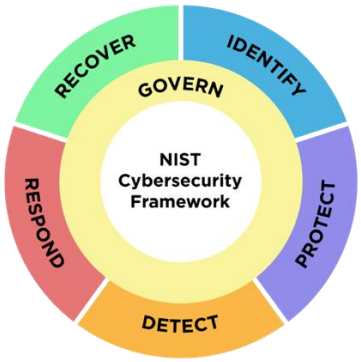
Discussion Draft: The NIST Cybersecurity Framework 2.0 Core with Implementation Examples

National Institute of Standards and Technology

Released August 8, 2023



Note to Reviewers

This is the discussion draft of Implementation Examples (Examples) for the NIST Cybersecurity Framework (CSF or Framework) 2.0. It complements and is based on the Core from the NIST CSF 2.0 Public Draft, also open for comment. NIST seeks input on:

- concrete improvements to the Examples;
- whether the Examples are written at an appropriate level of specificity and helpful for a diverse range of organizations;
- what other types of Examples would be most beneficial to Framework users;
- what existing sources of implementation guidance might be readily adopted as sources of Examples (such as the NICE Framework Tasks);
- how often Examples should be updated; and
- whether and how to accept Examples developed by the community.

Feedback on this draft may be submitted to cyberframework@nist.gov by Friday, November 4, 2023.

All relevant comments, including attachments and other supporting material, will be made publicly available on the NIST CSF 2.0 website. Personal, sensitive, confidential, or promotional business information should not be included. Comments with inappropriate language will not be considered.

CSF 2.0 Examples will be published and maintained *only* online on the NIST Cybersecurity Framework website, leveraging the NIST Cybersecurity and Privacy Reference Tool (CPRT). This will allow Examples and Informative References to be updated more frequently than the rest of the Core. In the coming weeks, NIST will release an initial version of this online tool for users to download and search the draft Core. Resource owners and authors who are interested in mapping their resources to the final CSF 2.0 to create Informative References should reach out to NIST.

Cherilyn Pascoe
NIST Cybersecurity Framework Program Lead
cyberframework@nist.gov

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

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

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	
	GV.OC-02: Internal and external stakeholders are determined, and their needs and expectations regarding cybersecurity risk management are understood	**Ex1:** Identify relevant internal stakeholders and their cybersecurity-related expectations (e.g., performance and risk expectations of officers, directors, and advisors; cultural expectations of employees) **Ex2:** Identify relevant external stakeholders and their cybersecurity-related expectations (e.g., privacy expectations of	

Category	Subcategory	Implementation Examples	Informative References
		customers, business expectations of partnerships, compliance expectations of regulators, ethics expectations of society)	
	GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed (formerly ID.GV-03)	**Ex1:** Determine a process to track and manage legal and regulatory requirements regarding protection of individuals' information (e.g., Health Insurance Portability and Accountability Act, California Consumer Privacy Act, General Data Protection Regulation) **Ex2:** Determine a process to track and manage contractual requirements for cybersecurity management of supplier, customer, and partner information **Ex3:** Align the organization's cybersecurity strategy with legal, regulatory, and contractual requirements	
	GV.OC-04: Critical objectives, capabilities, and services that stakeholders depend on or expect from the organization are determined and communicated (formerly ID.BE-04, ID.BE-05)	**Ex1:** Establish criteria for determining the criticality of capabilities and services as viewed by internal and external stakeholders **Ex2:** Determine (e.g., from a business impact analysis) assets and business operations that are vital to achieving mission objectives and the potential impact of a loss (or partial loss) of such operations **Ex3:** Establish and communicate resilience objectives (e.g., recovery time objectives) for delivering critical capabilities and services in various operating states (e.g., under attack, during recovery, normal operation)	
	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	
Risk Management Strategy (GV.RM): The organization's priorities, constraints, risk tolerance and appetite statements,			

Category	Subcategory	Implementation Examples	Informative References
and assumptions are established, communicated, and used to support operational risk decisions (formerly ID.RM)			
	GV.RM-01: Risk management objectives are established and agreed to by organizational stakeholders (formerly ID.RM-01)	**Ex1:** Update near-term and long-term cybersecurity risk management objectives as part of annual strategic planning and when major changes occur **Ex2:** Establish measurable objectives for cybersecurity risk management (e.g., manage the quality of user training, ensure adequate risk protection for industrial control systems) **Ex3:** Senior leaders agree about cybersecurity objectives and use them for measuring and managing risk and performance	
	GV.RM-02: Risk appetite and risk tolerance statements are determined, communicated, and maintained (formerly ID.RM-02, ID.RM-03)	**Ex1:** Determine and communicate risk appetite statements that convey expectations about the appropriate level of risk for the organization **Ex2:** Translate risk appetite statements into specific, measurable, and broadly understandable risk tolerance statements **Ex3:** Refine organizational objectives and risk appetite periodically based on known risk exposure and residual risk	
	GV.RM-03: Enterprise risk management processes include cybersecurity risk management activities and outcomes (formerly ID.GV-04)	**Ex1:** Aggregate and manage cybersecurity risks alongside other enterprise risks (e.g., compliance, financial, regulatory) **Ex2:** Include cybersecurity risk managers in enterprise risk management planning **Ex3:** Establish criteria for escalating cybersecurity risks within enterprise risk management	
	GV.RM-04: Strategic direction that describes appropriate risk response options is established and communicated	**Ex1:** Specify criteria for accepting and avoiding cybersecurity risk for various classifications of data **Ex2:** Determine whether to purchase cybersecurity insurance **Ex3:** Document conditions under which shared responsibility models are acceptable (e.g., outsourcing certain cybersecurity functions, having a third party perform financial transactions on behalf of the organization, using public cloud-based services)	

Category	Subcategory	Implementation Examples	Informative References
	GV.RM-05: Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties	**Ex1:** Determine how to update senior executives, directors, and management on the organization's cybersecurity posture at agreed-upon intervals **Ex2:** Identify how all departments across the organization — such as management, internal auditors, legal, acquisition, physical security, and HR — will communicate with each other about cybersecurity risks **Ex3:** Identify how third parties will communicate with the organization about cybersecurity risks	
	GV.RM-06: A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated	**Ex1:** Establish criteria for using a quantitative approach to cybersecurity risk analysis, and specify probability and exposure formulas **Ex2:** Create and use templates (e.g., a risk register) to document cybersecurity risk information (e.g., risk description, exposure, treatment, and ownership) **Ex3:** Establish criteria for risk prioritization at the appropriate levels within the enterprise **Ex4:** Use a consistent list of risk categories to support integrating, aggregating, and comparing cybersecurity risks	
	GV.RM-07: Strategic opportunities (i.e., positive risks) are identified and included in organizational cybersecurity risk discussions	**Ex1:** Define and communicate guidance and methods for identifying opportunities and including them in risk discussions (e.g., strengths, weaknesses, opportunities, and threats [SWOT] analysis) **Ex2:** Identify stretch goals and document them **Ex3:** Calculate, document, and prioritize positive risks alongside negative risks	
Cybersecurity Supply Chain Risk Management (GV.SC): Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by			