

Appendix C: Examples of security measures according to measure requirements

- Examples of security measures for each of the High Advanced, Advanced, and Basic levels are stated for implementing measure requirements described in Part III. To implement High Advanced-level measures, there is a need to include not only High Advanced-level measures but also Advanced- and Basic-level measures.

- The level of a measure is determined according to the costs in implementing/operating the measure, the scope of the measure (e.g., whether the scope is applied only to the organization or other related organizations), etc., based on management measures stratified into levels.

- The subject that implements measures is classified as “S” (implemented by a system through technical means), as “O” (implemented by an organization (e.g., by people through non-technical means)), and as “O/S” (implemented by both a system and an organization).

- In describing the examples of security measures, reference is made to major security documents and other relevant materials (shown as “Reference Guidelines” in the table).

- The measures described in this section are just examples and do not deny other implementation methods. Use this document as a reference for risk management according to the characteristics of the business of each organization, the results of the risk analyses, etc.

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measure	Reference Guidelines				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 Annex A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.GV.OC-01	The organization understands its mission and uses it to inform cybersecurity risk management decisions.	L1_1_a_ORG L1_1_b_ORG L1_1_c_ORG	Common among <High-Advanced>, <Advanced> and <Basic> - The organization communicates its mission to internal and external personnel, utilizing it as material for judgement to identify, analyze, evaluate, and respond to cybersecurity risks that could impede mission execution.	O	-	○ (PM-11)	-	-	-
CPS.GV.OC-02	The organization understands legal, regulatory, and contractual requirements regarding cybersecurity—including privacy and civil liberties obligations—as well as industry guidelines, and establishes internal rules that appropriately reflect and address these requirements or guidelines.	L1_1_a_PEO L1_1_b_PEO L1_1_c_PEO L1_2_a_ORG L1_2_a_COM L1_2_a_SYS L1_2_a_PRO L1_2_a_DAT L3_4_a_ORG L3_4_b_ORG	Common among <High-Advanced>, <Advanced> and <Basic> - The organization identifies all laws and regulations which are applied to each organization to satisfy requirements related to the type of business. - When the organization operates businesses in other countries, managers consider complying with the laws and regulations in all related countries. - Within its business activities, the organization clearly identifies all related laws, regulations, and contractual requirements in the context of security as well as the organization’s effort to fulfill these requirements, documents them, and maintains those documents at their latest. - Prior to formulating internal rules, the organization determines whether any applicable laws and regulations, industry standards, or customer contractual obligations related to monitoring operations exist, and if so, identifies the constraints imposed. - The organization defines and documents detailed management measures and details of responsibilities to satisfy the requirements. - The organization disseminates established and revised internal rules to officers, employees, established, and seconded personnel. - The organization monitors revision statuses of applicable laws, regulations, and contractual requirements, reviewing and assessing internal rules at least annually. [Reference] Information security-related statutes include, for example, the Unfair Competition Prevention Act, the Act on Electronic Signatures and Certification Business, the e-Document Act, the Act on the Protection of Personal Information, and the Act on Prohibition of Unauthorized Computer Access. Furthermore, to ensure compliance with these laws and regulations, it is advised to refer to regulatory guidance issued by relevant ministries and agencies (e.g., Unfair Competition Prevention Act: “Management Guidelines for Trade Secrets” (Ministry of Economy, Trade and Industry, March 2025), “Guidelines on Shared Data with Limited Access” (February 2024); Act on the Protection of Personal Information: “Guidelines on the Act on the Protection of Personal Information (General Rules)” (Personal Information Protection Commission, June 2026), “Guidelines on the Act on the Protection of Personal Information (Anonymously Processed Information)” (Personal Information Protection Commission, April 2026)).	O	○ (03.15.03 Rules of Behavior a.)	○ (AC-01, AT-01, AU-01, CA-01, CM-01, CP-01, IA-01, IR-01, MA-01, MP-01, PE-01, PL-01, PM-01, PS-01, PT, RA-01, SA-01, SC-01, SI-01, SR-01)	○ (A.5.31)	-	-
CPS.GV.OC-03	The organization identifies dependencies and critical functions across both its own organization and related external entities to sustain business operations and shares them with those external entities.	L1_3_b_ORG	<High-Advanced> - The organization identifies the functions of the following support utilities for the continuation of its business and the dependence relationship between them. - Communication service - Electrical power equipment (including power cables) - Among the above identified utilities, for those which have important roles for the continuation of its business, the organization examines the possibility of taking measures as follows: - Establishment of alternative communication services - Physical protection of electrical power equipment and power cables - Preparation of short-term uninterruptible power supply (UPS) - When examining the possibility of using an alternative communication service, the organization considers the following: - Identify the requirements on the availability of the organization (including the target recovery time) when examining a contract with a communication service provider. - Reduce the possibility of sharing a single point of failure with a primary communication service.	O	-	○ (In addition to the following, CP-02(08), RA-09)	-	-	-
			<Advanced> - The organization identifies assets and operations critical to achieving its mission, as well as the potential impact resulting from the total or partial loss of those operations. - The organization identifies and documents external dependencies that could become points of failure for its critical capabilities and services, sharing this information with relevant personnel. - The organization identifies the requirements for the capacity/capability of an applicable system according to the requirements for its availability. - In order to fulfill the required system performance, the organization monitors/adjusts the use of resources in the information systems and industrial control systems in operation, and pre-estimates the storage capacity/performance required in the future.	O	-		-	-	-
			<Basic> - The organization establishes criteria for determining critical organizational capabilities and services from the perspective of its business continuity. - The organization creates an inventory mapping dependencies on external resources (e.g., facilities and cloud-based hosting providers) and suppliers, and their relationships with the organization’s assets and business functions.	O	-	○ (CP-02, PM-08, PM-11, PM-30(01), SA-09)	-	-	-
CPS.GV.RM-01	The organization defines risk management objectives and agrees on them with relevant stakeholders.	L1_1_a_PRO L1_1_b_PRO L1_1_c_PRO	Common among <High-Advanced> and <Advanced> - The organization updates its short- and long-term cybersecurity risk management objectives during annual cybersecurity strategy formulation and the occurrence of significant changes. - Senior management agrees on cybersecurity objectives, and measures and manages risks and outcomes based on those objectives.	O	-	○ (PM-09, RA-07, SR-02)	-	-	-
			<Basic> - The organization establishes measurable targets that concretize cybersecurity risk management objectives (e.g., managing the quality of user training, and adequately safeguarding industrial control systems against risks).	O	-		-	-	-

- Examples of security measures for each of the High Advanced, Advanced, and Basic levels are stated for implementing measure requirements described in Part III. To implement High Advanced-level measures, there is a need to include not only High Advanced-level measures but also Advanced- and Basic-level measures.

- The level of a measure is determined according to the costs in implementing/operating the measure, the scope of the measure (e.g., whether the scope is applied only to the organization or other related organizations), etc., based on management measures stratified into levels.

- The subject that implements measures is classified as “S” (implemented by a system through technical means), as “O” (implemented by an organization (e.g., by people through non-technical means)), and as “O/S” (implemented by both a system and an organization).

- In describing the examples of security measures, reference is made to major security documents and other relevant materials (shown as “Reference Guidelines” in the table).

- The measures described in this section are just examples and do not deny other implementation methods. Use this document as a reference for risk management according to the characteristics of the business of each organization, the results of the risk analyses, etc.

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measure	Reference Guidelines				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 Annex A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.GV.RM-02	The organization develops a cybersecurity strategy to ensure effective cybersecurity risk management.	L1_1_a_PRO L1_1_b_PRO L1_1_c_PRO	<High-Advanced> - When formulating and revising a cybersecurity strategy, the organization performs an interview regarding cybersecurity strategies with highly important business partners to align awareness on security risks and necessary measures. In that case, it is desirable to handle the following. - Major security risks related to the business of the organization and continuance of the business - Details and scale of impact on the business partner when the above risks are manifested - Handling policy for the above security risks - (When the risk management strategy is revised) changes in the internal and external conditions and important point to be changed from the previous versions	O	-	-	-	-	-
			Common among <Advanced> and <Basic> - The organization formulates a comprehensive cybersecurity strategy to manage risks to the organization's business, capital, persons, and other organizations caused by operating and using information system and industrial control system. - The organization implements the cybersecurity strategy while keeping consistency in the entire organization. - The organization's senior management periodically reviews the following aspects of the organization's cybersecurity strategy that are concerned with security. - How many attacks are you facing (detected) (Detection number by anti-virus products/IDS, latest threat trends etc.) - Is the status of security measures implementation as planned? (Application rate of security measures to be implemented such as anti-malware and security patch application etc.) - Did you allow the attacker (including insider) to intrude? (Description of an event suspected of external intrusion or internal fraud through security monitoring activities) - What is the state of security that is not directly related to information systems or industrial control systems (Retirement, loss of PC and devices, occurrence of physical theft etc.) - The organization documents and stores the results of reviews by the management. - The organization reviews and updates the cybersecurity strategy periodically or when it is necessary to cope with an organizational change.	O	-	-	-	-	-
CPS.GV.RM-03	The organization establishes its risk appetite and risk tolerance, and communicates them across the organization.	L1_1_a_SYS L1_1_a_PRO L1_1_b_SYS L1_1_b_PRO L1_1_c_SYS L1_1_c_PRO	<High-Advanced> - The organization interviews important business partners who may suffer from an undesirable impact because of a security incident in the organization to discuss the organization's risk tolerance level.	O	-	○ (PM-09)	-	-	-
			<Advanced> - The organization determines its risk appetite and risk tolerance based on an understanding of current supply chain risks and the results of risk assessments, and communicates them throughout the organization. - The organization periodically reviews its risk appetite and risk tolerance based on the status of identified risks, including residual risks.	O	-		-	○ (6.3.1.1, 8.2.6.1)	-
			<Basic> - The organization determines its risk appetite and risk tolerance based on the results of risk assessments, and communicates them throughout the organization. - The organization obtains approvals to remaining risks from the owners of the risks. - The organization documents the risk management results and safely maintains lists of risk tolerance criteria and accepted risks.	O	-		-	-	-
CPS.GV.RM-04	The organization integrates cybersecurity risk management activities and their outcomes into the organizational risk management process, managing cybersecurity risks within that process.	-	Common among <High-Advanced> and <Advanced> - The organization integrates and manages cybersecurity risks alongside other enterprise risks (e.g., compliance, financial, operational, regulatory, reputational, and safety).	O	-	○ (In addition to the following, SA-24)	-	○ (6.2.1.1)	-
			<Basic> - The organization involves cybersecurity risk managers in organizational risk management planning. - Within its risk management framework, the organization establishes criteria for escalating cybersecurity risks (e.g., detection of risks exceeding risk tolerance, significant changes in the risk environment requiring revisions to risk response policies, and risk acceptance decisions beyond the authority of the department in charge).	O	-	○ (PM-03, PM-09, PM-30, RA-07, SR-02)	-		-
CPS.GV.RM-05	The organization formulates policies regarding risk response options and their operations, and shares them within the organization.	L1_1_a_PRO L1_1_b_PRO L1_1_c_PRO	Common among <High-Advanced> and <Advanced> - The organization assesses the need for cyber insurance coverage.	O	-	○ (PM-09, PM-28, PM-30, SR-02)	-	○ (6.3.1.1)	-
			<Basic> - The organization specifies criteria for cybersecurity risk acceptance and risk avoidance across each data classification level. - The organization documents the conditions under which a shared responsibility model is permissible (e.g., outsourcing specific cybersecurity functions, permitting third parties to conduct financial transactions on behalf of the organization, and utilizing public cloud-based services).	O	-		-		-
CPS.GV.RM-06	The organization establishes and maintains lines of communication across the organization regarding cybersecurity risks, including risks posed by partners and other third parties.	L1_1_a_PEO L1_1_b_PEO	Common among <High-Advanced> and <Advanced> - The frequency and methods for reporting organizational cybersecurity posture to executive management, directors, and managers are defined and agreed upon among stakeholders. - The organization defines clear mechanisms for all internal departments (e.g., executive management, operations, internal audit, legal, procurement, physical security, and human resources) to communicate with each other regarding cybersecurity risks.	O	○ (03.14.03 Security Alerts, Advisories, and Directives a.)	○ (PM-09, PM-30)	-	-	-
			<Basic> - The organization establishes a contact list of officers (e.g., the CISO, if designated) and security departments required for security promotion activities in normal conditions. - The organization reviews the contact list of officers and security departments required for security promotion activities in normal conditions at least annually.	O	-		-	-	-

- Examples of security measures for each of the High Advanced, Advanced, and Basic levels are stated for implementing measure requirements described in Part III. To implement High Advanced-level measures, there is a need to include not only High Advanced-level measures but also Advanced- and Basic-level measures.

- The level of a measure is determined according to the costs in implementing/operating the measure, the scope of the measure (e.g., whether the scope is applied only to the organization or other related organizations), etc., based on management measures stratified into levels.

- The subject that implements measures is classified as “S” (implemented by a system through technical means), as “O” (implemented by an organization (e.g., by people through non-technical means)), and as “O/S” (implemented by both a system and an organization).

- In describing the examples of security measures, reference is made to major security documents and other relevant materials (shown as “Reference Guidelines” in the table).

- The measures described in this section are just examples and do not deny other implementation methods. Use this document as a reference for risk management according to the characteristics of the business of each organization, the results of the risk analyses, etc.

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measure	Reference Guidelines				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 Annex A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.GV.RM-07	The organization standardizes methodologies for assessing, documenting, classifying, and prioritizing cybersecurity risks, and shares them within the organization.	L1_1_a_PRO L1_1_b_PRO L1_1_c_PRO	Common among <High-Advanced>, <Advanced> and <Basic> - The organization establishes criteria for applying a quantitative approach in cybersecurity risk analysis, and defines calculation formulas for risk likelihood and impact. - The organization establishes criteria for prioritizing risks for each unit conducting risk management within the organization. - The organization utilizes a standardized risk taxonomy when consolidating, aggregating, and comparing cybersecurity risks. - The organization creates and uses templates (e.g., risk registers) to document cybersecurity risk information (e.g., risk descriptions, impact levels, response plans, and risk owners).	O	-	○ (PM-09, PM-18, PM-28, PM-30, RA-03)	-	○ (6.3.1.1)	-
CPS.GV.RM-08	The organization identifies strategic opportunities (positive risks for the organization), clarifies their characteristics, and integrates them into organizational cybersecurity risk deliberations.	L1_1_a_ORG L1_1_b_ORG L1_1_c_ORG	Common among <High-Advanced> and <Advanced> - The organization defines and communicates methodologies (e.g., SWOT analysis) to identify strategic opportunities (positive risks) and incorporate them into risk discussions.	O	-	○ (PM-09, PM-18, PM-28, PM-30, RA-03)	-	-	-
			<Basic> - The organization assesses, documents, and prioritizes both positive and negative risks in an integrated manner.	O	-		-	-	-
CPS.GV.RR-01	Organizational senior management is responsible and accountable for cybersecurity risk, fostering a culture that is risk-aware, ethical, and continually improving.	L1_1_a_PEO L1_1_b_PEO L1_1_c_PEO	Common among <High-Advanced> and <Advanced> - Recognizing that security risks have a significant impact on business management, the organization establishes a structure capable of making executive decisions regarding risk response, such as an Information Security Committee with senior management participation. - When a cybersecurity-related event occurs, the organization communicates senior management's expectations and messages regarding security and ethics throughout the organization. - Senior management instructs the organization's CISO to maintain the cybersecurity risk strategy and to review and update the strategy at least annually and after the occurrence of significant events.	O	-	○ (PM-02, PM-19, PM-23, PM-24, PM-29)	○ (In addition to the following, A.5.4)	○ (6.2.3.1)	-
			<Basic> - Senior executives (e.g., members of the board of directors) mutually agree upon their roles and responsibilities in the formulation, implementation, and evaluation of the organization's cybersecurity strategy.	O	-		○ (A.5.2)		-
CPS.GV.RR-02	The organization establishes roles, responsibilities, and authorities related to its cybersecurity risk management and communicates them within the organization.	L1_1_a_PEO L1_1_b_PEO L1_1_c_PEO L1_3_a_ORG L1_3_c_PEO	Common among <High-Advanced> and <Advanced> - The organization defines the roles and responsibilities of designated departments, from the collection of vulnerability and threat information to response. - The organization establishes a cross-functional coordination structure among departments involved in supply chain risk management, such as cybersecurity, IT, operations, legal, human resources, and engineering. - Senior management periodically conducts reviews to ensure that individuals responsible for cybersecurity risk management possess the requisite authority to execute their duties. - The organization establishes and maintains continuous coordination on cybersecurity risk management between departments involved in the operation of information systems and those involved in the operation of industrial control systems. - The organization graphically represents the overview of a supply chain related to the organization, with clarification of the roles in the entire organization by considering the component flow, data flow, etc., between organizations. - The organization shares the above diagrammed results with related organizations (suppliers to the organization, related departments within the organization, and customers of the organization).	O	-	○ (PM-02, PM-13, PM-19, PM-23, PM-24, PM-29)	○ (A.5.2)	○ (6.2.3.1)	-
			<Basic> - The organization defines the roles and responsibilities of the officer overseeing security (e.g., the CISO, if designated) and security departments. - The organization defines the roles and responsibilities of the officer overseeing security (e.g., the CISO, if designated) and security departments in the event of a security incident. - The organization delineates cybersecurity responsibilities across operational divisions, risk management divisions, and internal audit divisions. - The organization identifies the person responsible for security risk management both in information systems and in industrial control systems. - The organization documents roles and responsibilities regarding cybersecurity risk management in its security policies. - The organization incorporates roles and responsibilities regarding cybersecurity risk management into job descriptions. - The organization establishes a responsibility assignment matrix to document who is responsible and accountable for cybersecurity supply chain risk management activities, as well as how relevant teams and individuals are consulted and informed. - The organization graphically represents the overview of the business connections among suppliers to the organization, related departments within the organization, and customers of the organization, with clarification of the roles in the organization by considering component flow, data flow, etc., between organizations. - The organization shares the above diagrammed results with related organizations (suppliers to the organization, related departments within the organization, and customers of the organization). - In a contract with a contractor or an outsourcer, the organization specifies the scope of the responsibilities of the organization and that of the business partner (state the disclaimer and an upper limit on agreed compensation for damages) in case of damage caused by a security incident in the business. [Reference] For additional information, particularly regarding roles and responsibilities of cloud service providers and the organization, "I.6. Responsibilities of Cloud Service Providers and Cloud Service Users" of the "Guidelines on Information Security Measures in Cloud Service Provision (3rd Edition)" issued by the Ministry of Internal Affairs and Communications is available for reference.	O	○ (03.06.05 Incident Response Plan a.)				-
CPS.GV.RR-03	The organization appoints a security manager, establishes a security response organization (SOC/CSIRT), and maintains a structure to detect, analyze, and respond to security incidents within the organization.	L1_3_a_ORG	<High-Advanced> - The organization establishes a security response organization whose scope covers industrial control systems, IoT systems, etc., and puts in place a structure for implementing security measures in an integrated manner across the organization. [Reference] Metrics for evaluating security response organizations (SOC/CSIRT) include the "Service portfolio self-check sheet for security response organisation" (ISOG-J, 2024) and the Security Incident Management Maturity Model (SIM3).	O	-	-	○ (A.5.2, A.5.24)	-	-
			<Advanced> - The organization establishes a structure to utilize public information or non-public information regarding cyberattacks and vulnerabilities. - The organization, with a chief security officer at the center, establishes a security management team mainly for information systems and IoT systems with high business importance, and prepares a structure for handling security measures within the organization. [Reference] For information regarding the operations and recommended scale of security response organization (SOC/CSIRT), it is advised to refer to documents such as the "Textbook for security response organisation (SOC/CSIRT)" - using X.1060 -" (ISOG-J, October 2025).	O	○ (In addition to the following, 03.06.01 Incident Handling)	-		○ (6.2.3.1)	-
			<Basic> - The organization identifies who the chief security officer/contact person is in both information system and industrial control system so that the officer/contact person can handle security-related internal and external communications.	O	○ (03.06.02 Incident Monitoring, Reporting, and Response Assistance d.)	-	○ (A.5.2, A.5.24, A.6.8)		-

- Examples of security measures for each of the High Advanced, Advanced, and Basic levels are stated for implementing measure requirements described in Part III. To implement High Advanced-level measures, there is a need to include not only High Advanced-level measures but also Advanced- and Basic-level measures.

- The level of a measure is determined according to the costs in implementing/operating the measure, the scope of the measure (e.g., whether the scope is applied only to the organization or other related organizations), etc., based on management measures stratified into levels.

- The subject that implements measures is classified as “S” (implemented by a system through technical means), as “O” (implemented by an organization (e.g., by people through non-technical means)), and as “O/S” (implemented by both a system and an organization).

- In describing the examples of security measures, reference is made to major security documents and other relevant materials (shown as “Reference Guidelines” in the table).

- The measures described in this section are just examples and do not deny other implementation methods. Use this document as a reference for risk management according to the characteristics of the business of each organization, the results of the risk analyses, etc.

