NIST Cybersecurity Framework 2.0
Initial Public Draft

NIST Cybersecurity Framework 2.0 Potential Uses

- Create and use Framework Profiles to understand, assess, and communicate the organization's current or target cybersecurity posture in terms of the Framework Core's cybersecurity outcomes, and prioritize outcomes for achieving the target cybersecurity posture
- Assess the organization's achievement of cybersecurity outcomes
- Characterize cybersecurity risk management outcomes with Framework Tiers
- Improve cybersecurity communication with internal and external stakeholders
- Manage cybersecurity risk throughout supply chains

NIST Cybersecurity Framework 2.0 Framework Components

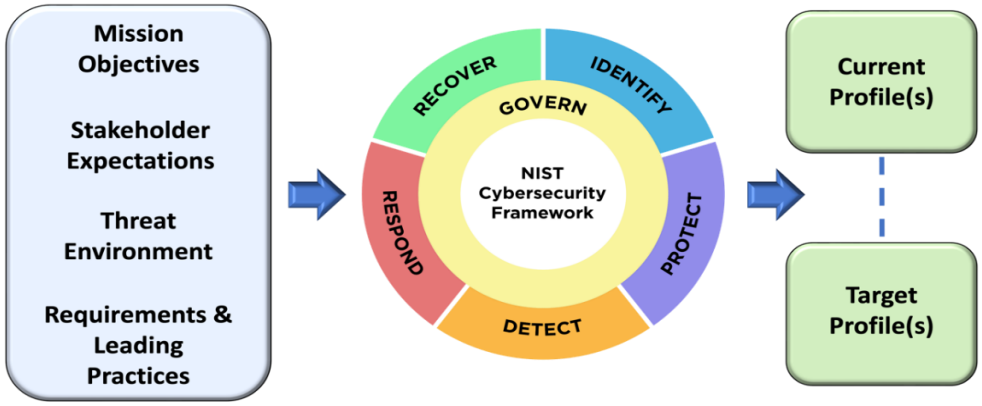
- Framework Core - a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors.
  - Consists of five concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover
  - Identifies underlying key Categories and Subcategories – which are discrete outcomes – for each Function
- Framework Implementation Tiers ("Tiers") - Describe the degree to which an organization's cybersecurity risk management practices exhibit the characteristics defined in the Framework (e.g., risk and threat aware, repeatable, and adaptive). The Tiers characterize an organization's practices over a range, from Partial (Tier 1) to Adaptive (Tier 4)
- Framework Profile ("Profile"): represents the outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories. The Profile can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario

NIST Cybersecurity Framework 2.0 Framework Profiles

Used to understand, assess, prioritize, and tailor the sector- and technology-neutral Core outcomes (i.e., Functions, Categories, and Subcategories) based on an organization's mission objectives, stakeholder expectations, threat environment, and requirements and leading practices

Types of Profiles:

- A *Current Profile* covers the Core's outcomes that an organization is currently achieving (or attempting to achieve) and characterizes how or to what extent each outcome is being achieved
- A *Target Profile* covers the desired outcomes that an organization has selected and prioritized from the Core for achieving its cybersecurity risk management objectives. A Target Profile takes into account anticipated changes to the organization's cybersecurity posture, such as new requirements, new technology adoption, and cybersecurity threat intelligence trends.



NIST Cybersecurity Framework 2.0 Framework Profiles – Ways to Use Them

- Organizations can create and use Profiles to utilize the full capabilities of the Framework (as discussed in Section 1). While organizations can use the Framework without Profiles, they provide the opportunity to develop a prioritized roadmap to achieve the cybersecurity outcomes of the Framework. There are many ways to use Profiles, including to:
- Compare current cybersecurity practices to sector-specific standards and regulatory requirements
- Document the Informative References (e.g., standards, guidelines, and policies) and the practices (e.g., procedures and safeguards) currently in place and planned in the future
- Set cybersecurity goals for the organization, identify gaps between current practices and the goals, and plan how to address the gaps in a cost-effective manner
- Prioritize cybersecurity outcomes
- Assess progress toward achieving the organization's cybersecurity goals
- Determine where the organization may have cybersecurity gaps with respect to an emerging threat or a new technology
- Communicate about the cybersecurity capabilities an organization provides — for example, to business partners or to prospective customers of the organization's technology products and services
- Express the organization's cybersecurity requirements and expectations to suppliers, partners, and other third parties
- Integrate cybersecurity and privacy risk management programs by analyzing gaps between NIST Cybersecurity and Privacy Framework Profiles

