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

# Discussion Draft of the NIST Cybersecurity Framework 2.0 Core

April 24, 2023

## Note to Reviewers

This discussion draft identifies the potential Functions, Categories, and Subcategories (also called cybersecurity outcomes) of the NIST Cybersecurity Framework (CSF) 2.0 Core. NIST is releasing this document for discussion to inform the development of the complete NIST CSF 2.0 Draft.

**This early draft of the NIST CSF 2.0 Core is preliminary**—it is intended to increase transparency of the update process and promote discussion to generate concrete suggestions for improving the Framework. The draft covers cybersecurity outcomes across 6 Functions, 21 Categories, and 112 Subcategories (Tables 1 and 3). It also includes a sampling of the potential new CSF 2.0 Informative Examples column, to provide notional actions that interpret the CSF Subcategories (Table 2). The draft does not yet identify all Implementation Examples, Informative References, or other information that may be included in the CSF 2.0 Core. In addition to PDF and Excel formats, the final CSF 2.0 Core will be showcased through the online Cybersecurity and Privacy Reference Tool (CPRT) to provide a machine-readable format and updates to crosswalk and mappings to other resources.

The modifications from CSF 1.1 are intended to increase clarity, ensure a consistent level of abstraction, address changes in technologies and risks, and improve alignment with national and international cybersecurity standards and practices. While many organizations have told NIST the CSF 1.1 is still effective in addressing cybersecurity risks, NIST believes these changes are warranted to make it easier for organizations to address their current and future cybersecurity challenges more effectively. The NIST CSF has been widely used to reduce cybersecurity risks since initial publication in 2014; NIST is working with the community to ensure the CSF 2.0 is effective for the next decade.

**Feedback on this discussion draft may be submitted to cyberframework@nist.gov at any time. Feedback will inform the complete NIST CSF 2.0 draft anticipated to be released for public comment this summer.**

NIST seeks feedback as to whether the cybersecurity outcomes address current cybersecurity challenges faced by organizations, are aligned with existing practices and resources, and are responsive to the comments. NIST seeks concrete suggestions about improvements to the draft, including revisions to Functions, Categories, and Subcategories, and submissions of omitted cybersecurity outcomes. NIST also requests feedback on the format, content, and scope of Implementation Examples; suggestions of possible Examples; and the appropriate level of abstraction between Subcategories and Examples. In addition, NIST requests feedback on the best way to showcase final modifications from CSF 1.1 to CSF 2.0 to ease transition.

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

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

# Overview

The Discussion Draft of the NIST Cybersecurity Framework 2.0 Core is a continuation of NIST's extensive engagement with the community to craft CSF 2.0. The Discussion Core presented here reflects feedback received thus far through:

- The 92 written responses to the January 2023 CSF 2.0 Concept Paper;
- The February 2023 In-Person Working Sessions (attended by approximately 250 participants in Rockville, MD);
- The "Journey to the NIST Cybersecurity Framework 2.0" February 2023 Workshop #2 (attended virtually by more than 2,000 participants from 69 countries);
- The "Journey to the NIST Cybersecurity Framework 2.0" August 2022 Workshop #1 (attended virtually by approximately 4,000 participants from 100 countries);
- The 134 written responses to the February 2022 NIST Cybersecurity RFI;
- Feedback from organizations that have leveraged the CSF over the years; and
- NIST participation at conferences, webinars, roundtables, and meetings around the world.

It reflects changes—some larger, some smaller—across the CSF 1.1 Core through reordering, merging, and otherwise modifying the cybersecurity outcomes of the Framework. Table 3 of the CSF 2.0 Core includes the CSF 1.1 Category and Subcategory text for comparison. That table also identifies when and where an outcome from CSF 1.1. has been moved. The CSF 2.0 Discussion Core increases focus on:

- Cybersecurity outcomes applicable to all organizations, removing language specific to critical infrastructure across the Core;
- The prevention of cybersecurity incidents through outcomes focused in Govern, Identify, and Protect Functions and the detection and response of incidents through the Detect, Respond, and Recover Functions;
- Cybersecurity governance through a new Govern Function covering organizational context, risk management strategy, policies and procedures, and roles and responsibilities;
- Cybersecurity supply chain risk management outcomes;
- Continuous improvement through a new Improvement Category in the Identify Function;
- Leveraging the combination of people, process, and technology to secure assets across all Categories in the Protect Function;
- Resilience of technology infrastructure through a new Protect Function Category; and
- Cybersecurity incident response management, including the importance of incident forensics, through new Categories in the Respond and Recover Functions.

While the Core is arguably the most recognizable piece of the CSF, it is not the only element of the CSF that will be updated. There is still much to do to implement the CSF 2.0 Concept Paper, including development of guidance on CSF implementation, the relationship and alignment of the CSF to other NIST and non-NIST resources, and the use of the CSF for assessment and measurement. NIST encourages the community to continue engaging in the update process, including the Calls to Action identified in the CSF 2.0 Concept Paper. Progress in the CSF 2.0 effort, as well as ways to engage, can be found on the NIST CSF 2.0 webpage.