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measure	Reference Guidelines				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 Annex A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.GV.RR-04	The organization allocates necessary resources commensurate with its cybersecurity strategy, roles, responsibilities, and policies.	L1_3_a_ORG	Common among <High-Advanced>, <Advanced> and <Basic> - The organization determines, documents, and allocates resources necessary to protect information systems, industrial control systems, and system services, based on its risk tolerance and risk response policies. - The organization states each security budget item in the organization's plans and budget-related materials.	O	-	○ (PM-03)	-	-	-
CPS.GV.RR-05	The organization incorporates security-related matters (e.g., revoking access privileges and screening employees) into measures that address role changes resulting from personnel transfers.	L1_1_a_PEO L1_1_b_PEO L1_1_c_PEO	<High-Advanced> - The organization conducts pre-onboarding background screenings for personnel assuming sensitive roles and performs periodic rescreening for incumbents in those positions. - To minimize impacts when a staff member leaves the organization, it designates backup members regarding important duties as a supplier including operation and maintenance. - The organization conducts an interview on information security when organizational personnel leave.	O	-	○ (PM-13, PS-01, PS-07, PS-09)	○ (A.6.1, A.6.5)	○ (6.2.2.1)	-
			<Advanced> - The organization incorporates the perspective of cybersecurity risk management into human resource processes (e.g., personnel screening, onboarding, transfer notifications, and offboarding). - The organization ensures that responsibilities for security are met, particularly of personnel handling sensitive information, throughout the whole process from hiring to retirement. - The organization considers cybersecurity proficiency as a positive factor in decisions regarding hiring, training, and talent retention. - The organization identifies conditions in which re-screening is required such as changes in access authority to its own systems, and re-screens if necessary. - The organization retrieves sensitive information and IT assets upon the departure or conclusion of the term of office of its personnel. - Collected items include information (printed materials and storage media), personal computers, smart devices, and access credentials (IDs and keys). - The organization establishes procedures to prevent unreturned items (e.g., developing a checklist of returned items). - The organization reviews the status of sensitive information and IT asset retrieval upon departure or conclusion of the term of office at least annually.	O	○ (In addition to the following, 03.01.01 Account Management g, 03.09.02 Personnel Termination and Transfer a.)		○ (A.5.11, A.6.1, A.6.5)	○ (6.2.2.1, 11.2.2.1)	-
			<Basic> - The organization reviews a staff member before granting him or her access to its systems. - The organization identifies the responsibility for security of personnel in the employment contract. The organization states that this responsibility should be sustained for a reasonable period of time after the termination of employment, in order to prevent information leakage after the termination of employment. - The organization makes changes to its staff members' rights to access certain systems and/or rooms on the premises when they are reshuffled or transferred internally. - The organization conducts the following when a staff member resigns or retires: - Disables the staff member's access to its systems within a certain period; - Disables the authentication and credentials related to the staff member; - Retains access to the information about the organization and information systems that have been managed by the individual who is leaving.	O	○ (03.01.01 Account Management f, 3.09.01 Personnel Screening a, 3.09.02 Personnel Termination and Transfer b, 03.10.01 Physical Access Authorizations d.)		○ (A.6.1, A.6.5)		-
CPS.GV.PO-01	The organization formulates security policies based on its organizational context, cybersecurity strategy, and priorities, communicates them within the organization and to relevant external parties (including suppliers and third-party providers, as needed), and implements them.	L1_1_a_PEO L1_1_a_PRO L1_1_b_PEO L1_1_b_PRO L1_1_c_PEO L1_1_c_PRO	<High-Advanced> - While sharing the basic policy with operations used in a conventional IT environment, the organization formulates security policies and operational procedures by fully considering the characteristics of sites where industrial control systems and IoT devices are installed. [Reference] For example, IEC 62443-2-1, a security management standard for industrial control systems (ICS), requires the development of high-level cybersecurity policies for ICS environments. In particular, when developing security policies and operational procedures for the industrial sector, resources such as the “Guideline for Security Operation of Control System” (Nippon Electric Control Equipment Industries Association, 2017) are available for reference.	O	-	○ (03.15.01 Policy and Procedures a, 03.15.03 Rules of Behavior b.)	○ (A.5.1, A.5.10)	○ (6.2.1.1)	-
			<Advanced> - The organization defines its missions and business processes and gives priorities to actions, in consideration of risks to its business, its assets, persons, other organizations, etc. - The organization formulates a series of security policies by fully considering its business strategies, relevant rules, laws, regulations, and contracts, and the security threat landscape, so that the policies sufficiently reflect the organization's actual circumstances. - The organization formulates a series of lower level security policies, such as the policies and implementation procedures of the following individual topics, to support policies at a higher level. - Access control and authentication - Physical security measures - System development and maintenance - Management of external contractors - Classification and handling of information - When formulating ICS-specific policies and procedures, the organization takes into account that security controls for information systems cannot be applied directly without adaptation, and identifies critical operational functions, ICS-specific security concerns, and the priority of alternative controls. - The organization obtains consent regarding compliance with its security policies from its personnel upon onboarding, annually, and whenever security policies are updated. [Reference] When formulating policies at a more detailed level, it is advised to refer to relevant standards such as ISO/IEC 27002 to identify the areas where policies are needed, and to consult resources such as Appendix 5 “Information Security Related Regulations (Sample)” of the “Information Security Measures Guidelines for Small and Medium-sized Enterprises, Version 4.0” (IPA, 2026) and the “Information Security Policy Sample Revision (Version 1.0)” (JNSA, 2016).	O			○ (A.5.1, A.5.4, A.5.10)	-	-
			<Basic> - The organization formulates a basic security policy at the highest level of its series of security policies, obtains an approval of the management, and operates it appropriately. - The organization reviews and updates the security policy periodically (e.g., once a year), and obtains approval from senior management. - The organization identifies in advance the core businesses that should be continued and restored in priority, and the operations considered to be important. In addition, identify and prioritize important resources (relevant organizations, people, components, data, system, etc.) and functions from the viewpoint of business continuity. - The organization classifies and prioritizes resources particularly in industrial control systems, taking into consideration whether adverse effects on health, safety and environment (HSE) may occur due to malfunction or stoppage. [Reference] When formulating security policies, descriptions such as “1. Organizational Measures” in Appendix 5 “Information Security Related Regulations (Sample)” of the “Information Security Measures Guidelines for Small and Medium-sized Enterprises, Version 4.0” (IPA, 2026) as well as “01_Basic Information Security Policy” and “01_Information Security Policy” in the “Information Security Policy Sample Revision (Version 1.0)” (JNSA, 2016) are available for reference.	O	-		○ (A.5.1)	-	-

- Examples of security measures for each of the High Advanced, Advanced, and Basic levels are stated for implementing measure requirements described in Part III. To implement High Advanced-level measures, there is a need to include not only High Advanced-level measures but also Advanced- and Basic-level measures.

- The level of a measure is determined according to the costs in implementing/operating the measure, the scope of the measure (e.g., whether the scope is applied only to the organization or other related organizations), etc., based on management measures stratified into levels.

- The subject that implements measures is classified as “S” (implemented by a system through technical means), as “O” (implemented by an organization (e.g., by people through non-technical means)), and as “O/S” (implemented by both a system and an organization).

- In describing the examples of security measures, reference is made to major security documents and other relevant materials (shown as “Reference Guidelines” in the table).

- The measures described in this section are just examples and do not deny other implementation methods. Use this document as a reference for risk management according to the characteristics of the business of each organization, the results of the risk analyses, etc.

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measure	Reference Guidelines				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 Annex A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.GV.PO-02	The organization periodically reviews its security policies and updates them as necessary, based on changes in requirements, threats, technology, and the organization's mission.	L1_1_a_PRO L1_1_a_PRO L1_1_b_PRO L1_1_b_PRO L1_1_c_PRO L1_1_c_PRO	Common among <High-Advanced>, <Advanced> and <Basic> - The organization updates security policies at least annually, accounting for changes in applicable laws and regulations, technological advancements (e.g., introduction of artificial intelligence), and business changes (e.g., new business acquisitions and novel contractual requirements).	O	○ (03.15.01 Policy and Procedures b, 03.15.03 Rules of Behavior b.)	○ (AC-01, AT-01, AU-01, CA-01, CM-01, CP-01, IA-01, IR-01, MA-01, MP-01, PE-01, PL-01, PM-01, PS-01, PT-01, RA-01, SA-01, SC-01, SI-01, SR-01)	○ (A.5.1)	○ (6.3.4.1)	-
CPS.GV.OV-01	The organization reviews the outcomes of its cybersecurity strategy and, taking into account these results and changes in the internal and external context, revises the cybersecurity strategy as well as enterprise-wide strategy and direction as necessary.	-	Common among <High-Advanced>, <Advanced> and <Basic> - The organization measures the extent to which the cybersecurity strategy and its outcomes contribute to senior management decision-making and the achievement of organizational objectives. - The organization confirms whether the cybersecurity strategy impedes business operations or innovation, and revises it as necessary. - The organization verifies that the existing cybersecurity strategy aligns with internal and external requirements, taking into account audit results and other findings. - The organization reviews its cybersecurity strategy in light of cybersecurity incidents.	O	-	○ (AC-01, AT-01, AU-01, CA-01, CM-01, CP-01, IA-01, IR-01, MA-01, MP-01, PE-01, PL-01, PM-01, PM-09, PM-18, PM-19, PM-30, PM-31, PS-01, PT-01, RA-01, RA-07, SA-01, SC-01, SI-01, SR-01, SR-06)	-	-	-
CPS.GV.OV-02	The organization reviews the implementation status of its cybersecurity risk management and updates it as necessary.	-	<High-Advanced> - To identify risks facing the organization, the security department periodically reviews key risk indicators (KRIs), including likelihood of occurrence and potential impact.	O	-	○ (In addition to the following, SR-06)	-	-	-
			<Advanced> - The organization continues to collect and manage information about assets, device configurations, and network configurations in order to evaluate its security status. - The organization regularly reports the security status of its operations and systems to the chief security officer or other appropriate staff members. It is desirable that the regular report should include the following shown below: - Results of log analysis (e.g., the number of incidents handled; summaries of typical incidents that have been handled; threats that have emerged; issues in monitoring); - Policy for future improvements in monitoring. - At least annually, the security department reports to the officer overseeing security (e.g., the CISO, if designated) on the operational state of security safeguards based on internal review findings, as well as on a forward-looking action plan formulated from those findings, obtains approval, and then shares the approved report results with internal departments. - If the officer overseeing security (e.g., the CISO) provides instructions for improvement upon receiving the report on the action plan, the security department records those instructions, incorporates them into the plan, and remediates deficiencies. - The organization conducts third-party security assessments (e.g., cybersecurity audits).	O	-		○ (In addition to the following, A.5.35)	○ (6.3.4.1)	-
			<Basic> - To evaluate its security posture properly and systematically, the organization develops a self-assessment plan that includes the following items and conducts self-assessments: - Security measures subject to assessment - Assessment procedures used to measure the effectiveness of security measures - Settings and operational structures for carrying out assessments - Methods of putting together and utilizing assessment results	O	○ (03.12.01 Security Assessment, 03.15.02 System Security Plan b.)	○ (PM-04, PM-06, RA-07)	○ (A.5.36)		-
CPS.GV.SC-01	The organization establishes supply chain risk management programs, strategies, objectives, policies, and processes, and operates them upon agreement with organizational stakeholders.	L1_1_a_ORG L1_1_a_PRO L1_1_b_ORG L1_1_b_PRO L1_1_c_ORG L1_1_c_PRO	<High-Advanced> - N/A	-	-	-	-	-	-
			Common among <Advanced> and <Basic> - The organization develops a cybersecurity supply chain risk management program that includes implementation and improvement plans (with milestones), policies, and procedures, and shares these policies and procedures with organizational stakeholders. - Based on strategies, objectives, policies, and procedures agreed upon and executed by organizational stakeholders, the organization develops and implements processes for the cybersecurity supply chain risk management program.	O	○ (03.17.01 Supply Chain Risk Management Plan a, 3.17.02 Acquisition Strategies, Tools, and Methods)	○ (PM-30, SR-02, SR-03)	○ (A.5.19, A.5.21)	-	-
CPS.GV.SC-02	The organization establishes cybersecurity roles and responsibilities for suppliers and partners, communicates them internally and externally, and coordinates adjustments as necessary.	L1_1_a_ORG L1_1_a_PRO L1_1_b_ORG L1_1_b_PRO L1_1_c_ORG L1_1_c_PRO L1_3_b_ORG L1_3_b_PRO L1_3_c_PRO	Common among <High-Advanced> and <Advanced> - To share responsibility for cybersecurity risks with relevant personnel, the organization establishes roles and responsibilities for suppliers, customers, and business partners—covering both normal and adverse conditions—and incorporates them into organizational policies and contracts with applicable third parties. - To increase the effectiveness of the requirements related to security which a business partner requires or is required to satisfy in a contract, it is desirable that the organization makes an agreement in meeting the requirements, identifying deficiencies and details of actions, paying expenses, and using alternative measures if a requirement cannot be satisfied, at the time of the contract or in the early stage of the contract. [Reference] For additional information, particularly regarding roles and responsibilities of cloud service providers and the organization, “I.6. Responsibilities of Cloud Service Providers and Cloud Service Users” of the “Guidelines on Information Security Measures in Cloud Service Provision (3rd Edition)” issued by the Ministry of Internal Affairs and Communications is available for reference.	O	○ (03.16.03 External System Services b.)	○ (SR-02, SR-03, SR-05)	○ (A.5.2)	○ (6.2.3.1)	-
			<Basic> - In a contract with a contractor or an outsourcer, the organization specifies the scope of the responsibilities of the organization and that of the business partner (state the disclaimer and an upper limit on agreed compensation for damages) in case of damage caused by a security incident in the business.	O	-		-		-

- Examples of security measures for each of the High Advanced, Advanced, and Basic levels are stated for implementing measure requirements described in Part III. To implement High Advanced-level measures, there is a need to include not only High Advanced-level measures but also Advanced- and Basic-level measures.

- The level of a measure is determined according to the costs in implementing/operating the measure, the scope of the measure (e.g., whether the scope is applied only to the organization or other related organizations), etc., based on management measures stratified into levels.

- The subject that implements measures is classified as “S” (implemented by a system through technical means), as “O” (implemented by an organization (e.g., by people through non-technical means)), and as “O/S” (implemented by both a system and an organization).

- In describing the examples of security measures, reference is made to major security documents and other relevant materials (shown as “Reference Guidelines” in the table).

- The measures described in this section are just examples and do not deny other implementation methods. Use this document as a reference for risk management according to the characteristics of the business of each organization, the results of the risk analyses, etc.

Measure Requirement ID	Measure Requirement	Correspondin g Vulnerability ID	Examples of security measure	Subject that implements measure	Reference Guidelines				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 Annex A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.GV.SC-03	The organization integrates cybersecurity supply chain risk management into its cybersecurity and enterprise risk management, risk assessment, and improvement processes.	L1_1_a_ORG L1_1_a_PRO L1_1_b_ORG L1_1_b_PRO L1_1_c_ORG L1_1_c_PRO	Common among <High-Advanced> and <Advanced> - The organization clarifies the overlaps and areas requiring coordination between cybersecurity risk management and enterprise risk management.	O	-	○ (In addition to the following, SR-06)	-	-	-
			<Basic> - The organization escalates critical cybersecurity risks within the supply chain to senior management and addresses them as enterprise-wide risks.	O	○ (03.11.01 Risk Assessment a, 03.17.01 Supply Chain Risk Management Plan b.)	○ (AC-01, AT-01, AU-01, CA-01, CM-01, CP-01, IA-01, IR-01, MA-01, MP-01, PE-01, PL-01, PM-01, PM-09, PM-18, PM-19, PM-28, PM-30, PM-31, PS-01, PT-01, RA-01, RA-03, RA-07, SA-01, SA-04, SA-09SC-01, SI-01, SR-01, SR-02, SR-03, SR-05)	-	-	-
CPS.GV.SC-04	The organization identifies and prioritizes organizations and people that play an important role relevant in each layer of the three-layer structure to sustain business operations.	L1_1_a_ORG L1_1_b_ORG L1_1_c_ORG L1_3_b_ORG	<High-Advanced> - The organization estimates the nature, likelihood, and scale of the impact on the organization in the event that a security incident with adverse business impacts occurs at a business partner. * Related measure requirements include CPS.ID.AM-04 and CPS.GV.PO-01.	O	-	○ (In addition to the following, SR-06)	-	-	-
			<Advanced> - The organization maintains an inventory of all suppliers and prioritizes them based on predetermined criticality criteria. - The organization monitors changes in risk conditions for critical suppliers, services, and products, reassessing the criticality of suppliers in response to those changes. - The organization confirms whether critical suppliers (e.g., business partners that can significantly impact the organization's mission or business processes) can fulfill the security roles and responsibilities specified in its security policies.	O	-	-	-	-	-
			<Basic> - The organization should identify in advance the core businesses that should be continued and restored in priority, and the operations considered to be important. In addition, identify and prioritize important resources (relevant organizations, people, components, data, system, etc.) and functions from the viewpoint of business continuity. - The organization establishes criteria for determining the criticality of suppliers, considering factors such as the sensitivity of data handled or retained by them, the degree of access privileges to the organization's systems, and the importance of provided products or services to the organization's mission. - When the organization is assumed to use an IoT device for a long period of time, the organization selects a business partner (device vendor) that has adequate organizations of management (e.g., service desk(s), maintenance system) from which long-term support can be expected. - The organization confirms with the partner (the device vendor) whether to replace a device at the end of support before implementing a system. - When the organization selects a business partner (service provider), it is desirable to select a service provider who operates and manages IT services efficiently and effectively. - It has acquired ITSMS certification based on JIS Q 20000. - It has implemented the equivalent measures to ITSMS certification based on self declaration of conformity.	O	-	○ (PM-09, PM-18, PM-30, SA-04, SR-03, SA-09, SR-05, SR-08)	-	-	-
CPS.GV.SC-05	The organization establishes supply chain cybersecurity standards considering the lifecycle of business relationships, clearly defines the scope of responsibilities, and agrees on them with partners through contracts or other means.	L1_1_a_ORG L1_1_a_PRO L1_1_b_ORG L1_1_b_PRO L1_1_c_ORG L1_1_c_PRO L1_3_b_ORG L1_1_d_PRO L2_1_a_PRO L2_2_a_ORG L2_3_c_PRO L3_1_b_DAT L3_1_a_PRO L3_1_c_DAT	<High-Advanced> - For critical products, the organization contractually obligates suppliers to provide and maintain an up-to-date inventory of components, including a Software Bill of Materials (SBOM) and Hardware Bill of Materials (HBOM). - The organization permits outsourcing of data handling operation to subcontractors only if it confirms that such subcontractors have implemented security measures whose level is equivalent to those required to direct business partners.	O	-	○ (In addition to the following, SR-06)	○ (A.5.20)	○ (6.2.6.1)	-
			<Advanced> - The organization, in reference to security measure criteria regarding supply chain, prepares and provides to potential partners tender documents such as ITT (Invitation To Tender) and RFP (Request For Proposal). In particular, it is advisable that the following items be included in the tender documents. - Specifications of products or services to be procured - Security requirements that the supplier should comply with during the supply period of the products or services - Service levels and the indices to comply with during the supply period of the products or services - Penalties that the purchaser may impose if the supplier breaches security requirements - Confidentiality clauses to protect the data transmitted during the supplier selection process, the systems, etc. - The organization specifies concrete security measure requirements considering importance of exchanged data and assumed risks, and requires business partners to implement them. - The organization incorporates into contract templates all cybersecurity and supply chain requirements to be complied with by third parties, as well as methods to verify compliance with these requirements. - The organization specifies in contracts the rules and procedures for information sharing among the organization, its suppliers, and their subcontractors. - The organization specifies security requirements in service level agreements (SLAs) to monitor whether the security posture of suppliers remains at an acceptable level throughout the lifecycle of the business relationship. - The organization contractually obligates suppliers to disclose cybersecurity features, specifications, and vulnerabilities of products and services during the product usage period or service provision period. - The organization contractually obligates suppliers to screen employees and implement measures against insider threats.	O	○ (In addition to the following, 03.12.05 Information Exchange b.)			○ (6.2.2.1, 6.2.6.1)	-
			<Basic> - Prior to commencing business, the organization establishes agreements on the following matters regarding the handling of sensitive information with subsidiaries or business partners with which it shares its sensitive information: - Definition of sensitive information - Restrictions on use, storage methods, and permissibility of reproduction and third-party disclosure - Return or disposal of sensitive information - The organization concludes an agreement with external information service providers regarding the handling of sensitive information. - The organization incorporates requirements for protection against environmental threats and the assurance of an appropriate operational infrastructure into agreements with service providers that operate systems on its behalf. - The organization prohibits direct business partners from subcontracting operations related to data management.	O	○ (03.01.20 Use of External Systems b.c, 03.12.05 Information Exchange a, 03.16.03 External System Services a.)	○ (SA-04, SA-09, SR-03, SR-05, SR-10)	○ (A.5.20, A.5.23)	-	-

- Examples of security measures for each of the High Advanced, Advanced, and Basic levels are stated for implementing measure requirements described in Part III. To implement High Advanced-level measures, there is a need to include not only High Advanced-level measures but also Advanced- and Basic-level measures.

- The level of a measure is determined according to the costs in implementing/operating the measure, the scope of the measure (e.g., whether the scope is applied only to the organization or other related organizations), etc., based on management measures stratified into levels.

- The subject that implements measures is classified as “S” (implemented by a system through technical means), as “O” (implemented by an organization (e.g., by people through non-technical means)), and as “O/S” (implemented by both a system and an organization).

- In describing the examples of security measures, reference is made to major security documents and other relevant materials (shown as “Reference Guidelines” in the table).

- The measures described in this section are just examples and do not deny other implementation methods. Use this document as a reference for risk management according to the characteristics of the business of each organization, the results of the risk analyses, etc.