NIST Cybersecurity Framework 2.0
Framework Tiers

Tier	Cybersecurity Risk Governance	Cybersecurity Risk Management	Third-Party Cybersecurity Risks
Tier 1: Partial	Application of organizational cybersecurity risk strategy is managed in an ad hoc manner. Prioritization is ad hoc and not formally based on objectives or threat environment.	There is limited awareness of cybersecurity risks at the organizational level. The organization implements cybersecurity risk management on an irregular, case-by-case basis. The organization may not have processes that enable cybersecurity information to be shared within the organization.	The organization is generally unaware of the cybersecurity risks of the products and services it provides and uses. The organization does not understand its role in the larger ecosystem with respect to either its dependencies or dependents. The organization has not formalized its capabilities to internally manage cybersecurity risks in its supply chains or with its partners and may do these activities in a one-off manner.
Tier 2: Risk Informed	Risk management practices are approved by management but may not be established as organizational-wide policy. Prioritization of cybersecurity activities and protection needs is directly informed by organizational risk objectives, the threat environment, or business/mission requirements.	There is an awareness of cybersecurity risks at the organizational level, but an organization-wide approach to managing cybersecurity risks has not been established. Consideration of cybersecurity in organizational objectives and programs may occur at some but not all levels of the organization. Cyber risk assessment of organizational and external assets occurs, but is not typically repeatable or reoccurring. Cybersecurity information is shared within the organization on an informal basis.	The organization understands the cybersecurity risks in its supply chains that are associated with the products and services that either support the business and mission functions of the organization or are utilized in the organization's products or services. The organization is aware of the cybersecurity risks associated with the products and services it provides and uses, but does not act consistently or formally in response to those risks.

NIST Cybersecurity Framework 2.0
Framework Tiers

Tier	Cybersecurity Risk Governance	Cybersecurity Risk Management	Third-Party Cybersecurity Risks
Tier 3: Repeatable	The organization's risk management practices are formally approved and expressed as policy. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements, threats, and technological landscape.	There is an organization-wide approach to managing cybersecurity risks. Consistent methods are in place to respond effectively to changes in risk. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities. The organization consistently and accurately monitors cybersecurity risks of assets. Senior cybersecurity and non-cybersecurity executives communicate regularly regarding cybersecurity risks. Senior executives ensure that cybersecurity is considered through all lines of operation in the organization.	The organization risk strategy is informed by cybersecurity risks associated with the products and services it provides and uses. Personnel formally act upon those risks, including through mechanisms such as written agreements to communicate baseline requirements, governance structures (e.g., risk councils), and policy implementation and monitoring. An organization-wide approach to managing cybersecurity risks in its supply chains is instantiated in the organization's enterprise risk management policies, processes, and procedures, which are in turn implemented consistently and as intended and continuously monitored and reviewed.

