

# The NIST Cybersecurity Framework (CSF) 2.0 Core With Withdrawn CSF 1.1 Elements

This document presents the Functions, Categories, and Subcategories of the CSF 2.0 Core along with the indicators for CSF 1.1 Categories and Subcategories that were withdrawn from CSF 2.0. It also includes the only Subcategory, PR.DS-09, that was new in the CSF 2.0 public comment draft but withdrawn from the final CSF 2.0.

Table 1 shows the CSF 2.0 Core Function and Category names and unique alphabetic identifiers. Each Function in Table 1 links to a separate table that defines that Function and its Categories and Subcategories. The supporting tables denote withdrawn items with italics and the label “Withdrawn.” Each withdrawn item has been either *moved* to another location in the Core with relatively minor changes to its definition or *incorporated* into one or more other locations in the Core with significant changes.

Table 1. CSF 2.0 Core Function and Category names and identifiers

Function	Category	Category Identifier
<b><u>Govern (GV)</u></b>	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
<b><u>Identify (ID)</u></b>	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
<b><u>Protect (PR)</u></b>	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
<b><u>Detect (DE)</u></b>	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
<b><u>Respond (RS)</u></b>	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
<b><u>Recover (RC)</u></b>	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

**Table 2. GOVERN (GV): The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored**

Category	Subcategory
<p><b>Organizational Context (GV.OC):</b> The circumstances — mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements — surrounding the organization’s cybersecurity risk management decisions are understood</p>	
	<p><b>GV.OC-01:</b> The organizational mission is understood and informs cybersecurity risk management</p>
	<p><b>GV.OC-02:</b> Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered</p>
	<p><b>GV.OC-03:</b> Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed</p>
	<p><b>GV.OC-04:</b> Critical objectives, capabilities, and services that stakeholders depend on or expect from the organization are understood and communicated</p>
	<p><b>GV.OC-05:</b> Outcomes, capabilities, and services that the organization depends on are understood and communicated</p>
<p><b>Risk Management Strategy (GV.RM):</b> The organization’s priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions</p>	
	<p><b>GV.RM-01:</b> Risk management objectives are established and agreed to by organizational stakeholders</p>
	<p><b>GV.RM-02:</b> Risk appetite and risk tolerance statements are established, communicated, and maintained</p>
	<p><b>GV.RM-03:</b> Cybersecurity risk management activities and outcomes are included in enterprise risk management processes</p>
	<p><b>GV.RM-04:</b> Strategic direction that describes appropriate risk response options is established and communicated</p>
	<p><b>GV.RM-05:</b> Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties</p>
	<p><b>GV.RM-06:</b> A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated</p>
	<p><b>GV.RM-07:</b> Strategic opportunities (i.e., positive risks) are characterized and are included in organizational cybersecurity risk discussions</p>

NIST CSF 2.0 Core With Withdrawn CSF 1.1 Elements

Category	Subcategory
<p><b>Cybersecurity Supply Chain Risk Management (GV.SC):</b> Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders</p>	
	<p><b>GV.SC-01:</b> A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders</p>
	<p><b>GV.SC-02:</b> Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally</p>
	<p><b>GV.SC-03:</b> Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes</p>
	<p><b>GV.SC-04:</b> Suppliers are known and prioritized by criticality</p>
	<p><b>GV.SC-05:</b> 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</p>
	<p><b>GV.SC-06:</b> Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships</p>
	<p><b>GV.SC-07:</b> The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship</p>
	<p><b>GV.SC-08:</b> Relevant suppliers and other third parties are included in incident planning, response, and recovery activities</p>
	<p><b>GV.SC-09:</b> 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</p>
	<p><b>GV.SC-10:</b> Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement</p>
<p><b>Roles, Responsibilities, and Authorities (GV.RR):</b> Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated</p>	
	<p><b>GV.RR-01:</b> Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving</p>