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measure	Reference Guidelines				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 Annex A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.GV.SC-06	Before concluding contracts with suppliers and other third parties, the organization evaluates the cybersecurity management posture of said suppliers and third parties, and takes necessary measures to mitigate risks as needed.	L1_1_a_ORG L1_1_b_ORG L1_1_c_ORG L1_1_d_PRO L2_3_c_ORG L2_3_c_PRO L3_3_b_ORG L3_3_c_ORG L3_1_b_ORG L3_1_b_PEO L3_3_d_ORG L3_1_c_ORG L3_1_c_PEO L3_3_a_ORG	<High-Advanced> - In a contract with a business partner who provides systems/components/services, the organization requires the following of the partner. - Create evidence of the implementation of the security assessment plan, and submit results of security tests/evaluations. - Develop a plan for remedying defects identified during security testing / evaluation - Disclose a plan for defect remediation and its implementation status - It is desirable that the organization applies necessary requirements among those for security measures to contractors and accompanying requirements to subcontractors (and where appropriate, to all suppliers throughout the downstream supply chain) by considering the scales of risks originating from the supply chains. [Reference] To obtain additional information regarding items recommended for inclusion in outsourcing contracts and for implementation verification, the description in “3.2. Overview of IT Supply Chain Risk Management” of the “Survey Report on Security Incidents and Management in IT Supply Chain Outsourcing” (IPA, 2018) is available for reference.	O	-	○ (In addition to the following, RA-09, SR-06)	-	○ (6.2.6.1)	-
			<Advanced> - The organization adjusts the format and frequency of assessments according to the reputation of third parties and the criticality of provided products or services. - The organization conducts supplier risk assessments based on business requirements and applicable cybersecurity requirements. [Reference] As cybersecurity requirements imposed on suppliers, it is advised to consider utilizing, for example, the requirements and evaluation criteria of Supply Chain Security Assessment Program of Japan (SCS AP). - The organization evaluates whether prospective supplier’s technical and cybersecurity capabilities, as well as risk management practices, meet its requirements. - The organization is advised to consider the following items in advance when determining security requirements based on laws and regulations and requiring business partners to comply with them. - Identification of potential risks in terms of legal regulations that may arise due to difference of applicable laws between the organization and the business partner - Negative impacts on the contract in terms of security due to legal and regulatory obligations applicable to the business partner - The organization requires business partners, in a procurement contract, to implement security requirements that comply with applicable laws and regulations, implement additional measures when they are recognized necessary because of the characteristics of the contracted duty, etc. - In accordance with the missions/business needs of the organization, state the following requirements, descriptions, and criteria in a procurement contract of a system, component, or service. - Requirements for security measures - Requirements for security-related documents - Requirements for protection of security-related documents - Confidentiality clauses - Implementation body and method of each handling: reporting destination at the time of incident occurrence, reporting details, initial reaction, investigation, recovery, etc. - Conditions to allow to confirm the observance to the security requirement which is inspected and defined by the organization or the authorized third party. - How to handle an information asset at the end of the contract	O	-		-		-
			<Basic> - In the process of selecting and evaluating contractors, the organization confirms that the business partner has declared “SECURITY ACTION,” a self-declaration program operated by Japan’s Ministry of Economy, Trade and Industry (METI) for companies committed to implementing information security measures. - The organization requires business partners to implement security requirements that comply with applicable laws and regulations.	O	-	○ (SA-04, SA-09, SR-03, SR-05)	-	-	-
CPS.GV.SC-07	When entering into contracts with other relevant organizations such as business partners, the organization considers its objectives and risk management outcomes, verifying that products and services provided by them conform to the organization’s security requirements.	L1_1_d_ORG L1_1_d_COM L1_1_d_PRO L2_1_a_COM L2_1_a_PRO L2_2_a_ORG L2_3_a_ORG L2_3_c_ORG L2_3_c_PRO L2_3_d_ORG L3_3_b_ORG L3_3_c_ORG L3_1_b_ORG L3_3_d_ORG L3_1_c_ORG L3_3_a_ORG	<High-Advanced> - A third party tests the procured devices to see whether the security requirements stipulated in the contract are fulfilled. - The organization checks throughout the entire relevant supply chain (including reconsigned organizations) as to whether the devices especially important for their operation are manufactured under appropriate procedures by organizations that have quality and security management ability above a certain level.	O	-	○ (In addition to the following, RA-09, SR-06)	-	-	-
			<Advanced> - It is desirable that the organization should, at the phase of planning procurement, secure a budget for security requirements regarding products or services themselves, or protection of assets used for procurement and supply of such products or services. - The organization adjusts the format and frequency of assessments according to the reputation of third parties and the criticality of provided products or services. - The organization specifies in the contract the security requirements that the products and services procured from the partner should comply with, such as the following. - Specific certifications related to security (e.g., ISMS certification, ISASecure CSA certification, Japan Information Technology Security Evaluation and Certification Scheme (JISEC)) have been gained. - The vendor itself confirms that it has implemented the security measures in accordance with the standards of specific certifications related to security - It has implemented the necessary security requirements from the design phase (security by design) based on the results of risk analysis, etc., and test them. - The organization formulates, manages and improves security measurement rules to evaluate procurement or supply of products or services, including the following. - Target for measurement - Method and frequency of reporting on measures taken - Measures to be taken when measures are not implemented - The organization checks means of detecting (or preventing) falsifications and leakages during shipments and whether or not the IoT devices and software being delivered have been operated without authorization. - Goods: security courier, protection seal, etc. - Digital transfer: encryption, hash of the entire transmitted data, etc. [Reference] When examining security requirement specifications for systems and components, resources such as the “Practical Guidebook on the List of Security Requirements for IT Product Procurement, Version 2.1” (IPA, 2026), the “Labeling Scheme based on Japan Cyber-Security Technical Assessment Requirements” (JC-STAR), and the “Non-Functional Requirements Grade” (IPA, 2018) are available for reference.	O	-		-	○ (6.2.6.1)	-
			<Basic> - The organization confirms the following when selecting relevant parties for the provision of products and services. - The product/service support period is sufficient, including the distribution of security patches. - The response after the support period has been identified. - During procurement, the organization confirms whether the IoT devices which the organization possesses are genuine products by checking the label. - By utilizing IDs, secret keys, and electronic certificates included in the IoT devices and software, an organization confirms that procured devices are genuine products.	O	○ (03.17.03 Supply Chain Requirements and Processes b.)	○ (SA-04, SA-09, SR-03)	-	-	-

- Examples of security measures for each of the High Advanced, Advanced, and Basic levels are stated for implementing measure requirements described in Part III. To implement High Advanced-level measures, there is a need to include not only High Advanced-level measures but also Advanced- and Basic-level measures.

- The level of a measure is determined according to the costs in implementing/operating the measure, the scope of the measure (e.g., whether the scope is applied only to the organization or other related organizations), etc., based on management measures stratified into levels.

- The subject that implements measures is classified as “S” (implemented by a system through technical means), as “O” (implemented by an organization (e.g., by people through non-technical means)), and as “O/S” (implemented by both a system and an organization).

- In describing the examples of security measures, reference is made to major security documents and other relevant materials (shown as “Reference Guidelines” in the table).

- The measures described in this section are just examples and do not deny other implementation methods. Use this document as a reference for risk management according to the characteristics of the business of each organization, the results of the risk analyses, etc.

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measure	Reference Guidelines				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 Annex A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.GV.SC-08	The organization periodically evaluates other relevant organizations such as business partners using audits, test results, or other forms of assessment to confirm that they are fulfilling their contractual obligations.	L1_1_d_ORG L3_3_b_ORG L3_3_c_ORG L3_1_b_ORG L3_3_d_ORG L3_1_c_ORG L3_3_a_ORG	<High-Advanced> - The organization prepares a procedure to continuously monitor whether the security requirements from the contractee are complied with by the staff of the contractor, and to enable notification to the organization's personnel in charge in the case where irregular behavior is found. - The organization adopts an automatic mechanism integrating review, analysis, and report that supports the investigation and addresses procedures for deviation or signs of deviation from contract matters. - The organization uses a mechanism that allows it to list and check whether obligatory matters stipulated in the contract are fulfilled, matters which are concerned with security management of the organization and security functions implemented in the products and services that will be delivered, especially for important clients and reconsigned organizations. - State of compliance with security management measures of the external service provider is regularly checked by external audits and field surveys conducted by the outsourcer. - The important business partners and if possible their re-contractors etc. investigate whether there is any sign of attack related or any fact of information leakage, and regularly report the result to the organization. - The organization checks whether requirements that are prescribed in the contract with the client can be audited on the system. - The information system provides a function that allows for audit records to be created for events defined above that can be audited on the system. - The organization regularly reviews and analyzes audit records that are made manually or automatically by the system, and checks whether there is any deviation or sign of deviation from contract matters.	O/S	○ (In addition to the following, 03.16.03 External System Services c.)	○ (In addition to the following, RA-09, SR-06)	○ (A.5.22)	-	-
			<Advanced> - The organization adjusts the format and frequency of assessments according to the reputation of third parties and the criticality of provided products or services. - The organization assesses, at least annually, the security posture of subsidiaries or business partners meeting one or more of the following conditions, referring to the examples below. [Conditions for subsidiaries or business partners subject to security assessments] - Receiving or sharing the organization's critical and sensitive information - Playing a critical role in the organization's business continuity - Having access to the organization's internal systems from their own environments [Examples of methods for monitoring security implementation] - Conducting on-site inspections of business partners - Preparing security measure checklists and receiving completed responses - The organization evaluates evidence from third parties (e.g., self-declarations, letters of attestation, certifications, and other deliverables) regarding compliance with contractual cybersecurity requirements. - The organization monitors critical suppliers using various methods, such as on-site inspections, audits, tests, and other assessment means, to verify that they fulfill their security obligations throughout the lifecycle of the business relationship. - The organization ensures that it can maintain consistency in security audits with other organizations that require information on the audit.	O	○ (03.17.03 Supply Chain Requirements and Processes a.)			-	-
			<Basic> - The organization verifies certificates of various certifications and schemes (e.g., ISMS certification, CSMS certification, PrivacyMark, and the SCS-AP) in place of confirming the implementation of required security measures.	O	-	○ (PM-31, RA-03, RA-05, RA-07, SA-04, SA-09, SR-02, SR-03, SR-05)		-	-
CPS.GV.SC-09	The organization establishes and implements procedures to be followed when non-compliance with contractual requirements is identified through audits or testing of other relevant organizations such as business partners.	L1_1_a_PRO L1_1_b_PRO L1_1_c_PRO	<High-Advanced> - The organization formulates and manages a procedure to execute the following when nonconformity by the partner is found at an audit or test. 1) Identify and assess the influence in terms of security arising from such nonconformity. 2) Decide whether to review the security requirements defined in the contract. 3) Decide the corrective action to be taken to achieve the acceptable security level within the procured products and services. 4) Agree with the partner on the above.	O	-	○ (In addition to the following, RA-09, SR-06)	○ (A.5.22)	-	-
			<Advanced> - The organization formulates and manages a procedure to, when nonconformities are found in audits of business partners or in tests of products or services, the organization identifies the risks to itself arising from the resulting defects.	O	○ (03.17.03 Supply Chain Requirements and Processes a.)			-	-
			<Basic> - The organization is aware of the risk to its own organization due to the failure of its products and services when nonconformities are found in audits of business partners or in tests of products or services, the organization identifies the risks to itself arising from the resulting defects.	O	-	○ (PM-31, RA-03, RA-05, RA-07, SA-04, SA-09, SR-02, SR-03, SR-05)		-	-
CPS.GV.SC-10	The organization establishes policies and procedures for determining, based on the criticality of the technology products and services to be procured, those for which records of their sources and, to the extent reasonably ascertainable, their distribution channels are to be obtained.	L1_1_a_ORG L1_1_b_ORG L1_1_c_ORG	Common among <High-Advanced>, <Advanced> and <Basic> - The organization establishes policies and procedures to obtain records of the origin and distribution channels for all procured technology products and services.	O	○ (03.16.03 External System Services c.)	○ (PM-09, PM-19, PM-28, PM-30, PM-31, RA-03, RA-05, RA-07, SA-04, SA-06, SA-09, SR-02, SR-03, SR-05)	-	-	-

- Examples of security measures for each of the High Advanced, Advanced, and Basic levels are stated for implementing measure requirements described in Part III. To implement High Advanced-level measures, there is a need to include not only High Advanced-level measures but also Advanced- and Basic-level measures.

- The level of a measure is determined according to the costs in implementing/operating the measure, the scope of the measure (e.g., whether the scope is applied only to the organization or other related organizations), etc., based on management measures stratified into levels.

- The subject that implements measures is classified as “S” (implemented by a system through technical means), as “O” (implemented by an organization (e.g., by people through non-technical means)), and as “O/S” (implemented by both a system and an organization).

- In describing the examples of security measures, reference is made to major security documents and other relevant materials (shown as “Reference Guidelines” in the table).

- The measures described in this section are just examples and do not deny other implementation methods. Use this document as a reference for risk management according to the characteristics of the business of each organization, the results of the risk analyses, etc.

Measure Requirement ID	Measure Requirement	Correspondin g Vulnerability ID	Examples of security measure	Subject that implements measure	Reference Guidelines					
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 Annex A	IEC 62443-2-1:2024	IEC 62443-3-3:2013	
CPS.GV.SC-11	The organization establishes and implements procedures to be followed upon the termination of contracts with partners and other parties.	L1_1_a_PRO L1_1_b_PRO L1_1_c_PRO	Common among <High-Advanced> and <Advanced> - The organization agrees with the present business partner whether the supply of the products or services should be cancelled or they should be returned to the organization or the other business partner. - The organization communicates with the stakeholders who are influenced by the supply of the products or services to provide information on the discontinuation. - The organization executes the discontinuation of the supply of the products or services in accordance with the discontinuation plan. - The organization manages data leakage risks associated with the termination of business with suppliers. - The organization verifies that access privileges of suppliers to its resources are promptly revoked when they are no longer needed. - The organization verifies that assets containing its data are returned or disposed of in a timely manner through managed and secure methods. - The organization agrees with business partners on the accomplishment of the discontinuation of the supplied products or services.	O	-	○ (In addition to the following, SR-06)	○ (A.5.11)	-	-	
			<Basic> - The organization develops and executes plans for terminating or transitioning business relationships with suppliers, considering supply chain security risks and resiliency. - The organization always keeps track of when contracts with other relevant organizations such as business partners expire or are terminated.	O	-	○ (PM-31, RA-03, RA-05, RA-07, SA-04, SA-09, SR-02, SR-03, SR-05)	-	-	-	
CPS.GV.SC-12	The organization collects and securely retains information (data) to demonstrate that it is fulfilling its contractual obligations to other relevant organizations and individuals, ensuring it can be disclosed to an appropriate extent when necessary.	-	<High-Advanced> - The organization uses a trail storage system with the following features to flexibly fulfill the needs of clients and other related organizations, such as a third-party auditing institution, on a real-time basis. - Eligibility of the subject audit trail for the contract matter can be verified quickly. - Only authorized entities such as clients and outsourced auditing agencies can access the system. - Stored data has reliable trails such as time stamps and electronic signatures.	O	-	-	-	-	○ (SR 6.1)	
			<Advanced> - The organization takes measures so that those records among the audit records generated by the system that are acquired over a long period of time can be obtained with certainty. - In order to protect audit records from the following threats, it is desirable for the system to apply fine-grained access control to the components and systems in which audit records are stored. - Change format of recorded message - Change or delete log file - Exceed storage space of log file medium	O/S	-	-	-	-		
			<Basic> - The organization preserves audit records for an appropriate period of time so as to satisfy the requirements of laws and regulations.	O	-	-	-	-	-	
CPS.ID.AM-01	The organization develops and appropriately manages inventories of hardware, software, and their management information (e.g., name, version, network address, designated manager, and license information) that comprise its system.	L1_1_a_COM L1_1_b_COM L1_1_c_COM L2_1_a_ORG L2_1_c_ORG	<High-Advanced> - The organization identifies assets constituting its information systems and industrial control systems (hardware, including IoT devices; software; and information) uniquely and assigns a responsible person to each asset. And the organization maintains/manages lists, including configuration information of assets (e.g., names, version information, license information, and locations), periodically or upon request from operators, while recognizing situations in real time. - It is envisaged that some IoT devices cannot connect to the existing asset management system. Hence, the organization manages assets and configurations with the possibility of operating more than one asset management system in mind, within the organization's manageable bounds. - The information system and industrial control system implement and operate a mechanism that automatically detects unauthorized assets and removes them from management information, disconnects them from the system, or takes other such actions.	O/S	-	○ (In addition to the following, 03.04.10 System Component Inventory b.)	○ (AC-20, CM-08, PM-05, SA-05, SA-09)	○ (A.5.9)	○ (6.3.2.1, 7.2.1.1)	○ (SR 7.8)
			<Advanced> - The organization creates and maintains an up-to-date list of smart devices, including manufacturers, operating systems, and quantities. - The organization creates and maintains an up-to-date list of IoT devices and equipment comprising industrial control systems, including manufacturers, operating systems, and quantities. - The organization creates and maintains an up-to-date list of all types of software and services, including commercial off-the-shelf software, open-source software, custom-developed applications, API services, and cloud-based application services. - The organization creates and maintains an up-to-date list of software permitted for internal use on company-issued computers. - The organization maintains and manages created inventories including configuration information of assets (e.g., names, version information, license information, and location) by periodically reviewing and updating them at least annually.	O					○ (7.2.1.1)	
			<Basic> - The organization identifies assets constituting its information system and industrial control system (hardware, software and information), assigns a responsible person to each asset, and documents a list of them. - It is desirable to list all the assets held, but if the target is huge, consider narrowing down the target assets through integration (grouping) of the analysis target and exclusion from the analysis target. - The organization sets priorities to the identified assets based on the importance of them in its business operation. - The organization documents information that serves as a baseline including an information system's and an industrial control system's network configuration, assets, information about device setups and configurations, and regularly checks the document to see if its content remains relevant. - The organization manages peripherals in use (e.g., USB flash drives) using a management ledger and keeps them in a locked place.	O					○ (03.04.10 System Component Inventory a.)	

- Examples of security measures for each of the High Advanced, Advanced, and Basic levels are stated for implementing measure requirements described in Part III. To implement High Advanced-level measures, there is a need to include not only High Advanced-level measures but also Advanced- and Basic-level measures.

- The level of a measure is determined according to the costs in implementing/operating the measure, the scope of the measure (e.g., whether the scope is applied only to the organization or other related organizations), etc., based on management measures stratified into levels.

- The subject that implements measures is classified as “S” (implemented by a system through technical means), as “O” (implemented by an organization (e.g., by people through non-technical means)), and as “O/S” (implemented by both a system and an organization).

- In describing the examples of security measures, reference is made to major security documents and other relevant materials (shown as “Reference Guidelines” in the table).

- The measures described in this section are just examples and do not deny other implementation methods. Use this document as a reference for risk management according to the characteristics of the business of each organization, the results of the risk analyses, etc.

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measure	Reference Guidelines				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 Annex A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.ID.AM-02	The organization develops and appropriately manages communication network diagrams and data flow diagrams within the organization.	L1_1_a_COM L1_1_b_COM L1_1_c_COM L1_3_b_ORG L1_3_c_ORG	<High-Advanced> - The organization implements/manages an automated mechanism for monitoring and managing system configurations, communication network configurations, and data flows of their information systems and industrial control systems in real time.	O/S	-	○ (In addition to the following, AC-04, PL-08)	-	○ (In addition to the following, 8.2.2.1, 8.3.1.1)	○ (SR 7.6)
			<Advanced> - The organization establishes and maintains an up-to-date baseline of communications and data flows within its wired and wireless networks. - The organization establishes and maintains an up-to-date baseline of communications and data flows between the organization and third parties. - The organization establishes and maintains an up-to-date baseline of communications and data flows within Infrastructure as a Service (IaaS) environments it utilizes. - The organization establishes and maintains an up-to-date inventory of network ports, protocols, and services routinely used among authorized systems. - The organization states the characteristics of the interface, security requirements, and characteristics of transmitted data for network connection in a diagram in the associated documents. [Reference] For procedures on documenting system architectures, network configurations, and data flows, sections 3.2 and 3.3 in “Security Risk Assessment Guide for Industrial Control Systems, 2nd Edition” (IPA, 2026) are available for reference.	O/S	-		-		-
			<Basic> - The organization establishes a mechanism to identify and track the locations, purposes, and other details of its networks. - The organization establishes a mechanism to identify the manufacturers, models, maintenance service providers, and other details of its network equipment.	O	-	○ (CA-03, CA-09, PL-02, PM-07)	-	○ (7.2.1.1, 7.2.2.1)	-
CPS.ID.AM-03	The organization develops and appropriately manages inventories of external information systems connected to its organizational assets.	L1_1_a_COM L1_1_b_COM L1_1_c_COM L1_3_b_ORG L1_3_c_ORG	<High-Advanced> - The information system automatically makes a list of external information services utilized by the organization in real time, and manages the users, devices, and other relevant entities as well as services in use. - The information system uses a mechanism to give notice to the system administrator when an unpermitted external information system service is detected.	S	-	○ (AC-20, SA-09, SR-02)	-	-	-
			<Advanced> - The organization sets conditions for allowing other organizations which own or operate external information systems to do the following: a. Accessing an information system in the organization from an external information system b. Processing, saving, or transmitting information under the control of the organization using an external information system - The information system restricts access to organization-owned storage hosted on external systems to authorized individuals only. - The organization reviews the inventory of external services utilized at least annually, updating the inventory as necessary, as well as when a new external service is adopted.	O/S	-		-	-	-
			<Basic> - The organization establishes an inventory of all external services it uses (including systems managed or provided by customers, subsidiaries, affiliates, and business partners, as well as third-party provided IaaS, PaaS, SaaS, APIs, and other externally hosted application services) and defines the roles and responsibilities as a user for each service.	O	-		-	-	-
CPS.ID.AM-04	The organization categorizes and prioritizes resources (e.g., components, data, and systems) based on their function, criticality, and business value, defines management responsibilities, and communicates them to relevant organizations and people involved in their operation.	L3_4_a_ORG L3_4_a_DAT L3_4_b_DAT L3_1_b_DAT L3_1_a_ORG L3_1_c_DAT	Common among <High-Advanced> and <Advanced> - The organization considers business requirements and legal requirements which share or restrict data when classifying resources of the information system and industrial control system (data, components processing data, system, etc.). - The organization includes classification rules and criteria for periodically reviewing classifications in its resource classification system. - The organization identifies asset priorities and updates them periodically or whenever significant changes occur within the organization.	O	-	○ (In addition to the following, RA-09)	○ (A.5.12)	○ (10.2.1.1)	-
			<Basic> - The organization designates system administrators and responsible persons for all servers and network devices. - When related laws or regulations require certain classifications for its resources (e.g., systems and data), the organization applies an appropriate classification to the asset. - The organization sets priorities on identified information assets according to importance to the organization. - When classifying and prioritizing components, systems, and other items, particularly in industrial control systems, the organization conducts such processes taking into account whether adverse effects on health, safety, and environment (HSE) may arise from improper operations of its business activities. [Reference] Methods for calculating asset criticality include approaches evaluating the confidentiality, integrity, and availability of information described on pages 44 and 45 of “Information Security Measures Guidelines for Small and Medium-sized Enterprises, Version 4.0” (IPA, 2026), as well as approaches evaluating the magnitude of business damage described on page 14 of the “Security Risk Assessment Guide for Industrial Control Systems, 2nd Edition” (IPA, 2026). Furthermore, regarding criteria for determining asset criticality specifically in industrial control systems, sections 4.2.2 and 4.2.3 of the “Security Risk Assessment Guide for Industrial Control Systems, 2nd Edition” (IPA, 2026) are available for reference.	O	-	○ (RA-02, RA-03)		-	-
CPS.ID.AM-05	The organization develops and appropriately manages inventories of data and metadata in its possession.	L3_4_a_DAT L3_4_b_DAT L3_1_b_DAT L3_1_c_DAT	Common among <High-Advanced> and <Advanced> - The organization continuously searches for and analyzes unstructured data across the organization to determine whether data subject to protection is newly included. - The organization continuously identifies the source of acquisition, data custodian, and storage location for each individual record of data subject to protection. - The organization reviews, at least annually, its critical and sensitive information and the associated details for each piece of information, including administrator name, department, storage location, retention period, disclosure recipients, and administrator’s contact information.	O	○ (03.04.11 Information Location a.)	○ (In addition to the following, CM-12)	○ (A.5.9)	○ (10.2.1.1)	-
			<Basic> - The organization creates and maintains an up-to-date inventory of specific types of data to be protected (e.g., personal information, medical information, financial account numbers, the organization’s intellectual property, and data related to industrial control systems).	O	-	○ (SI-12)		-	-

- Examples of security measures for each of the High Advanced, Advanced, and Basic levels are stated for implementing measure requirements described in Part III. To implement High Advanced-level measures, there is a need to include not only High Advanced-level measures but also Advanced- and Basic-level measures.