NIST Cybersecurity Framework 2.0
Framework Tiers

Tier	Cybersecurity Risk Governance	Cybersecurity Risk Management	Third-Party Cybersecurity Risks
Tier 4: Adaptive	There is an organization-wide approach to managing cybersecurity risks that uses risk-informed policies, processes, and procedures to address potential cybersecurity events. The relationship between cybersecurity risks and organizational objectives is clearly understood and considered when making decisions. Senior executives monitor cybersecurity risks in the same context as financial and other organizational risks. The organizational budget is based on an understanding of the current and predicted risk environment and risk tolerance. Business units implement executive vision and analyze system-level risks in the context of the organizational risk tolerances. Cybersecurity risk management is part of the organizational culture. It evolves from an awareness of previous activities and continuous awareness of activities on organizational systems and networks. The organization can quickly and efficiently account for changes to business/mission objectives in how risk is approached and communicated	The organization adapts its cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive indicators. Through a process of continuous improvement that incorporates advanced cybersecurity technologies and practices, the organization actively adapts to a changing technological landscape and responds in a timely and effective manner to evolving, sophisticated threats.	The organization uses real-time or near real-time information to understand and consistently act upon cybersecurity risks associated with the products and services it provides and uses. The organization has a governance structure (e.g., Risk Council) that manages the organizational risk silos as well as up and down the supply chain and addresses its supply chain security requirements in tandem with other risks. The organization collaborates with its suppliers and proactively manages its relationships with its suppliers and downstream dependents (e.g., customers).

NIST Cybersecurity Framework 2.0 Framework Tiers - Uses

- Help set the overall tone for how cybersecurity risks will be managed within the organization, and determine the effort required to reach a selected Tier
- Inform their Current and Target Profiles
- Characterize the rigor of an organization's cybersecurity risk governance and management outcomes
- Provide context on how an organization views cybersecurity risks and the processes in place to manage those risks
- Capture an organization's outcomes over a range, from Partial (Tier 1) to Adaptive (Tier 4)
- Reflect a progression from informal, ad hoc responses to approaches that are agile, risk-informed, and continuously improving

NIST Cybersecurity Framework 2.0 Framework Core Functions

- **Govern (GO) -** Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy
- **Identify (ID)** – Help determine the current cybersecurity risk to the organization
- **Protect (PR)** – Use safeguards to prevent or reduce cybersecurity risk
- **Detect (DE)** – Find and analyze possible cybersecurity attacks and compromises
- **Respond (RS)** – Take action regarding a detected cybersecurity incident
- **Recover** – Restore assets and operations that were impacted by a cybersecurity incident

NIST Cybersecurity Framework 2.0
Framework Core Functions /Category Names

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Cybersecurity Supply Chain Risk Management	GV.SC
	Roles, Responsibilities, and Authorities	GV.RR
	Policies, Processes, and Procedures	GV.PO
	Oversight	GV.OV
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

NIST Cybersecurity Framework 2.0
Framework Core Functions /Category Names

Function	Category	Category Identifier
Respond (RE)	Incident Response Reporting and Communication	RS.CO
	Incident Management	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

NIST Cybersecurity Framework 2.0 Govern Core Function Categories/Subcategories

Category	Subcategory
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)
	GV.OC-02: Internal and external stakeholders are determined, and their needs and expectations regarding cybersecurity risk management are understood
	GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed (formerly ID.GV-03)
	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)
	GV.OC-05: Outcomes, capabilities, and services that the organization depends on are determined and communicated (formerly ID.BE-01, ID.BE-04)

NIST Cybersecurity Framework 2.0 Govern Core Function Categories/Subcategories

Category	Subcategory
Cybersecurity Supply Chain Risk Management (GV.SC): Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders (formerly ID.SC)	
	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)
	GV.SC-06: Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships

NIST Cybersecurity Framework 2.0 Govern Core Function Categories/Subcategories

Category	Subcategory
Cybersecurity Supply Chain Risk Management (GV.SC): Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders (formerly ID.SC)	
	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

