John Beltz
NIST PSCR

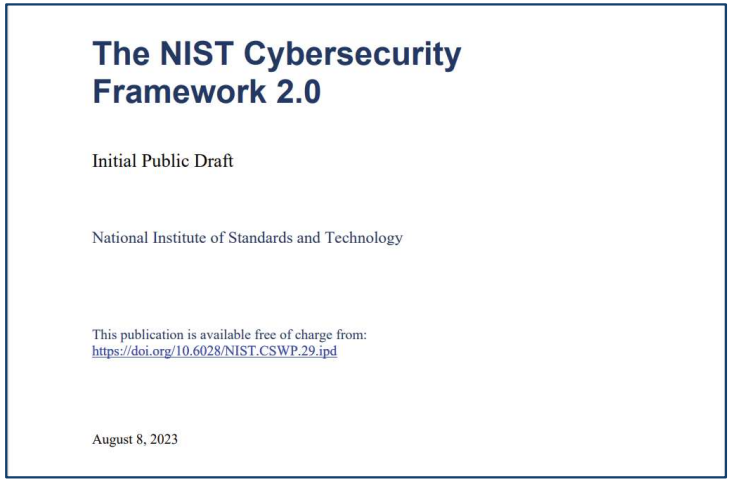
NIST PUBLIC SAFETY COMMUNICATIONS RESEARCH

UNCREWED AIRCRAFT SYSTEMS

Cybersecurity Framework (CSF) 2.0

John Beltz

NIST PSCR Cybersecurity Lead



The NIST Cybersecurity Framework 2.0

Initial Public Draft

National Institute of Standards and Technology

This publication is available free of charge from:
https://doi.org/10.6028/NIST.CSWP.29.ipd

August 8, 2023

- Document and online tools
- Guidelines, best practices, and standards
- Identification of security and privacy controls needed to manage cybersecurity risks
- Common language for understanding, managing, and expressing cybersecurity risk, both internally and externally
- Flexible for size, sector, maturity

**CSF Functions as a wheel because all Framework Functions relate to one another and govern applies to all function

Govern: Establish and monitor the organization's cybersecurity risk management strategy

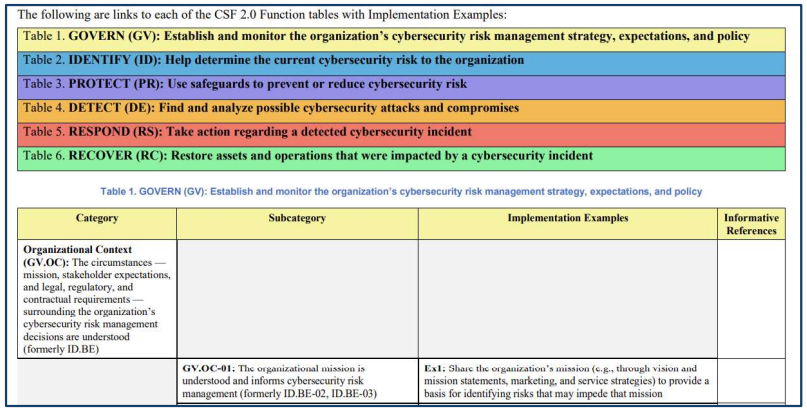
- **Identify:** What are we protecting?
- **Protect:** Safeguards to ensure delivery of services
- **Detect:** Identification of cybersecurity events
- **Respond:** Action regarding a detected incident
- **Recover:** Restoring capabilities or services

Additional Resources to Support Functions

Informative References are standards, guidelines, regulations, and other resources to help inform how an organization achieves the functions

- UAS Laws and regulations (FAA Regulations)
- NIST Artificial Intelligence Risk Management Framework (AI RMF 1.0)
- NIST SP 800-53 (5) Security and Privacy Controls for Information Systems and Organizations
- CJIS Security Policy
- Nist provides an Informative Reference Catalog

Implementation Examples provide notional examples of action-oriented steps to help achieve the desired outcomes in addition to the guidance provided by Informative References.



The following are links to each of the CSF 2.0 Function tables with Implementation Examples:

Table 1. **GOVERN (GV): Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy**

Table 2. **IDENTIFY (ID): Help determine the current cybersecurity risk to the organization**

Table 3. **PROTECT (PR): Use safeguards to prevent or reduce cybersecurity risk**

Table 4. **DETECT (DE): Find and analyze possible cybersecurity attacks and compromises**