- The level of a measure is determined according to the costs in implementing/operating the measure, the scope of the measure (e.g., whether the scope is applied only to the organization or other related organizations), etc., based on management measures stratified into levels.

- The subject that implements measures is classified as “S” (implemented by a system through technical means), as “O” (implemented by an organization (e.g., by people through non-technical means)), and as “O/S” (implemented by both a system and an organization).

- In describing the examples of security measures, reference is made to major security documents and other relevant materials (shown as “Reference Guidelines” in the table).

- The measures described in this section are just examples and do not deny other implementation methods. Use this document as a reference for risk management according to the characteristics of the business of each organization, the results of the risk analyses, etc.

Measure Requirement ID	Measure Requirement	Correspondin g Vulnerability ID	Examples of security measure	Subject that implements measure	Reference Guidelines				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 Annex A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.ID.AM-06	The organization manages systems, hardware, software, services, and data throughout their entire lifecycle, from acquisition to disposal.	L1_1_a_COM L1_1_b_COM L1_1_c_COM	Common among <High-Advanced>, <Advanced> and <Basic> - The organization incorporates cybersecurity perspectives throughout the entire lifecycle of systems, hardware, software, services, and products. - The organization establishes management rules for information equipment, operating systems, and software, including rules for adoption, installation, network connection, and security patch application. - The organization reviews, at least annually, compliance with management rules for information equipment, operating systems, and software, including rules for adoption, installation, network connection, and security patch application.	O	○ (03.04.08 Authorized Software – Allow by Exception a, 03.04.10 System Component Inventory c, 03.08.07 Media Use a, 03.16.02 Unsupported System Components a.)	○ (CM-09, MA-02, MA-06, PL-02, PM-22, PM-23, SA-03, SA-04, SA-08, SA-22, SI-12, SR-05, SR-12)	○ (A.7.10)	-	-
CPS.ID.AM-07	The organization establishes identification methods to ensure traceability according to the importance of the components it produces within the supply chain.	L1_3_a_COM L1_3_b_COM	<High-Advanced> - When traceability is a requirement, the organization manages a unique identification to outputs (products) and maintains documented necessary information for enabling traceability. - It is desirable for the organization to consider a method of unique identification in accordance with the rules applicable to different industries such as cross-industry common numbering rules. [Reference] “ISO 9001:2015” 8.5.2 Identification and Traceability	O	-	-	-	-	-
			Common among <Advanced> and <Basic> - The organization prioritizes the products of the organization into multiple stages from the viewpoint of the following example. - Extent of the impact in the supply chain when problems (e.g., regarding product quality) are found. - Magnitude of the impact on the business of the organization when problems (e.g., regarding product quality) are found. - The organization specifies an appropriate method of identifying outputs (e.g., adding serial numbers) such as adding numbers depending on the importance of the components produced by the organization on its supply chain. - The organization identifies the conditions of output products and services with respect to compliance requirements under applicable laws, regulations, and contracts throughout organizationally defined processes during production and service provision (e.g., up to the point of customer delivery).	O	-	-	-	-	-
CPS.ID.AM-08	The organization prepares and implements internal rules regarding records of production activities in order to create records concerning production date and time, conditions, and states, and store them for a certain period according to importance.	L1_3_a_COM L1_3_b_COM	<High-Advanced> - The organization prepares internal rules related to production activities, and based on the possibility that records of produced components may be later audited in accordance with their importance, shares awareness with partners regarding importance in advance, and ensures an appropriate level of record management. - It is desirable that records of production activities that are created and managed can be quickly searched by production date, classification of components (e.g., product name), and the like.	O	-	-	-	-	-
			Common among <Advanced> and <Basic> - The organization creates a record such as the date of production and condition of components depending on the importance of the produced component on the supply chain, and prepares and manages internal rules of production activities in order to store components for a certain period of time. - The organization considers the following when creating or updating the above records. - Making an appropriate identification and description (e.g., title, date, documenter, reference number) - Recording in appropriate format (e.g., language, software version, charts) and media (e.g., paper, electronic media) - Obtaining appropriate review and approval regarding adequacy and validity	O	-	-	-	-	-
CPS.ID.RA-01	The organization identifies vulnerabilities in its assets and manages them by linking them to the corresponding assets.	L1_1_a_SYS L1_1_b_SYS L1_1_c_SYS L2_1_a_ORG L2_1_c_ORG L3_3_d_SYS L3_1_a_SYS L3_3_a_SYS	<High-Advanced> - The organization conducts vulnerability scans at planned timings such as planned stopping so as not to adversely affect the operation of the system managed by the organization. And then, identify and list vulnerabilities that exist in the system owned by the organization. - When conducting vulnerability scans, it is desirable to use a vulnerability scanning tool that can update its vulnerability database for the systems to be scanned. - The organization develops mechanisms to temporarily permit privileged access to an inspector during vulnerability scans to more thoroughly identify vulnerabilities. - The organization is encouraged to periodically conduct a penetration test to recognize an existing vulnerability in a system it manages.	O	-	○ (In addition to the following, CA-08)	○ (A.8.8)	○ (6.3.2.1, 12.2.9.1)	-
			<Advanced> - The organization carries out vulnerability scans to recognize vulnerabilities existing in the information system which has high importance (e.g., internet-facing devices), and makes a list of them. - The organization utilizes vulnerability management tools to identify unpatched software and misconfigured software. - The organization evaluates network and system architectures to identify design and implementation weaknesses that affect cybersecurity. - The organization evaluates facilities where critical equipment is installed to clarify physical vulnerabilities and resilience issues. - In the operation phase of an information system owned by the organization, the organization uses a vulnerability scanning tool to periodically identify its system vulnerability within vulnerabilities collected from various sources, which are supposed to be related to the organization. The organization add the identified vulnerability and its impact degree to a list. [Reference] Japan Vulnerability Notes (https://jvn.jp/) and other sources of information are available for reference to obtain information regarding vulnerability. Also, CVSS (https://www.ipa.go.jp/security/vuln/scap/cvssv3.html , explained by IPA) could be used as a referential indicator to evaluate the impact level of vulnerability.	O	-	○ (In addition to the following, SA-11, SA-15)		○ (8.2.2.1)	-
			<Basic> - The organization utilizes alerts such as critical security information published by IPA and JPCERT/CC to identify control vulnerabilities in its information systems.	O	○ (03.14.01 Flaw Remediation a)	○ (CA-02, CA-07, RA-03, RA-05, SI-04, SI-05)		-	-

- Examples of security measures for each of the High Advanced, Advanced, and Basic levels are stated for implementing measure requirements described in Part III. To implement High Advanced-level measures, there is a need to include not only High Advanced-level measures but also Advanced- and Basic-level measures.

- The level of a measure is determined according to the costs in implementing/operating the measure, the scope of the measure (e.g., whether the scope is applied only to the organization or other related organizations), etc., based on management measures stratified into levels.

- The subject that implements measures is classified as “S” (implemented by a system through technical means), as “O” (implemented by an organization (e.g., by people through non-technical means)), and as “O/S” (implemented by both a system and an organization).

- In describing the examples of security measures, reference is made to major security documents and other relevant materials (shown as “Reference Guidelines” in the table).

- The measures described in this section are just examples and do not deny other implementation methods. Use this document as a reference for risk management according to the characteristics of the business of each organization, the results of the risk analyses, etc.

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measure	Reference Guidelines				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 Annex A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.ID.RA-02	The organization establishes a process to collect, analyze, respond to, and utilize vulnerability and threat information from internal and external sources (e.g., internal tests, security information, and security researchers).	L1_1_a_SYS L2_1_a_ORG L3_3_d_SYS L3_1_a_SYS L3_3_a_SYS	<High-Advanced> - The organization updates knowledge about security in both an information system and industrial control system to the latest by attending workshops and meetings related to security and by maintaining an appropriate communication structure with security professional associations/institutions. - The organization updates security knowledge to the latest by attending workshops and meetings related to security and by maintaining an appropriate communication structure with security professional associations/institutions. - The organization continuously identifies and monitors potential threat actors targeting it and the tactics, techniques, and procedures (TTPs) they are likely to use, from trusted third parties and cyber threat intelligence sources. - The organization continuously collects information on specific vulnerabilities introduced by advanced technologies from cyber threat intelligence sources. - The organization configures cybersecurity tools with detection or response capabilities to receive cyber threat intelligence automatically and securely. - The organization analyzes mainly the products and services it provides to check if any new vulnerability is contained, and if detected, submit related information to IPA.	O	-	○ (PM-15, PM-16, RA-05, SI-05)	○ (In addition to the following, A.5.6)	○ (12.2.9.1)	-
			<Advanced> - The organization defines the sources, tools, and frequency for collecting vulnerability and threat information. - The organization defines criteria for determining the necessity of action regarding collected vulnerability and threat information, as well as response procedures. - The organization continuously collects information on new vulnerabilities in products and services from cyber threat intelligence sources. - The organization shares vulnerability information between itself and its suppliers in accordance with contractually established rules and procedures. [Reference] When planning, establishing, and operating a security response organization, in addition to utilizing services from external providers, documents such as the “CSIRT Materials” published by JPCERT/CC and the “Textbook for security response organisation (SOC/CSIRT) - using X.1060 -” published by the Information Security Operation providers Group Japan (ISOG-J) are available for reference.	O	○ (In addition to the following, 03.11.02 Vulnerability Monitoring and Scanning c.)		○ (A.5.7)		-
			<Basic> - In addition to information such as the critical security information published by IPA and JPCERT/CC, the organization checks security-related cautions offered by device vendors and software vendors, and notifies stakeholders within the organization about them.	O	○ (03.14.03 Security Alerts, Advisories, and Directives a.)				-
CPS.ID.RA-03	- The organization identifies and documents potential security incidents, their impacts, and their causal factors regarding organizational assets. - From the planning and design stages of IoT devices and IoT-integrated systems, the organization verifies that no unacceptable known security risks exist, incorporating safety hazard perspectives.	L1_1_a_SYS L1_1_b_SYS L1_1_c_SYS L2_1_a_COM L2_2_a_SYS	<High-Advanced> - The organization conducts threat hunting to actively search for traces of attackers lurking within the organization. - As necessary, the organization utilizes services provided by experts, obtains information that only some experts can know, and uses them to identify threats. - When developing a new device or a new component which may have an impact on a physical space such as components of an industrial control system, the organization collects/analyzes accident case studies of conventional products and others to identify safety-related hazards. - The organization analyzes a situation where a hazard leads to harm and identifies the possibility of occurrence and the severity of the harm to estimate a possible risk especially regarding an industrial control system. At the time, it is desirable to check whether there is any hazard caused by a security issue.	O	-	○ (PM-12, PM-16, RA-03, SI-05)	-	○ (6.3.1.1, 8.2.6.1)	-
			<Advanced> - The organization collects information including newly released attacking trends, malware behaviors, and malicious IP addresses/domains (external intelligence). - The organization evaluates the reliability of the obtained threat information, impacts on the organization, etc., selects vulnerabilities to be handled, and documents threats to be handled. - When planning/designing a new system using an IoT device, the organization identifies existing assets and assets to be protected in the system to be implemented and organizes security measures according to use and configuration of the system. When handling a component or a system with a long life cycle and a component or a system requiring availability, consideration in security measures at a phase before designing is especially important.	O	-		-	○ (6.3.1.1, 8.2.6.1, 12.2.9.1)	-
			<Basic> - The organization identifies security threats to the organization and their likelihood of occurrence, utilizing baseline documents for identifying security threats, such as section 4 (1) of Part 2 “Asset-Based Risk Analysis” and Appendix 6 “Asset Management Ledger” of the “Information Security Measures Guidelines for Small and Medium-sized Enterprises, Version 4.0” (IPA, 2026).	O	○ (03.11.01 Risk Assessment a.)		-	○ (6.3.1.1, 8.2.6.1)	-

- Examples of security measures for each of the High Advanced, Advanced, and Basic levels are stated for implementing measure requirements described in Part III. To implement High Advanced-level measures, there is a need to include not only High Advanced-level measures but also Advanced- and Basic-level measures.

- The level of a measure is determined according to the costs in implementing/operating the measure, the scope of the measure (e.g., whether the scope is applied only to the organization or other related organizations), etc., based on management measures stratified into levels.

- The subject that implements measures is classified as "S" (implemented by a system through technical means), as "O" (implemented by an organization (e.g., by people through non-technical means)), and as "O/S" (implemented by both a system and an organization).

- In describing the examples of security measures, reference is made to major security documents and other relevant materials (shown as "Reference Guidelines" in the table).

- The measures described in this section are just examples and do not deny other implementation methods. Use this document as a reference for risk management according to the characteristics of the business of each organization, the results of the risk analyses, etc.

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measure	Reference Guidelines				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 Annex A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.ID.RA-04	The organization identifies the potential impact and likelihood of threats exploiting vulnerabilities by periodically conducting risk assessments to evaluate the effectiveness of security rules for component management, including their implementation methods.	L1_1_a_SYS L1_1_b_SYS L1_1_c_SYS L2_1_a_ORG	<High-Advanced> - The organization uses automated mechanisms for risk assessment (e.g., assessment of the scope of impact) when it receives information about newly identified threats and vulnerabilities. - The organization updates the risk assessment if there is a significant change in the industrial control system or the environment in which it operates, or when other circumstances arise that affect the security state of the industrial control system.	O	-	○ (In addition to the following, RA-09)	-	○ (6.3.1.1, 8.2.6.1, 12.2.9.1)	-
			<Advanced> - The organization updates a risk assessment when there is a big change in information systems, industrial control systems, or the environment where such systems are running (including identification of a new threat or vulnerability) or when any situation which impacts the security status of the system occurs. In doing so, the organization prioritizes critical information systems. - The organization determines the potential impacts when cascading failures occur in architectures where multiple systems are interconnected.	O	-		-		-
			<Basic> - The organization defines a security risk assessment process for information systems and industrial control systems and applies it periodically (e.g., annually for critical information systems). - Establish and maintain security risk criteria. - Identify security risks in the following way. 1) Clarify the target of analysis. 2) Identify incidents (including changes in circumstances) and their causes. - Analyze security risks in the following way. 1) Evaluate possible results when the above identified risks occur. 2) Evaluate the possibility of the actual occurrence of the above identified risks. - Refer to the risk criteria, determine a risk level, and prioritize the risk. - The organization documents and stores the information security risk assessment process. - The organization prioritizes systems and sets risk assessment frequencies and scopes, taking into account perspectives such as the anticipated magnitude of damage in the event of a security incident, the likelihood of an incident occurring (e.g., whether the system is connected to the internet), and the person-hours required to conduct the risk assessment. - The organization creates threat models to deepen its understanding of risks to data and to implement appropriate risk responses.	O	○ (03.11.01 Risk Assessment a.b, 03.12.01 Security Assessment)	○ (PM-09, PM-11, PM-16, RA-02, RA-03, RA-07)	-		-
CPS.ID.RA-05	The organization shares information regarding the effectiveness of protective technologies with appropriate partners.	L2_1_a_ORG	<High-Advanced> - The organization prepares a setting through an automated mechanism at just the right time that enables it and its appropriate partners to interactively share new information about data protection technologies or information about the effectiveness of the protection technologies.	O	-	-	○ (A.5.6)	-	-
			<Advanced> - The organization prepares a setting that enables it to share new information about data protection technologies or information about the effectiveness of the protection technologies with its partners at just the right time.	O	-	-		-	-
			<Basic> - The organization prepares a setting that enables it to acquire new information about data protection technologies or information about the effectiveness of the protection technologies from its appropriate partners. [Reference] When selecting an appropriate partner, services from providers listed on the "List of Services Compliant with the Information Security Service Standards" may be utilized. Additionally, the partner is expected to include personnel holding security-related credentials, such as Registered Information Security Specialist (RISS) or CISSP.	O	-	-		-	-
CPS.ID.RA-06	- Based on risk assessments, the organization clearly defines response measures for potential security risks, documents the defined scope and priorities of response actions, monitors the implementation progress, and communicates this status to relevant parties. - The organization appropriately addresses security and associated safety risks identified through the assessment in the planning and design stages of IoT devices and IoT-integrated systems.	L1_1_a_SYS L1_1_b_SYS L1_1_c_SYS L2_1_a_ORG L2_1_a_COM L2_1_c_ORG L2_2_a_SYS	<High-Advanced> - On the basis of the results of the hazard analysis performed in CPS.ID.RA-03, mainly for the industrial control system, the organization appropriately treats the source of a risk which may lead to a critical hazard as necessary. [Reference] For integrating security into safety-related control systems, standards such as IEC TS 63074:2023 and IEC TR 63069:2019 are available for reference.	O	-	○ (PM-09, PM-18, PM-30, RA-07)	-	○ (6.3.1.1, 8.2.6.1, 12.2.9.1)	-
			<Advanced> - When the organization selects a measure according to the risk assessment results, it is desirable that the organization documents the measure to be taken and the reason why the measure is adopted. - Regarding the application of measures, the organization formulates a security risk treatment plan and obtains approval from the risk owner. - The organization reviews the security risk treatment plan and checks that the applicable plan conforms to the priority order of the entire organization's risk management strategy. - The organization communicates formulated risk response measures to affected stakeholders in descending order of criticality. - The organization informs applicable external business operators regarding security measures necessary for a new system including an IoT device which are extracted in CPS.ID.RA-03 as required specifications. - The organization verifies whether the security measures defined in the required specifications and contracts are implemented at the time of deployment of the systems including an IoT device via User Acceptance Test (UAT). If there is anything unclear, the organization confirms it with the external business operator. - The organization continuously tracks the implementation status of risk responses using action plans and milestones, risk registers, detailed risk reports, and other relevant information. - The organization periodically reviews risks that have been accepted on the condition of future remediation. - The organization securely stores the documented information on security risk treatment processes.	O	○ (In addition to the following, 03.12.02 Plan of Action and Milestones a.)		-		-
			<Basic> - The organization considers the risk assessment results and selects handling measures to identified risks. - The organization selects alternative measures in preparation for cases where primary risk reduction measures cannot be implemented. - The organization obtains approval from the risk owner for acceptance of the security risk.	O	○ (03.11.04 Risk Response)		-		-

- Examples of security measures for each of the High Advanced, Advanced, and Basic levels are stated for implementing measure requirements described in Part III. To implement High Advanced-level measures, there is a need to include not only High Advanced-level measures but also Advanced- and Basic-level measures.

- The level of a measure is determined according to the costs in implementing/operating the measure, the scope of the measure (e.g., whether the scope is applied only to the organization or other related organizations), etc., based on management measures stratified into levels.

- The subject that implements measures is classified as “S” (implemented by a system through technical means), as “O” (implemented by an organization (e.g., by people through non-technical means)), and as “O/S” (implemented by both a system and an organization).

- In describing the examples of security measures, reference is made to major security documents and other relevant materials (shown as “Reference Guidelines” in the table).

- The measures described in this section are just examples and do not deny other implementation methods. Use this document as a reference for risk management according to the characteristics of the business of each organization, the results of the risk analyses, etc.

