C-SCRM in Draft CSF 2.0

September 2023

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

Cybersecurity Framework Attributes

The NIST Cybersecurity Framework (CSF) helps organizations reduce their cybersecurity risks and is widely recognized as foundational to securing organizations & technology.

- Cybersecurity outcomes – the "what", not "how" or "who"
- Review priorities and gaps; align legal/regulatory requirements and organizational and risk management priorities
- Common and accessible language for communication on cybersecurity posture
- Based on and mapped to international standards and resources
- Adaptable to many technologies, lifecycle phases, sectors and uses
- Guided by many perspectives – private sector, academia, public sector

Governmental Policies on CSF

Adapted in several countries and regions

- United States (federal and state)
  - **The White House National Cybersecurity Strategy (March 2023): https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf**
    - "Regulations should be performance-based, leverage existing cybersecurity frameworks, voluntary consensus standards, and guidance – including the Cybersecurity and Infrastructure Security Agency (CISA)'s Cybersecurity Performance Goals and the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity – …"
- Italy
- Ireland
- Israel
- Japan
- Uruguay
- Australia and more

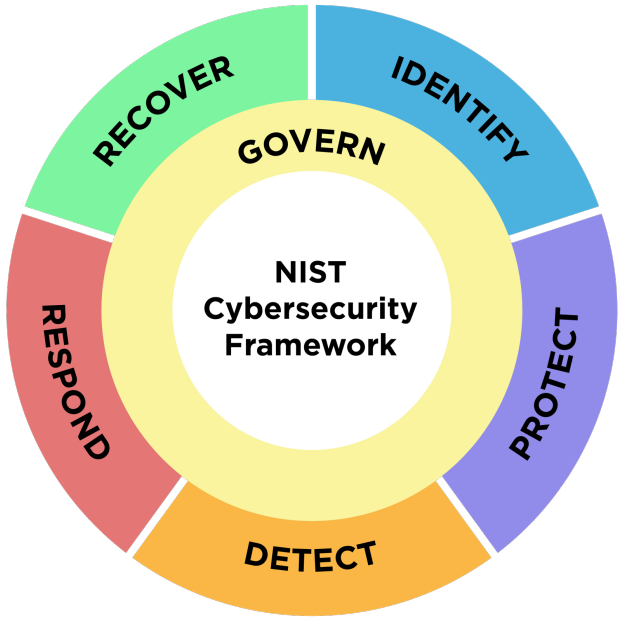
Examples highlighted on the NIST International Cybersecurity and Privacy Resource Site: https://www.nist.gov/cybersecurity/international-cybersecurity-and-privacy-resources

CSF Update | Journey to CSF 2.0

- **NIST is updating the CSF** to address the evolving cybersecurity risk and standards landscape and make it easier for organizations to address risks. NIST is actively relying on and seeking diverse stakeholder feedback in the update process.

Ways to engage: www.nist.gov/cyberframework

JUST RELEASED | Draft CSF 2.0



This newly released draft represents a major update to the CSF, which was first released in 2014.

Key Updates:

- Reflects changes in the cybersecurity landscape (risks, technologies, standard changes)
- Makes it easier to put the CSF into practice for all organizations through additional guidance on implementing the CSF
- An expanded scope beyond critical infrastructure.
- The addition of a sixth function, Govern.
- Additional coverage of supply chain security.

Comments on the Draft Core may be sent to cyberframework@nist.gov by November 4, 2023.