# Table 1: Discussion Draft NIST Cybersecurity Framework 2.0 Core: Function and Category Names and Identifiers

This table shows the proposed CSF 2.0 Core Function and Category names. Each Function and Category has a unique alphabetic identifier.

| NIST Cybersecurity Framework 2.0 | | |
|---|---|---|
| **CSF 2.0 Function** | **CSF 2.0 Category** | **CSF 2.0 Category Identifier** |
| **Govern** (GV) | Organizational Context | GV.OC |
| | Risk Management Strategy | GV.RM |
| | Roles and Responsibilities | GV.RR |
| | Policies and Procedures | GV.PO |
| **Identify** (ID) | Asset Management | ID.AM |
| | Risk Assessment | ID.RA |
| | Supply Chain Risk Management | ID.SC |
| | 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) | Adverse Event Analysis | DE.AE |
| | Continuous Monitoring | DE.CM |
| **Respond** (RS) | Incident Management | RS.MA |
| | Incident Analysis | RS.AN |
| | Incident Response Reporting and Communication | RS.CO |
| | Incident Mitigation | RS.MI |
| **Recover** (RC) | Incident Recovery Plan Execution | RC.RP |
| | Incident Recovery Communication | RC.CO |

## Table 2: Discussion Draft NIST Cybersecurity Framework 2.0 Core: Sample of Implementation Examples

This table shows the sample layout of the proposed new CSF 2.0 Core Implementation Examples column (a new fifth column, alongside the Functions, Categories, Subcategories, and (Online) Informative References). These are intended to provide notional implementation examples of concise, action-oriented steps to help achieve the outcomes of the CSF Subcategories in addition to the guidance provided in CSF Informative References. While this table currently showcases a few samples to encourage discussion about what this column might cover, the CSF 2.0 Core will provide such examples for each Subcategory.

As discussed in the CSF 2.0 Concept Paper, adding notional examples was suggested in the RFI responses and has been successfully leveraged in other NIST Frameworks such as the Secure Software Development Framework and the Artificial Intelligence Risk Management Framework Playbook. This small list of examples would not be a comprehensive list of all actions that could be taken by an organization to meet CSF outcomes, nor would they represent a baseline of required actions to address cybersecurity risks.

| CSF 2.0 Subcategory | CSF 2.0 Implementation Examples |
|---|---|
| **ID.RA-01:** Vulnerabilities in first-party and third-party assets are identified, validated, and recorded | • **Example 1**: Vulnerability scans are performed to identify unpatched and misconfigured software<br>• **Example 2**: Network and system architectures are assessed for design and implementation weaknesses affecting confidentiality, integrity, availability, and resilience<br>• **Example 3**: The authenticity and cybersecurity of critical technology products and services is assessed prior to acquisition and use<br>• **Example 4**: Software developed by the organization is reviewed, analyzed, or tested to identify vulnerabilities<br>• **Example 5**: Facilities housing critical computing assets are assessed for physical vulnerabilities<br>• … |
| **PR.PS-02:** Software is patched, updated, replaced, and removed commensurate with risk | • **Example 1**: Routine patching occurs in a phased deployment within the timeframe specified in the software maintenance plan<br>• **Example 2**: Container images are updated and new container instances are deployed to replace existing instances, instead of updating the existing instances<br>• **Example 3**: End-of-life software versions are replaced with supported, maintained versions<br>• **Example 4**: Unauthorized software posing undue risk is uninstalled and removed<br>• … |
| **DE.AE-07:** Contextual information (e.g., cyber threat intelligence, inventories, security advisories) is integrated into the adverse event analysis | • **Example 1**: Cyber threat intelligence feeds are securely provided to detection technologies, processes, and personnel<br>• **Example 2**: Information from asset inventories is securely provided to detection technologies, processes, and personnel |

| CSF 2.0 Subcategory | CSF 2.0 Implementation Examples |
|---|---|
| | • **Example 3**: Vulnerability disclosures from suppliers and vendors, and third-party security advisories for the organization's technologies, are rapidly acquired and analyzed upon release<br>• … |
| **DE.CM-09:** Computing hardware and software and their data are monitored to find adverse cybersecurity events | • **Example 1**: Email and web services are monitored to detect malware, phishing, data leaks and exfiltration, and other adverse events<br>• **Example 2**: Operating systems allow only authorized and integrity-verified software and software updates to be installed<br>• **Example 3**: Authentication attempts are monitored to identify attacks against credentials and unauthorized credential reuse<br>• **Example 4**: Software configurations are monitored for deviations from security baselines<br>• … |

## Table 3: Discussion Draft NIST Cybersecurity Framework 2.0 Core: Functions, Categories, and Subcategories

This Table shows the proposed CSF 2.0 Core Functions, Categories, and Subcategories (in red text). It also includes the CSF 1.1 Category and Subcategory text for comparison, as well as identifies when and where an outcome has been moved for traceability. A CSF 1.1 Subcategory may have been moved to one or more CSF 2.0 Subcategories. This table does not include CSF Informative References, or Implementation Examples as discussed in Table 2, that may be included in the full CSF 2.0 Core.

| | CSF 2.0 Category | CSF 1.1 Category | CSF 2.0 Subcategory | CSF 1.1 Subcategory |
|---|---|---|---|---|
| **CSF 2.0 Function - GOVERN (GV):** Establish and monitor organization risk management strategy, expectations, and policy. (formerly ID.GV, ID.RM) | | | | |
| | **Organizational Context (GV.OC):** The organization's risk context, including mission, mission priorities, stakeholders, objectives, and direction, is understood (formerly ID.BE) | Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions | **GV.OC-01**: Organizational mission is understood in order to prioritize cybersecurity risk management (formerly ID.BE-2 and ID.BE-3) | ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated<br>ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated |
| | | | **GV.OC-02:** Internal and external stakeholders, and their expectations regarding cybersecurity risk management, are determined | |
| | | | **GV.OC-03:** Legal, regulatory, and contractual requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed (formerly ID.GV-3) | ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed |
| | | | **GV.OC-04:** Critical objectives, capabilities, and services that stakeholders expect are determined and communicated (formerly ID.BE-4 and ID.BE-5) | ID.BE-4: Dependencies and critical functions for delivery of critical services are established<br>ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations) |