NIST CSF 2.0 Core With Withdrawn CSF 1.1 Elements

Category	Subcategory
	<b>GV.RR-02:</b> Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced
	<b>GV.RR-03:</b> Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies
	<b>GV.RR-04:</b> Cybersecurity is included in human resources practices
<b>Policy (GV.PO):</b> Organizational cybersecurity policy is established, communicated, and enforced	
	<b>GV.PO-01:</b> Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced
	<b>GV.PO-02:</b> Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission
<b>Oversight (GV.OV):</b> Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy	
	<b>GV.OV-01:</b> Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction
	<b>GV.OV-02:</b> The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks
	<b>GV.OV-03:</b> Organizational cybersecurity risk management performance is measured and reviewed for adjustments needed

**Table 3. IDENTIFY (ID): The organization's current cybersecurity risks are understood**

Category	Subcategory
<b>Asset Management (ID.AM):</b> 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	
	<b>ID.AM-01:</b> Inventories of hardware managed by the organization are maintained
	<b>ID.AM-02:</b> Inventories of software, services, and systems managed by the organization are maintained

NIST CSF 2.0 Core With Withdrawn CSF 1.1 Elements

Category	Subcategory
	<b>ID.AM-03:</b> Representations of the organization’s authorized network communication and internal and external network data flows are maintained
	<b>ID.AM-04:</b> Inventories of services provided by suppliers are maintained
	<b>ID.AM-05:</b> Assets are prioritized based on classification, criticality, resources, and impact on the mission
	<i>ID.AM-06: Withdrawn (incorporated into GV.RR-02, GV.SC-02)</i>
	<b>ID.AM-07:</b> Inventories of data and corresponding metadata for designated data types are maintained
	<b>ID.AM-08:</b> Systems, hardware, software, services, and data are managed throughout their life cycles
<i>Business Environment (ID.BE): Withdrawn (incorporated into GV.OC)</i>	
	<i>ID.BE-01: Withdrawn (incorporated into GV.OC-05)</i>
	<i>ID.BE-02: Withdrawn (incorporated into GV.OC-01)</i>
	<i>ID.BE-03: Withdrawn (incorporated into GV.OC-01)</i>
	<i>ID.BE-04: Withdrawn (incorporated into GV.OC-04, GV.OC-05)</i>
	<i>ID.BE-05: Withdrawn (incorporated into GV.OC-04)</i>
<i>Governance (ID.GV): Withdrawn (incorporated into GV)</i>	
	<i>ID.GV-01: Withdrawn (incorporated into GV.PO, GV.PO-01, GV.PO-02)</i>
	<i>ID.GV-02: Withdrawn (incorporated into GV.OC-02, GV.RR, GV.RR-02)</i>
	<i>ID.GV-03: Withdrawn (moved to GV.OC-03)</i>
	<i>ID.GV-04: Withdrawn (moved to GV.RM-03)</i>
<b>Risk Assessment (ID.RA):</b> The cybersecurity risk to the organization, assets, and individuals is understood by the organization	
	<b>ID.RA-01:</b> Vulnerabilities in assets are identified, validated, and recorded
	<b>ID.RA-02:</b> Cyber threat intelligence is received from information sharing forums and sources
	<b>ID.RA-03:</b> Internal and external threats to the organization are identified and recorded
	<b>ID.RA-04:</b> Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded
	<b>ID.RA-05:</b> Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization

NIST CSF 2.0 Core With Withdrawn CSF 1.1 Elements

Category	Subcategory
	<b>ID.RA-06:</b> Risk responses are chosen, prioritized, planned, tracked, and communicated
	<b>ID.RA-07:</b> Changes and exceptions are managed, assessed for risk impact, recorded, and tracked
	<b>ID.RA-08:</b> Processes for receiving, analyzing, and responding to vulnerability disclosures are established
	<b>ID.RA-09:</b> The authenticity and integrity of hardware and software are assessed prior to acquisition and use
	<b>ID.RA-10:</b> Critical suppliers are assessed prior to acquisition
<i>Risk Management Strategy (ID.RM): Withdrawn (moved to GV.RM)</i>	
	<i>ID.RM-01: Withdrawn (incorporated into GV.RM-01, GV.RM-06, GV.RR-03)</i>
	<i>ID.RM-02: Withdrawn (incorporated into GV.RM-02, GV.RM-04)</i>
	<i>ID.RM-03: Withdrawn (moved to GV.RM-02)</i>
<i>Supply Chain Risk Management (ID.SC): Withdrawn (incorporated into GV.SC)</i>	
	<i>ID.SC-01: Withdrawn (incorporated into GV.RM-05, GV.SC-01, GV.SC-06, GV.SC-09, GV.SC-10)</i>
	<i>ID.SC-02: Withdrawn (incorporated into GV.OC-02, GV.SC-03, GV.SC-04, GV.SC-07, ID.RA-10)</i>
	<i>ID.SC-03: Withdrawn (moved to GV.SC-05)</i>
	<i>ID.SC-04: Withdrawn (incorporated into GV.SC-07, ID.RA-10)</i>
	<i>ID.SC-05: Withdrawn (incorporated into GV.SC-08, ID.IM-02)</i>
<b>Improvement (ID.IM):</b> Improvements to organizational cybersecurity risk management processes, procedures and activities are identified across all CSF Functions	
	<b>ID.IM-01:</b> Improvements are identified from evaluations
	<b>ID.IM-02:</b> Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties
	<b>ID.IM-03:</b> Improvements are identified from execution of operational processes, procedures, and activities
	<b>ID.IM-04:</b> Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved

Table 4. PROTECT (PR): Safeguards to manage the organization's cybersecurity risks are used

Category	Subcategory
<p><b>Identity Management, Authentication, and Access Control (PR.AA):</b> 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</p>	
	<p><b>PR.AA-01:</b> Identities and credentials for authorized users, services, and hardware are managed by the organization</p>
	<p><b>PR.AA-02:</b> Identities are proofed and bound to credentials based on the context of interactions</p>
	<p><b>PR.AA-03:</b> Users, services, and hardware are authenticated</p>
	<p><b>PR.AA-04:</b> Identity assertions are protected, conveyed, and verified</p>
	<p><b>PR.AA-05:</b> 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</p>
	<p><b>PR.AA-06:</b> Physical access to assets is managed, monitored, and enforced commensurate with risk</p>
<p><i>Identity Management, Authentication, and Access Control (PR.AC): Withdrawn (moved to PR.AA)</i></p>	
	<p><i>PR.AC-01: Withdrawn (incorporated into PR.AA-01, PR.AA-05)</i></p>
	<p><i>PR.AC-02: Withdrawn (moved to PR.AA-06)</i></p>
	<p><i>PR.AC-03: Withdrawn (incorporated into PR.AA-03, PR.AA-05, PR.IR-01)</i></p>
	<p><i>PR.AC-04: Withdrawn (moved to PR.AA-05)</i></p>
	<p><i>PR.AC-05: Withdrawn (incorporated into PR.IR-01)</i></p>
	<p><i>PR.AC-06: Withdrawn (moved to PR.AA-02)</i></p>
	<p><i>PR.AC-07: Withdrawn (moved to PR.AA-03)</i></p>
<p><b>Awareness and Training (PR.AT):</b> The organization's personnel are provided with cybersecurity awareness and training so that they can perform their cybersecurity-related tasks</p>	
	<p><b>PR.AT-01:</b> Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with security risks in mind</p>
	<p><b>PR.AT-02:</b> Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with security risks in mind</p>
	<p><i>PR.AT-03: Withdrawn (incorporated into PR.AT-01, PR.AT-02)</i></p>