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measure	Reference Guidelines				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 Annex A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.ID.RA-07	The organization assesses the risk impact posed by significant organizational changes and security requirement exceptions, and records and manages the results.	L1_1_a_SYS L1_1_b_SYS L1_1_c_SYS	Common among <High-Advanced>, <Advanced> and <Basic> - The organization documents anticipated risks for both implementing and not implementing each proposed change, and establishes guidelines for rolling back the change. - The organization documents the risks associated with each requested exception and the response plan for those risks.	O	○ (03.04.02 Configuration Settings b, 03.04.03 Configuration Change Control b, 03.04.04 Impact Analyses a.)	○ (CA-07, CM-03, CM-04)	-	○ (7.2.4.1, 9.4.5.1)	-
CPS.ID.IM-01	The organization continuously improves its cybersecurity management posture under normal and adverse conditions, including the perspectives outlined in CPS.ID.IM-02 and subsequent requirements.		<High-Advanced> - Upon receiving approval from senior management, the organization conducts penetration testing on high-risk systems to identify opportunities for improving its security posture. - It is desirable for the organization to regularly evaluate the maturity of its security measure organizations in order to continue improving its security-related operations.	O	-	○ (In addition to the following, CA-08, SA-17, SA-17(06))	-	-	-
			<Advanced> - The organization collects and analyzes metrics that measure the effectiveness of security measures, using security tools and services, to improve its cybersecurity management system. - The organization invests in third-party assessments or independent audits to evaluate the effectiveness of its cybersecurity management system in order to identify areas requiring improvement.	O	-	○ (In addition to the following, IR-03, SA-11)	-	-	-
			<Basic> - The organization reviews, at least annually, its security incident response structure and implements improvements as necessary.	O	-	○ (AC-01, AT-01, AU-01, CA-01, CA-02, CA-05, CA-07, CM-01, CP-01, CP-02, CP-04, IA-01, IR-01, IR-04, IR-08, MA-01, MP-01, PE-01, PL-01, PL-02, PM-01, PM-04, PM-31, PS-01, PT-01, RA-01, RA-03, RA-05, RA-07, SA-01, SA-04, SA-08, SC-01, SI-01, SI-02, SI-04, SR-01, SR-05)	-	-	-
CPS.ID.IM-02	The organization continuously improves supply chain security standards and associated procedures.	-	Common among <High-Advanced>, <Advanced> and <Basic> - The organization continuously monitors the performance of business partners related to security, reviews and amends as needed the security measure criteria regarding the supply chain and related procedures based on the latest trends of security threats and regulations.	O	○ (03.17.01 Supply Chain Risk Management Plan b.)	-	-	-	-
CPS.ID.IM-03	The organization continuously improves security training and education programs for its personnel and designated contacts at critical partner organizations.	L1_1_a_PEO L1_1_b_PEO L1_1_c_PEO L1_3_c_PEO L1_1_d_PEO	Common among <High-Advanced> and <Advanced> - The organization continuously verifies the effects of education and training in order to ensure that members of the organization and persons of relevant parties in charge have a better understanding of security. - The organization reviews, at least annually, the content and execution of education and training for raising security awareness and implements improvements as necessary.	O	○ (In addition to the following, 03.02.01 Literacy Training and Awareness b, 03.02.02 Role-Based Training b.)	○ (In addition to the following, CA-08, IR-03, SA-11)	-	○ (6.2.4.1)	-
			<Basic> - The organization reviews, at least annually, the content and execution of education and training regarding security incident responses and implements improvements as necessary.	O	○ (03.06.04 Incident Response Training b.)	○ (AC-01, AT-01, AU-01, CA-01, CA-02, CA-05, CA-07, CM-01, CP-01, CP-02, CP-04, IA-01, IR-01, IR-04, IR-08, MA-01, MP-01, PE-01, PL-01, PL-02, PM-01, PM-04, PM-31, PS-01, PT-01, RA-01, RA-03, RA-05, RA-07, SA-01, SA-04, SA-08, SC-01, SI-01, SI-02, SI-04, SR-01, SR-05)	-	-	-

- Examples of security measures for each of the High Advanced, Advanced, and Basic levels are stated for implementing measure requirements described in Part III. To implement High Advanced-level measures, there is a need to include not only High Advanced-level measures but also Advanced- and Basic-level measures.

- The level of a measure is determined according to the costs in implementing/operating the measure, the scope of the measure (e.g., whether the scope is applied only to the organization or other related organizations), etc., based on management measures stratified into levels.

- The subject that implements measures is classified as “S” (implemented by a system through technical means), as “O” (implemented by an organization (e.g., by people through non-technical means)), and as “O/S” (implemented by both a system and an organization).

- In describing the examples of security measures, reference is made to major security documents and other relevant materials (shown as “Reference Guidelines” in the table).

- The measures described in this section are just examples and do not deny other implementation methods. Use this document as a reference for risk management according to the characteristics of the business of each organization, the results of the risk analyses, etc.

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measure	Reference Guidelines				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 Annex A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.ID.IM-04	The organization continuously improves asset protection processes by integrating lessons learned from security incident response as well as from monitoring, measuring, and assessing internal and external attacks.	-	Common among <High-Advanced>, <Advanced> and <Basic> - The organization derives lessons learned from the results of internal or third-party security assessments and continuously improves the processes for protecting assets.	O	○ (03.12.02 Plan of Action and Milestones b.)	-	○ (A.5.27)	○ (6.3.4.1)	-
CPS.ID.IM-05	The organization applies lessons learned from the analysis of detected events such as alerts and logs, to continuously improve security event detection processes.	L1_3_a_ORG L1_3_a_SYS	<High-Advanced> - The organization creates and tunes detection rules based on various information as sources in order to improve its detection ability. - Developing the rules of correlation analysis - Developing own signature of IPSs or IDSs - Developing the organization's own black list - The organization/system analyzes the patterns of its system's communication and security alerts to create and use a profile that summarizes typical patterns of communication and security alerts, thereby tuning its efforts to reduce the numbers of false detections and false negatives.	O	-	-	-	-	-
			<Advanced> - The organization prepares and manages a procedure for regularly reporting the state of organizational and system security to its appropriate staff members (e.g., management). It is desirable that the organization use these reports as an opportunity to recognize the latest threats and threats related to residual risks, and to improve its security. - For example, if alerts such as those shown below are issued and there is a sign of increasing security risks, raise the level of the system's monitoring activities based on information from reliable sources. * The following list is excerpted from "Six Ws on cybersecurity information sharing for enhancing SOC/CSIRT, Version 2.0" (ISOG-J, 2019). - Characteristics of attack > Attacking sequence, contents of related communication > Core of attacking code - Traces of attack > Contents of communication after being compromised > Log recorded on server or client > Other traces left on server or client - Detection name for security product	O	-	-	-	-	-
			<Basic> - N/A	-	-	-	-	-	-
CPS.ID.IM-06	The organization incorporates lessons learned from responses to security incidents to continuously improve its incident response plan.	L1_3_a_ORG L1_3_a_PEO L1_3_a_PRO L1_3_c_ORG	<High-Advanced> - The organization implements a mechanism to manage the types, number of cases, and response costs of past security incidents, enabling the identification of response trends and challenges.	O	-	○ (CP-02, IR-08, PL-02, SR-02)	○ (A.5.27)	-	-
			<Advanced> - The organization conducts a joint review with key suppliers following an incident response. - The organization identifies areas for improvement in future incident response activities based on exercises conducted in collaboration with key suppliers. - The organization reviews incident response plans annually or when improvements become necessary, and updates the plans accordingly.	O	○ (03.06.05 Incident Response Plan c.)			-	-
			<Basic> - It is advisable to use information about threats and vulnerability acquired from security incident assessment for the purpose of identifying incidents that may recur or have a major impact. - The organization identifies areas for improvement in future incident response activities based on the results of incident response evaluations (e.g., tabletop exercises, simulations, tests, internal reviews, and independent audits).	O	-			-	-
CPS.ID.IM-07	The organization incorporates lessons learned from responses to security incidents to continuously improve its business continuity plan or emergency response plan.	L1_3_a_PRO	Common among <High-Advanced>, <Advanced> and <Basic> - The organization makes sure that the procedures for business continuity and the functions of relevant measures go along with the business continuity policy for higher positions. - The organization identifies areas for improvement in business continuity plans or emergency response plans based on exercises conducted in collaboration with key suppliers. - The organization reviews and updates its business continuity plans or emergency response plans at least annually, or whenever improvements are required.	O	-	-	-	○ (13.2.1.1)	-

- Examples of security measures for each of the High Advanced, Advanced, and Basic levels are stated for implementing measure requirements described in Part III. To implement High Advanced-level measures, there is a need to include not only High Advanced-level measures but also Advanced- and Basic-level measures.

- The level of a measure is determined according to the costs in implementing/operating the measure, the scope of the measure (e.g., whether the scope is applied only to the organization or other related organizations), etc., based on management measures stratified into levels.

- The subject that implements measures is classified as “S” (implemented by a system through technical means), as “O” (implemented by an organization (e.g., by people through non-technical means)), and as “O/S” (implemented by both a system and an organization).

- In describing the examples of security measures, reference is made to major security documents and other relevant materials (shown as “Reference Guidelines” in the table).

- The measures described in this section are just examples and do not deny other implementation methods. Use this document as a reference for risk management according to the characteristics of the business of each organization, the results of the risk analyses, etc.

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measure	Reference Guidelines				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 Annex A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.PR.AA-01	The organization establishes and implements procedures to issue, manage, verify, revoke, and audit identities and credentials for authorized components, people, and procedures.	L1_1_a_SYS L1_1_b_SYS L2_1_b_SYS L2_1_c_SYS L2_3_c_SYS L3_3_a_SYS	<High-Advanced> - The organization introduces and operates, for example, the following automated mechanisms for managing accounts in their own information systems and industrial control systems. - Automatically collect account information periodically from the system to be managed - Automatically change password of privileged account - The industrial control system supports integrated account management. - After a certain period of time, the system automatically invalidates temporary accounts, emergency accounts, and accounts not in use on their system. - The information system automatically audits and reports account validation and invalidation that is associated with creation, change, and deletion of accounts in the system used by the organization.	O/S	-	○ (In addition to the following, IA-03)	○ (A.5.16, A.5.17)	-	○ (SR 1.1, SR 1.3, SR 1.5)
			<Advanced> - For each device, the organization selects either immutable hardware characteristics or identifiers securely deployed to the device as its unique identifier. - The organization discontinues the use of default user IDs across information systems and industrial control systems. - The organization changes default passwords for existing industrial control systems and establishes a policy to change default credentials for devices to be procured in the future. - With regard to the shared user account, a user who can know authentication information is managed in a list or the like, and the range of using the account can be identified. - If the information system resets the credentials for reasons such as user's forgetting credentials, the information system confirms securely that the account is its own to prevent unauthorized tampering with the credentials by a malicious party. - The organization notifies the user (or the person in charge of management) when the password is changed in an information system and an industrial control system. - The organization monitors the usage of system accounts used in an information system. - If an account needs change or becomes unnecessary, the organization notifies the management supervisor.	O/S	○ (In addition to the following, 03.05.12 Authenticator Management c,e)			○ (11.2.1.1, 11.2.8.1)	○ (SR 1.1, SR 1.4, SR 1.5)
			<Basic> - The organization appoints a management supervisor for the accounts in its information system and industrial control system. - The organization applies labels marked with identifiers to authorized hardware. - The organization establishes an application and approval process for the issuance, modification, and revocation of user IDs for its officers, employees, dispatched workers, and seconded personnel. - Regarding the sharing of user IDs, the organization applies one of the following requirements: - Do not share user IDs. - If sharing a user ID is unavoidable (e.g., when system specifications prevent issuing individual user IDs to each user), establish mechanisms to identify the individual who utilized the shared ID. - When a user ID is no longer required (e.g., when a user leaves the organization or a user ID has not been used for a certain period), the organization promptly deletes or disables the user ID. - The organization establishes an application and approval process for the issuance, modification, and revocation of administrator IDs. - The organization limits the officers, employees, dispatched workers, and seconded personnel to whom administrator privileges are granted, and then applies one of the following requirements regarding administrator IDs: - Do not share administrator IDs. - If sharing an administrator ID is unavoidable (e.g., when system specifications prevent issuing individual IDs to each administrator), establish mechanisms to identify the individual who utilized the shared administrator ID. - The organization establishes a mechanism to track which officers, employees, dispatched workers, and seconded personnel hold administrator IDs within the organization. - When an administrator ID is no longer required (e.g., when an administrator leaves the organization or an administrator ID has not been used for a certain period), the organization promptly deletes or disables the administrator ID. - The organization develops a policy on credentials (e.g., password and security key) for its own information systems and industrial control systems, and where systems support it, implements a function that cannot be set up unless the credential satisfies the policy. If such function cannot be utilized due to technical constraints, the organization implements alternative measures, such as restricting access paths and enhancing monitoring. - Develop and operate the requirements for passwords in order to ensure the minimum required complexity. - When new credentials are created, change them to at least the number of characters defined by the organization. - Store and transmit only cryptographically protected credentials. - Prohibit reuse of the same credentials for the period that the organization defines. - The organization issues, manages, and revokes cryptographic certificates, ID tokens, cryptographic keys (i.e., key management), and other credentials. - The organization allows its members to use temporary credentials to log on to the system when they have forgotten credentials, if they change immediately to a strong password. - When password compromise or unauthorized disclosure is suspected, or upon a change of users, the organization promptly changes the affected passwords.	O/S	○ (03.01.01 Account Management a,b,c,f, 03.05.05 Identifier Management b,c,d, 03.05.12 Authenticator Management a,b,d, 03.09.02 Personnel Termination and Transfer a, 03.10.01 Physical Access Authorizations b, 03.13.10 Cryptographic Key Establishment and Management)	○ (AC-01, AC-02, AC-14, IA-01, IA-02, IA-04, IA-05, IA-06, IA-07, IA-11)		○ (10.2.6.1, 11.2.1.1, 11.2.2.1, 11.2.8.1, 11.2.11.1, 11.2.12.1)	○ (SR 1.1, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 4.3)
CPS.PR.AA-02	The organization authenticates and authorizes logical access to components (physical items, systems, etc.) by IoT devices and users using highly reliable methods (e.g., multi-factor authentication) commensurate with transaction risks (personal security, privacy risks, and other organizational risks).	L1_1_a_SYS L1_1_b_SYS L1_1_c_SYS L2_1_b_SYS L2_1_c_SYS L2_3_c_SYS L3_1_a_SYS L3_3_a_SYS	<High-Advanced> - The organization requires multi-factor authentication for authenticating to information systems. - In industrial control systems, the organization enables multi-factor authentication for all remotely accessible accounts and systems, including vendor and maintenance accounts, user and engineering workstations, and human-machine interfaces (HMIs, where feasible). If multi-factor authentication is not feasible, the organization disables remote access, implements additional segmentation controls, and prioritizes credential management. - For its information systems that handle highly confidential data, the organization implements replay-resistant authentication mechanisms for access to systems, networks, etc. via privileged or non-privileged accounts. - The information system and industrial control system require authentication using a public key infrastructure (PKI), especially regarding login to a system that handles highly confidential data. * When performing authentication using PKI in an industrial control system, ensure that the processing wait time that occurs does not degrade system performance. - The information system protects wireless access to the system which handles highly confidential data by using user and device authentication in addition to encryption. - The information system allows privileged commands via remote access only for those purposes based on specified requirements. - The information system and industrial control system lay down conditions that require disconnection of the session for its system and implement a function that automatically terminates a user's session when it falls under these conditions.	S	○ (In addition to the following, 03.01.12 Remote Access d, 03.01.16 Wireless Access d, 03.05.03 Multi-Factor Authentication, 03.05.04 Replay-Resistant Authentication, 03.07.05 Nonlocal Maintenance)	○ (In addition to the following, IA-12, IA-03, AC-12)	○ (A.8.3, A.8.5)	○ (8.4.2.1, 8.4.3.1, 11.2.8.1, 11.2.9.1)	○ (SR 1.1, SR 2.6, SR 3.8)
			<Advanced> - For systems handling critical and sensitive information, the organization enforces multi-factor authentication in addition to accessing cloud services that process such information under all of the following circumstances: - When connecting to the internal environment via the internet - When administrators access systems via the internet - When users access systems handling critical and sensitive information via the internet - The organization establishes rules of approval for connecting mobile devices used in the organization to its system. - In consideration of the risk of unauthorized login to the privileged account in the system, the organization in principle prohibits login to the privileged account via the network when a sufficiently reliable authentication method cannot be implemented. - The organization periodically re-authenticates users, services, and hardware according to risk (e.g., applying Zero Trust Architecture principles). - The information system displays a notification message on the risk of the transaction (security-related risks for the user, privacy risks, etc.) when a user logs into the system. - The information system and the industrial control system make the feedback on the authentication information invisible in its system during the authentication process. - When determining access authorization, the organization considers attributes of the access requester and the target resource (e.g., geographic location, day of the week and time of day, and the security status of the requester's device).	O/S	-			-	○ (SR 1.1, SR 1.2, SR 1.10)
			<Basic> - For all user IDs and administrator IDs, the organization authenticates users with the credentials (e.g., passwords) configured for each user ID prior to granting access to systems and IT devices. - In cloud services handling critical and sensitive information, the organization uses multi-factor authentication when users and administrators access these services. - The organization in principle prohibits unauthorized wireless connections. - The organization limits wireless access to systems exclusively to pre-authorized devices and users.	O/S	○ (03.05.01 User Identification and Authentication a, 03.05.02 Device Identification and Authentication)	○ (AC-07, IA-02, IA-05, IA-07, IA-08, IA-11)		○ (11.2.8.1)	○ (SR 1.1, SR 2.2)

- Examples of security measures for each of the High Advanced, Advanced, and Basic levels are stated for implementing measure requirements described in Part III. To implement High Advanced-level measures, there is a need to include not only High Advanced-level measures but also Advanced- and Basic-level measures.

- The level of a measure is determined according to the costs in implementing/operating the measure, the scope of the measure (e.g., whether the scope is applied only to the organization or other related organizations), etc., based on management measures stratified into levels.

- The subject that implements measures is classified as “S” (implemented by a system through technical means), as “O” (implemented by an organization (e.g., by people through non-technical means)), and as “O/S” (implemented by both a system and an organization).

- In describing the examples of security measures, reference is made to major security documents and other relevant materials (shown as “Reference Guidelines” in the table).

- The measures described in this section are just examples and do not deny other implementation methods. Use this document as a reference for risk management according to the characteristics of the business of each organization, the results of the risk analyses, etc.

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measure	Reference Guidelines				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 Annex A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.PR.AA-03	The organization prevents unauthorized logins to IoT devices, servers, and related assets by implementing mechanisms such as account lockout after a specified number of failed authentication attempts and enforcing delays on subsequent login attempts until security conditions are verified.	L1_1_a_SYS L1_1_b_SYS L1_1_c_SYS L2_1_b_SYS	Common among <High-Advanced> and <Advanced> - The industrial control system sets a limit on the number of continuous login attempts on its system. If the user fails to log in, he or she will not be able to re-login for a certain period of time. - The information system and industrial control system lock the session manually or automatically if the system's non-operation continues beyond the time set by the organization. * In the industrial control system, it may be desirable not to lock session when it is assumed that a session in which an operator is required to respond immediately in an emergency may be conducted.	S	○ (In addition to the following, 03.01.08 Unsuccessful Logon Attempts b.)	-	○ (A.8.5)	○ (11.2.3.1, 11.2.15.1, 11.2.18.1)	○ (SR 1.11, SR 2.5)
			<Basic> - The information system enforces one of the following controls when logging on to personal computers and unlocking smart devices: - Adjust the number of attempts so that the retry interval increases each time an attempt fails. - Lock the device after 10 or more consecutive failed attempts. - If none of the above requirements can be configured, implement alternative measures, such as using strong passwords.	S	○ (03.01.08 Unsuccessful Logon Attempts a.)	-		-	-
CPS.PR.AA-04	The organization protects, transmits, receives, and verifies information regarding authenticated entities (ID assertions).	L1_1_a_SYS L1_1_b_SYS	Common among <High-Advanced> and <Advanced> - The organization adopts industry-standard methods for ID assertions across all scenarios and adheres to all guidance regarding the generation (e.g., data models and metadata), protection (e.g., digital signatures and encryption), and verification (e.g., signature verification) of ID assertions. - The information system protects ID assertions utilized to transmit credentials and user information between connected external systems.	O/S	-	-	-	-	-
			<Basic> - The information system protects ID assertions utilized to transmit credentials and user information within single sign-on (SSO) systems.	S	-		-	-	-
CPS.PR.AA-05	The organization defines rules regarding the granting of access privileges in its security policies and incorporates the principles of least privilege and separation of duties.	L2_1_b_SYS L2_1_c_SYS	<High-Advanced> - The organization specifies administrators who use the security functions (e.g., access authority setting) and regulates privileged accounts in its system. - The information system forces the application of users' access rights approved (by the administrator) in order to control data flows within a system (and between interconnected systems). - The information system prohibits non-privileged users from disabling, bypassing, or modifying security functions, or executing other privileged functions.	O/S	○ (In addition to the following, 03.01.05 Least Privilege b, 03.01.06 Least Privilege – Privileged Accounts a, 03.01.07 Least Privilege – Privileged Functions a, 03.03.08 Protection of Audit Information b.)	○ (In addition to the following, AC-10)	○ (A.5.15, A.8.2)	○ (11.3.2.1)	○ (SR 1.1)
			<Advanced> - The organization exercises discretionary access control according to the user's access rights in order to control data flows within an information system (and between interconnected systems). - The organization implements access control in the information system and the industrial control system based on separation of duties (e.g., user / system administrator). - The organization stipulates the results of the separation of duties assigned to the person in charge.	O/S	○ (In addition to the following, 03.01.05 Least Privilege a.)	○ (In addition to the following, AC-05, AC-06)	○ (A.5.3, A.5.15, A.8.2)	○ (11.2.4.1, 11.3.2.1)	○ (SR 1.1, SR 2.1)
			<Basic> - The organization implements access control based on separation of duties (e.g., user/system administrator) in the highly confidential information system of the organization. - If the separation of duties is difficult to implement due to the shortage of human resources, etc., it is desirable to take alternative measures such as, when a person other than the pre-designated official performs the specific duties, requiring another person to monitor the performance of such duties. - The organization limits the authority to grant, modify, or delete administrator IDs, as well as to modify settings for servers and network devices, to officers, employees, dispatched workers, and seconded personnel who require it for their duties. - The organization establishes management rules covering the following items regarding user access privileges upon logging on to systems and personal computers utilized for business operations: - Require formal application and approval for the issuance, modification, and revocation of access privileges. - Restrict granted access privileges to the minimum necessary scope. - Define requirements for periodic reviews of access privileges. - Maintain application forms or records of granted access privileges. - The organization ensures that authorized personnel can access accounts essential for maintaining safety in the event of an emergency.	O/S	○ (03.01.01 Account Management c, 03.01.02 Access Enforcement, 03.01.04 Separation of Duties a, 03.04.05 Access Restrictions for Change, 03.08.02 Media Access)	○ (AC-01, AC-02, AC-03, AC-17, AC-18, AC-19)		○ (11.2.4.1)	

- Examples of security measures for each of the High Advanced, Advanced, and Basic levels are stated for implementing measure requirements described in Part III. To implement High Advanced-level measures, there is a need to include not only High Advanced-level measures but also Advanced- and Basic-level measures.