NIST Cybersecurity Framework 2.0 Govern Core Function Categories/Subcategories

Category	Subcategory
Roles, Responsibilities, and Authorities (GV.RR): Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated (formerly ID.GV-02)	
	GV.RR-01: Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving
	GV.RR-02: Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced (formerly ID.AM-06, ID.GV-02, DE.DP-01)
	GV.RR-03: Adequate resources are allocated commensurate with cybersecurity risk strategy, roles and responsibilities, and policies
	GV.RR-04: Cybersecurity is included in human resources practices (formerly PR.IP-11)
Policies, Processes, and Procedures (GV.PO): Organizational cybersecurity policies, processes, and procedures are established, communicated, and enforced (formerly ID.GV-01)	**GV.PO-01:** Policies, processes, and procedures for managing cybersecurity risks are established based on organizational context, cybersecurity strategy, and priorities and are communicated and enforced (formerly ID.GV-01)
	GV.PO-02: Policies, processes, and procedures for managing cybersecurity risks are reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission (formerly ID.GV-01)

NIST Cybersecurity Framework 2.0 Govern Core Function Categories/Subcategories

Category	Subcategory
Cybersecurity Supply Chain Risk Management (GV.SC): Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders (formerly ID.SC)	
	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

NIST Cybersecurity Framework 2.0 Govern Core Function Categories/Subcategories

Category	Subcategory
Oversight (GV.OV): Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy	
	GV.OV-01: Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction
	GV.OV-02: The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks
	GV.OV-03: Organizational cybersecurity risk management performance is measured and reviewed to confirm and adjust strategic direction

NIST Cybersecurity Framework 2.0 Identity Core Function Categories/Subcategories

Category	Subcategory
Asset Management (ID.AM): Assets (e.g., data, hardware software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy	
	ID.AM-01: Inventories of hardware managed by the organization are maintained
	ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained
	ID.AM-03: Representations of the organization's authorized network communication and internal and external network data flows are maintained (formerly ID.AM-03, DE.AE-01)
	ID.AM-04: Inventories of services provided by suppliers are maintained
	ID.AM-05: Assets are prioritized based on classification, criticality, resources, and impact on the mission
	ID.AM-06: Dropped (moved to GV.RR-02, GV.SC-02)
	ID.AM-07: Inventories of data and corresponding metadata for designated data types are maintained
	ID.AM-08: Systems, hardware, software, and services are managed throughout their life cycle (formerly PR.DS-03, PR.IP-02, PR.MA-01, PR.MA-02)

NIST Cybersecurity Framework 2.0 Identity Core Function Categories/Subcategories

Category	Subcategory
Business Environment (ID.BE): Dropped (moved to GV.OC)	
	ID.BE-01: Dropped (moved to GV.OC-05)
	ID.BE-02: Dropped (moved to GV.OC-01)
	ID.BE-03: Dropped (moved to GV.OC-01)
	ID.BE-04: Dropped (moved to GV.OC-04, GV.OC-05)
	ID.BE-05: Dropped (moved to GV.OC-04)
Governance (ID.GV): Dropped (moved to GV)	*ID.GV-01: Dropped (moved to GV.PO)*
	ID.GV-02: Dropped (moved to GV.RR-02)
	ID.GV-03: Dropped (moved to GV.OC-03)
	ID.GV-04: Dropped (moved to GV.RM-03)

NIST Cybersecurity Framework 2.0 Identity Core Function Categories/Subcategories

Category	Subcategory
Risk Assessment (ID.RA): The organization understands the cybersecurity risk to the organization, assets, and individuals.	
	ID.RA-01: Vulnerabilities in assets are identified, validated, and recorded (formerly ID.RA-01, PR.IP-12, DE.CM-08)
	ID.RA-02: Cyber threat intelligence is received from information sharing forums and sources
	ID.RA-03: Internal and external threats to the organization are identified and recorded
	ID.RA-04: Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded
	ID.RA-05: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk and inform risk prioritization
	ID.RA-06: Risk responses are chosen from the available options, prioritized, planned, tracked, and communicated (formerly ID.RA-06, RS.MI-03)

