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

National Institute of Standards and Technology

Released August 8, 2023

Note to Reviewers

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

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

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

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

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

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

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

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

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

Category	Subcategory	Implementation Examples	Informative References
Organizational Context (GV.OC): The circumstances — mission, stakeholder expectations, and legal, regulatory, and contractual requirements — surrounding the organization's cybersecurity risk management decisions are understood (formerly ID.BE)			
	GV.OC-01: The organizational mission is understood and informs cybersecurity risk management (formerly ID.BE-02, ID.BE-03)	**Ex1:** Share the organization's mission (e.g., through vision and mission statements, marketing, and service strategies) to provide a basis for identifying risks that may impede that mission	
	GV.OC-02: Internal and external stakeholders are determined, and their needs and expectations regarding cybersecurity risk management are understood	**Ex1:** Identify relevant internal stakeholders and their cybersecurity-related expectations (e.g., performance and risk expectations of officers, directors, and advisors; cultural expectations of employees) **Ex2:** Identify relevant external stakeholders and their cybersecurity-related expectations (e.g., privacy expectations of	

Category	Subcategory	Implementation Examples	Informative References
		customers, business expectations of partnerships, compliance expectations of regulators, ethics expectations of society)	
	GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed (formerly ID.GV-03)	**Ex1:** Determine a process to track and manage legal and regulatory requirements regarding protection of individuals' information (e.g., Health Insurance Portability and Accountability Act, California Consumer Privacy Act, General Data Protection Regulation) **Ex2:** Determine a process to track and manage contractual requirements for cybersecurity management of supplier, customer, and partner information **Ex3:** Align the organization's cybersecurity strategy with legal, regulatory, and contractual requirements	
	GV.OC-04: Critical objectives, capabilities, and services that stakeholders depend on or expect from the organization are determined and communicated (formerly ID.BE-04, ID.BE-05)	**Ex1:** Establish criteria for determining the criticality of capabilities and services as viewed by internal and external stakeholders **Ex2:** Determine (e.g., from a business impact analysis) assets and business operations that are vital to achieving mission objectives and the potential impact of a loss (or partial loss) of such operations **Ex3:** Establish and communicate resilience objectives (e.g., recovery time objectives) for delivering critical capabilities and services in various operating states (e.g., under attack, during recovery, normal operation)	
	GV.OC-05: Outcomes, capabilities, and services that the organization depends on are determined and communicated (formerly ID.BE-01, ID.BE-04)	**Ex1:** Create an inventory of the organization's dependencies on external resources (e.g., facilities, cloud-based hosting providers) and their relationships to organizational assets and business functions **Ex2:** Identify and document external dependencies that are potential points of failure for the organization's critical capabilities and services	
Risk Management Strategy (GV.RM): The organization's priorities, constraints, risk tolerance and appetite statements,			

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

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

Category	Subcategory	Implementation Examples	Informative References
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)	**Ex1:** Establish a strategy that expresses the objectives of the cybersecurity supply chain risk management program **Ex2:** Develop the cybersecurity supply chain risk management program, including a plan (with milestones), policies, and procedures that guide implementation and improvement of the program, and share the policies and procedures with the organizational stakeholders **Ex3:** Develop and implement program processes based on the strategy, objectives, policies, and procedures that are agreed upon and performed by the organizational stakeholders **Ex4:** Establish a cross-organizational mechanism that ensures alignment between functions that contribute to cybersecurity supply chain risk management, such as cybersecurity, IT, legal, human resources, and engineering	
	GV.SC-02: Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally (formerly ID.AM-06)	**Ex1:** Identify one or more specific roles or positions that will be responsible and accountable for planning, resourcing, and executing cybersecurity supply chain risk management activities **Ex2:** Document cybersecurity supply chain risk management roles and responsibilities in policy **Ex3:** Create responsibility matrixes to document who will be responsible and accountable for cybersecurity supply chain risk management activities and how those teams and individuals will be consulted and informed **Ex4:** Include cybersecurity supply chain risk management responsibilities and performance requirements in personnel descriptions to ensure clarity and improve accountability **Ex5:** Document performance goals for personnel with cybersecurity risk management-specific responsibilities, and periodically measure them to demonstrate and improve performance **Ex6:** Develop roles and responsibilities for suppliers, customers, and business partners to address shared responsibilities for	

Category	Subcategory	Implementation Examples	Informative References
		applicable cybersecurity risks, and integrate them into organizational policies and applicable third-party agreements **Ex7:** Internally communicate cybersecurity supply chain risk management roles and responsibilities for third parties **Ex8:** Establish rules and protocols for information sharing and reporting processes between the organization and its suppliers	
	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)	**Ex1:** Identify areas of alignment and overlap with cybersecurity and enterprise risk management **Ex2:** Establish integrated control sets for cybersecurity risk management and cybersecurity supply chain risk management **Ex3:** Integrate cybersecurity supply chain risk management into improvement processes **Ex4:** Escalate material cybersecurity risks in supply chains to senior management, and address them at the enterprise risk management level	
	GV.SC-04: Suppliers are known and prioritized by criticality	**Ex1:** Develop criteria for supplier criticality based on, for example, the sensitivity of data processed or possessed by suppliers, the degree of access to the organization's systems, and the importance of the products or services to the organization's mission **Ex2:** Keep a record of all suppliers, and prioritize suppliers based on the criticality criteria	
	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)	**Ex1:** Establish security requirements for suppliers, products, and services commensurate with their criticality level and potential impact if compromised **Ex2:** Include all cybersecurity and supply chain requirements that third parties must follow and how compliance with the requirements may be verified in default contractual language **Ex3:** Define the rules and protocols for information sharing between the organization and its suppliers and sub-tier suppliers in contracts **Ex4:** Manage risk by including security requirements in contracts based on their criticality and potential impact if compromised	

