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

Public Draft: The NIST Cybersecurity Framework 2.0
www.nist.gov/cyberframework

Function	Category	Subcategory	Implementation Examples	Explaination
GOVERN (GV): Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy	**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-03**: Legal, regulatory, and contractual requirements regarding cybersecurity - including privacy and civil liberties obligations - are understood and managed **periodically(e.g. once per year)** (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	Legal requirements chage from time to time, so it is necessary to check and manage them regularly
IDENTIFY (ID): Help determine the current cybersecurity risk to the organization	**Asset Management (ID.AM)**: Assets (e.g., data, hardware software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy	**ID.AM-07**: Inventories of data and corresponding metadata for designated data types **and categorizations** are maintained **as different levels of supervision**	**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	Depending on the type and classification of data, the level of supervision of management needs to be different
식별 (ID): 조직에 대한 현재의 사이버 보안 위험을 파악하는 데 도움	**Risk Assessment (ID.RA)**: The organization understands the cybersecurity risk to the organization, assets, and individuals.	**ID.RA-09 → GV.SC-11**: 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	Assessing reliability and cybersecurity prior to purchasing and using products and services appears to be a case of supply chain security. Accordingly, it is proposed to move from a risk assessment category to a supply chain security category.

Function	Category	Subcategory	Implementation Examples	Explaination
PROTECT (PR): Use safeguards to prevent or reduce cybersecurity risk	**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-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 **Ex4: Keep and manage a record of the destruction** **Ex5: Implement and notify privacy protection measures for dormant users**	It is necessary to add Implementation Examples, such as keeping and managing a record of the destruction, implementing and notifying privacy protection measures for dormant users.
PROTECT (PR): Use safeguards to prevent or reduce cybersecurity risk	**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-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 **EX4: Consider the appication of active cyber defense technology or architecture.**	In order to reverse the attacker dominant and asymmetric attack-defence relationship, it is necessary to add implementation examples of active and proactive security strategies to prevent various cyberattacks by changing the main attributes of target.