NIST CSF 2.0 Core With Withdrawn CSF 1.1 Elements

Category	Subcategory
	<i>PR.AT-04: Withdrawn (incorporated into PR.AT-02)</i>
	<i>PR.AT-05: Withdrawn (incorporated into PR.AT-02)</i>
<b>Data Security (PR.DS):</b> Data are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information	
	<b>PR.DS-01:</b> The confidentiality, integrity, and availability of data-at-rest are protected
	<b>PR.DS-02:</b> The confidentiality, integrity, and availability of data-in-transit are protected
	<i>PR.DS-03: Withdrawn (incorporated into ID.AM-08, PR.PS-03)</i>
	<i>PR.DS-04: Withdrawn (moved to PR.IR-04)</i>
	<i>PR.DS-05: Withdrawn (incorporated into PR.DS-01, PR.DS-02, PR.DS-10)</i>
	<i>PR.DS-06: Withdrawn (incorporated into PR.DS-01, DE.CM-09)</i>
	<i>PR.DS-07: Withdrawn (incorporated into PR.IR-01)</i>
	<i>PR.DS-08: Withdrawn (incorporated into ID.RA-09, DE.CM-09)</i>
	<i>PR.DS-09: Withdrawn (incorporated into ID.AM-08)</i>
	<b>PR.DS-10:</b> The confidentiality, integrity, and availability of data-in-use are protected
	<b>PR.DS-11:</b> Backups of data are created, protected, maintained, and tested
<i>Information Protection Processes and Procedures (PR.IP): Withdrawn (incorporated into other Categories and Functions)</i>	
	<i>PR.IP-01: Withdrawn (incorporated into PR.PS-01)</i>
	<i>PR.IP-02: Withdrawn (incorporated into ID.AM-08, PR.PS-06)</i>
	<i>PR.IP-03: Withdrawn (incorporated into PR.PS-01, ID.RA-07)</i>
	<i>PR.IP-04: Withdrawn (moved to PR.DS-11)</i>
	<i>PR.IP-05: Withdrawn (moved to PR.IR-02)</i>
	<i>PR.IP-06: Withdrawn (incorporated into ID.AM-08)</i>
	<i>PR.IP-07: Withdrawn (incorporated into ID.IM, ID.IM-03)</i>
	<i>PR.IP-08: Withdrawn (incorporated into ID.IM-03)</i>
	<i>PR.IP-09: Withdrawn (incorporated into ID.IM-04)</i>
	<i>PR.IP-10: Withdrawn (incorporated into ID.IM-02, ID.IM-04)</i>
	<i>PR.IP-11: Withdrawn (moved to GV.RR-04)</i>

NIST CSF 2.0 Core With Withdrawn CSF 1.1 Elements

Category	Subcategory
	<i>PR.IP-12: Withdrawn (incorporated into ID.RA-01, PR.PS-02)</i>
<i>Maintenance (PR.MA): Withdrawn (incorporated into ID.AM-08)</i>	
	<i>PR.MA-01: Withdrawn (incorporated into ID.AM-08, PR.PS-03)</i>
	<i>PR.MA-02: Withdrawn (incorporated into ID.AM-08, PR.PS-02)</i>
<i>Protective Technology (PR.PT): Withdrawn (incorporated into other Protect Categories)</i>	
	<i>PR.PT-01: Withdrawn (incorporated into PR.PS-04)</i>
	<i>PR.PT-02: Withdrawn (incorporated into PR.DS-01, PR.PS-01)</i>
	<i>PR.PT-03: Withdrawn (incorporated into PR.PS-01)</i>
	<i>PR.PT-04: Withdrawn (incorporated into PR.AA-06, PR.IR-01)</i>
	<i>PR.PT-05: Withdrawn (moved to PR.IR-03)</i>
<b>Platform Security (PR.PS):</b> 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	
	<b>PR.PS-01:</b> Configuration management practices are established and applied
	<b>PR.PS-02:</b> Software is maintained, replaced, and removed commensurate with risk
	<b>PR.PS-03:</b> Hardware is maintained, replaced, and removed commensurate with risk
	<b>PR.PS-04:</b> Log records are generated and made available for continuous monitoring
	<b>PR.PS-05:</b> Installation and execution of unauthorized software are prevented
	<b>PR.PS-06:</b> Secure software development practices are integrated and their performance is monitored throughout the software development life cycle
<b>Technology Infrastructure Resilience (PR.IR):</b> Security architectures are managed with the organization’s risk strategy to protect asset confidentiality, integrity, and availability, and organizational resilience	
	<b>PR.IR-01:</b> Networks and environments are protected from unauthorized logical access and usage