NIST Cybersecurity Framework 2.0 Identity Core Function Categories/Subcategories

Category	Subcategory
Risk Assessment (ID.RA): The organization understands the cybersecurity risk to the organization, assets, and individuals.	**ID.RA-07**: Changes and exceptions are managed, assessed for risk impact, recorded, and tracked (formerly part of PR.IP-03)
	ID.RA-08: Processes for receiving, analyzing, and responding to vulnerability disclosures are established (formerly RS.AN-05)
	ID.RA-09: The authenticity and integrity of hardware and software are assessed prior to acquisition and use (formerly PR.DS-08)
Risk Management Strategy (ID.RM): Dropped (moved to GV.RM)	*ID.RM-01: Dropped (moved to GV.RM-01)*
	ID.RM-02: Dropped (moved to GV.RM-02)
	ID.RM-03: Dropped (moved to GV.RM-02)
Supply Chain Risk Management (ID.SC): Dropped (moved to GV.SC)	*ID.SC-01: Dropped (moved to GV.SC-01)*
	ID.SC-02: Dropped (moved to GV.SC-03, GV.SC-07)
	ID.SC-03: Dropped (moved to GV.SC-05)
	ID.SC-04: Dropped (moved to GV.SC-07)
	ID.SC-05: Dropped (moved to GV.SC-08, ID.IM-02)

NIST Cybersecurity Framework 2.0 Identity Core Function Categories/Subcategories

Category	Subcategory
Improvement (ID.IM): Improvements to organizational cybersecurity risk management processes, procedures and activities are identified across all Framework Functions	**ID.IM-01:** Continuous evaluation is applied to identify improvements
	ID.IM-02: Security tests and exercises, including those done in coordination with suppliers and relevant third parties, are conducted to identify improvements (formerly ID.SC-05, PR.IP-10, DE.DP-03)
	ID.IM-03: Lessons learned during execution of operational processes, procedures, and activities are used to identify improvements (formerly PR.IP-07, PR.IP-08, DE.DP-05, RS.IM-01, RS.IM-02, RC.IM-01, RC.IM02)
	ID.IM-04: Cybersecurity plans that affect operations are communicated, maintained, and improved (formerly PR.IP-09)

NIST Cybersecurity Framework 2.0 Protect Core Function Categories/Subcategories

Category	Subcategory
Identity Management, Authentication, and Access Control (PR.AA): Access to physical and logical assets is limited to authorized users, services, and hardware, and is managed commensurate with the assessed risk of unauthorized access (formerly PR.AC)	
	PR.AA-01: Identities and credentials for authorized users, services, and hardware are managed by the organization (formerly PR.AC-01)
	PR.AA-02: Identities are proofed and bound to credentials based on the context of interactions (formerly PR.AC-06)

NIST Cybersecurity Framework 2.0 Protect Core Function Categories/Subcategories

Category	Subcategory
Identity Management, Authentication and Access Control (PR.AC): Dropped (moved to PR.AA)	*PR.AC-07: Dropped (moved to PR.AA-03)*
Awareness and Training (PR.AT): The organization's personnel are provided cybersecurity awareness and training so they can perform their cybersecurity-related tasks	**PR.AT-01:** Users are provided awareness and training so they possess the knowledge and skills to perform general tasks with security risks in mind (formerly PR.AT-01, PR.AT-03, RS.CO-01)
	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)
	PR.AT-03: Dropped (moved to PR.AT-01, PR.AT-02)
	PR.AT-04: Dropped (moved to PR.AT-02)
	PR.AT-05: Dropped (moved to PR.AT-02)