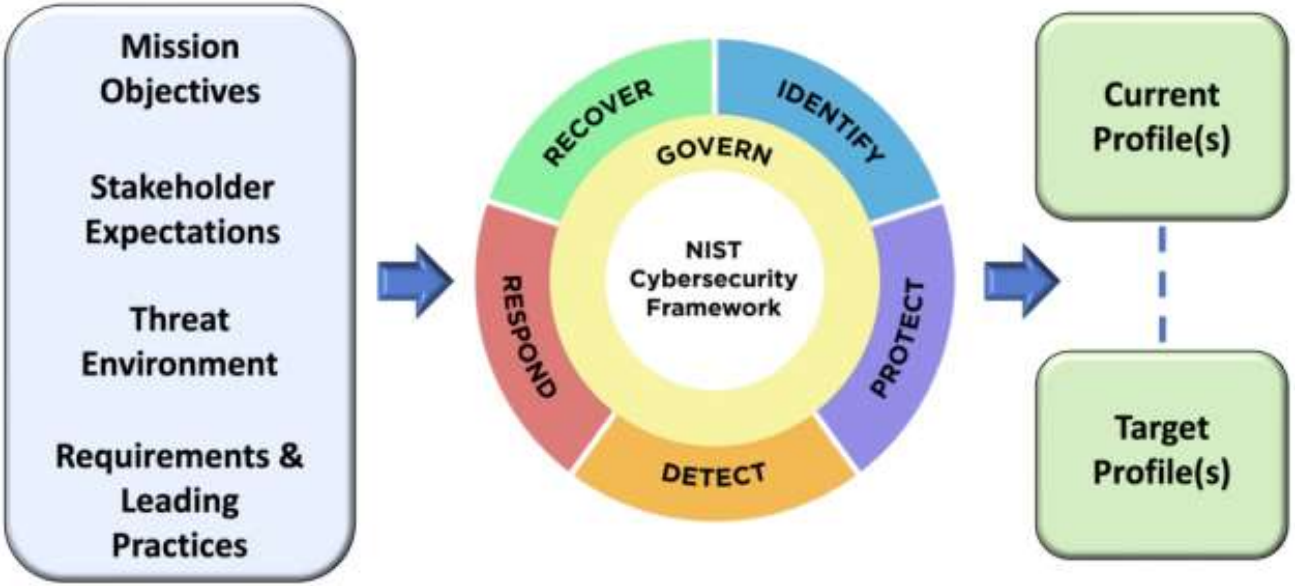
Table 5. **RESPOND (RS): Take action regarding a detected cybersecurity incident**

Table 6. **RECOVER (RC): Restore assets and operations that were impacted by a cybersecurity incident**

Table 1. GOVERN (GV): Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy

Category	Subcategory	Implementation Examples	Informative References
Organizational Context (GV.OC): The circumstances — mission, stakeholder expectations, and legal, regulatory, and contractual requirements — surrounding the organization's cybersecurity risk management decisions are understood (formerly ID.BE)			
	GV.OC-01: The organizational mission is understood and informs cybersecurity risk management (formerly ID.BE-02, ID.BE-03)	**Ex1:** Share the organization's mission (e.g., through vision and mission statements, marketing, and service strategies) to provide a basis for identifying risks that may impede that mission	