| | CSF 2.0 Category | CSF 1.1 Category | CSF 2.0 Subcategory | CSF 1.1 Subcategory |
|---|---|---|---|---|
| | | | **GV.OC-05:** Critical outcomes, capabilities, and services that the organization relies on are determined and communicated (formerly ID.BE-1 and ID.BE-4) | ID.BE-1: The organization's role in the supply chain is identified and communicated<br>ID.BE-4: Dependencies and critical functions for delivery of critical services are established |
| | **Risk Management Strategy (GV.RM):** The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established and used to support operational risk decisions (formerly ID.RM) | Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions | **GV.RM-01:** Cybersecurity risk management objectives are established and agreed to by organizational stakeholders (formerly ID.RM-1) | ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders |
| | | | **GV.RM-02:** Cybersecurity supply chain risk management strategy is established, agreed to by organizational stakeholders, and managed (formerly ID.SC-1) | ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders |
| | | | **GV.RM-03:** Risk appetite and risk tolerance statements are determined and communicated based on the organization's business environment (formerly ID.RM-2 and ID.RM-3) | ID.RM-2: Organizational risk tolerance is determined and clearly expressed<br>ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis |
| | | | **GV.RM-04:** Cybersecurity risk management is considered part of enterprise risk management (formerly ID.GV-4) | ID.GV-4: Governance and risk management processes address cybersecurity risks |
| | | | **GV.RM-05**: Strategic direction describing appropriate risk response options, including cybersecurity risk transfer mechanisms (e.g., insurance, outsourcing), investment in mitigations, and risk acceptance is established and communicated | |
| | | | **GV.RM-06:** Responsibility and accountability are determined and communicated for ensuring that the risk management strategy and program are resourced, implemented, assessed, and maintained | |

| | CSF 2.0 Category | CSF 1.1 Category | CSF 2.0 Subcategory | CSF 1.1 Subcategory |
|---|---|---|---|---|
| | | | **GV.RM-07:** Risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks | |
| | | | **GV.RM-08:** Effectiveness and adequacy of cybersecurity risk management strategy and results are assessed and reviewed by organizational leaders | |
| | **Roles and Responsibilities (GV.RR):** Cybersecurity roles and responsibilities are coordinated and aligned with all internal and external stakeholders to enable accountability, performance assessment, and continuous improvement (formerly ID.GV-2) | | **GV.RR-01:** Organizational leadership takes responsibility for decisions associated with cybersecurity risks and establishes a culture that is risk-aware, behaves in an ethical manner, and promotes continuous improvement | |
| | | | **GV.RR-02:** Roles and responsibilities related to cybersecurity risk management are established and communicated (formerly ID.GV-2, ID.AM-6, and DE.DP-1) | ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners<br>ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established<br>DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability |
| | | | **GV.RR-03:** Roles and responsibilities for customers, partners, and other third-party stakeholders are established and communicated (formerly ID.AM-6) | ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established |
| | | | **GV.RR-04:** Roles and responsibilities for suppliers are established, documented in contractual language, and communicated (formerly ID.AM-6) | ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established |

| | CSF 2.0 Category | CSF 1.1 Category | CSF 2.0 Subcategory | CSF 1.1 Subcategory |
|---|---|---|---|---|
| | | | **GV.RR-05:** Lines of communication across the organization are established for cybersecurity risks, including supply chain risks | |
| | | | **GV.RR-06:** Resourcing and authorities for cybersecurity are decided commensurate with risk strategy, roles, and policies | |
| | | | **GV.RR-07:** Cybersecurity is included in human resources practices (e.g., training, deprovisioning, personnel screening) (formerly PR.IP-11) | PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening) |
| | **Policies and Procedures (GV.PO):** Organizational cybersecurity policies, processes, and procedures are established and communicated (formerly ID.GV-1) | | **GV.PO-01:** Policies, processes, and procedures for managing cybersecurity risks are established based on organizational context, risk management strategy, and priorities and are communicated (formerly ID.GV-1) | ID.GV-1: Organizational cybersecurity policy is established and communicated |
| | | | **GV.PO-02:** The same policies used internally are applied to suppliers | |
| | | | **GV.PO-03:** Policies and procedures are reviewed, updated, and communicated to reflect changes in requirements, threats, technology, and organizational mission | |
| **CSF 2.0 Function - IDENTIFY** (ID): Determine the current cybersecurity risk to the organization. | | | | |
| | **Asset Management (ID.AM):** Assets (e.g., data, devices, software, systems, facilities, 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 | Asset Management (ID.AM): The data, personnel, devices, systems, and facilities 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 physical devices managed by the organization are maintained | ID.AM-1: Physical devices and systems within the organization are inventoried |
| | | | **ID.AM-02:** Inventories of software and services managed by the organization are maintained | ID.AM-2: Software platforms and applications within the organization are inventoried |
| | | | **ID.AM-03:** Representations of the organization's authorized network communication and network data flows are maintained (formerly ID.AM-3 and DE.AE-1) | ID.AM-3: Organizational communication and data flows are mapped<br>DE.AE-1: A baseline of network operations and expected data flows for |

| | CSF 2.0 Category | CSF 1.1 Category | CSF 2.0 Subcategory | CSF 1.1 Subcategory |
|---|---|---|---|---|
| | | | | users and systems is established and managed |
| | | | **ID.AM-04:** Inventories of external assets and suppliers are maintained | ID.AM-4: External information systems are catalogued |
| | | | **ID.AM-05:** Assets are prioritized based on classification, criticality, resources, and organizational value | ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value |
| | | | **ID.AM-06:** Dropped (moved to GV.RR-02, GV.RR-03, and GV.RR-04) | ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established |
| | | | **ID.AM-07:** Sensitive data and corresponding metadata are inventoried and tracked | |
| | | | **ID.AM-08:** Systems, devices, and software are managed throughout their life cycle, including pre-deployment checks, preventive maintenance, transfers, end-of-life, and disposition (formerly PR.DS-3, PR.IP-2, PR.MA-1, and PR.MA-2) | PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition<br>PR.IP-2: A System Development Life Cycle to manage systems is implemented<br>PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools<br>PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access |
| | **Business Environment (ID.BE):** Dropped (moved to GV.OC) | Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, | **ID.BE-01:** Dropped (moved to GV.OC-05) | ID.BE-1: The organization's role in the supply chain is identified and communicated |
| | | | **ID.BE-02:** Dropped (moved to GV.OC-01) | ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated |

| | CSF 2.0 Category | CSF 1.1 Category | CSF 2.0 Subcategory | CSF 1.1 Subcategory |
|---|---|---|---|---|
| | | responsibilities, and risk management decisions | **ID.BE-03:** Dropped (moved to GV.OC-01) | ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated |
| | | | **ID.BE-04:** Dropped (moved to GV.OC-04 and GV.OC-05) | ID.BE-4: Dependencies and critical functions for delivery of critical services are established |
| | | | **ID.BE-05:** Dropped (moved to GV.OC-04) | ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations) |
| | **Governance (ID.GV):** Dropped (moved to GV) | Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization’s regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk | **ID.GV-01:** Dropped (moved to GV.PO) | ID.GV-1: Organizational cybersecurity policy is established and communicated |
| | | | **ID.GV-02:** Dropped (moved to GV.RR-02) | ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners |
| | | | **ID.GV-03:** Dropped (moved to GV.OC-03) | ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed |
| | | | **ID.GV-04:** Dropped (moved to GV.RM-04) | ID.GV-4: Governance and risk management processes address cybersecurity risks |
| | **Risk Assessment (ID.RA):** The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals | Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals | **ID.RA-01:** Vulnerabilities in first-party and third-party assets are identified, validated, and recorded (formerly ID.RA-1 and DE.CM-8) | ID.RA-1: Asset vulnerabilities are identified and documented<br>DE.CM-8: Vulnerability scans are performed |
| | | | **ID.RA-02:** Cyber threat intelligence is received from information sharing forums and sources | ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources |
| | | | **ID.RA-03:** Threats, both internal and external, are identified and recorded | ID.RA-3: Threats, both internal and external, are identified and documented |

| | CSF 2.0 Category | CSF 1.1 Category | CSF 2.0 Subcategory | CSF 1.1 Subcategory |
|---|---|---|---|---|
| | | | **ID.RA-04:** Potential business impacts and likelihoods are identified and recorded | ID.RA-4: Potential business impacts and likelihoods are identified |
| | | | **ID.RA-05:** Threats, vulnerabilities, likelihoods, and impacts are used to determine exposure and inform risk prioritization | ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk |
| | | | **ID.RA-06:** Risk responses are chosen, prioritized, planned, tracked, and communicated (formerly ID.RA-6 and RS.MI-3) | ID.RA-6: Risk responses are identified and prioritized<br>RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks |
| | | | **ID.RA-07**: Changes are managed, assessed for risk impact, and recorded (formerly part of PR.IP-3) | PR.IP-3: Configuration change control processes are in place |
| | | | **ID.RA-08:** Risks associated with technology suppliers and their supplied products and services are identified, recorded, prioritized, and monitored (formerly ID.SC-2 and PR.DS-8) | ID.SC-2:-Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process<br>PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity |
| | | | **ID.RA-09:** Processes for receiving, analyzing, and responding to vulnerability disclosures are established (formerly RS.AN-5) | RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers) |
| | | | **ID.RA-10:** Exceptions to security measures are reviewed, tracked, and compensated for | |
| | **Risk Management Strategy (ID.RM):** Dropped (moved to GV.RM) | Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are | **ID.RM-01:** Dropped (moved to GV.RM-01) | ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders |
| | | | **ID.RM-02:** Dropped (moved to GV.RM-03) | ID.RM-2: Organizational risk tolerance is determined and clearly expressed |

| | CSF 2.0 Category | CSF 1.1 Category | CSF 2.0 Subcategory | CSF 1.1 Subcategory |
|---|---|---|---|---|
| | | established and used to support operational risk decisions. | **ID.RM-03:** Dropped (moved to GV.RM-03) | ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis |
| | **Supply Chain Risk Management (ID.SC):** The organization's supply chain risks are identified, assessed, and managed consistent with the organization's priorities, constraints, risk tolerances, and assumptions | Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks | **ID.SC-01:** Dropped (moved to GV.RM-02) | ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders |
| | | | **ID.SC-02:** Dropped (moved to ID.RA-08) | ID.SC-2:-Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process |
| | | | **ID.SC-03**: Cybersecurity requirements are integrated into contracts with suppliers and third-party partners | ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan. |
| | | | **ID.SC-04:** Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations | ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations. |
| | | | **ID.SC-05:** Dropped (moved to ID.IM-02) | ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers |
| | | | **ID.SC-06:** Supplier termination and transition processes include security considerations | |
| | **Improvement (ID.IM):** Improvements to organizational cybersecurity risk management processes and activities are identified | | **ID.IM-01:** Continuous evaluation, including through reviews, audits, and assessments (including self-assessments), is applied to identify opportunities for improvement across all Framework Functions | |