Category	Subcategory
	<b>PR.IR-02:</b> The organization’s technology assets are protected from environmental threats
	<b>PR.IR-03:</b> Mechanisms are implemented to achieve resilience requirements in normal and adverse situations
	<b>PR.IR-04:</b> Adequate resource capacity to ensure availability is maintained

Table 5. DETECT (DE): Possible cybersecurity attacks and compromises are found and analyzed

Category	Subcategory
<b>Continuous Monitoring (DE.CM):</b> Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events	
	<b>DE.CM-01:</b> Networks and network services are monitored to find potentially adverse events
	<b>DE.CM-02:</b> The physical environment is monitored to find potentially adverse events
	<b>DE.CM-03:</b> Personnel activity and technology usage are monitored to find potentially adverse events
	<i>DE.CM-04: Withdrawn (incorporated into DE.CM-01, DE.CM-09)</i>
	<i>DE.CM-05: Withdrawn (incorporated into DE.CM-01, DE.CM-09)</i>
	<b>DE.CM-06:</b> External service provider activities and services are monitored to find potentially adverse events
	<i>DE.CM-07: Withdrawn (incorporated into DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09)</i>
	<i>DE.CM-08: Withdrawn (incorporated into ID.RA-01)</i>
	<b>DE.CM-09:</b> Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events
<b>Adverse Event Analysis (DE.AE):</b> Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents	
	<i>DE.AE-01: Withdrawn (incorporated into ID.AM-03)</i>
	<b>DE.AE-02:</b> Potentially adverse events are analyzed to better understand associated activities
	<b>DE.AE-03:</b> Information is correlated from multiple sources
	<b>DE.AE-04:</b> The estimated impact and scope of adverse events are determined
	<i>DE.AE-05: Withdrawn (moved to DE.AE-08)</i>

NIST CSF 2.0 Core With Withdrawn CSF 1.1 Elements

Category	Subcategory
	<b>DE.AE-06:</b> Information on adverse events is provided to authorized staff and tools
	<b>DE.AE-07:</b> Cyber threat intelligence and other contextual information are integrated into the analysis
	<b>DE.AE-08:</b> Incidents are declared when adverse events meet the defined incident criteria
<i>Detection Processes (DE.DP): Withdrawn (incorporated into other Categories and Functions)</i>	
	<i>DE.DP-01: Withdrawn (incorporated into GV.RR-02)</i>
	<i>DE.DP-02: Withdrawn (incorporated into DE.AE)</i>
	<i>DE.DP-03: Withdrawn (incorporated into ID.IM-02)</i>
	<i>DE.DP-04: Withdrawn (incorporated into DE.AE-06)</i>
	<i>DE.DP-05: Withdrawn (incorporated into ID.IM, ID.IM-03)</i>

**Table 6. RESPOND (RS): Actions regarding a detected cybersecurity incident are taken**

Category	Subcategory
<i>Response Planning (RS.RP): Withdrawn (incorporated into RS.MA)</i>	
	<i>RS.RP-01: Withdrawn (incorporated into RS.MA-01)</i>
<b>Incident Management (RS.MA):</b> Responses to detected cybersecurity incidents are managed	
	<b>RS.MA-01:</b> The incident response plan is executed in coordination with relevant third parties once an incident is declared
	<b>RS.MA-02:</b> Incident reports are triaged and validated
	<b>RS.MA-03:</b> Incidents are categorized and prioritized
	<b>RS.MA-04:</b> Incidents are escalated or elevated as needed
	<b>RS.MA-05:</b> The criteria for initiating incident recovery are applied
<b>Incident Analysis (RS.AN):</b> Investigations are conducted to ensure effective response and support forensics and recovery activities	
	<i>RS.AN-01: Withdrawn (incorporated into RS.MA-02)</i>
	<i>RS.AN-02: Withdrawn (incorporated into RS.MA-02, RS.MA-03, RS.MA-04)</i>
	<b>RS.AN-03:</b> Analysis is performed to determine what has taken place during an incident and the root cause of the incident
	<i>RS.AN-04: Withdrawn (moved to RS.MA-03)</i>