Category	Subcategory	Implementation Examples	Informative References
		Ex5: Define security requirements in service-level agreements (SLAs) for monitoring suppliers for acceptable security performance throughout the supplier relationship lifecycle **Ex6:** Contractually require suppliers to disclose cybersecurity features, functions, and vulnerabilities of their products and services for the life of the product or the term of service **Ex7:** Contractually require suppliers to provide and maintain a current component inventory (e.g., software or hardware bill of materials) for critical products **Ex8:** Contractually require suppliers to vet their employees and guard against insider threats **Ex9:** Contractually require suppliers to provide evidence of performing acceptable security practices through, for example, self-attestation, conformance to known standards, certifications, or inspections **Ex10:** Specify in contracts the rights and responsibilities of the organization, its suppliers, and applicable lower-tier suppliers and supply chains, with respect to potential cybersecurity risks	
	GV.SC-06: Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships	**Ex1:** Perform thorough due diligence on prospective suppliers that is consistent with procurement planning and commensurate with the level of risk, criticality, and complexity of each supplier relationship **Ex2:** Assess the suitability of the technology and cybersecurity capabilities and the risk management practices of prospective suppliers **Ex3:** Conduct supplier risk assessments against business and applicable cybersecurity requirements, including lower-tier suppliers and the supply chain for critical suppliers **Ex4:** Assess the authenticity, integrity, and security of critical products prior to acquisition and use	
	GV.SC-07: The risks posed by a supplier, their products and services, and other third parties are identified, recorded, prioritized, assessed, responded	**Ex1:** Adjust assessment formats and frequencies based on the third party's reputation and the criticality of the products or services they provide	

Category	Subcategory	Implementation Examples	Informative References
	to, and monitored over the course of the relationship (formerly ID.SC-02, ID.SC-04)	**Ex2:** Evaluate third parties' evidence of compliance with contractual cybersecurity requirements, such as self-attestations, warranties, certifications, and other artifacts **Ex3:** Monitor critical suppliers to ensure that they are fulfilling their security obligations throughout the supplier relationship lifecycle using a variety of methods and techniques, such as inspections, audits, tests, or other forms of evaluation **Ex4:** Monitor critical suppliers, services, and products for changes to their risk profiles, and reevaluate supplier criticality and risk impact accordingly **Ex5:** Plan for unexpected supplier and supply chain-related interruptions to ensure business continuity	
	GV.SC-08: Relevant suppliers and other third parties are included in incident planning, response, and recovery activities (formerly ID.SC-05)	**Ex1:** Define and use rules and protocols for reporting incident response and recovery activities and the status between the organization and its suppliers **Ex2:** Identify and document the roles and responsibilities of the organization and its suppliers for incident response **Ex3:** Include critical suppliers in incident response exercises and simulations **Ex4:** Define and coordinate crisis communication methods and protocols between the organization and its critical suppliers **Ex5:** Conduct collaborative lessons learned sessions with critical suppliers	
	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	**Ex1:** Policies and procedures require provenance records for all acquired technology products and services **Ex2:** Periodically provide risk reporting to leaders about how acquired components are proven to be untampered and authentic. **Ex3:** Communicate regularly among cybersecurity risk managers and operations personnel about the need to acquire software patches, updates, and upgrades only from authenticated and trustworthy software providers **Ex4:** Review policies to ensure that they require approved supplier personnel to perform maintenance on supplier products	

Category	Subcategory	Implementation Examples	Informative References
		Ex5: Policies and procedure require checking upgrades to critical hardware for unauthorized changes	
	GV.SC-10: Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement	**Ex1:** Establish processes for terminating critical relationships under both normal and adverse circumstances **Ex2:** Define and implement plans for component end-of-life maintenance support and obsolescence **Ex3:** Verify that supplier access to organization resources is deactivated promptly when it is no longer needed **Ex4:** Verify that assets containing the organization's data are returned or properly disposed of in a timely, controlled, and safe manner **Ex5:** Develop and execute a plan for terminating or transitioning supplier relationships that takes supply chain security risk and resiliency into account **Ex6:** Mitigate risks to data and systems created by supplier termination **Ex7:** Manage data leakage risks associated with supplier termination	
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	**Ex1:** Leaders (e.g., directors) agree on their roles and responsibilities in developing, implementing, and assessing the organization's cybersecurity strategy **Ex2:** Share leaders' expectations regarding a secure and ethical culture, especially when current events present the opportunity to highlight positive or negative examples of cybersecurity risk management	

Category	Subcategory	Implementation Examples	Informative References
		Ex3: Leaders direct the CISO to maintain a comprehensive cybersecurity risk strategy and review and update it at least annually and after major events **Ex4:** Conduct reviews to ensure adequate authority and coordination among those responsible for managing cybersecurity risk	
	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)	**Ex1:** Document risk management roles and responsibilities in policy **Ex2:** Document who is responsible and accountable for cybersecurity risk management activities and how those teams and individuals are to be consulted and informed **Ex3:** Include cybersecurity responsibilities and performance requirements in personnel descriptions **Ex4:** Document performance goals for personnel with cybersecurity risk management responsibilities, and periodically measure performance to identify areas for improvement **Ex5:** Clearly articulate cybersecurity responsibilities within operations, risk functions, and internal audit functions	
	GV.RR-03: Adequate resources are allocated commensurate with cybersecurity risk strategy, roles and responsibilities, and policies	**Ex1:** Conduct periodic management reviews to ensure that those given cybersecurity risk management responsibilities have the necessary authority **Ex2:** Identify resource allocation and investment in line with risk tolerance and response **Ex3:** Provide adequate and sufficient people, process, and technical resources to support the cybersecurity strategy	
	GV.RR-04: Cybersecurity is included in human resources practices (formerly PR.IP-11)	**Ex1:** Integrate cybersecurity risk management considerations into human resources processes (e.g., personnel screening, onboarding, change notification, offboarding) **Ex2:** Consider cybersecurity knowledge to be a positive factor in hiring, training, and retention decisions **Ex3:** Conduct background checks prior to onboarding new personnel for sensitive roles	