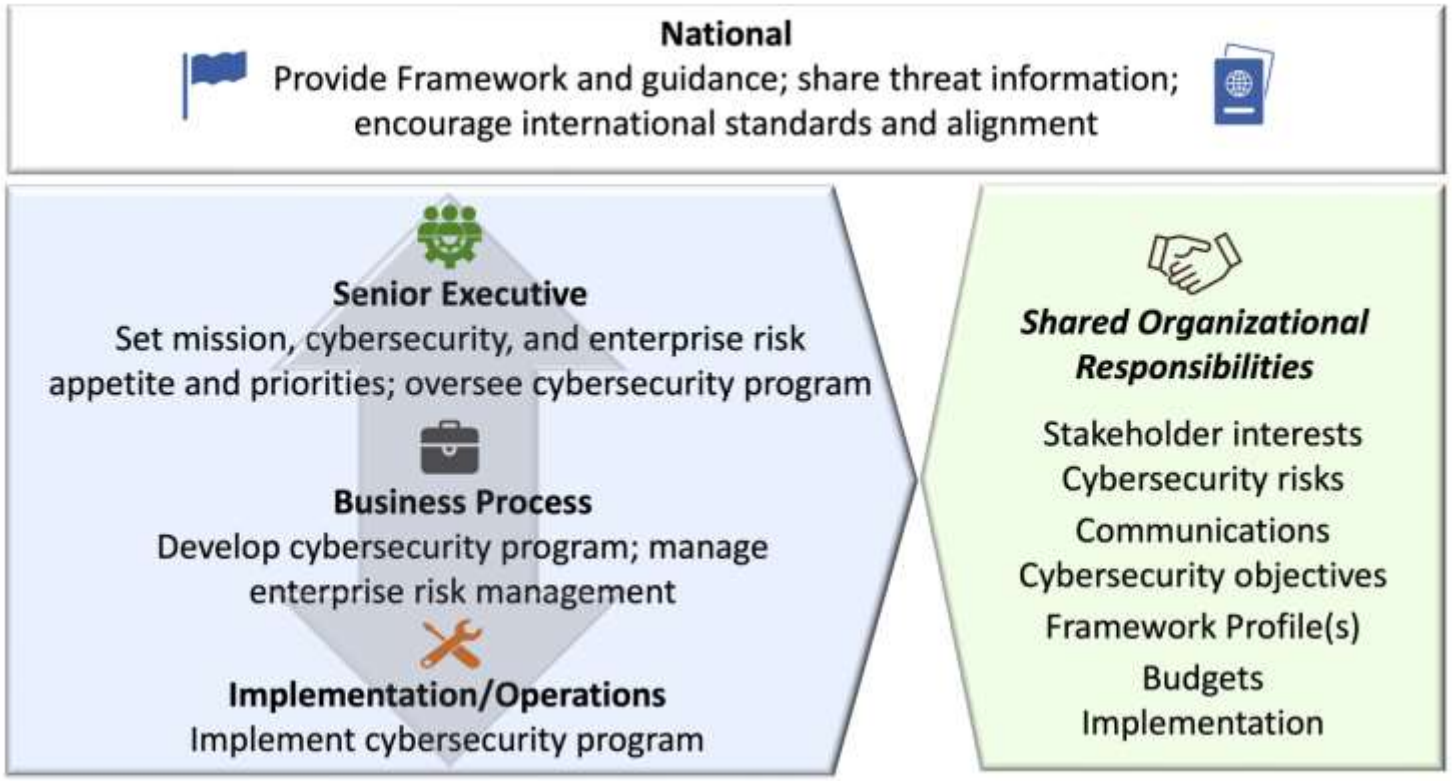
Current Profile to Target Profile



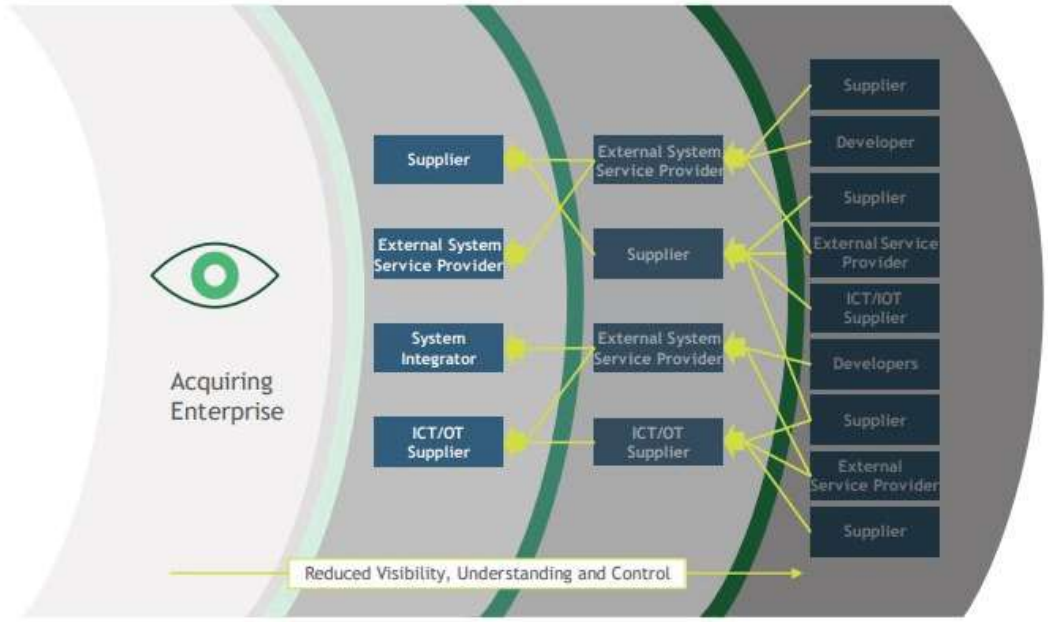
Framework Tiers

Determine the appropriate Tier to ensure the target profile meets the risk management strategy

Communication is Imperative



Managing Cybersecurity Risk in Supply Chains With the Framework



C-SCRM - Cybersecurity Supply Chain Risk Management

Integration with other Frameworks

- NIST Artificial Intelligence Risk Management Framework (AI RMF)
- Privacy Framework: NIST Privacy Framework
- Integrating Cybersecurity and Enterprise Risk Management
- Zero Trust Architecture
- NIST Cybersecurity for IoT Program

- AI is an application that requires securing as well as a tool to provide security
- AI can supplement and provide enhancement for security analyst
- Detect threats
- AI applications still require security and privacy controls