NIST Cybersecurity Framework 2.0 Protect Core Function Categories/Subcategories

Category	Subcategory
Identity Management, Authentication, and Access Control (PR.AA): Access to physical and logical assets is limited to authorized users, services, and hardware, and is managed commensurate with the assessed risk of unauthorized access (formerly PR.AC)	**PR.AA-03:** Users, services, and hardware are authenticated (formerly PR.AC-03, PR.AC-07)
	PR.AA-04: Identity assertions are protected, conveyed, and verified
	PR.AA-01: Identities and credentials for authorized users, services, and hardware are managed by the organization (formerly PR.AC-01)
	PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties (formerly PR.AC-01, PR.AC-03, PR.AC-04)
	PR.AA-06: Physical access to assets is managed, monitored, and enforced commensurate with risk (formerly PR.AC-02, PR.PT-04)
Identity Management, Authentication and Access Control (PR.AC): Dropped (moved to PR.AA)	*PR.AC-01: Dropped (moved to PR.AA-01, PR.AA-05)*
	PR.AC-02: Dropped (moved to PR.AA-06)
	PR.AC-03: Dropped (moved to PR.AA-03, PR.AA-05, PR.IR-01)
	PR.AC-04: Dropped (moved to PR.AA-05)
	PR.AC-05: Dropped (moved to PR.IR-01)
	PR.AC-06: Dropped (moved to PR.AA-02)

NIST Cybersecurity Framework 2.0
Protect Core Function
Categories/Subcategories

Category	Subcategory
Data Security (PR.DS): Data is managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information	**PR.DS-01:** The confidentiality, integrity, and availability of data-at-rest are protected (formerly PR.DS-01, PR-DS.05, PR.DS-06, PR.PT-02)
	PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected (formerly PR.DS-02, PR.DS-05)
	PR.DS-03: Dropped (moved to ID.AM-08)
	PR.DS-04: Dropped (moved to PR.IR-04)
	PR.DS-05: Dropped (moved to PR.DS-01, PR-DS-02, PR.DS-10)
	PR.DS-06: Dropped (moved to PR.DS-01, DE.CM-09)
	PR.DS-07: Dropped (moved to PR.IR-01)
	PR.DS-08: Dropped (moved to ID.RA-09, DE.CM-09)
	PR.DS-09: Data is managed throughout its life cycle, including destruction (formerly PR.IP-06)
	PR.DS-10: The confidentiality, integrity, and availability of data-in-use are protected (formerly PR.DS-05)
	PR.DS-11: Backups of data are created, protected, maintained, and tested (formerly PR.IP-04)

NIST Cybersecurity Framework 2.0 Protect Core Function Categories/Subcategories

Category	Subcategory
Information Protection Processes and Procedures (PR.IP): Dropped (moved to other Categories and Functions)	*PR.IP-01: Dropped (moved to PR.PS-01)*
	PR.IP-02: Dropped (moved to ID.AM-08)
	PR.IP-03: Dropped (moved to PR.PS-01, ID.RA-07)
	PR.IP-04: Dropped (moved to PR.DS-11)
	PR.IP-05: Dropped (moved to PR.IR-02)
	PR.IP-06: Dropped (moved to PR.DS-09)
	PR.IP-07: Dropped (moved to ID.IM-03)
	PR.IP-08: Dropped (moved to ID.IM-03)
	PR.IP-09: Dropped (moved to ID.IM-04)
	PR.IP-10: Dropped (moved to ID.IM-02)
	PR.IP-11: Dropped (moved to GV.RR-04)
	PR.IP-12: Dropped (moved to ID.RA-01, PR.PS-02)

NIST Cybersecurity Framework 2.0 Protect Core Function Categories/Subcategories

Category	Subcategory
Maintenance (PR.MA): Dropped (moved to ID.AM-08)	*PR.MA-01: Dropped (moved to ID.AM-08, PR.PS-03)*
	PR.MA-02: Dropped (moved to ID.AM-08, PR.PS-02)
Protective Technology (PR.PT): Dropped (moved to other Protect Categories	*PR.PT-01: Dropped (moved to PR.PS-04)*
	PR.PT-02: Dropped (moved to PR.DS-01, PR.PS-01)
	PR.PT-01: Dropped (moved to PR.PS-04)
	PR.PT-02: Dropped (moved to PR.DS-01, PR.PS-01)
	PR.PT-01: Dropped (moved to PR.PS-04)
Platform Security (PR.PS): The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability	**PR.PS-01:** Configuration management practices are applied (formerly PR.IP-01, PR.IP-03, PR.PT-02, PR.PT-03)
	PR.PS-02: Software is maintained, replaced, and removed commensurate with risk (formerly PR.IP-12, PR.MA-02)
	PR.PS-03: Hardware is maintained, replaced, and removed commensurate with risk (formerly PR.MA-01)
	PR.PS-04: Log records are generated and made available for continuous monitoring (formerly PR.PT-01)
	PR.PS-05: Installation and execution of unauthorized software are prevented
	PR.PS-06: Secure software development practices are integrated and their performance is monitored throughout the software development life cycle