Category	Subcategory	Implementation Examples	Informative References
		Ex4: Define and enforce obligations for personnel to be aware of, adhere to, and uphold security policies as they relate to their roles	
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)	**Ex1:** Create, disseminate, and maintain a risk management policy with statements of management intent, expectations, and direction **Ex2:** Periodically review policies and procedures to ensure that they align with risk management strategy objectives and priorities, as well as the high-level direction of the cybersecurity policy **Ex3:** Require approval from senior management on policies **Ex4:** Communicate cybersecurity risk management policies, procedures, and processes across the organization **Ex5:** Require personnel to acknowledge receipt of policies when first hired, annually, and whenever a policy is updated	
	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)	**Ex1:** Update policies based on periodic reviews of cybersecurity risk management results to ensure that policies and supporting processes adequately maintain risk at an acceptable level **Ex2:** Provide a timeline for reviewing changes to the organization's risk environment (e.g., changes in risk or in the organization's mission objectives), and communicate recommended policy updates **Ex3:** Update policies to reflect changes in legal and regulatory requirements **Ex4:** Update policies to reflect changes in technology (e.g., adoption of artificial intelligence) and changes to the business (e.g., acquisition of a new business, new contract requirements)	
Oversight (GV.OV): Results of organization-wide cybersecurity			

Category	Subcategory	Implementation Examples	Informative References
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	**Ex1:** Measure how well the risk management strategy and risk results have helped leaders make decisions and achieve organizational objectives **Ex2:** Examine whether cybersecurity risk strategies that impede operations or innovation should be adjusted	
	GV.OV-02: The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks	**Ex1:** Review audit findings to confirm whether the existing cybersecurity strategy has ensured compliance with internal and external requirements **Ex2:** Review the performance oversight of those in cybersecurity-related roles to determine whether policy changes are necessary **Ex3:** Review strategy in light of cybersecurity incidents	
	GV.OV-03: Organizational cybersecurity risk management performance is measured and reviewed to confirm and adjust strategic direction	**Ex1:** Review key performance indicators (KPIs) to ensure that organization-wide policies and procedures achieve objectives **Ex2:** Review key risk indicators (KRIs) to identify risks the organization faces, including likelihood and potential impact **Ex3:** Collect and communicate metrics on cybersecurity risk management with senior leadership	

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

Category	Subcategory	Implementation Examples	Informative References
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			

Category	Subcategory	Implementation Examples	Informative References
relative importance to organizational objectives and the organization's risk strategy			
	ID.AM-01: Inventories of hardware managed by the organization are maintained	**Ex1:** Maintain inventories for all types of hardware, including IT, IoT, OT, and mobile devices **Ex2:** Constantly monitor networks to detect new hardware and automatically update inventories	
	ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained	**Ex1:** Maintain inventories for all types of software and services, including commercial-off-the-shelf, open-source, custom applications, API services, and cloud-based applications and services **Ex2:** Constantly monitor all platforms, including containers and virtual machines, for software and service inventory changes **Ex3:** Maintain an inventory of the organization's systems	
	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)	**Ex1:** Maintain baselines of communication and data flows within the organization's wired and wireless networks **Ex2:** Maintain baselines of communication and data flows between the organization and third parties **Ex3:** Maintain documentation of expected network ports, protocols, and services that are typically used among authorized systems	
	ID.AM-04: Inventories of services provided by suppliers are maintained	**Ex1:** Inventory all external services used by the organization, including third-party infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS) offerings; APIs; and other externally hosted application services **Ex2:** Update the inventory when a new external service is going to be utilized to ensure adequate cybersecurity risk management monitoring of the organization's use of that service	
	ID.AM-05: Assets are prioritized based on classification, criticality, resources, and impact on the mission	**Ex1:** Define criteria for prioritizing each class of assets **Ex2:** Apply the prioritization criteria to assets **Ex3:** Track the asset priorities and update them periodically or when significant changes to the organization occur	

Category	Subcategory	Implementation Examples	Informative References
	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	**Ex1:** Maintain a list of the designated data types of interest (e.g., personally identifiable information, protected health information, financial account numbers, organization intellectual property) **Ex2:** Continuously discover and analyze ad hoc data to identify new instances of designated data types **Ex3:** Assign data classifications to designated data types through tags or labels **Ex4:** Track the provenance, data owner, and geolocation of each instance of designated data types	
	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)	**Ex1:** Integrate cybersecurity considerations throughout the life cycles of systems, hardware, software, and services **Ex2:** Integrate cybersecurity considerations into product life cycles **Ex3:** Identify unofficial uses of technology to meet mission objectives (i.e., "shadow IT") **Ex4:** Identify redundant systems, hardware, software, and services that unnecessarily increase the organization's attack surface **Ex5:** Properly configure and secure systems, hardware, software, and services prior to their deployment in production **Ex6:** Update inventories when systems, hardware, software, and services are moved or transferred within the organization	
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)		

Category	Subcategory	Implementation Examples	Informative References
	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)		
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)	**Ex1:** Use vulnerability management technologies to identify unpatched and misconfigured software **Ex2:** Assess network and system architectures for design and implementation weaknesses that affect cybersecurity **Ex3:** Review, analyze, or test organization-developed software to identify design, coding, and default configuration vulnerabilities **Ex4:** Assess facilities that house critical computing assets for physical vulnerabilities and resilience issues **Ex5:** Monitor sources of cyber threat intelligence for information on new vulnerabilities in products and services	
	ID.RA-02: Cyber threat intelligence is received from information sharing forums and sources	**Ex1:** Configure cybersecurity tools and technologies with detection or response capabilities to securely ingest cyber threat intelligence feeds **Ex2:** Receive and review advisories from reputable third parties on current threat actors and their tactics, techniques, and procedures (TTPs) **Ex3:** Monitor sources of cyber threat intelligence for information on the types of vulnerabilities that emerging technologies may have	

