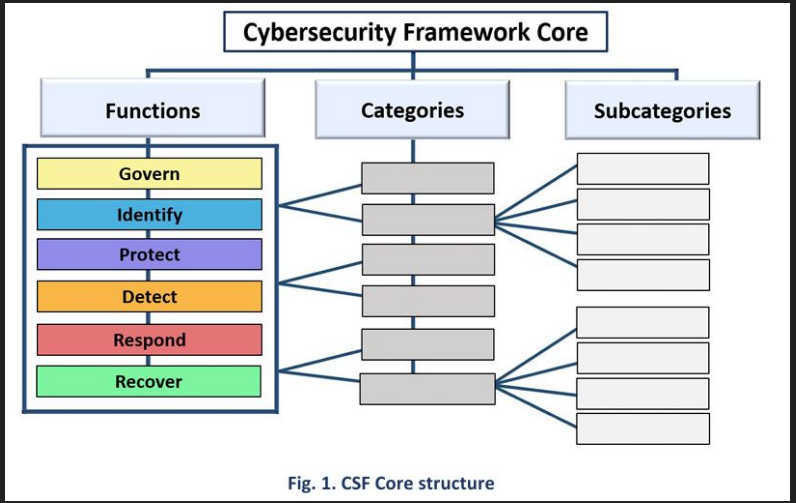

Fig. 1. CSF Core structure

Functions

Govern

- CyberSec risk management strategy, -expectations, and -policy are established, communicated, and monitored
- Describes how cyberSec fits with organizational risk strategy to non-technical stakeholders
- Informs how the organization implement the other 5 strategies in the core
- Provides outcomes informing roadmap to achieve & prioritize outcomes of the other functions
- addresses
  - Org. context
  - Strategy
  - Supply chain risk management
  - roles, responsibilities & authorities
  - policy

Identify

- Understand current cyberSec risks
- Understand assets, suppliers, & similar risks
- Aids prioritization
- Identify possible improvements in policies, plans, processes, procedures, and practices

Protect

- Supports ability to secure assets to lower the likelihood and impact cyber events
- increase likelihood and impact of taking advantage of opportunities
- Addresses
  - identity management, authentication, and access control
  - awareness and training
  - data security
  - platform security (i.e., securing the hardware, software, and services of physical and virtual platforms)
  - resilience of technology infrastructure

Functions

Detect

- Possible cybersecurity attacks and compromises are found and analyzed
- timely discovery and analysis of anomalies, indicators of compromise, and other potentially adverse events
- Addresses
  - successful incident response
  - recovery activities

Respond

- Actions regarding a detected incident are taken
- ability to contain the effects
- Outcomes
  - incident management
  - -analysis
  - -mitigation
  - -reporting
  - communication

Recover

- Assets and operations affected by an incident are restored
- timely restoration of operations
- reduce the effects of incidents
- enable appropriate communication during recovery efforts

Functions

- Functions should be addressed concurrently
- actions that support RESPOND and RECOVER should be ready at all times
- Each Function is divided into Categories, which are related cybersecurity outcomes that collectively comprise the Function
- Subcategories further divide each Category (not exhaustive) into more specific outcomes of technical and management activities

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

See subcategories on link:
The NIST Cybersecurity Framework (CSF) 2.0

Pages 21-28

CSF Organizational Profiles

Framework Profile

- For describing an organization’s current and/or target cybersecurity posture in terms of the CSF Core’s outcomes
- Roadmap detailing how to move from current to target

Current- & Target Profile

- A *Current Profile* specifies the Core outcomes that an organization is currently achieving (or attempting to achieve) and characterizes how or to what extent each outcome is being achieved -p11

- A *Target Profile* specifies the desired outcomes that an organization has selected and prioritized for achieving its cybersecurity risk management objectives. A Target Profile considers anticipated changes to the organization’s cybersecurity posture, such as new requirements, new technology adoption, and threat intelligence trends. -p11

Steps for creating a CSF Organizational Profile

1. Document the high-level facts and assumptions on which the Profile will be based to define scope. An org. can have multiple profiles each with a different scope
2. Like policies, risk management priorities and resources, enterprise risk profiles, business impact analysis registers, cyberSec requirements & standards, practices and tools (e.g., procedures and safeguards), and work roles
3. Determine types of info the Profile should include for CSF outcomes, & document. Consider risk implications of the Current Profile to inform Target Profile planning & prioritization
4. Gap analysis to identify and analyze differences between the C & T Profiles. Develop a prioritized action plan (e.g., risk register, risk detail report, Plan of Action & Milestones) to address gaps
5. Follow the action plan to address the gaps and move the organization toward the Target Profile

Fig. 3. Steps for creating and using a CSF Organizational Profile

CSF Tiers

About CSF Tiers

- applied to CSF Organizational Profiles to characterize the rigor of an organization’s cybersecurity risk

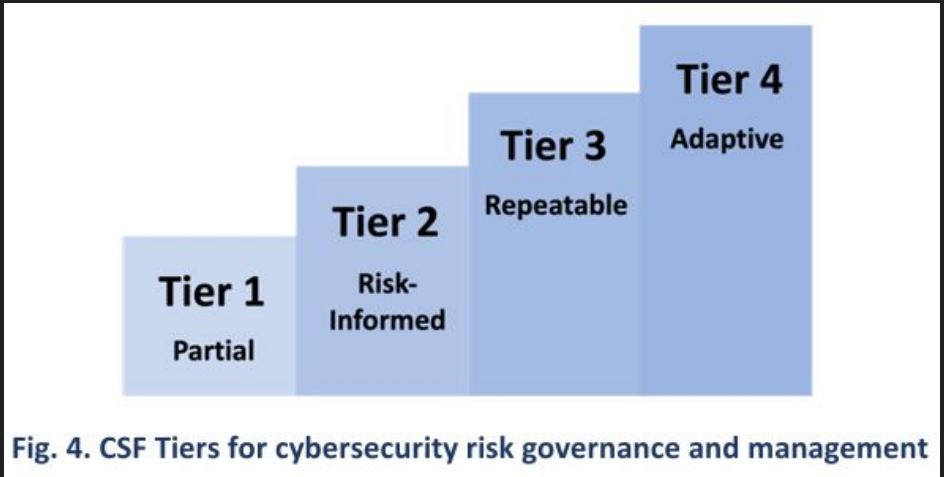

Fig. 4. CSF Tiers for cybersecurity risk governance and management