- The level of a measure is determined according to the costs in implementing/operating the measure, the scope of the measure (e.g., whether the scope is applied only to the organization or other related organizations), etc., based on management measures stratified into levels.

- The subject that implements measures is classified as “S” (implemented by a system through technical means), as “O” (implemented by an organization (e.g., by people through non-technical means)), and as “O/S” (implemented by both a system and an organization).

- In describing the examples of security measures, reference is made to major security documents and other relevant materials (shown as “Reference Guidelines” in the table).

- The measures described in this section are just examples and do not deny other implementation methods. Use this document as a reference for risk management according to the characteristics of the business of each organization, the results of the risk analyses, etc.

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measure	Reference Guidelines				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 Annex A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.PR.AA-06	The organization periodically reviews granted access privileges and remediates unnecessary or excessive permissions.	L2_1_b_SYS L2_1_c_SYS	Common among <High-Advanced> and <Advanced> - The organization conducts periodic reviews of access privileges granted to officers, employees, dispatched workers, and seconded personnel at least annually.	O	○ (In addition to the following, 03.01.05 Least Privilege c, 03.10.01 Physical Access Authorizations c.)	○ (In addition to the following, AC-05, AC-06, AC-10)	○ (A.5.18, A.8.2)	○ (11.2.5.1)	-
			<Basic> - When access privileges granted to a user ID are no longer necessary (e.g., when a user's business role changes), the organization promptly revokes or disables these privileges.	O	○ (03.01.01 Account Management f, 03.01.05 Least Privilege d, 03.09.02 Personnel Termination and Transfer b.)	○ (AC-01, AC-02, AC-03, AC-17, AC-18, AC-19)		○ (11.2.2.1, 11.2.4.1)	-
CPS.PR.AA-07	The organization implements physical safeguards, such as locking installation areas for IoT devices, servers, and related assets, controlling entry and exit, deploying biometric authentication, installing surveillance cameras, and conducting baggage and weight inspections.	L1_1_a_SYS L1_1_c_SYS L2_3_b_PEO L2_3_b_SYS L2_3_d_SYS L3_1_a_SYS	<High-Advanced> - The organization regulates service wires and transmission paths that are related to their IoT devices and servers by physical access. - The organization regulates output devices of its system by physical access. - The organization monitors alarms and monitoring devices (e.g., surveillance cameras) for physical intrusions into the areas within the physical security boundaries.	O/S	○ (In addition to the following, 03.10.02 Monitoring Physical Access a, 03.10.07 Physical Access Control e, 03.10.08 Access Control for Transmission)	○ (In addition to the following, PE-18)	○ (A.7.2, A.7.8)	○ (In addition to the following, 13.2.2.1)	-
			<Advanced> - The organization locks server areas or racks housing servers, designates administrators for the associated physical keys, and manages them securely. - The organization adopts additional physical security measures for areas containing high-risk assets. - The organization establishes rules for bringing devices into the company facilities, covering personal computers, smart devices, cameras, and external storage media (including the business use of personally owned devices (BYOD)). - The organization reviews, at least annually, the content and compliance status of the rules for bringing devices into company facilities, covering personal computers, smart devices, cameras, and external storage media (including BYOD). - The organization monitors physical accesses to the areas within the physical security boundaries and regularly reviews the audit log. - The organization keeps the records of visitor's access to the areas within the physical security boundaries and regularly reviews them.	O	○ (In addition to the following, 03.10.07 Physical Access Control d.)	○ (In addition to the following, PE-04, PE-05)	○ (A.7.2, A.7.3)	○ (6.4.1.1)	-
			<Basic> - The organization defines physical security boundaries at its facilities, and implements access control according to the security requirements of assets placed within the boundaries and the results of risk assessment. - The organization establishes management rules for entry into areas and rooms requiring confidential considerations, covering the following items: - Restrict granted physical access permissions to the minimum necessary scope. - Define requirements for periodic reviews of physical access permissions. - Maintain application forms or records of granted physical access permissions. - The organization maintains upkeep of the access list for areas where their IoT devices and servers are located and issues permission certificates necessary for access. - The organization monitors the work of temporarily authorized party within the physical security boundaries, such as by authorized attendants or monitoring cameras.	O/S	○ (03.10.01 Physical Access Authorizations a, 03.10.07 Physical Access Control a.)	○ (PE-02, PE-03, PE-06, PE-08)	○ (A.7.2, A.7.6)		-
CPS.PR.AT-01	The organization conducts appropriate training and education for all personnel to carry out their assigned roles and responsibilities to minimize the occurrence and impact of security incidents, and maintains records of such activities.	L1_1_a_PEO L1_1_b_PEO L1_1_c_PEO L1_2_a_PEO L1_3_a_PEO L1_3_c_PEO L1_1_d_PEO L3_4_a_PEO L3_4_b_PEO	<High-Advanced> - The organization provides security awareness trainings to all necessary personnel so that they will recognize and report signs of internal fraud. - The organization conducts exercises based on the incident response plan in preparation for cases where procured products or services are found to be delivered by non-legitimate suppliers or to be tampered with.	O	-	○ (AT-02, AT-03)	○ (A.6.3)	○ (6.2.4.1)	-
			<Advanced> - The organization provides opportunities for executive management to understand their roles and responsibilities regarding information security. - The organization conducts education and training for officers, employees, dispatched workers, and seconded personnel upon their initial onboarding and at least annually, through methods such as distribution or posting of educational materials, e-learning, or group training, covering the following topics. - Prevention of malware infection via email - Prevention of malware infection via web browsing - Definition and handling of confidentiality classifications - If understanding workplace-specific security risks and complying with rules are required, the organization communicates important rules and risks to each workplace at least annually. - The organization creates a program for each role (e.g., system/software developer, purchasing personnel, system administrator, personnel in charge of security measures) to train information security personnel and to improve their skills. The program is conducted regularly on applicable personnel. - The organization clearly identifies specialized internal roles requiring additional security training (e.g., personnel responsible for physical security and cybersecurity, finance personnel, executive management, and individuals with access to business-critical data). - The relevant personnel should receive security awareness and training for industrial control systems. Furthermore, the organization should identify, document, and train all personnel who have critical OT roles and responsibilities. - The organization trains personnel on information security aspects of supplier relationships to particularly ensure that the handling of sensitive information is correctly understood. - The organization periodically assesses or tests its personnel's understanding of basic security measures. - The organization periodically assesses or tests whether individuals in specialized roles understand the cybersecurity practices required for their assigned responsibilities.	O	○ (In addition to the following, 03.01.22 Publicly Accessible Content a, 03.02.02 Role-Based Training a, 03.06.03 Incident Response Testing, 03.06.04 Incident Response Training a.)			○ (6.2.4.1, 6.2.5.1)	-
			<Basic> - The organization conducts training for its personnel on how to recognize social engineering and other common attacks, report attacks and suspicious activities, comply with usage policies, and implement basic security practices (e.g., software patch management, password selection, and protection of credentials). - The organization communicates the impact that violations of cybersecurity policies have on its personnel and the organization as a whole. - Upon onboarding and at least annually, the organization provides education and training on security incident response procedures for officers, employees, dispatched workers, and seconded personnel through e-learning or group training, in addition to distribution or posting of educational materials. - The organization involves internal stakeholders (e.g., executive management, the legal department, and the human resources department) in security tests and exercises as necessary. - The organization records and manages the contents and results of security education and training for personnel in the organization.	O	○ (03.02.01 Literacy Training and Awareness a.)			-	-

- Examples of security measures for each of the High Advanced, Advanced, and Basic levels are stated for implementing measure requirements described in Part III. To implement High Advanced-level measures, there is a need to include not only High Advanced-level measures but also Advanced- and Basic-level measures.

- The level of a measure is determined according to the costs in implementing/operating the measure, the scope of the measure (e.g., whether the scope is applied only to the organization or other related organizations), etc., based on management measures stratified into levels.

- The subject that implements measures is classified as “S” (implemented by a system through technical means), as “O” (implemented by an organization (e.g., by people through non-technical means)), and as “O/S” (implemented by both a system and an organization).

- In describing the examples of security measures, reference is made to major security documents and other relevant materials (shown as “Reference Guidelines” in the table).

- The measures described in this section are just examples and do not deny other implementation methods. Use this document as a reference for risk management according to the characteristics of the business of each organization, the results of the risk analyses, etc.

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measure	Reference Guidelines				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 Annex A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.PR.AT-02	The organization provides appropriate training and security education to designated personnel of external partners critical to security management, who may be involved in security incident response for the organization, enabling them to fulfill their assigned roles, and maintains records of such activities.	L1_3_a_PEO L1_3_b_PEO L1_3_c_ORG L3_4_a_PEO L3_4_b_PEO L3_3_a_PEO	<High-Advanced> - The organization monitors its personnel and related organizations that may be involved in security incidents for the accomplishment status of the roles assigned to the personnel in charge. - To reinforce existing security measures and communicate new measures, the organization mandates annual refresher training for personnel of highly important related organizations.	O	-	○ (AT-03)	-	-	-
			Common among <Advanced> and <Basic> - The organization determines which contractors, partners, suppliers, and other third parties are to receive cybersecurity awareness and training, based on their criticality to the organization, and provides them with cybersecurity awareness and training appropriate to their respective roles. - The organization includes critical suppliers in incident response training and exercises. - The organization periodically assesses or tests whether individuals in specialized roles understand the cybersecurity practices required for their assigned responsibilities. - The organization records and manages the contents and results of security education and training for member in the organization.	O	-		○ (A.6.3)	○ (6.2.4.1, 6.2.5.1)	-
CPS.PR.DS-01	The organization accurately understands the required level of data protection mandated by various laws, regulations, and agreements regarding data shared exclusively among relevant organizations, establishes data classification methods based on respective requirements, and appropriately protects data commensurate with its classification throughout the entire lifecycle.	L1_1_a_DAT L1_2_a_DAT L3_4_a_ORG L3_4_a_PRO L3_4_a_DAT L3_4_b_ORG L3_4_b_PRO L3_4_b_DAT	Common among <High-Advanced>, <Advanced> and <Basic> - The organization identifies and documents all legal requirements and contract requirements related to data protection for each system and each organization and the organization's activities to satisfy these requirements, and updates them to the latest. - The organization takes measures for systems, components, etc., handling the applicable data in accordance with the requirements of the identified rules. When the implementation of a measure is considered difficult, measures such as tokenization of an applicable data in the organization may be considered. (e.g., tokenization of card information due to the Installment Sales Law) - The organization establishes and complies with data management rules for information in its possession, including the following: - Identification of sensitive information - Classification and labeling of sensitive information - Handling procedures commensurate with classification - Classification and restriction of handling areas - At least annually, the organization reviews the adequacy of its information management rules (covering the identification of sensitive information, classification and labeling of sensitive information, handling procedures commensurate with classification, and classification and restriction of handling areas). - The organization prohibits reusing sensitive information from the production environments (e.g., customer information) in development, testing, or other non-production environments. - In accordance with its data retention policy, the organization securely erases stored data using predetermined methods and maintains records of the erasure.	O	○ (03.08.04 Media Marking, 03.14.08 Information Management and Retention)	-	○ (A.5.12, A.5.13, A.8.11)	○ (10.2.1.1, 10.2.2.1, 10.2.4.1)	-
CPS.PR.DS-02	The organization protects the confidentiality, integrity, and availability of data-at-rest.	L1_1_a_DAT L1_1_b_DAT L3_4_b_SYS L3_3_d_SYS L3_1_a_DAT L3_2_a_DAT	<High-Advanced> - The organization selects products that have been authenticated based on Cryptographic Module Validation Program (CMVP) in order to suitably implement selected algorithms to software and hardware, and to protect keys, identification codes, and entity authentication information that is used to decrypt encrypted information or to grant electronic signatures. - The organization uses IoT devices that can encrypt and store data in internal memory. - To protect against the loss of cryptographic keys, the organization maintains the availability of encrypted information through key backups, recovery, or other methods. - In addition to securely managing private keys, the organization is advised to consider the authenticity of public keys. This authentication process is carried out using the public key certificate issued normally by a certificate authority. It is desirable that the certificate authority should be a recognized organization that implements appropriate measures and procedures to provide the required reliability.	O	-	○ (In addition to the following, SC-04, SC-28, SI-07)	○ (A.5.33, A.8.12, A.8.24)	○ (10.2.6.1)	○ (SR 4.1, SR 4.3)
			<Advanced> - The organization establishes rules for taking assets off-premises, covering personal computers, smart devices, cameras, external storage media (including the business use of personally owned devices (BYOD)), and printed materials (confidential documents such as drawings). - At least annually, the organization reviews the adequacy and compliance status of the rules for bringing assets into and removing them from the company premises, covering personal computers, smart devices, cameras, and external storage media (including personally owned devices (BYOD)). - The organization establishes rules for encrypting critical and sensitive information and communicates them to officers, employees, dispatched workers, and seconded personnel. - The organization establishes rules requiring business-critical data whose compromise by malware would disrupt operations to be stored on servers in relatively secure zones on the internal network (including cloud services) rather than on personal computers, and communicates these rules to officers, employees, dispatched workers, and seconded personnel. - The organization considers the level of security and trustworthiness required for the information, chooses an algorithm, and encrypts and stores high importance information handled by industrial control systems with appropriate strength without causing unacceptable impact on performance. - It is desirable that the organization should set out a policy and procedure regarding the following items to take appropriate measures without delay when the private key is compromised. - A structure to take measures to address compromise of the private key (including the stakeholders, roles, cooperation with contractors) - Criteria for determining whether the private key has been compromised or is at risk of compromise - Investigation of the cause of the compromise of the private key and removal of the cause - Suspension of the services using the key - To create a new pair of keys and issue a certificate for the new key - Disclosure of information regarding compromise of the private key (notified parties, a method of notification, disclosure policy, etc.) - It is desirable that the organization should protect all encryption keys from modification and loss.	O/S	○ (In addition to the following, 03.01.18 Access Control for Mobile Devices c.)		○ (A.5.33, A.8.1, A.8.12, A.8.24)	○ (10.2.2.1, 10.2.5.1, 10.2.6.1)	

- Examples of security measures for each of the High Advanced, Advanced, and Basic levels are stated for implementing measure requirements described in Part III. To implement High Advanced-level measures, there is a need to include not only High Advanced-level measures but also Advanced- and Basic-level measures.

- The level of a measure is determined according to the costs in implementing/operating the measure, the scope of the measure (e.g., whether the scope is applied only to the organization or other related organizations), etc., based on management measures stratified into levels.

- The subject that implements measures is classified as “S” (implemented by a system through technical means), as “O” (implemented by an organization (e.g., by people through non-technical means)), and as “O/S” (implemented by both a system and an organization).

- In describing the examples of security measures, reference is made to major security documents and other relevant materials (shown as “Reference Guidelines” in the table).

- The measures described in this section are just examples and do not deny other implementation methods. Use this document as a reference for risk management according to the characteristics of the business of each organization, the results of the risk analyses, etc.

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measure	Reference Guidelines				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 Annex A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
			<Basic> - The organization physically protects removable media containing unencrypted sensitive information by storing such media in locked offices, cabinets, or other secure places.	O	○ (03.05.07 Password Management d, 03.05.12 Authenticator Management f, 03.06.05 Incident Response Plan d, 03.08.01 Media Storage, 03.08.09 System Backup – Cryptographic Protection a, b, 03.13.08 Transmission and Storage Confidentiality, 03.13.11 Cryptographic Protection, 03.15.02 System Security Plan c, 03.17.01 Supply Chain Risk Management Plan c.)	○ (CA-07, CP-09, SC-07, SC-12, SC-13, SC-39, SI-03, SI-04)		-	-
CPS.PR.DS-03	The organization protects the confidentiality, integrity, and availability of data-in-transit.	L1_1_a_DAT L1_1_b_DAT L3_3_d_SYS L3_1_a_DAT L3_2_b_DAT L3_3_a_SYS	<High-Advanced> - The information system encrypts all communications destined outside the organization, regardless of the criticality level of the data handled. - The organization protects the networks composing the industrial control system that handles important data by implementing encryption of communication channels or by alternative physical measures. - It is desirable that the systems/IoT devices introduce a cryptographic module that can be implemented with limited resources without compromising availability, and encrypt the communication data from critical, resource-constrained devices with appropriate strength. - The organization detects tampering with data transmitted from IoT devices, servers, etc. in industrial control systems, if possible, using integrity checking tools.	O/S	○ (In addition to the following, 03.13.08 Transmission and Storage Confidentiality)		○ (A.8.12, A.8.24)	○ (In addition to the following, 10.2.2.1)	○ (SR 3.1, SR 3.8, SR 4.1)
			<Advanced> - The organization establishes rules governing information sharing and transmission with business partners, and communicates them to officers, employees, dispatched workers, and seconded personnel, incorporating the following requirements: - Share files externally only with verified and trusted parties. - When transferring files externally, maintain transmission logs. - Based on data classification, the organization automatically encrypts or blocks the transmission of emails or other communications containing sensitive information. - To protect the integrity of data in transit, the organization implements appropriate cryptographic controls, such as digital signatures and message authentication codes. - The organization uses an integrity verification tool in an information system to detect any unauthorized changes that are made to communication data transmitted from IoT devices and servers. - The information system supports the technology of authenticating the sending domain in e-mail, and detects spoofing and tampering of e-mail. [Reference] For protection of communication paths, there are several methods such as IP-VPN, IPsec-VPN, and SSL-VPN. It is desirable that the organization should select the method considering the importance of the data transmitted in the communication paths, the budget, and so on.	O/S	○ (03.05.07 Password Management c)	○ (CA-03, SC-07, SC-12, SC-13, SI-03, SI-04, SC-04, SC-08, SI-07)	○ (A.5.14, A.8.12, A.8.24)	○ (10.2.7.1)	○ (SR 3.1, SR 3.8)
			<Basic> - N/A	-	-	-	-	-	-
CPS.PR.DS-04	The organization protects the confidentiality, integrity, and availability of data-in-use.	L1_1_a_DAT L1_1_b_DAT L3_3_d_SYS L3_1_a_DAT L3_2_b_DAT	Common among <High-Advanced>, <Advanced> and <Basic> - The organization promptly deletes confidential data once it is no longer needed (e.g., data residing in processors or memory). - The organization prevents unauthorized users and processes on the same system from accessing data in use.	O/S	○ (03.13.04 Information in Shared System Resources)	○ (AC-02, AC-03, AC-04, AU-09, CA-03, CP-09, SA-08, SC-04, SC-07, SC-13, SC-24, SC-39, SI-03, SI-04, SI-07, SI-10, SI-16)	○ (A.8.1, A.8.12)	-	○ (SR 4.2)
CPS.PR.DS-05	The organization maintains, updates, and manages data provenance, including data sources and processing history, throughout the entire lifecycle.	L1_1_b_DAT L3_2_a_DAT	<High-Advanced> - The organization checks whether or not there is an entity that does not implement the countermeasures that meet the level requested by the organization to the outsourced organization among the supply chain in the cyberspace where data managed by the organization is processed.	O	-	-	-	-	-
			<Advanced> - The organization identifies the source of data that is utilized by the organization and the organization/personnel that processed the data concerned. - The organization links the source of the data obtained from other organizations or individuals/IoT devices outside of the organization to the data concerned and manages the entire lifecycle of the data from acquisition to deletion.	O	-	-	-	-	-
			<Basic> - N/A	-	-	-	-	-	-

- Examples of security measures for each of the High Advanced, Advanced, and Basic levels are stated for implementing measure requirements described in Part III. To implement High Advanced-level measures, there is a need to include not only High Advanced-level measures but also Advanced- and Basic-level measures.

- The level of a measure is determined according to the costs in implementing/operating the measure, the scope of the measure (e.g., whether the scope is applied only to the organization or other related organizations), etc., based on management measures stratified into levels.

- The subject that implements measures is classified as “S” (implemented by a system through technical means), as “O” (implemented by an organization (e.g., by people through non-technical means)), and as “O/S” (implemented by both a system and an organization).

- In describing the examples of security measures, reference is made to major security documents and other relevant materials (shown as “Reference Guidelines” in the table).

- The measures described in this section are just examples and do not deny other implementation methods. Use this document as a reference for risk management according to the characteristics of the business of each organization, the results of the risk analyses, etc.