Category	Subcategory	Implementation Examples	Informative References
	ID.RA-03: Internal and external threats to the organization are identified and recorded	**Ex1:** Use cyber threat intelligence to maintain awareness of the types of threat actors likely to target the organization and the TTPs they are likely to use **Ex2:** Perform threat hunting to look for signs of threat actors within the environment **Ex3:** Implement processes for identifying internal threat actors	
	ID.RA-04: Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded	**Ex1:** Business leaders and cybersecurity risk management practitioners work together to estimate the likelihood and impact of risk scenarios and record them in risk registers **Ex2:** Enumerate the potential business impacts of unauthorized access to the organization's communications, systems, and data processed in or by those systems **Ex3:** Account for the potential impacts of cascading failures for systems of systems	
	ID.RA-05: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk and inform risk prioritization	**Ex1:** Develop threat models to better understand risks to the data and identify appropriate risk responses **Ex2:** Prioritize cybersecurity resource allocations and investments based on estimated likelihoods and impacts	
	ID.RA-06: Risk responses are chosen from the available options, prioritized, planned, tracked, and communicated (formerly ID.RA-06, RS.MI-03)	**Ex1:** Apply the vulnerability management plan's criteria for deciding whether to accept, transfer, mitigate, or avoid risk **Ex2:** Apply the vulnerability management plan's criteria for selecting compensating controls to mitigate risk **Ex3:** Track the progress of risk response implementation (e.g., plan of action and milestones [POA&M], risk register) **Ex4:** Use risk assessment findings to inform risk response decisions and actions **Ex5:** Communicate planned risk responses to affected stakeholders in priority order	
	ID.RA-07: Changes and exceptions are managed, assessed for risk impact, recorded, and tracked (formerly part of PR.IP-03)	**Ex1:** Implement and follow procedures for the formal documentation, review, testing, and approval of proposed changes and requested exceptions	

Category	Subcategory	Implementation Examples	Informative References
		Ex2: Document the possible risks of making or not making each proposed change, and provide guidance on rolling back changes **Ex3:** Document the risks related to each requested exception and the plan for responding to those risks **Ex4:** Periodically review risks that were accepted based upon planned future actions or milestones	
	ID.RA-08: Processes for receiving, analyzing, and responding to vulnerability disclosures are established (formerly RS.AN-05)	**Ex1:** Conduct vulnerability information sharing between the organization and its suppliers following the rules and protocols defined in contracts **Ex2:** Assign responsibilities and verify the execution of procedures for processing, analyzing the impact of, and responding to cybersecurity threat, vulnerability, or incident disclosures by suppliers, customers, partners, and government cybersecurity organizations	
	ID.RA-09: The authenticity and integrity of hardware and software are assessed prior to acquisition and use (formerly PR.DS-08)	**Ex1:** Assess the authenticity and cybersecurity of critical technology products and services prior to acquisition and use	
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)		

Category	Subcategory	Implementation Examples	Informative References
	ID.SC-05: Dropped (moved to GV.SC-08, ID.IM-02)		
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	**Ex1:** Perform self-assessments of critical services that take current threats and TTPs into consideration **Ex2:** Invest in third-party assessments or independent audits of the effectiveness of the organization's cybersecurity program to identify areas that need improvement **Ex3:** Constantly evaluate compliance with selected cybersecurity requirements through automated means	
	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)	**Ex1:** Identify improvements for future incident response activities based on findings from incident response assessments (e.g., tabletop exercises and simulations, tests, internal reviews, independent audits) **Ex2:** Identify improvements for future business continuity, disaster recovery, and incident response activities based on exercises performed in coordination with critical service providers and product suppliers **Ex3:** Involve internal stakeholders (e.g., senior executives, legal department, HR) in security tests and exercises as appropriate **Ex4:** Perform penetration testing to identify opportunities to improve the security posture of selected high-risk systems **Ex5:** Exercise contingency plans for responding to and recovering from the discovery that products or services did not originate with the contracted supplier or partner or were altered before receipt **Ex6:** Collect and analyze performance metrics using security tools and services to inform improvements to the cybersecurity program	
	ID.IM-03: Lessons learned during execution of operational processes, procedures, and activities are	**Ex1:** Conduct collaborative lessons learned sessions with suppliers	

Category	Subcategory	Implementation Examples	Informative References
	used to identify improvements (formerly PR.IP-07, PR.IP-08, DE.DP-05, RS.IM-01, RS.IM-02, RC.IM-01, RC.IM-02)	**Ex2:** Annually review cybersecurity policies, processes, and procedures to take lessons learned into account **Ex3:** Use metrics to assess operational cybersecurity performance over time	
	ID.IM-04: Cybersecurity plans that affect operations are communicated, maintained, and improved (formerly PR.IP-09)	**Ex1:** Establish contingency plans (e.g., incident response, business continuity, disaster recovery) for responding to and recovering from adverse events that can interfere with operations, expose confidential information, or otherwise endanger the organization's mission and viability **Ex2:** Include contact and communication information, processes for handling common scenarios, and criteria for prioritization, escalation, and elevation in all contingency plans **Ex3:** Create a vulnerability management plan to identify and assess all types of vulnerabilities and to prioritize, test, and implement risk responses **Ex4:** Communicate cybersecurity plans (including updates) to those responsible for carrying them out and to affected parties **Ex5:** Review and update all cybersecurity plans annually or when a need for significant improvements is identified	