NIST Cybersecurity Framework 2.0 Protect Core Function Categories/Subcategories

Category	Subcategory
Technology Infrastructure Resilience (PR.IR): Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, and availability, and organizational resilience	**PR.IR-01:** Networks and environments are protected from unauthorized logical access and usage (formerly PR.AC-03, PR.AC-05, PR.DS-07, PR.PT-04)
	PR.IR-02: The organization's technology assets are protected from environmental threats (formerly PR.IP-05)
	PR.IR-03: Mechanisms are implemented to achieve resilience requirements in normal and adverse situations (formerly PR.PT-05)
	PR.IR-04: Adequate resource capacity to ensure availability is maintained (formerly PR.DS-04)

NIST Cybersecurity Framework 2.0
Detect Core Function
Categories/Subcategories

Category	Subcategory
Continuous Monitoring (DE.CM): Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events	**DE.CM-01:** Networks and network services are monitored to find potentially adverse events (formerly DE.CM-01, DE.CM-04, DE.CM-05, DE.CM-07)
	DE.CM-02: The physical environment is monitored to find potentially adverse events
	DE.CM-03: Personnel activity and technology usage are monitored to find potentially adverse events (formerly DE.CM-03, DE.CM-07)
	DE.CM-04: Dropped (moved to DE.CM-01, DE.CM-09)
	DE.CM-05: Dropped (moved to DE.CM-01, DE.CM-09)

NIST Cybersecurity Framework 2.0 Detect Core Function Categories/Subcategories

Category	Subcategory
Continuous Monitoring (DE.CM): Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events	**DE.CM-06:** External service provider activities and services are monitored to find potentially adverse events (formerly DE.CM-06, DE.CM-07)
	DE.CM-07: Dropped (moved to DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09)
	DE.CM-08: Dropped (moved to ID.RA-01)
	DE.CM-09: Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events (formerly PR.DS-06, PR.DS-08, DE.CM-04, DE.CM-05, DE.CM-07)
Adverse Event Analysis (DE.AE): Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents (formerly DE.AE, DE.DP-02)	*DE.AE-01: Dropped (moved to ID.AM-03)*
	DE.AE-02: Potentially adverse events are analyzed to better understand associated activities
	DE.AE-03: Information is correlated from multiple sources
	DE.AE-04: The estimated impact and scope of adverse events are determined
	DE.AE-05: Dropped (moved to DE.AE-08)
	DE.AE-06: Information on adverse events is provided to authorized staff and tools (formerly DE.DP-04)

NIST Cybersecurity Framework 2.0 Detect Core Function Categories/Subcategories

Category	Subcategory
Adverse Event Analysis (DE.AE): Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents (formerly DE.AE, DE.DP-02)	**DE.AE-07:** Cyber threat intelligence and other contextual information are integrated into the analysis
	DE.AE-08: Incidents are declared when adverse events meet the defined incident criteria (formerly DE.AE-05)
Detection Processes (DE.DP): Dropped (moved to other Categories and Functions)	*DE.DP-01: Dropped (moved to GV.RR-02)*
	DE.DP-02: Dropped (moved to DE.AE)
	DE.DP-03: Dropped (moved to ID.IM-02)
	DE.DP-04: Dropped (moved to DE.AE-06)
	DE.DP-05: Dropped (moved to ID.IM-03)