Measure Requirement ID	Measure Requirement	Correspondin g Vulnerability ID	Examples of security measure	Subject that implements measure	Reference Guidelines				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 Annex A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.PR.DS-06	The organization performs routine backups of data (e.g., component configurations and operational data), protects backup data, and tests restoration capabilities.	L1_1_a_DAT L1_3_a_DAT L3_3_d_SYS L3_1_a_DAT	<High-Advanced> - The organization confirms the trustworthiness of the medium and integrity of the information by regularly testing the backup process.	O	-	○ (In addition to the following, CP-06)	○ (A.8.13)	○ (13.3.3.1)	○ (SR 7.3)
			<Advanced> - For systems critical to business continuity, the organization implements the following measures in anticipation of cyberattacks: - Store created backups in a manner that enables recovery to achieve the defined recovery point objective. - Verify that backups can be restored according to the established restoration procedures and within the recovery time objective. - For critical data, the organization performs continuous, near-real-time backups where feasible based on the system characteristics, and conducts backups of other data periodically in accordance with a defined schedule. - The organization protects the confidentiality, integrity, and availability of the information backed up on the storage base.	O	○ (03.08.09 System Backup – Cryptographic Protection)			○ (13.3.1.1, 13.3.3.1, 13.3.4.1, 13.3.5.1)	
			<Basic> - The organization creates backups of data it handles, defining the scope, frequency, and retention period. - The organization develops restoration procedures for each designated backup scope. - The organization tests the recoverability of data from backups at least annually. - To mitigate the impact of accidents and disasters, the organization securely stores a part of backups offline and at a separate location.	O	-	○ (CP-09)			
CPS.PR.PS-01	The organization evaluates the authenticity and integrity of hardware and software prior to acquisition and deployment, and verifies their integrity during operation.	L2_3_b_ORG L2_3_b_SYS L2_3_c_ORG L2_3_c_PRO	<High-Advanced> - The organization detects hardware tampering (insertion of hardware trojan) based on the difference between the genuine and counterfeit side channel information of the IC chip. - The organization detects hardware tampering (insertion of a hardware trojan) through testing physically readable ID of chip generated with the technology of PUF (Physically Unclonable Function). - The organization utilizes a tool having an automated mechanism to periodically check that the IoT device and installed software are genuine, using the device serial number, hash value, and the like.	O/S	-	○ (In addition to the following, SA-17)	○ (A.8.19)	-	○ (SR 3.4)
			<Advanced> - The organization confirms software integrity through signature verification. - The organization periodically reports to executive management on the verification status of authenticity and evidence of tampering for procured technology products and services. - When operating industrial control systems, the organization documents and tracks serial numbers, checksums, digital certificates or signatures, or other vendor-provided identification features that verify the authenticity of OT hardware, software, and firmware. - The organization uses tools that detect unauthorized changes made to hardware components, labels that cannot be replicated easily, and verifiable serial numbers so that integrity can be verified. - By monitoring the site with surveillance cameras, the organization shall be able to detect physical tampering on the hardware that is significant to its operation. - The organization regularly checks that the IoT devices and the installed software are genuine products by using the serial numbers and hash values of the devices.	O/S	-	○ (In addition to the following, SA-10, SA-11, SA-15, SI-07, SA-06)	○ (A.8.7, A.8.19)	○ (9.4.1.1)	
			<Basic> - During procurement and inventory count, the organization confirms that the IoT devices which the organization possesses are genuine products by checking the label.	O	-	○ (SA-04, SA-05, SR-05, SR-10, SR-11)	-	-	
CPS.PR.PS-02	When procuring devices that process sensitive information or have[TN122.1] important functions for its organization, the organization utilizes tamper-resistant devices.	L1_1_d_COM L2_3_a_ORG L2_3_b_PEO L2_3_b_COM	<High-Advanced> - When handling information that shall be protected or when procuring devices that have a function important to the organization, the organization procures devices that use anti-tampering devices. - When storing encryption keys for the cryptographic mechanism used in the information system and the industrial control system, the organization uses anti-tampering devices.	O	-	-	-	-	○ (SR 1.9)
			Common among <Advanced> and <Basic> - N/A	-	-	-	-	-	-
CPS.PR.PS-03	The organization utilizes products that implement appropriate security measures to ensure the trustworthiness of sensing data by preserving measurement availability and integrity.	L1_2_a_COM L2_1_a_COM L2_1_a_PRO L2_2_a_ORG L2_1_a_PRO L2_3_a_ORG L2_3_d_ORG	Common among <High-Advanced> and <Advanced> - When adopting a device (sensor) that has network connectivity, digitalizes dynamics in physical space, and transmits them to cyberspace, it is desirable to procure the said device with consideration of the following points: - Whether function that uses integrity verification tools to detect unauthorized changes made to communication data is implemented or not; - Whether the device has a unique ID identifiable by other IoT devices and servers, or has a certificate that can prove its genuineness through mutual authentication with the destination; - Whether or not the device's resource is at a level which can maintain the availability when subjected to a denial-of-service attack of a certain scale; [Reference] When procuring IoT devices with internet connectivity, the "Labeling Scheme based on Japan Cyber-Security Technical Assessment Requirements (JC-STAR)" operated by IPA is available for reference.	O	-	-	-	○ (13.2.2.1)	○ (SR.1.2, SR 3.1)
			<Basic> - The organization procures IoT devices (e.g., sensor) that are resistant to physical attacks.	O	-	-	-		-

- Examples of security measures for each of the High Advanced, Advanced, and Basic levels are stated for implementing measure requirements described in Part III. To implement High Advanced-level measures, there is a need to include not only High Advanced-level measures but also Advanced- and Basic-level measures.

- The level of a measure is determined according to the costs in implementing/operating the measure, the scope of the measure (e.g., whether the scope is applied only to the organization or other related organizations), etc., based on management measures stratified into levels.

- The subject that implements measures is classified as “S” (implemented by a system through technical means), as “O” (implemented by an organization (e.g., by people through non-technical means)), and as “O/S” (implemented by both a system and an organization).

- In describing the examples of security measures, reference is made to major security documents and other relevant materials (shown as “Reference Guidelines” in the table).

- The measures described in this section are just examples and do not deny other implementation methods. Use this document as a reference for risk management according to the characteristics of the business of each organization, the results of the risk analyses, etc.

Measure Requirement ID	Measure Requirement	Correspondin g Vulnerability ID	Examples of security measure	Subject that implements measure	Reference Guidelines				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 Annex A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.PR.PS-04	The organization deploys IoT devices that implement security safeguards designed for network connectivity.	L2_1_a_COM L2_1_a_PRO L2_2_a_ORG	<High-Advanced> - The organization adopts inherently safe design measures to address high-severity hazards, thereby minimizing damage (e.g., a design that lowers the energy of a hazard in order to limit an impact of an accident).	O	-	-	-	-	-
			<Advanced> - The organization carries out a security risk assessment that considers the safety aspect (CPS.ID.RA-06) to determine whether measures for physical safety are needed in the target system and, if so, at what level. - The organization reduces hazards through intrinsic safe designing. If any hazard of high severity persists through this process, it is advisable to take alternative measures such as the following: - Ensure safety using an add-on such as a safety device; - Adopt a space design that keeps staff members away from hazardous devices. - The industrial control system is configured to operate in a predetermined manner when normal operation cannot be maintained due to cyberattacks or other causes.	O/S	-	-	-	○ (8.2.4.1, 13.2.3.1)	○ (SR 3.6)
			<Basic> - N/A	-	-	-	-	-	-
CPS.PR.PS-05	The organization integrates secure software development practices (e.g., security reviews during the design stage, application of secure coding rules, and pre-release vulnerability assessments) into the system development life cycle and verifies their implementation.	L3_4_b_SYS	Common among <High-Advanced> and <Advanced> - The organization protects all components of software developed in-house and their development environments (e.g., source code, build environments, dependency libraries, and container images) against tampering and unauthorized access. - The organization reviews, analyzes, or tests software developed in-house to identify vulnerabilities in design, coding, and initial configuration.	O	-	○ (SA-10, SA-11, SA-15, SA-17)	○ (A.8.25, A.8.28, A.8.29)	○ (6.3.3.1)	-
			<Basic> - The organization applies the general rules of the system’s security engineering to specifications, design, development, introduction, and changes in building the system. [Reference] When considering specific initiatives to ensure security across the stages of system specification, design, development, deployment, and modification, the “Guidelines on the Roles Expected of Cyber Infrastructure Providers” published by the Ministry of Economy, Trade and Industry is available for reference.	O	○ (03.16.01 Security Engineering Principles)	○ (SA-03, SA-08)	○ (A.8.25, A.8.26, A.8.27)		-
CPS.PR.PS-06	The organization establishes and applies configuration management practices for hardware and software of IoT devices, servers, and related assets (including minimizing functionality by physically or logically disabling unnecessary network, USB, and serial ports).	L1_1_a_SYS L1_1_b_SYS L1_1_c_SYS L2_1_a_ORG L2_1_b_COM L2_1_b_PRO L2_1_c_ORG L2_3_c_SYS L3_3_d_SYS L3_1_a_SYS	<High-Advanced> - When the information system detects a device whose actual configuration does not conform to the baseline configuration, it automatically takes corrective actions, such as blocking the device's connection, unless the device is permitted as an exception by the organization. - The organization uses a mechanism for automatically collecting information about network configurations and the software configurations of devices in order to monitor the most recent status at all times. - The information system prevents the remote activation of devices, such as cameras, microphones, and whiteboards, connected to networks that handle sensitive data, and provides mechanisms that enable users to recognize when these devices are in use (e.g., an illuminated indicator light). - The organization uses an automated mechanism to manage, apply, and confirm settings of IoT devices and servers from a single location. - The organization integrates security change management procedures particularly for industrial control systems, into existing process safety management procedures. - The organization records past versions of baseline configurations (e.g., hardware, software, firmware, configuration files, configuration records) to enable rollback of baseline configurations of information systems.	O/S	-	○ (In addition to the following, CM-03, CM-09)	○ (A.8.9, A.8.32)	○ (6.3.2.1, 7.2.3.1, 7.2.4.1, 8.2.8.1, 8.3.1.1, 9.2.1.1, 9.2.2.1)	○ (SR 7.6)
			<Advanced> - The organization establishes mechanisms to continuously track the configuration settings of information devices that comprise critical systems. - At least annually, the organization periodically reviews the configuration settings of information devices that comprise critical systems to verify that they are maintained in accordance with configuration standards. - The organization disables unnecessary services and protocols on network-connected devices, such as personal computers, servers, and multifunction printers. - For industrial control systems, the organization establishes procedures to remove, disable, or otherwise secure physical ports where feasible, to prevent unauthorized device connections. - The organization restricts functionality in industrial control systems by permitting only specific functions, protocols, and services necessary for operations. - If any changes are made to the baseline configuration of an information system and industrial control system, the organization promptly updates the baseline configuration so that the most recent status is available at all times. - When changes are made to the IoT devices and servers that are subjects of configuration management, the organization analyzes the impact the change has on security, decides whether the change can be made or not, and creates a document on the procedure. - The organization conducts testing (operational verification) prior to making changes to IoT devices and servers subject to configuration management. - The organization makes changes to approved IoT devices and servers, as well as implements, records, and monitors those changes. - The organization regularly reviews policies and procedures for operation and change management to ensure that changes do not adversely affect the availability or safety of information system and industrial control system. - The organization reviews the functions and services provided by its systems and items in order to identify the functions and services that could be deleted. - The organization uses network scanning tools, intrusion detection and prevention systems, and endpoint protection (e.g., a firewall, host-based intrusion detection system) in order to detect and prevent the use of banned functions, ports, protocols, and services.	O	○ (In addition to the following, 03.01.16 Wireless Access c, 03.04.01 Baseline Configuration a, 03.04.03 Configuration Change Control a,c, 03.04.06 Least Functionality a,b,d, 03.13.06 Network Communications – Deny by Default – Allow by Exception)				
			<Basic> - The organization disables auto-run or auto-play functions on endpoint devices that use external storage media. - The organization requires a formal request and approval process for configuration changes to servers and network devices. - The organization uninstalls or removes software components that are unnecessary for business operations and could be exploited by attackers (e.g., OS utilities). - Upon determining the most restrictive setting criteria that conform to their operation, the organization creates a document on the initial setting procedures and setting details for the IoT devices and servers that will be introduced and adjusts the settings according to the document. - The organization checks initial setting values of IoT devices before installing them, and adjusts the settings appropriately if they do not comply with predetermined policy. - The organization plugs USB ports and serial ports out of use to physically block them.	O	○ (03.04.02 Configuration Settings a.)	○ (CM-01, CM-02, CM-04, CM-05, CM-06, CM-07, CM-08, CM-10, CM-11)	○ (7.2.3.1, 7.2.4.1, 8.2.8.1, 9.2.1.1, 9.2.2.1)	○ (SR 7.7)	

- Examples of security measures for each of the High Advanced, Advanced, and Basic levels are stated for implementing measure requirements described in Part III. To implement High Advanced-level measures, there is a need to include not only High Advanced-level measures but also Advanced- and Basic-level measures.

- The level of a measure is determined according to the costs in implementing/operating the measure, the scope of the measure (e.g., whether the scope is applied only to the organization or other related organizations), etc., based on management measures stratified into levels.

- The subject that implements measures is classified as “S” (implemented by a system through technical means), as “O” (implemented by an organization (e.g., by people through non-technical means)), and as “O/S” (implemented by both a system and an organization).

- In describing the examples of security measures, reference is made to major security documents and other relevant materials (shown as “Reference Guidelines” in the table).

- The measures described in this section are just examples and do not deny other implementation methods. Use this document as a reference for risk management according to the characteristics of the business of each organization, the results of the risk analyses, etc.

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measure	Reference Guidelines				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 Annex A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.PR.PS-07	The organization prevents the installation and execution of unauthorized software.	L1_1_a_SYS L1_1_b_SYS	<High-Advanced> - The organization uses tools to prevent the launch of the software if malicious software is detected. - The organization prohibits the installation of unauthorized software through list-based controls, including blacklists (lists of prohibited software). - The organization identifies software programs that are not allowed to be executed on a system. - The organization regularly reviews and updates blacklists or whitelists. - The industrial control system blocks or isolates malicious code, or notifies the administrator, when such code is detected by an IDS/IPS.	O/S	-	○ (In addition to the following, CM-07(02), CM-07(05))	○ (A.8.7, A.8.19)	-	○ (SR 3.2)
			<Advanced> - The organization adopts and manages a mechanism that manages software installation that is performed by users on the organization's system (information system or industrial control system) and monitors the events. - Where supported by system functionality, the information system and the industrial control system prevent the execution of unregistered software through a whitelisting approach that pre-registers authorized software.	O/S	○ (03.04.08 Authorized Software – Allow by Exception b.)			○ (9.3.2.1)	
			<Basic> - The organization removes or disables all software not authorized for use on personal computers, servers, and smart devices, or restricts the installation of any software other than authorized software. - The organization establishes a policy on software installation performed by users on the organization's system (information system or industrial control system) and has the users follow it. - The organization checks external storage devices connected to IoT devices or servers (e.g., USB flash drives) using antivirus software, uses USB flash drives that can be checked for viruses, or takes any appropriate action. - The organization updates anti-malware software definition files in accordance with vendor recommendations. - The organization maintains information systems and their software in the following states: - Licensed and supported. - Removed upon reaching end-of-support, or taken out of scope by blocking all internet traffic. - Configured to have automatic updates enabled, where feasible. - When deploying patches and updates in industrial control systems, the organization takes into account organization-specific additional requirements. - For industrial control system assets where patching is impossible or could significantly compromise availability or safety, the organization applies and documents compensating controls (e.g., segmentation and monitoring).	O/S	-	○ (CM-07)		○ (9.2.1.1, 9.3.1.1)	
CPS.PR.PS-08	The organization develops a vulnerability remediation plan and remediates component vulnerabilities in accordance with the plan.	L1_1_a_SYS L2_1_a_ORG L2_1_c_SYS L3_3_d_SYS L3_1_a_SYS L3_3_a_SYS	<High-Advanced> - The organization adopts and administers an automated mechanism for managing vulnerability remediation status.	O	-	-	○ (A.8.8)	○ (9.4.3.1)	-
			<Advanced> - The organization performs periodic and emergency patching within the respective timeframes defined in the vulnerability management plan. - The organization defines tolerable risk by identifying through investigations and tests the impacts of patch application on the functions of other software applications and services on operations of IoT devices and servers. - The organization conducts tests to measure the effectiveness of corrections and the possibility of any secondary adverse effects, remediates vulnerabilities, and manages the corrections as part of the configuration management.	O	○ (In addition to the following, 03.11.02 Vulnerability Monitoring and Scanning b.)	-		○ (9.4.2.1, 9.4.4.1, 12.2.9.1)	-
			<Basic> - The organization develops a vulnerability management plan to identify and evaluate various vulnerabilities, as well as prioritize, test, and implement risk response measures, and remediates component vulnerabilities in accordance with the plan. - When developing the vulnerability management plan, the organization considers factors such as the severity of threats or vulnerabilities and risks associated with applying remediation measures.	O	○ (03.12.02 Plan of Action and Milestones a, 03.14.01 Flaw Remediation a.)	-		○ (12.2.9.1)	-
CPS.PR.PS-09	The organization applies security-critical updates for IoT devices, servers, and related assets in a timely manner using managed tools while appropriately recording history.	L1_1_a_SYS L2_1_a_ORG L2_1_c_ORG L2_1_c_SYS L3_3_d_SYS L3_1_a_SYS L3_3_a_SYS	<High-Advanced> - The organization gives prior approval for the use of devices and/or tools needed for maintenance to update its IoT devices and servers, and conducts monitoring. - The organization inspects the devices and/or tools for maintenance brought in by the staff members who update its IoT devices and servers in order to make sure that no inappropriate or unauthorized changes will be made. - The organization inspects the media used for maintenance to update its IoT devices and servers in order to make sure that the media contain no malicious code before they are used. - The organization introduces an IoT device designed to remotely update different software programs (OS, driver, application) at the same time.	O	-	○ (In addition to the following, MA-03, SA-10, SI-07)	-	○ (9.3.1.1)	-
			<Advanced> - The organization applies either of the following conditions to the operating systems, software, hardware, and related components utilized in information systems and industrial control systems: - The organization utilizes operating systems, software, and hardware that are actively supported by vendors or equipped with required security capabilities. - In unavoidable cases where unsupported components or those lacking required security capabilities are utilized (e.g., when immediate replacement is not feasible due to the need to procure an alternative system), the organization establishes a migration plan and implements measures to mitigate the risk of vulnerability exploitation until replacement is completed. - When conducting maintenance work such as updates for its IoT devices and servers, the organization formulates a maintenance implementation plan and executes the maintenance in accordance with that plan. - The organization gives prior approval for maintenance work such as updating its IoT devices and servers, and conducts monitoring. - The organization checks all security measures that may have been affected by maintenance work, such as updating its IoT devices and servers, after the work is complete in order to make sure that the relevant equipment works correctly. - The organization keeps the records of maintenance work done, such as updating its IoT devices and servers.	O	-			○ (9.4.2.1, 9.4.3.1, 9.4.4.1, 9.4.5.1)	-
			<Basic> - Regarding the functions or settings of the information systems in use, the organization sets response deadlines and applies updates based on the severity of detected vulnerabilities, the probability of attacks exploiting those vulnerabilities, and the internet exposure status of the devices to be updated. - In unavoidable cases where updates cannot be applied (e.g., when operational verification requires a certain period of time and the update cannot be completed within the deadline), the organization documents this exception in the vulnerability management plan and implements measures to reduce the risk of vulnerability exploitation through any of the following until the update is applied: - Disabling functions subject to vulnerability exploitation. - Implementing workarounds recommended by vendors. - Isolating the target information devices from the network within the scope. - Deploying devices or software that monitor communications between the target information devices and the network within the scope and block unauthorized communications exploiting the vulnerability.	O	○ (03.11.02 Vulnerability Monitoring and Scanning b, 03.14.01 Flaw Remediation b, 03.14.02 Malicious Code Protection b.)	○ (CM-11, SI-02)	-	-	-

- Examples of security measures for each of the High Advanced, Advanced, and Basic levels are stated for implementing measure requirements described in Part III. To implement High Advanced-level measures, there is a need to include not only High Advanced-level measures but also Advanced- and Basic-level measures.

- The level of a measure is determined according to the costs in implementing/operating the measure, the scope of the measure (e.g., whether the scope is applied only to the organization or other related organizations), etc., based on management measures stratified into levels.

- The subject that implements measures is classified as “S” (implemented by a system through technical means), as “O” (implemented by an organization (e.g., by people through non-technical means)), and as “O/S” (implemented by both a system and an organization).

- In describing the examples of security measures, reference is made to major security documents and other relevant materials (shown as “Reference Guidelines” in the table).

- The measures described in this section are just examples and do not deny other implementation methods. Use this document as a reference for risk management according to the characteristics of the business of each organization, the results of the risk analyses, etc.