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

Category	Subcategory	Implementation Examples	Informative References
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)			

Category	Subcategory	Implementation Examples	Informative References
	PR.AA-01: Identities and credentials for authorized users, services, and hardware are managed by the organization (formerly PR.AC-01)	**Ex1:** Initiate requests for new access or additional access for employees, contractors, and others, and track, review, and fulfill the requests, with permission from system or data owners when needed **Ex2:** Issue, manage, and revoke cryptographic certificates and identity tokens, cryptographic keys (i.e., key management), and other credentials **Ex3:** Select a unique identifier for each device from immutable hardware characteristics or an identifier securely provisioned to the device **Ex4:** Physically label authorized hardware with an identifier for inventory and servicing purposes	
	PR.AA-02: Identities are proofed and bound to credentials based on the context of interactions (formerly PR.AC-06)	**Ex1:** Verify a person's claimed identity at enrollment time using government-issued identity credentials (e.g., passport, visa, driver's license) **Ex2:** Issue credentials only to individuals (i.e., no credential sharing)	
	PR.AA-03: Users, services, and hardware are authenticated (formerly PR.AC-03, PR.AC-07)	**Ex1:** Require multifactor authentication **Ex2:** Enforce policies for the minimum strength of passwords, PINs, and similar authenticators **Ex3:** Periodically reauthenticate users, services, and hardware based on risk (e.g., in zero trust architectures)	
	PR.AA-04: Identity assertions are protected, conveyed, and verified	**Ex1:** Protect identity assertions that are used to convey authentication and user information through single sign-on systems **Ex2:** Protect identity assertions that are used to convey authentication and user information between federated systems **Ex3:** Implement standards-based approaches for identity assertions in all contexts, and follow all guidance for the generation (e.g., data models, metadata), protection (e.g., digital signing, encryption), and verification (e.g., signature validation) of identity assertions	

Category	Subcategory	Implementation Examples	Informative References
	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)	**Ex1:** Review logical and physical access privileges periodically and whenever someone changes roles or leaves the organization, and promptly rescind privileges that are no longer needed **Ex2:** Take attributes of the requester and the requested resource into account for authorization decisions (e.g., geolocation, day/time, requester endpoint's cyber health) **Ex3:** Restrict access and privileges to the minimum necessary (e.g., zero trust architecture) **Ex4:** Periodically review the privileges associated with critical business functions to confirm proper separation of duties	
	PR.AA-06: Physical access to assets is managed, monitored, and enforced commensurate with risk (formerly PR.AC-02, PR.PT-04)	**Ex1:** Use security guards, security cameras, locked entrances, alarm systems, and other physical controls to monitor facilities and restrict access **Ex2:** Employ additional physical security controls for areas that contain high-risk assets **Ex3:** Escort guests, vendors, and other third parties within areas that contain business-critical assets	
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)		
	PR.AC-07: Dropped (moved to PR.AA-03)		

Category	Subcategory	Implementation Examples	Informative References
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)	**Ex1:** Provide basic cybersecurity awareness and training to employees, contractors, partners, suppliers, and all other users of the organization's non-public resources **Ex2:** Train users to recognize social engineering attempts and other common attacks, report attacks and suspicious activity, comply with acceptable use policies, and perform basic cyber hygiene tasks (e.g., patching software, choosing passwords, protecting credentials) **Ex3:** Explain the consequences of cybersecurity policy violations, both to individual users and the organization as a whole **Ex4:** Periodically assess or test users on their understanding of basic cybersecurity practices **Ex5:** Require annual refreshers to reinforce existing practices and introduce new practices	
	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)	**Ex1:** Identify the specialized roles within the organization that require additional cybersecurity training, such as physical and cybersecurity personnel, finance personnel, senior leadership, and anyone with access to business-critical data **Ex2:** Provide role-based cybersecurity awareness and training to all those in specialized roles, including contractors, partners, suppliers, and other third parties **Ex3:** Periodically assess or test users on their understanding of cybersecurity practices for their specialized roles **Ex4:** Require annual refreshers to reinforce existing practices and introduce new practices	
	PR.AT-03: Dropped (moved to PR.AT-01, PR.AT-02)		
	PR.AT-04: Dropped (moved to PR.AT-02)		

Category	Subcategory	Implementation Examples	Informative References
	PR.AT-05: Dropped (moved to PR.AT-02)		
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)	**Ex1:** Use encryption, digital signatures, and cryptographic hashes to protect the confidentiality and integrity of stored data in files, databases, virtual machine disk images, container images, and other resources **Ex2:** Use full disk encryption to protect data stored on user endpoints **Ex3:** Confirm the integrity of software by validating signatures **Ex4:** Restrict the use of removable media to prevent data exfiltration **Ex5:** Physically secure removable media containing unencrypted sensitive information, such as within locked offices or file cabinets	
	PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected (formerly PR.DS-02, PR.DS-05)	**Ex1:** Use encryption, digital signatures, and cryptographic hashes to protect the confidentiality and integrity of network communications **Ex2:** Automatically encrypt or block outbound emails and other communications that contain sensitive data, depending on the data classification **Ex3:** Block access to personal email, file sharing, file storage services, and other personal communications applications and services from organizational systems and networks **Ex4:** Prevent reuse of sensitive data from production environments (e.g., customer records) in development, testing, and other non-production environments	
	PR.DS-03: Dropped (moved to ID.AM-08)		
	PR.DS-04: Dropped (moved to PR.IR-04)		