| | CSF 2.0 Category | CSF 1.1 Category | CSF 2.0 Subcategory | CSF 1.1 Subcategory |
|---|---|---|---|---|
| | | | **ID.IM-02:** Security tests and exercises, including in coordination with suppliers and third-party providers, are carried out to identify improvements (formerly ID.SC-5, PR.IP-10, and DE.DP-3) | ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers<br>PR.IP-10: Response and recovery plans are tested<br>DE.DP-3: Detection processes are tested |
| | | | **ID.IM-03:** Improvements for processes and activities across all Framework Functions are identified based on lessons learned (formerly PR.IP-7, PR.IP-8, DE.DP-5, RS.IM-1, RS.IM-2, and RC.IM-2) | PR.IP-7: Protection processes are improved<br>PR.IP-8: Effectiveness of protection technologies is shared<br>DE.DP-5: Detection processes are continuously improved<br>RS.IM-1: Response plans incorporate lessons learned<br>RS.IM-2: Response strategies are updated<br>RC.IM-2: Recovery strategies are updated |
| **CSF 2.0 Function - PROTECT (PR):** Use safeguards to sufficiently mitigate and reduce cybersecurity risk. | | | | |
| | **Identity Management, Authentication and Access Control (PR.AC):** Dropped (moved to PR.AA) | Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions | **PR.AC-01:** Dropped (moved to PR.AA-01 and PR.AA-06) | PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes |
| | | | **PR.AC-02:** Dropped (moved to PR.AA-07) | PR.AC-2: Physical access to assets is managed and protected |
| | | | **PR.AC-03:** Dropped (moved to PR.AA-03, PR.AA-05, PR.AA-06, and PR.IR-02) | PR.AC-3: Remote access is managed |
| | | | **PR.AC-04:** Dropped (moved to PR.AA-05) | PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties |
| | | | **PR.AC-05:** Dropped (moved to PR.IR-02) | PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation) |

| | CSF 2.0 Category | CSF 1.1 Category | CSF 2.0 Subcategory | CSF 1.1 Subcategory |
|---|---|---|---|---|
| | | | **PR.AC-06:** Dropped (moved to PR.AA-02) | PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions |
| | | | **PR.AC-07:** Dropped (moved to PR.AA-03) | PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks) |
| | **Identity Management, Authentication, and Access Control (PR.AA):** Access to physical and logical assets is limited to authorized users, processes, and devices, and is managed commensurate with the assessed risk of unauthorized access (formerly PR.AC) | Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions | **PR.AA-01:** Identities and credentials for authorized users, processes, and devices are managed by the organization (formerly PR.AC-1) | PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes |
| | | | **PR.AA-02:** Identities are proofed and bound to credentials based on the context of interactions (formerly PR.AC-6) | PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions |
| | | | **PR.AA-03:** Users, processes, and devices are authenticated (formerly PR.AC-3 and PR.AC-7) | PR.AC-3: Remote access is managed<br>PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks) |
| | | | **PR.AA-04:** Federated assertions are generated, protected, conveyed, and verified | |
| | | | **PR.AA-05:** Access permissions, entitlements, and authorizations are managed and enforced, incorporating the principles of least privilege and separation of duties (formerly PR.AC-3 and PR.AC-4) | PR.AC-3: Remote access is managed<br>PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties |
| | | | **PR.AA-06**: Account activities and access events are audited and monitored to enforce authorized access (formerly PR.AC-1 and PR.AC-3) | PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes<br>PR.AC-3: Remote access is managed |

| | CSF 2.0 Category | CSF 1.1 Category | CSF 2.0 Subcategory | CSF 1.1 Subcategory |
|---|---|---|---|---|
| | | | **PR.AA-07**: Physical access to assets is managed, monitored, and enforced (formerly PR.AC-2 and PR.PT-4) | PR.AC-2: Physical access to assets is managed and protected<br>PR.PT-4: Communications and control networks are protected |
| | **Awareness and Training (PR.AT):** The organization's personnel and third-parties are provided cybersecurity awareness and training to perform their cybersecurity-related tasks consistent with related policies, procedures, and agreements | Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements | **PR.AT-01:** Awareness and training are provided for users so they possess the knowledge and skills to perform relevant tasks (formerly PR.AT-1 and RS.CO-1) | PR.AT-1: All users are informed and trained<br>RS.CO-1: Personnel know their roles and order of operations when a response is needed |
| | | | **PR.AT-02:** Awareness and training are provided for users with elevated privileges so they possess the knowledge and skills to perform relevant tasks (formerly PR.AT-2 and PR.AT-5) | PR.AT-2: Privileged users understand their roles and responsibilities<br>PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities |
| | | | **PR.AT-03:** Awareness and training are provided for third parties with cybersecurity responsibilities (e.g., suppliers, partners, customers) so they possess the knowledge and skills to perform relevant tasks | PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities |
| | | | **PR.AT-04:** Awareness and training are provided to senior leaders so they possess the knowledge and skills to govern and lead a cybersecurity risk-aware culture | PR.AT-4: Senior executives understand their roles and responsibilities |
| | | | **PR.AT-05:** Dropped (moved to PR.AT-02) | PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities |
| | **Data Security (PR.DS):** Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information | Data Security (PR.DS): Information and records (data) are 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 is protected (formerly PR.DS-1, PR-DS.5, PR.DS-6, and PR.PT-2) | PR.DS-1: Data-at-rest is protected<br>PR.DS-5: Protections against data leaks are implemented<br>PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity<br>PR.PT-2: Removable media is protected and its use restricted according to policy |