C-SCRM in Draft CSF 2.0 Short History

- Draft 1 Core: Conflation and Abstraction
- Draft 2 Core: Untangling Spaghetti
- Some Subcategories called out in the Prose are really only 1st Party in the Core

Governance Function: C-SCRM Category

GV.SC-01: A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders (formerly ID.SC-01)

GV.SC-02: Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally (formerly ID.AM-06)

GV.SC-03: Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes (formerly ID.SC-02

GV.SC-04: Suppliers are known and prioritized by criticality

GV.SC-05: Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties (formerly ID.SC-03)

Governance Function: C-SCRM Category

GV.SC-06: Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships

GV.SC-07: The risks posed by a supplier, their products and services, and other third parties are identified, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship (formerly ID.SC-02, ID.SC-04)

GV.SC-08: Relevant suppliers and other third parties are included in incident planning, response, and recovery activities (formerly ID.SC-05)

GV.SC-09: Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle

GV.SC-10: Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement

Multi Function/Category 3rd Party Only Examples

GV.OC-05: Outcomes, capabilities, and services that the organization depends on are determined and communicated (formerly ID.BE-01, ID.BE-04)

- Ex1: Create an inventory of the organization's dependencies on external resources (e.g., facilities, cloud-based hosting providers) and their relationships to organizational assets and business functions
- Ex2: Identify and document external dependencies that are potential points of failure for the organization's critical capabilities and services

ID.AM-04: Inventories of services provided by suppliers are maintained

- Ex1: Inventory all external services used by the organization, including third-party infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS) offerings; APIs; and other externally hosted application services
- Ex2: Update the inventory when a new external service is going to be utilized to ensure adequate cybersecurity risk management monitoring of the organization's use of that service

Multi Function/Category 3rd Party Only Examples

ID.RA-09: The authenticity and integrity of hardware and software are assessed prior to acquisition and use (formerly PR.DS-08)

- Ex1: Assess the authenticity and cybersecurity of critical technology products and services prior to acquisition and use

DE.CM-06: External service provider activities and services are monitored to find potentially adverse events (formerly DE.CM-06, DE.CM-07)

- Ex1: Monitor remote administration and maintenance activities that external providers perform on organizational systems
- Ex2: Monitor cloud-based services, internet service providers, and other service providers for deviations from expected behavior

Multi Function/Category 3rd Party Only Examples

RS.MA-01: The incident response plan is executed once an incident is declared in coordination with relevant third parties (formerly RS.RP-01, RS.CO-04)

- Ex1: Detection technologies automatically report confirmed incidents
- Ex2: Request incident response assistance from the organization's incident response outsourcer
- Ex3: Designate an incident lead for each incident

DE.CM-06: External service provider activities and services are monitored to find potentially adverse events (formerly DE.CM-06, DE.CM-07)

- Ex1: Monitor remote administration and maintenance activities that external providers perform on organizational systems
- Ex2: Monitor cloud-based services, internet service providers, and other service providers for deviations from expected behavior

1st Party and 3rd Party Conflation and Abstraction Examples

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

GV.RM-05: Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties

ID.RA-03: Internal and external threats to the organization are identified and recorded

PR.AT-02: Individuals in specialized roles are provided awareness and training so they possess the knowledge and skills to perform relevant tasks with security risks in mind (formerly PR.AT-02, PR.AT-03, PR.AT-04, PR.AT-05)

CSF Calls to Action

Ways in which the community can contribute to improvements to CSF 2.0 and associated resources.

- ❑ Share International Resources
- ❑ Provide Mappings
- ❑ Share Example Profiles
- ❑ Submit CSF Resources
- ❑ Share Success Stories
- ❑ Share Use of the CSF in Measuring and Assessing Cybersecurity

CSF 2.0 Next Steps

- **Public workshops and events**
  - **Save the Date:** Third and final CSF 2.0 Workshop → September 19-20 at the NIST NCCoE.
  - Find recordings of CSF Workshop #1 (August 2022) and #2 (February 2023) online.
- **Comment on drafts**
  - Provide comments on the Draft CSF 2.0 and the Discussion Draft by November 4, 2023 (all prior comments received can be found online).
- **Continuing to seek and develop CSF resources, success stories, and mappings to other frameworks and standards.**

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

STAY IN TOUCH

CONTACT US

NIST.gov

@NISTcyber