Category	Subcategory	Implementation Examples	Informative References
	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)	**Ex1:** Securely destroy stored data based on the organization's data retention policy using the prescribed destruction method **Ex2:** Securely sanitize data storage when hardware is being retired, decommissioned, reassigned, or sent for repairs or replacement **Ex3:** Offer methods for destroying paper, storage media, and other physical forms of data storage	
	PR.DS-10: The confidentiality, integrity, and availability of data-in-use are protected (formerly PR.DS-05)	**Ex1:** Remove data that must remain confidential (e.g., from processors and memory) as soon as it is no longer needed **Ex2:** Protect data in use from access by other users and processes of the same platform	
	PR.DS-11: Backups of data are created, protected, maintained, and tested (formerly PR.IP-04)	**Ex1:** Continuously back up critical data in near-real-time, and back up other data frequently at agreed-upon schedules **Ex2:** Test backups and restores for all types of data sources at least annually **Ex3:** Securely store some backups offline and offsite so that an incident or disaster will not damage them **Ex4:** Enforce geolocation restrictions for data backup storage	
Information Protection Processes and Procedures (PR.IP): Dropped (moved to other Categories and Functions)			
	PR.IP-01: Dropped (moved to PR.PS-01)		

Category	Subcategory	Implementation Examples	Informative References
	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)		
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-03: Dropped (moved to PR.PS-01)		
	PR.PT-04: Dropped (moved to PR.AA-07, PR.IR-01)		
	PR.PT-05: Dropped (moved to PR.IR-04)		

Category	Subcategory	Implementation Examples	Informative References
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)	**Ex1:** Establish, test, deploy, and maintain hardened baselines that enforce the organization's cybersecurity policies and provide only essential capabilities (i.e., principle of least functionality) **Ex2:** Review all default configuration settings that may potentially impact cybersecurity when installing or upgrading software	
	PR.PS-02: Software is maintained, replaced, and removed commensurate with risk (formerly PR.IP-12, PR.MA-02)	**Ex1:** Perform routine and emergency patching within the timeframes specified in the vulnerability management plan **Ex2:** Update container images, and deploy new container instances to replace rather than update existing instances **Ex3:** Replace end-of-life software and service versions with supported, maintained versions **Ex4:** Uninstall and remove unauthorized software and services that pose undue risks **Ex5:** Uninstall and remove any unnecessary software components (e.g., operating system utilities) that attackers might misuse **Ex6:** Define and implement plans for software and service end-of-life maintenance support and obsolescence	
	PR.PS-03: Hardware is maintained, replaced, and removed commensurate with risk (formerly PR.MA-01)	**Ex1:** Replace hardware when it lacks needed security capabilities or when it cannot support software with needed security capabilities **Ex2:** Define and implement plans for hardware end-of-life maintenance support and obsolescence **Ex3:** Perform hardware disposal in a secure, responsible, and auditable manner	

Category	Subcategory	Implementation Examples	Informative References
	PR.PS-04: Log records are generated and made available for continuous monitoring (formerly PR.PT-01)	**Ex1:** Configure all operating systems, applications, and services (including cloud-based services) to generate log records **Ex2:** Configure log generators to securely share their logs with the organization's logging infrastructure systems and services **Ex3:** Configure log generators to record the data needed by zero-trust architectures	
	PR.PS-05: Installation and execution of unauthorized software are prevented	**Ex1:** When risk warrants it, restrict software execution to permitted products only or deny the execution of prohibited and unauthorized software **Ex2:** Verify the source of new software and the software's integrity before installing it **Ex3:** Configure platforms to use only approved DNS services that block access to known malicious domains **Ex4:** Configure platforms to allow the installation of organization-approved software only	
	PR.PS-06: Secure software development practices are integrated and their performance is monitored throughout the software development life cycle	**Ex1:** Protect all components of organization-developed software from tampering and unauthorized access **Ex2:** Secure all software produced by the organization, with minimal vulnerabilities in their releases **Ex3:** Maintain the software used in production environments, and securely dispose of software once it is no longer needed	
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)	**Ex1:** Logically segment organization networks and cloud-based platforms according to trust boundaries and platform types (e.g., IT, IoT, OT, mobile, guests), and permit required communications only between segments	

Category	Subcategory	Implementation Examples	Informative References
		Ex2: Logically segment organization networks from external networks, and permit only necessary communications to enter the organization's networks from the external networks **Ex3:** Implement zero trust architectures to restrict network access to each resource to the minimum necessary **Ex4:** Check the cyber health of endpoints before allowing them to access and use production resources	
	PR.IR-02: The organization's technology assets are protected from environmental threats (formerly PR.IP-05)	**Ex1:** Protect organizational equipment from known environmental threats, such as flooding, fire, wind, and excessive heat and humidity **Ex2:** Include protection from environmental threats and provisions for adequate operating infrastructure in requirements for service providers that operate systems on the organization's behalf	
	PR.IR-03: Mechanisms are implemented to achieve resilience requirements in normal and adverse situations (formerly PR.PT-05)	**Ex1:** Avoid single points of failure in systems and infrastructure **Ex2:** Use load balancing to increase capacity and improve reliability **Ex3:** Use high-availability components like redundant storage and power suppliers to improve system reliability	
	PR.IR-04: Adequate resource capacity to ensure availability is maintained (formerly PR.DS-04)	**Ex1:** Monitor usage of storage, power, compute, network bandwidth, and other resources **Ex2:** Forecast future needs, and scale resources accordingly	

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

Category	Subcategory	Implementation Examples	Informative References
Continuous Monitoring (DE.CM): Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events			