| | CSF 2.0 Category | CSF 1.1 Category | CSF 2.0 Subcategory | CSF 1.1 Subcategory |
|---|---|---|---|---|
| | | | **PR.DS-02:** The confidentiality, integrity, and availability of data-in-transit is protected (formerly PR.DS-2, PR.DS-5) | PR.DS-2: Data-in-transit is protected<br>PR.DS-5: Protections against data leaks are implemented |
| | | | **PR.DS-03:** Dropped (moved to ID.AM-08) | PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition |
| | | | **PR.DS-04:** Dropped (moved to PR.IR-05) | PR.DS-4: Adequate capacity to ensure availability is maintained |
| | | | **PR.DS-05:** Dropped (moved to PR.DS-01, PR-DS-02, PR.DS-10) | PR.DS-5: Protections against data leaks are implemented |
| | | | **PR.DS-06:** Dropped (data portion moved to PR.DS-01, software portion moved to DE.CM-09) | PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity |
| | | | **PR.DS-07:** Dropped (moved to PR.IR-02) | PR.DS-7: The development and testing environment(s) are separate from the production environment |
| | | | **PR.DS-08:** Dropped (moved to ID.RA-08 and DE.CM-09) | PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity |
| | | | **PR.DS-09:** Data is managed throughout its life cycle, including discovery, maintenance, and destruction (formerly PR.IP-6) | PR.IP-6: Data is destroyed according to policy |
| | | | **PR.DS-10:** The confidentiality, integrity, and availability of data-in-use is protected (formerly PR.DS-5) | PR.DS-5: Protections against data leaks are implemented |
| | | | **PR.DS-11:** Backups of data are conducted, protected, maintained, and tested (formerly PR.IP-4) | PR.IP-4: Backups of information are conducted, maintained, and tested |
| | **Information Protection Processes and Procedures (PR.IP):** Dropped (moved to other Categories and Functions) | Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and | **PR.IP-01:** Dropped (moved to PR.PS-01) | PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality) |

| | CSF 2.0 Category | CSF 1.1 Category | CSF 2.0 Subcategory | CSF 1.1 Subcategory |
|---|---|---|---|---|
| | | coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets | **PR.IP-02:** Dropped (moved to ID.AM-08) | PR.IP-2: A System Development Life Cycle to manage systems is implemented |
| | | | **PR.IP-03:** Dropped (moved to PR.PS-01 and ID.RA-07) | PR.IP-3: Configuration change control processes are in place |
| | | | **PR.IP-04:** Dropped (moved to PR.DS-11) | PR.IP-4: Backups of information are conducted, maintained, and tested |
| | | | **PR.IP-05:** Dropped (moved to PR.IR-03) | PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met |
| | | | **PR.IP-06:** Dropped (moved to PR.DS-09) | PR.IP-6: Data is destroyed according to policy |
| | | | **PR.IP-07:** Dropped (moved to ID.IM-03) | PR.IP-7: Protection processes are improved |
| | | | **PR.IP-08:** Dropped (moved to ID.IM-03) | PR.IP-8: Effectiveness of protection technologies is shared |
| | | | **PR.IP-09:** Dropped (moved to PR.IR-01) | PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed |
| | | | **PR.IP-10:** Dropped (moved to ID.IM-02) | PR.IP-10: Response and recovery plans are tested |
| | | | **PR.IP-11:** Dropped (moved to GV.RR-07) | PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening) |
| | | | **PR.IP-12:** Dropped (moved to ID.RA-01 and PR.PS-02) | PR.IP-12: A vulnerability management plan is developed and implemented |
| | **Maintenance (PR.MA):** Dropped (moved to ID.AM-08) | Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures | **PR.MA-01:** Dropped (moved to ID.AM-08) | PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools |
| | | | **PR.MA-02:** Dropped (moved to ID.AM-08) | PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access |

| | CSF 2.0 Category | CSF 1.1 Category | CSF 2.0 Subcategory | CSF 1.1 Subcategory |
|---|---|---|---|---|
| | **Protective Technology (PR.PT):** Dropped (moved to other Protect Categories) | Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements | **PR.PT-01:** Dropped (moved to PR.PS-04) | PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy |
| | | | **PR.PT-02:** Dropped (moved to PR.PS-01 for restricting removable media use and PR.DS-01 for data at rest protection) | PR.PT-2: Removable media is protected and its use restricted according to policy |
| | | | **PR.PT-03:** Dropped (moved to PR.PS-01) | PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities |
| | | | **PR.PT-04:** Dropped (moved to PR.AA-07 and PR.IR-02) | PR.PT-4: Communications and control networks are protected |
| | | | **PR.PT-05:** Dropped (moved to PR.IR-04) | PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations |
| | **Platform Security (PR.PS):** The hardware and software (e.g., firmware, operating systems, applications) 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 (e.g., least functionality, least privilege) (formerly PR.IP-1, PR.IP-3, PR.PT-2, and PR.PT-3) | PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)<br>PR.IP-3: Configuration change control processes are in place<br>PR.PT-2: Removable media is protected and its use restricted according to policy<br>PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities |
| | | | **PR.PS-02:** Software is patched, updated, replaced, and removed commensurate with risk (formerly PR.IP-12) | PR.IP-12: A vulnerability management plan is developed and implemented |
| | | | **PR.PS-03:** Hardware is maintained, replaced, and removed commensurate with risk | |

| | CSF 2.0 Category | CSF 1.1 Category | CSF 2.0 Subcategory | CSF 1.1 Subcategory |
|---|---|---|---|---|
| | | | **PR.PS-04:** Log records are generated for cybersecurity events and made available for continuous monitoring (formerly PR.PT-1) | PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy |
| | | | **PR.PS-05:** Protective technologies are executed on or within platforms to stop unauthorized software execution | |
| | | | **PR.PS-06:** Backups of platform software are conducted, protected, maintained, and tested | |
| | | | **PR.PS-07:** Secure software development practices are integrated and their performance is monitored throughout the software development life cycle | |
| | | | **PR.PS-08:** Supply chain security practices are integrated and their performance is monitored throughout the technology product and service life cycle | |
| | **Technology Infrastructure Resilience (PR.IR):** Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, and availability, and organization resilience | | **PR.IR-01:** Response and recovery plans (e.g., incident response plan, business continuity plan, disaster recovery plan, contingency plan) are communicated and maintained (formerly PR.IP-9) | PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed |
| | | | **PR.IR-02:** The organization's networks and environments are protected from unauthorized logical access and usage (formerly PR.AC-3, PR.AC-5, PR.DS-7, and PR.PT-4) | PR.AC-3: Remote access is managed<br>PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)<br>PR.DS-7: The development and testing environment(s) are separate from the production environment<br>PR.PT-4: Communications and control networks are protected |
| | | | **PR.IR-03:** The organization's computing assets are protected from environmental threats (formerly PR.IP-5) | PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met |