NIST Cybersecurity Framework 2.0 Response Core Function Categories/Subcategories

Category	Subcategory
Response Planning (RS.RP): Dropped (moved to RS.MA)	*RS.RP-01: Dropped (moved to RS.MA-01)*
Incident Management (RS.MA): Responses to detected cybersecurity incidents are managed (formerly RS.RP)	**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)
	RS.MA-02: Incident reports are triaged and validated (formerly RS.AN-01, RS.AN-02)
	RS.MA-03: Incidents are categorized and prioritized (formerly RS.AN-04, RS.AN-02)
	RS.MA-04: Incidents are escalated or elevated as needed (formerly RS.AN-02, RS.CO-04)
	RS.MA-05: The criteria for initiating incident recovery are applied
Incident Analysis (RS.AN): Investigation is conducted to ensure effective response and support forensics and recovery activities	*RS.AN-01: Dropped (moved to RS.MA-02)*
	RS.AN-02: Dropped (moved to RS.MA-02, RS.MA-03, RS.MA-04)
	RS.AN-03: Analysis is performed to determine what has taken place during an incident and the root cause of the incident
	RS.AN-04: Dropped (moved to RS.MA-03)
	RS.AN-05: Dropped (moved to ID.RA-08)
	RS.AN-06: Actions performed during an investigation are recorded and the records' integrity and provenance are preserved (formerly part of RS.AN-03)

NIST Cybersecurity Framework 2.0 Response Core Function Categories/Subcategories

Category	Subcategory
Incident Analysis (RS.AN): Investigation is conducted to ensure effective response and support forensics and recovery activities	**RS.AN-07:** Incident data and metadata are collected, and their integrity and provenance are preserved
	RS.AN-08: The incident's magnitude is estimated and validated
Incident Response Reporting and Communication (RS.CO): Response activities are coordinated with internal and external stakeholders as required by laws, regulations, or policies	*RS.CO-01: Dropped (moved to PR.AT-01)*
	RS.CO-02: Internal and external stakeholders are notified of incidents
	RS.CO-03: Information is shared with designated internal and external stakeholders (formerly RS.CO-03, RS.CO-05)
	RS.CO-04: Dropped (moved to RS.MA-01, RS.MA-04)
	RS.CO-05: Dropped (moved to RS.CO-03)
Incident Mitigation (RS.MI): Activities are performed to prevent expansion of an event and mitigate its effects	**RS.MI-01:** Incidents are contained
	RS.MI-02: Incidents are eradicated
	RS.MI-03: Dropped (moved to ID.RA-06)
Improvements (RS.IM): Dropped (moved to ID.IM)	*RS.IM-01: Dropped (moved to ID.IM-03)*
	RS.IM-01: Dropped (moved to ID.IM-03)

NIST Cybersecurity Framework 2.0 Recover Core Function Categories/Subcategories

Category	Subcategory
Incident Recovery Plan Execution (RC.RP): Restoration activities are performed to ensure operational availability of systems and services affected by cybersecurity incidents	**RC.RP-01:** The recovery portion of the incident response plan is executed once initiated from the incident response process
	RC.RP-02: Recovery actions are determined, scoped, prioritized, and performed
	RC.RP-03: The integrity of backups and other restoration assets is verified before using them for restoration
	RC.RP-04: Critical mission functions and cybersecurity risk management are considered to establish postincident operational norms
	RC.RP-05: The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed
	RC.RP-06: The criteria for determining the end of incident recovery are applied, and incident-related documentation is completed

NIST Cybersecurity Framework 2.0 Recover Core Function Categories/Subcategories

Category	Subcategory
Incident Recovery Communication (RC.CO): Restoration activities are coordinated with internal and external parties	*RC.CO-01: Dropped (moved to RC.CO-04)*
	RC.CO-02: Dropped (moved to RC.CO-04)
	RC.CO-03: Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders
	RC.CO-04: Public updates on incident recovery are properly shared using approved methods and messaging (formerly RC.CO-01, RC.CO-02)
Improvements (RC.IM): Dropped (moved to ID.IM)	*RC.IM-01: Dropped (moved to ID.IM-03)*
	RC.IM-02: Dropped (moved to ID.IM-03)