NIST CSF 2.0 Core With Withdrawn CSF 1.1 Elements

Category	Subcategory
	<i>RS.AN-05: Withdrawn (moved to ID.RA-08)</i>
	<b>RS.AN-06:</b> Actions performed during an investigation are recorded, and the records' integrity and provenance are preserved
	<b>RS.AN-07:</b> Incident data and metadata are collected, and their integrity and provenance are preserved
	<b>RS.AN-08:</b> An incident's magnitude is estimated and validated
<b>Incident Response Reporting and Communication (RS.CO):</b> Response activities are coordinated with internal and external stakeholders as required by laws, regulations, or policies	
	<i>RS.CO-01: Withdrawn (incorporated into PR.AT-01)</i>
	<b>RS.CO-02:</b> Internal and external stakeholders are notified of incidents
	<b>RS.CO-03:</b> Information is shared with designated internal and external stakeholders
	<i>RS.CO-04: Withdrawn (incorporated into RS.MA-01, RS.MA-04)</i>
	<i>RS.CO-05: Withdrawn (incorporated into RS.CO-03)</i>
<b>Incident Mitigation (RS.MI):</b> Activities are performed to prevent expansion of an event and mitigate its effects	
	<b>RS.MI-01:</b> Incidents are contained
	<b>RS.MI-02:</b> Incidents are eradicated
	<i>RS.MI-03: Withdrawn (incorporated into ID.RA-06)</i>
<i>Improvements (RS.IM): Withdrawn (incorporated into ID.IM)</i>	
	<i>RS.IM-01: Withdrawn (incorporated into ID.IM-03, ID.IM-04)</i>
	<i>RS.IM-02: Withdrawn (incorporated into ID.IM-03)</i>

**Table 7. RECOVER (RC): Assets and operations affected by a cybersecurity incident are restored**

Category	Subcategory
<b>Incident Recovery Plan Execution (RC.RP):</b> Restoration activities are performed to ensure operational availability of systems and services affected by cybersecurity incidents	
	<b>RC.RP-01:</b> The recovery portion of the incident response plan is executed once initiated from the incident response process
	<b>RC.RP-02:</b> Recovery actions are selected, scoped, prioritized, and performed

NIST CSF 2.0 Core With Withdrawn CSF 1.1 Elements

Category	Subcategory
	<b>RC.RP-03:</b> The integrity of backups and other restoration assets is verified before using them for restoration
	<b>RC.RP-04:</b> Critical mission functions and cybersecurity risk management are considered to establish post-incident operational norms
	<b>RC.RP-05:</b> The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed
	<b>RC.RP-06:</b> The criteria for determining the end of incident recovery are applied, and incident-related documentation is completed
<b>Incident Recovery Communication (RC.CO):</b> Restoration activities are coordinated with internal and external parties	
	<i>RC.CO-01: Withdrawn (incorporated into RC.CO-04)</i>
	<i>RC.CO-02: Withdrawn (incorporated into RC.CO-04)</i>
	<b>RC.CO-03:</b> Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders
	<b>RC.CO-04:</b> Public updates on incident recovery are shared using approved methods and messaging
<i>Improvements (RC.IM): Withdrawn (incorporated into ID.IM)</i>	
	<i>RC.IM-01: Withdrawn (incorporated into ID.IM-03, ID.IM-04)</i>
	<i>RC.IM-02: Withdrawn (incorporated into ID.IM-03)</i>