| | CSF 2.0 Category | CSF 1.1 Category | CSF 2.0 Subcategory | CSF 1.1 Subcategory |
|---|---|---|---|---|
| | | | **PR.IR-04:** Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations (formerly PR.PT-5) | PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations |
| | | | **PR.IR-05:** Adequate resource capacity (e.g., storage, power, network bandwidth, computing) to ensure availability is maintained (formerly PR.DS-4) | PR.DS-4: Adequate capacity to ensure availability is maintained |
| **CSF 2.0 Function - DETECT (DE):** Find and analyze possible cybersecurity attacks and compromises. | | | | |
| | **Adverse Event Analysis (DE.AE):** Adverse cybersecurity events are analyzed to find and characterize possible attacks and compromises, unauthorized and inappropriate activities, protection deficiencies, and other activity with a potentially negative impact on cybersecurity | Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood | **DE.AE-01:** Dropped (moved to ID.AM-03) | DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed |
| | | | **DE.AE-02:** Adverse events are analyzed to find possible attacks and compromises | DE.AE-2: Detected events are analyzed to understand attack targets and methods |
| | | | **DE.AE-03:** Information on adverse events is correlated from multiple sources | DE.AE-3: Event data are collected and correlated from multiple sources and sensors |
| | | | **DE.AE-04:** The estimated impact and scope of adverse events is determined | DE.AE-4: Impact of events is determined |
| | | | **DE.AE-05:** Incident alert thresholds are established | DE.AE-5: Incident alert thresholds are established |
| | | | **DE.AE-06:** Information on adverse events is provided to cybersecurity and incident response tools and staff (formerly DE.DP-4) | DE.DP-4: Event detection information is communicated |
| | | | **DE.AE-07:** Contextual information (e.g., cyber threat intelligence, inventories, security advisories) is integrated into the adverse event analysis | |
| | | | **DE.AE-08:** Adverse cybersecurity events are categorized and potential incidents are escalated for triage | |

| | CSF 2.0 Category | CSF 1.1 Category | CSF 2.0 Subcategory | CSF 1.1 Subcategory |
|---|---|---|---|---|
| | **Continuous Monitoring (DE.CM):** Assets are monitored to find potential adverse cybersecurity events, including indicators of attacks and compromise, unauthorized and inappropriate activity, protection deficiencies and failures and other activity with a potentially negative impact on cybersecurity | Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures | **DE.CM-01:** Networks and network services are monitored to find adverse cybersecurity events (formerly DE.CM-1, DE.CM-4, DE.CM-5, and DE.CM-7) | DE.CM-1: The network is monitored to detect potential cybersecurity events<br>DE.CM-4: Malicious code is detected<br>DE.CM-5: Unauthorized mobile code is detected<br>DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed |
| | | | **DE.CM-02:** The physical environment is monitored to find adverse cybersecurity events | DE.CM-2: The physical environment is monitored to detect potential cybersecurity events |
| | | | **DE.CM-03**: Personnel activity and technology usage are monitored to find adverse cybersecurity events (formerly DE.CM-3 and DE.CM-7) | DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events<br>DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed |
| | | | **DE.CM-04:** Dropped (moved to DE.CM-01 and DE.CM-09) | DE.CM-4: Malicious code is detected |
| | | | **DE.CM-05:** Dropped (moved to DE.CM-01 and DE.CM-09) | DE.CM-5: Unauthorized mobile code is detected |
| | | | **DE.CM-06:** External service providers and the services they provide are monitored to find adverse cybersecurity events (formerly DE.CM-6 and DE.CM-7) | DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events<br>DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed |
| | | | **DE.CM-07:** Dropped (moved to DE.CM-01, DE.CM-03, DE.CM-06, and DE.CM-09) | DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed |
| | | | **DE.CM-08:** Dropped (moved to ID.RA-01) | DE.CM-8: Vulnerability scans are performed |
| | | | **DE.CM-09:** Computing hardware and software and their data are monitored to find adverse cybersecurity events (formerly | PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity |

| | CSF 2.0 Category | CSF 1.1 Category | CSF 2.0 Subcategory | CSF 1.1 Subcategory |
|---|---|---|---|---|
| | | | PR.DS-6, PR.DS-8, DE.CM-4, DE.CM-5, and DE.CM-7) | PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity<br>DE.CM-4: Malicious code is detected<br>DE.CM-5: Unauthorized mobile code is detected<br>DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed |
| | **Detection Processes (DE.DP):** Dropped (moved to other Categories and Functions) | Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events | **DE.DP-01:** Dropped (moved to GV.RR-02) | DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability |
| | | | **DE.DP-02:** Dropped | DE.DP-2: Detection activities comply with all applicable requirements |
| | | | **DE.DP-03:** Dropped (moved to ID.IM-02) | DE.DP-3: Detection processes are tested |
| | | | **DE.DP-04:** Dropped (moved to DE.AE-06) | DE.DP-4: Event detection information is communicated |
| | | | **DE.DP-05:** Dropped (moved to ID.IM-03) | DE.DP-5: Detection processes are continuously improved |
| **CSF 2.0 Function - RESPOND (RS):** Take action regarding a detected cybersecurity incident. | | | | |
| | **Response Planning (RS.RP):** Dropped (moved to RS.MA) | Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents | **RS.RP-01:** Dropped (moved to RS.MA-01) | RS.RP-1: Response plan is executed during or after an incident |
| | **Incident Management (RS.MA)**: Responses to detected cybersecurity incidents are managed (formerly RS.RP) | Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents | **RS.MA-01:** The incident response plan is executed (formerly RS.RP-1) | RS.RP-1: Response plan is executed during or after an incident |
| | | | **RS.MA-02:** Incident reports are triaged and validated (formerly RS.AN-1 and RS.AN-2) | RS.AN-1: Notifications from detection systems are investigated<br>RS.AN-2: The impact of the incident is understood |
| | | | **RS.MA-03:** Incidents are categorized and prioritized (formerly RS.AN-4 and RS.AN-2) | RS.AN-4: Incidents are categorized consistent with response plans |