Category	Subcategory	Implementation Examples	Informative References
	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)	**Ex1:** Monitor DNS, BGP, and other network services for adverse events **Ex2:** Monitor wired and wireless networks for connections from unauthorized endpoints **Ex3:** Monitor facilities for unauthorized or rogue wireless networks **Ex4:** Compare actual network flows against baselines to detect deviations **Ex5:** Monitor network communications to identify changes in security postures for zero trust purposes	
	DE.CM-02: The physical environment is monitored to find potentially adverse events	**Ex1:** Monitor logs from physical access control systems (e.g., badge readers) to find unusual access patterns (e.g., deviations from the norm) and failed access attempts **Ex2:** Review and monitor physical access records (e.g., from visitor registration, sign-in sheets) **Ex3:** Monitor physical access controls (e.g., door locks, latches, hinge pins) for signs of tampering **Ex4:** Monitor the physical environment using alarm systems, cameras, and security guards	
	DE.CM-03: Personnel activity and technology usage are monitored to find potentially adverse events (formerly DE.CM-03, DE.CM-07)	**Ex1:** Use behavior analytics software to detect anomalous user activity to mitigate insider threats **Ex2:** Monitor logs from logical access control systems to find unusual access patterns and failed access attempts **Ex3:** Continuously monitor deception technology, including user accounts, for any usage	
	DE.CM-04: Dropped (moved to DE.CM-01, DE.CM-09)		
	DE.CM-05: Dropped (moved to DE.CM-01, DE.CM-09)		
	DE.CM-06: External service provider activities and services are monitored to find potentially adverse events (formerly DE.CM-06, DE.CM-07)	**Ex1:** Monitor remote administration and maintenance activities that external providers perform on organizational systems	

Category	Subcategory	Implementation Examples	Informative References
		Ex2: Monitor cloud-based services, internet service providers, and other service providers for deviations from expected behavior	
	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)	**Ex1:** Monitor email, web, file sharing, collaboration services, and other common attack vectors to detect malware, phishing, data leaks and exfiltration, and other adverse events **Ex2:** Monitor authentication attempts to identify attacks against credentials and unauthorized credential reuse **Ex3:** Monitor software configurations for deviations from security baselines **Ex4:** Use technologies with a presence on endpoints to detect cyber health issues (e.g., missing patches, malware infections, unauthorized software), and redirect the endpoints to a remediation environment before access is authorized	
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	**Ex1:** Use security information and event management (SIEM) or other tools to continuously monitor log events for known malicious and suspicious activity **Ex2:** Utilize up-to-date cyber threat intelligence in log analysis tools to improve detection accuracy and characterize threat actors, their methods, and indicators of compromise	

Category	Subcategory	Implementation Examples	Informative References
		Ex3: Regularly conduct manual reviews of log events for technologies that cannot be sufficiently monitored through automation **Ex4:** Use log analysis tools to generate reports on their findings	
	DE.AE-03: Information is correlated from multiple sources	**Ex1:** Constantly transfer log data generated by other sources to a relatively small number of log servers **Ex2:** Use event correlation technology (e.g., SIEM) to collect information captured by multiple sources **Ex3:** Utilize cyber threat intelligence to help correlate events among log sources	
	DE.AE-04: The estimated impact and scope of adverse events are determined	**Ex1:** Use SIEMs or other tools to estimate impact and scope, and review and refine the estimates **Ex2:** A person creates their own estimates of impact and scope	
	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)	**Ex1:** Use cybersecurity software to generate alerts and provide them to the security operations center (SOC), incident responders, and incident response tools **Ex2:** Incident responders and other authorized personnel can access log analysis findings at all times **Ex3:** Automatically create and assign tickets in the organization's ticketing system when certain types of alerts occur **Ex4:** Manually create and assign tickets in the organization's ticketing system when technical staff discover indicators of compromise	
	DE.AE-07: Cyber threat intelligence and other contextual information are integrated into the analysis	**Ex1:** Securely provide cyber threat intelligence feeds to detection technologies, processes, and personnel **Ex2:** Securely provide information from asset inventories to detection technologies, processes, and personnel **Ex3:** Rapidly acquire and analyze vulnerability disclosures for the organization's technologies from suppliers, vendors, and third-party security advisories	

Category	Subcategory	Implementation Examples	Informative References
	DE.AE-08: Incidents are declared when adverse events meet the defined incident criteria (formerly DE.AE-05)	**Ex1:** Apply incident criteria to known and assumed characteristics of activity in order to determine whether an incident should be declared **Ex2:** Take known false positives into account when applying incident criteria	
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)		

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

Category	Subcategory	Implementation Examples	Informative References
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)	**Ex1:** Detection technologies automatically report confirmed incidents **Ex2:** Request incident response assistance from the organization's incident response outsourcer	

Category	Subcategory	Implementation Examples	Informative References
		Ex3: Designate an incident lead for each incident	
	RS.MA-02: Incident reports are triaged and validated (formerly RS.AN-01, RS.AN-02)	**Ex1:** Preliminarily review incident reports to confirm that they are cybersecurity-related and necessitate incident response activities **Ex2:** Apply criteria to estimate the severity of an incident	
	RS.MA-03: Incidents are categorized and prioritized (formerly RS.AN-04, RS.AN-02)	**Ex1:** Further review and categorize incidents based on the type of incident (e.g., data breach, ransomware, DDoS, account compromise) **Ex2:** Prioritize incidents based on their scope, likely impact, and time-critical nature **Ex3:** Select incident response strategies for active incidents by balancing the need to quickly recover from an incident with the need to observe the attacker or conduct a more thorough investigation	
	RS.MA-04: Incidents are escalated or elevated as needed (formerly RS.AN-02, RS.CO-04)	**Ex1:** Track and validate the status of all ongoing incidents **Ex2:** Coordinate incident escalation or elevation with designated internal and external stakeholders	
	RS.MA-05: The criteria for initiating incident recovery are applied	**Ex1:** Apply incident recovery criteria to known and assumed characteristics of the incident to determine whether incident recovery processes should be initiated **Ex2:** Take the possible operational disruption of incident recovery activities into account	
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)		

Category	Subcategory	Implementation Examples	Informative References
	RS.AN-03: Analysis is performed to determine what has taken place during an incident and the root cause of the incident	**Ex1:** Determine the sequence of events that occurred during the incident and which assets and resources were involved in each event **Ex2:** Attempt to determine what vulnerabilities, threats, and threat actors were directly or indirectly involved in the incident **Ex3:** Analyze the incident to find the underlying, systemic root causes **Ex4:** Check any cyber deception technology for additional information on attacker behavior	
	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)	**Ex1:** Require each incident responder and others (e.g., system administrators, cybersecurity engineers) who perform incident response tasks to record their actions and make the record immutable **Ex2:** Require the incident lead to document the incident in detail and be responsible for preserving the integrity of the documentation and the sources of all information being reported	
	RS.AN-07: Incident data and metadata are collected, and their integrity and provenance are preserved	**Ex1:** Collect, preserve, and safeguard the integrity of all pertinent incident data and metadata (e.g., data source, date/time of collection) based on evidence preservation and chain-of-custody procedures	
	RS.AN-08: The incident's magnitude is estimated and validated	**Ex1:** Review other potential targets of the incident to search for indicators of compromise and evidence of persistence **Ex2:** Automatically run tools on targets to look for indicators of compromise and evidence of persistence	
Incident Response Reporting and Communication (RS.CO): Response activities are coordinated with internal and external stakeholders as required by laws, regulations, or policies			

Category	Subcategory	Implementation Examples	Informative References
	RS.CO-01: Dropped (moved to PR.AT-01)		
	RS.CO-02: Internal and external stakeholders are notified of incidents	**Ex1:** Follow the organization's breach notification procedures after discovering a data breach incident, including notifying affected customers **Ex2:** Notify business partners and customers of incidents in accordance with contractual requirements **Ex3:** Notify law enforcement agencies and regulatory bodies of incidents based on criteria in the incident response plan and management approval	
	RS.CO-03: Information is shared with designated internal and external stakeholders (formerly RS.CO-03, RS.CO-05)	**Ex1:** Securely share information consistent with response plans and information sharing agreements **Ex2:** Voluntarily share information about an attacker's observed TTPs, with all sensitive data removed, with an Information Sharing and Analysis Center (ISAC) **Ex3:** Notify HR when malicious insider activity occurs **Ex4:** Regularly update senior leadership on the status of major incidents **Ex5:** Follow the rules and protocols defined in contracts for incident information sharing between the organization and its suppliers **Ex6:** Coordinate crisis communication methods between the organization and its critical suppliers	
	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	**Ex1:** Cybersecurity technologies (e.g., antivirus software) and cybersecurity features of other technologies (e.g., operating	

Category	Subcategory	Implementation Examples	Informative References
		systems, network infrastructure devices) automatically perform containment actions **Ex2:** Allow incident responders to manually select and perform containment actions **Ex3:** Allow a third party (e.g., internet service provider, managed security service provider) to perform containment actions on behalf of the organization **Ex4:** Automatically transfer compromised endpoints to a remediation virtual local area network (VLAN)	
	RS.MI-02: Incidents are eradicated	**Ex1:** Cybersecurity technologies and cybersecurity features of other technologies (e.g., operating systems, network infrastructure devices) automatically perform eradication actions **Ex2:** Allow incident responders to manually select and perform eradication actions **Ex3:** Allow a third party (e.g., managed security service provider) to perform eradication actions on behalf of the organization	
	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-02: Dropped (moved to ID.IM-03)		

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

Category	Subcategory	Implementation Examples	Informative References
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	**Ex1:** Begin recovery procedures during or after incident response processes **Ex2:** Make all individuals with recovery responsibilities aware of the plans for recovery and the authorizations required to implement each aspect of the plans	
	RC.RP-02: Recovery actions are determined, scoped, prioritized, and performed	**Ex1:** Select recovery actions based on the criteria defined in the incident response plan and available resources **Ex2:** Change planned recovery actions based on a reassessment of organizational needs and resources	
	RC.RP-03: The integrity of backups and other restoration assets is verified before using them for restoration	**Ex1:** Check restoration assets for indicators of compromise, file corruption, and other integrity issues before use	
	RC.RP-04: Critical mission functions and cybersecurity risk management are considered to establish post-incident operational norms	**Ex1:** Use business impact and system categorization records (including service delivery objectives) to validate that essential services are restored in the appropriate order **Ex2:** Work with system owners to confirm the successful restoration of systems and the return to normal operations **Ex3:** Monitor the performance of restored systems to verify the adequacy of the restoration	
	RC.RP-05: The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed	**Ex1:** Check restored assets for indicators of compromise and remediation of root causes of the incident before production use **Ex2:** Verify the correctness and adequacy of the restoration actions taken before putting a restored system online	

Category	Subcategory	Implementation Examples	Informative References
	RC.RP-06: The criteria for determining the end of incident recovery are applied, and incident-related documentation is completed	**Ex1:** Prepare an after-action report that documents the incident itself, the response and recovery actions taken, and lessons learned **Ex2:** Declare the end of incident recovery once the criteria are met	
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	**Ex1:** Securely share recovery information, including restoration progress, consistent with response plans and information sharing agreements **Ex2:** Regularly update senior leadership on recovery status and restoration progress for major incidents **Ex3:** Follow the rules and protocols defined in contracts for incident information sharing between the organization and its suppliers **Ex4:** Coordinate crisis communication between the organization and its critical suppliers	
	RC.CO-04: Public updates on incident recovery are properly shared using approved methods and messaging (formerly RC.CO-01, RC.CO-02)	**Ex1:** Follow the organization's breach notification procedures for recovering from a data breach incident **Ex2:** Explain the steps being taken to recover from the incident and to prevent a recurrence	
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)		