| | CSF 2.0 Category | CSF 1.1 Category | CSF 2.0 Subcategory | CSF 1.1 Subcategory |
|---|---|---|---|---|
| 🟥 | | | | RS.AN-2: The impact of the incident is understood |
| | | | **RS.MA-04:** Incidents are escalated or elevated as needed (formerly RS.AN-2) | RS.AN-2: The impact of the incident is understood |
| | | | **RS.MA-05:** Criteria for initiating incident recovery defined and applied | |
| | **Incident Analysis (RS.AN):** Investigation is conducted to ensure effective response and support recovery activities | Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities | **RS.AN-01:** Dropped (moved to RS.MA-02) | RS.AN-1: Notifications from detection systems are investigated |
| | | | **RS.AN-02:** Dropped (moved to RS.MA-02, RS.MA-03, and RS.MA-04) | RS.AN-2: The impact of the incident is understood |
| | | | **RS.AN-03:** Analysis is performed to determine what has taken place during an incident and the root cause of the incident | RS.AN-3: Forensics are performed |
| | | | **RS.AN-04:** Dropped (moved to RS.MA-03) | RS.AN-4: Incidents are categorized consistent with response plans |
| | | | **RS.AN-05:** Dropped (moved to ID.RA-09) | RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers) |
| | | | **RS.AN-06:** Actions performed during an investigation are recorded and the record's integrity and provenance are preserved (formerly part of RS.AN-3) | RS.AN-3: Forensics are performed |
| | | | **RS.AN-07:** Incident data and metadata are collected and their integrity and provenance are preserved | |
| | | | **RS.AN-08**: Incident magnitude is estimated and validated | |
| | | | **RS.AN-09:** Incident status is tracked and validated | |

| | CSF 2.0 Category | CSF 1.1 Category | CSF 2.0 Subcategory | CSF 1.1 Subcategory |
|---|---|---|---|---|
| | **Incident Response Reporting and Communication (RS.CO):** Response activities are coordinated with internal and external stakeholders (e.g., external support from law enforcement agencies) | Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies) | **RS.CO-01:** Dropped (moved to PR.AT-01) | RS.CO-1: Personnel know their roles and order of operations when a response is needed |
| | | | **RS.CO-02:** Internal and external stakeholders are notified of incidents, as required by law, regulation, or policy | RS.CO-2: Incidents are reported consistent with established criteria |
| | | | **RS.CO-03:** Information is shared with designated internal and external stakeholders, as required by law, regulation, or policy | RS.CO-3: Information is shared consistent with response plans |
| | | | **RS.CO-04:** Escalation is coordinated with designated internal and external stakeholders, as required by law, regulation, or policy | RS.CO-4: Coordination with stakeholders occurs consistent with response plans |
| | | | **RS.CO-05:** Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness | RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness |
| | **Incident Mitigation (RS.MI):** Activities are performed to prevent expansion of an event and mitigate its effects | Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident | **RS.MI-01:** Incidents are contained | RS.MI-1: Incidents are contained |
| | | | **RS.MI-02:** Incidents are eradicated | RS.MI-2: Incidents are mitigated |
| | | | **RS.MI-03:** Dropped (moved to ID.RA-06) | RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks |
| | **Improvements (RS.IM):** Dropped (moved to ID.IM) | Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities | **RS.IM-01:** Dropped (moved to ID.IM-03) | RS.IM-1: Response plans incorporate lessons learned |
| | | | **RS.IM-02:** Dropped (moved to ID.IM-03) | RS.IM-2: Response strategies are updated |
| **CSF 2.0 Function - RECOVER (RC):** Restore assets and operations that were impacted by a cybersecurity incident. | | | | |
| | **Incident Recovery Plan Execution (RC.RP):** Restoration activities are | Recovery Planning (RC.RP): Recovery processes and | **RC.RP-01:** The incident recovery plan is executed | RC.RP-1: Recovery plan is executed during or after a cybersecurity incident |

| | CSF 2.0 Category | CSF 1.1 Category | CSF 2.0 Subcategory | CSF 1.1 Subcategory |
|---|---|---|---|---|
| 🟩 | planned and performed to ensure full operational availability of systems and services affected by cybersecurity incidents | procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents | **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 post-incident 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:** Criteria for determining the end of incident recovery are defined and applied, and incident-related documentation is completed | |
| | **Incident Recovery Communication (RC.CO):** Restoration activities are coordinated with internal and external parties (e.g., coordinating centers, Internet Service Providers, owners of attacking systems, victims, other computer security incident response teams, and vendors) | Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors | **RC.CO-01:** Public relations are managed | RC.CO-1: Public relations are managed |
| | | | **RC.CO-02:** Reputation is repaired after an incident | RC.CO-2: Reputation is repaired after an incident |
| | | | **RC.CO-03:** Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders | RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams |
| | **Improvements (RC.IM):** Dropped (moved to ID.IM) | Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities | **RC.IM-01:** Dropped (moved to ID.IM-03) | RC.IM-1: Recovery plans incorporate lessons learned |
| | | | **RC.IM-02:** Dropped (moved to ID.IM-03) | RC.IM-2: Recovery strategies are updated |