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measure	Reference Guidelines				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 Annex A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.PR.PS-10	The organization performs maintenance on its own IoT devices, servers, and related assets with prior approval from the department that owns the target component or system, logging maintenance activities and preventing unauthorized access.	L1_1_a_SYS L2_1_a_ORG L2_1_c_SYS L3_3_d_SYS L3_1_a_SYS L3_3_a_SYS	Common among <High-Advanced> and <Advanced> - The organization documents the policy and procedure relating to establishing and implementing a connection designed for remote maintenance, and implements the connection in accordance with the policy and procedure. - When performing remote maintenance, the organization enforces the authentication it requires for network access, and ensures that sessions and network connections are terminated once remote maintenance is complete.	O/S	○ (03.07.05 Nonlocal Maintenance a.)	-	○ (A.7.13)	-	-
			<Basic> - The organization develops and agrees to an implementation plan for remote maintenance before carrying out the maintenance, and checks the results of the maintenance done. - The organization keeps the records of remote maintenance done. - The organization makes sure that a maintenance staff member sent without an escort to do maintenance work on its information system and industrial control system has the necessary access rights. - The organization appoints its staff member with the access rights and technical skills needed so as to supervise maintenance work done by a staff member without the necessary access rights.	O	-	-		-	-
CPS.PR.PS-11	To appropriately detect security incidents, the organization determines and documents the scope and types of events for audit logging, and continuously records and reviews logs.	L1_1_a_SYS L1_3_a_SYS L2_1_b_ORG L3_3_d_SYS L3_1_a_SYS L3_3_a_SYS	<High-Advanced> - The organization configures log sources to record data required for a zero trust architecture. - The organization efficiently analyzes logs collected through 24/7 specialized security monitoring by using automated analysis tools. - The information system adopts a system monitoring mechanism to check the use of privileged functions. - In addition to the detection of security incidents, the collected logs are considered to be useful in tracking the cause of security incidents after the fact. Therefore, the information system collects, if possible, detailed logs (e.g., OS command level) that do not remain in the OS function. - If time stamps in multiple audit logs match, the audit logs of the subjects specified by the organization are managed as audit trails across the system, logically and physically. - The information system provides system functions designed to compare and synchronize internal system clocks by using an official source of information for generating time stamps for an audit record. - The information system adopts an automatic mechanism designed to handle an audit review, analysis, and report in an integrated manner. - It may be difficult to generate security-related logs for some of the IoT devices that the organization uses, or to connect some of those devices to the existing log management system. Hence, it is necessary to take measures that consider the specifications of the IoT devices, such as using a log management system different from the main one or using an alternative measure on the part of the system, when collecting and analyzing audit logs from the relevant IoT devices.	O/S	○ (In addition to the following, 03.01.07 Least Privilege – Privileged Functions b, 03.03.02 Audit Record Content b.)	○ (In addition to the following, AU-07, SA-15)	○ (A.8.15)	○ (8.2.9.1, 12.2.1.1)	○ (SR 2.8, SR 2.11)
			<Advanced> - The organization configures all operating systems, applications, and services (including cloud services) across information systems to generate logs. - The organization configures log sources to securely share generated logs with the organization's log infrastructure systems and services. - For industrial control systems where logs are non-standard or unavailable, the organization collects network traffic and communications between those systems and other assets. - The information system and the industrial control system use a cryptographic mechanism in order to ensure the integrity of both logs and audit tools. - The organization grants control over logs only to users assigned in accordance with the rules about security-related internal responsibility. - The information system issues an alert when an incident of failure takes place in the audit process. - The organization reviews and analyzes collected logs regularly to see if there are any signs of security incidents that may cause damage to the organization, and makes a report to the system administrator where necessary. - The organization ascertains that the audit log acquired by its service provider records activity of service users, exception handling, and security events, and is protected in a proper way.	O/S	○ (In addition to the following, 03.01.01 Account Management e, 03.03.03 Audit Record Generation a,b, 03.03.05 Audit Record Review, Analysis, and Reporting a,b.)			○ (12.2.1.1, 12.2.4.1)	○ (SR 2.8, SR 3.9)
			<Basic> - The organization determines the logs that would help detect security events and thus should be collected based on its strategies relating to risk management and assessment results. - The organization verifies that the logs designated for collection can be captured in a manner that identifies who performed what actions, and when, on the target system. - The organization confirms that the impact of log collection activities on the performance of industrial control systems is tolerable.	O	○ (03.03.01 Event Logging a,b, 03.03.02 Audit Record Content a.)	○ (AU-02, AU-03, AU-06, AU-11, AU-12)		○ (12.2.1.1, 12.2.4.1, 12.2.5.2)	○ (SR 2.8, SR 2.12)

- Examples of security measures for each of the High Advanced, Advanced, and Basic levels are stated for implementing measure requirements described in Part III. To implement High Advanced-level measures, there is a need to include not only High Advanced-level measures but also Advanced- and Basic-level measures.

- The level of a measure is determined according to the costs in implementing/operating the measure, the scope of the measure (e.g., whether the scope is applied only to the organization or other related organizations), etc., based on management measures stratified into levels.

- The subject that implements measures is classified as “S” (implemented by a system through technical means), as “O” (implemented by an organization (e.g., by people through non-technical means)), and as “O/S” (implemented by both a system and an organization).

- In describing the examples of security measures, reference is made to major security documents and other relevant materials (shown as “Reference Guidelines” in the table).

- The measures described in this section are just examples and do not deny other implementation methods. Use this document as a reference for risk management according to the characteristics of the business of each organization, the results of the risk analyses, etc.

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measure	Reference Guidelines				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 Annex A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.PR.PS-12	Upon the disposal of IoT devices, servers, and related assets, the organization deletes or renders unreadable all internally stored data, unique identifiers of legitimate devices and systems, and critical security information (e.g., private keys and digital certificates).	L2_3_b_DAT	<High-Advanced> - The organization defines classifications including security categories of data saved in an IoT device or server to be scrapped, and introduces a mechanism for using the proper technique for deleting data with the strength and integrity needed or making the data unreadable according to the definition.	O	-	○ (SC-03)	○ (A.7.14, A.8.10)	-	○ (SR 4.2)
			Common among <Advanced> and <Basic> - When disposing of servers, IoT devices, industrial control systems, company-provided personal computers, smart devices, and external storage media (including upon lease expiration), the organization performs data erasure to prevent data recovery (standard disk formatting is insufficient as data may be recovered). For devices to which general-purpose erasure methods cannot be applied, the organization renders data permanently unrecoverable through methods suited to device characteristics, such as physical destruction. - The organization retains records of data erasure for the storage areas of servers, IoT devices, industrial control systems, company-provided personal computers, smart devices, and external storage media. - The organization establishes a procedure for scrapping its equipment including its IoT devices and servers, carries out disposal in accordance with that procedure, and makes sure that the action has been done successfully.	O	○ (03.08.03 Media Sanitization)	○ (CM-07, SA-10, SC-39)		-	
CPS.PR.IR-01	The organization protects networks and environments from unauthorized access and use by implementing network segmentation (e.g., separating development/test environments from production environments, and isolating IoT device environments from other networks within the organization).	L1_1_c_SYS L3_3_a_SYS	<High-Advanced> - The organization implements a zero trust architecture to restrict access over the network to each resource to the minimum necessary. - The organization physically or logically separates a network of industrial control systems with high importance from a network of industrial control systems with lower importance. - The information system and the industrial control system monitor and control communications on the networks composing internal business systems of the organization. - If the information system that handles highly confidential data is connected to a remote device, the organization is to prevent multiple and simultaneous local connections between the device and the system, as well as prevent access to external network resources by other connections. - The organization prevents fraudulent and unexpected transfer of information via common system resources. - The information system and the industrial control system disable network access by any unauthorized components that have been detected, separate these components from the network, or take any primary action, and notify the system administrator of the components.	O/S	○ (In addition to the following, 03.01.12 Remote Access c.)	○ (In addition to the following, AC-04, SC-04)	○ (A.8.20, A.8.22)	○ (8.2.1.1, 8.2.7.1, 13.2.2.1)	○ (SR 5.1, SR 5.2)
			<Advanced> - The information system and the industrial control system allow only for remote access routed by the regulated access points. - The information system routes communications to the network to which a recipient's IP address belongs via a proxy server authenticated on a controlled interface. - The organization enables software firewalls on personal computers and servers that constitute the information system, unless the operating system in use lacks such capability. - The organization deploys public-facing servers and internal servers handling critical confidential data in separate and dedicated network segments, and restricts access into and out of each segment to the minimum necessary. - The information system blocks or isolates any malicious code for it detected through an IDS/IPS, or notifies the administrator of the code. - The organization collects information including newly released attacking trends, malware behaviors, and malicious IP addresses/domains (external intelligence). When necessary, the organization executes responses to restrict communications to highly dangerous IP addresses and other destinations. - The organization creates a network segment isolated from access to the internal network ("demilitarized zone [DMZ]") between the internal network and external networks (e.g., the Internet). - The organization detects unusual data communications (e.g., too large data size, unexpected communication destination) outbound the organization, and limits such execution of communications when necessary.	O/S	○ (In addition to the following, 03.13.01 Boundary Protection b.)			○ (8.2.1.1, 8.2.7.1, 8.4.2.1, 13.2.2.1)	○ (SR 1.13)
			<Basic> - The organization implements the following controls across all firewalls (or network devices with firewall capabilities) based on its data flow control policy: - Defines firewall rules concerning inbound communications. - Blocks unauthorized inbound communications. - Promptly deletes or disables firewall rules that are no longer necessary. - When modifying firewall rules via the internet, the organization applies multi-factor authentication or restricts access to trusted IP addresses. - To block access to known malicious domains, the organization configures platforms to use only approved DNS services. - Communication using IoT devices is denied by default. The protocol to be used is authorized as an exception. - Where applicable, the organization logically or physically segments the control system's network from the network composed of the information system. [Reference] Implement physical segmentation in environments physically separated from other networks. Alternatively, in environments physically close to other networks, it is possible to implement logical segmentation in consideration of the cost of the measure.	O/S	○ (03.01.03 Information Flow Enforcement)	○ (AC-03, SC-05, SC-07)		○ (8.2.1.1, 8.2.7.1, 13.2.2.1)	○ (SR 5.1, SR 5.2)
CPS.PR.IR-02	The organization implements physical safeguards to comply with policies and rules regarding the physical operating environment of its IoT devices, servers, and related assets, such as ensuring uninterruptible power supplies, fire protection equipment, and flood protection measures.	L1_1_a_SYS L1_1_c_SYS L2_3_b_SYS L2_3_d_SYS L3_1_a_SYS	<High-Advanced> - The organization adopts an automatic fire suppression system if a staffer is not stationed full time at a facility where its system is located.	O	-	○ (In addition to the following, PE-18)	○ (A.7.5)	-	-
			<Advanced> - The organization maintains machine safety of equipment located within the area of their IoT devices and servers by using an uninterruptible power supply. - The organization adopts and maintains equipment and systems that run on an independent power supply which detect and extinguish fire. - The organization has shut-off valves or isolation valves to protect areas with their IoT devices and servers from damages such as water leakages.	O	-	○ (In addition to the following, PE-09, PE-10, PE-11)	○ (A.7.5, A.7.8, A.7.11)	○ (13.2.2.1)	-
			<Basic> - The organization adopts a system that maintains the temperature and humidity of the area with its IoT devices and servers being within the acceptable level. - The organization regularly monitors the temperature and humidity of the area with its IoT devices and servers. - The organization protects communication cables and power cables that transmit data or that support information service from interception, interference, and harm.	O	-	○ (CP-02, PE-12, PE-13, PE-14, PE-15)	○ (A.7.5, A.7.8, A.7.11, A.7.12)	-	-
CPS.PR.IR-03	The organization implements mechanisms to achieve requirements for the continuous operation of systems and services under normal and adverse conditions.	L1_1_c_SYS L2_1_d_SYS L3_3_c_SYS	Common among <High-Advanced> and <Advanced> - The organization designs systems and infrastructure to eliminate single points of failure. - The organization uses load balancing to improve processing capacity and enhance system stability.	O	-	○ (CP, IR, SA-08, SC-24, SC-39)	○ (A.5.30, A.8.14)	○ (13.2.2.1)	○ (SR 7.1)
			<Basic> - N/A	-	-	-	-	-	-

- Examples of security measures for each of the High Advanced, Advanced, and Basic levels are stated for implementing measure requirements described in Part III. To implement High Advanced-level measures, there is a need to include not only High Advanced-level measures but also Advanced- and Basic-level measures.

- The level of a measure is determined according to the costs in implementing/operating the measure, the scope of the measure (e.g., whether the scope is applied only to the organization or other related organizations), etc., based on management measures stratified into levels.

- The subject that implements measures is classified as “S” (implemented by a system through technical means), as “O” (implemented by an organization (e.g., by people through non-technical means)), and as “O/S” (implemented by both a system and an organization).

- In describing the examples of security measures, reference is made to major security documents and other relevant materials (shown as “Reference Guidelines” in the table).

- The measures described in this section are just examples and do not deny other implementation methods. Use this document as a reference for risk management according to the characteristics of the business of each organization, the results of the risk analyses, etc.

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measure	Reference Guidelines				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 Annex A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.PR.IR-04	The organization secures sufficient resources (e.g., people, components, and systems) to minimize the impact of attacks and maintain critical functions, even in the event of cyberattacks such as ransomware or denial-of-service (DoS) attacks.	L1_1_c_SYS L2_1_d_SYS L3_3_c_SYS	<High-Advanced> - When a control device or IoT device does not have a rollback function for firmware etc., it is desirable for an organization to have a spare control device or IoT device. - By implementing the security measures which the organization decides on, the information system and the industrial control system minimize the impact or protect from the impact of service denial attacks which the organization specifies, or from attacks on references to sources of these information, while performing a fallback operation	O/S	-	(In addition to the following, CP-06, CP-07, CP-08)	○ (A.5.30, A.8.14)	○ (8.2.4.1, 13.2.2.1)	○ (SR 7.1)
			<Advanced> - The organization uses highly available components, such as redundant storage and power supplies, to enhance system stability. - The organization scales resources according to the estimation results of future resource demands. - The information system and industrial control system manage spare storage space, bandwidth, and other spares (People, components, system) and minimize the impact of service denial attacks that send a large amount of information. For example, if services provided by an attacked system cannot be stopped due to maintaining the level of availability, etc., in order to continue important functions, it is necessary to take the following measures. - Automatic or manual migration to standby system - Automatic or manual segregation of system components attacked by adversarial actor - The organization shall: (a) Use a monitoring tool which the organization specifies in order to find signs of service jamming attacks on the information system. (b) Monitor resources of information system and industrial control system identified by the organization and judge whether sufficient resource is secured to prevent effective service jamming attacks.	O/S	-		○ (A.5.30, A.8.6, A.8.14)	○ (13.2.2.1)	
			<Basic> - To ensure the required performance of information systems and industrial control systems, the organization monitors and adjusts resource usage and forecasts the capacity and performance required in the future.	O	-	○ (PM-03, PM-09)		○ (13.2.2.1)	-
CPS.DE.CM-01	The organization monitors networks and network services to properly detect security events.	L1_1_a_SYS L1_1_b_SYS L2_1_b_ORG L2_3_b_SYS L2_3_c_SYS L3_3_d_SYS L3_1_a_SYS L3_3_a_SYS	<High-Advanced> - The organization/system analyzes the regular patterns of its systems' communication status and security alerts to create and use a profile that summarizes typical patterns of communication and security alerts, thereby enabling the detection of unknown threats and suspicious behavior (communication). - The information system and the industrial control system monitor and control the use of mobile code. - The information system monitors and controls the use of protocols used for audio and video transmission (e.g., VoIP).	O/S	-	(In addition to the following, CM-03)	(In addition to the following, A.8.21)	○ (6.3.2.1)	○ (SR 2.4)
			<Advanced> - To detect adverse events, the organization monitors network services such as DNS and BGP. - To detect adverse events, the organization compares actual network traffic against baselines and detects deviations. - The organization monitors network communications and identifies changes in security posture from a zero trust perspective. - To detect malware, phishing, data leaks, unauthorized exfiltration, and other adverse events, the organization monitors common attack vectors such as email, web, file sharing, and collaboration services. - The organization monitors and controls communications at the boundary between industrial control system and information system. - The organization monitors communications at the external boundaries of the information system and at major internal boundaries within the information system for large amounts of communication from a particular source or multiple sources, and takes appropriate action when necessary (e.g., blocking of communication from a specific IP address).	O/S	○ (In addition to the following, 03.13.01 Boundary Protection a.)			○ (6.3.2.1, 13.2.2.1)	○ (SR 1.13, SR 5.2)
			<Basic> - The organization implements mechanisms to detect and block unauthorized access in real time at the boundary between internal and external networks or at endpoints, for both communications from the internet to internal networks and from internal networks to unauthorized servers. - For network devices or network services equipped with capabilities to detect and block unauthorized access in real time, the organization implements mechanisms to execute the following responses during anomalies: - Promptly issues alerts. - Generates and disseminates preliminary incident reports. - At the external boundaries of information systems (managed interfaces), the organization monitors and controls traffic to detect connections to unapproved components or systems, and communications containing inappropriate content. - The organization detects unusual data communications (e.g., too large data size, unexpected communication destination) outbound the organization, and limits such execution of communications when necessary.	O/S	○ (03.14.06 System Monitoring c.)	○ (AC-02, AU-12, CA-07, SC-05, SC-07, SI-04)	○ (A.8.16)	○ (6.3.2.1)	-
CPS.DE.CM-02	The organization monitors the operational status of hardware and software across IoT devices, servers, and related assets, as well as network connection status, to properly detect security events.	L1_1_a_COM L1_1_a_SYS L1_1_b_COM L1_1_c_COM L2_3_b_ORG L2_3_b_SYS L3_3_d_SYS L3_1_a_SYS L3_3_a_SYS	<High-Advanced> - It is desirable for the organization to include not only its information systems but also its industrial control systems and IoT devices in the scope of security monitoring. - The organization uses a mechanism for automatically detecting unauthorized hardware, software, or firmware in a system, if any.	O	-	(In addition to the following, AC-04, CM-03, SI-07)	○ (A.8.16)	○ (6.3.2.1, 7.2.3.1, 12.2.1.1, 13.2.2.1)	-
			<Advanced> - The organization continuously monitors deployed software for deviations from established standard configurations and setting rules, and detects any non-compliance. - The organization monitors for signs of tampering with hardware and software. - The organization monitors resource usage, such as storage, power supplies, and processing capacity. - The information system detects issues such as unapplied patches, malware infections, and unauthorized software, and isolates the devices in a remediation environment before granting access.	O/S	○ (3.14.06 System Monitoring a.)			○ (6.3.2.1)	-
			<Basic> - The organization regularly checks whether necessary measures are taken during operation (e.g., checking IoT devices for any unauthorized use or theft; applying a patch; checking logs) and the state of IoT devices.	O	-	○ (AU-12, CA-07, CM-06, CM-10, CM-11, SI-04)		-	-

- Examples of security measures for each of the High Advanced, Advanced, and Basic levels are stated for implementing measure requirements described in Part III. To implement High Advanced-level measures, there is a need to include not only High Advanced-level measures but also Advanced- and Basic-level measures.

- The level of a measure is determined according to the costs in implementing/operating the measure, the scope of the measure (e.g., whether the scope is applied only to the organization or other related organizations), etc., based on management measures stratified into levels.

- The subject that implements measures is classified as “S” (implemented by a system through technical means), as “O” (implemented by an organization (e.g., by people through non-technical means)), and as “O/S” (implemented by both a system and an organization).

- In describing the examples of security measures, reference is made to major security documents and other relevant materials (shown as “Reference Guidelines” in the table).

- The measures described in this section are just examples and do not deny other implementation methods. Use this document as a reference for risk management according to the characteristics of the business of each organization, the results of the risk analyses, etc.

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measure	Reference Guidelines				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 Annex A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.DE.CM-03	The organization monitors communications with external service providers to properly detect security events.	L1_1_a_SYS L1_1_b_SYS L2_3_c_SYS L3_3_d_SYS L3_1_a_SYS L3_3_a_SYS	Common among <High-Advanced> and <Advanced> - The organization monitors access to its system by its external service provider and system developer in order to detect any unauthorized access by these external businesses that results from an action or failure to act. - The organization reports the results of the monitoring of activities by its external service provider and system developer to the appropriate system administrator.	O/S	-	○ (CA-07, PS-07, SA-04, SA-09, SI-04)	○ (A.8.16)	-	-
			<Basic> - N/A	-	-	-	-	-	-
CPS.DE.CM-04	The organization monitors the activities of internal and external personnel, including their access to and operations on elements (components, systems, etc.), to properly detect security events.	L1_1_a_SYS L2_1_b_ORG L2_3_c_SYS L3_4_a_PRO L3_3_d_SYS L3_1_a_SYS L3_3_a_SYS	<High-Advanced> - The organization continuously monitors deception technologies, including decoy user accounts, for any access. - The information system and the industrial control system automatically monitor or regulate remote access to its system.	O/S	-	○ (AC-02, AU-12, CA-07, CM-10, CM-11)	○ (A.8.16)	○ (8.4.2.1)	○ (SR 1.13)
			<Advanced> - Systems handling critical and sensitive information provide mechanisms to monitor the operation/usage status of granted access rights. - To mitigate internal fraud, the organization uses behavioral analysis software to detect abnormal user behavior. - The organization monitors remote and on-site administration and maintenance activities conducted by external service providers on its systems. - The organization monitors system access logs and identifies abnormal access patterns and access failures. The organization monitors authentication server logs at least monthly to detect suspicious authentication attempts.	O/S	○ (03.01.01 Account Management e, 03.14.06 System Monitoring b.)			-	-
			<Basic> - N/A	-	-	-	-	-	-
CPS.DE.CM-05	The organization implements appropriate physical access settings, logging, and monitoring, commensurate with the criticality of IoT devices, servers, and related assets.	L1_1_a_SYS L2_3_b_PEO L2_3_b_SYS L2_3_d_SYS	<High-Advanced> - The organization tracks and monitors the locations and relocation of important assets within the scope of its management of particularly important assets.	O	-	○ (In addition to the following, 03.10.02 Monitoring Physical Access a,b) ○ (CA-07, PE-03, PE-06)	○ (A.7.4)	-	-
			<Advanced> - The organization monitors the physical environment by utilizing alarm systems, cameras, and security guards. - The organization monitors physical access controls, such as locks, latches, hinges, and alarm devices, for signs of tampering. - The organization maintains entry and exit logs for server installation areas, including the date, time, and names of individuals entering and exiting, and retains these records for at least six months. - The organization monitors logs from physical access control systems (e.g., card readers) to identify unusual access patterns and access failures. - The organization reviews the relevant audit logs regularly, as well as when an incident or a sign of an incident appears, in cases where access logs from physical access control are available, even if continuous monitoring is not conducted through security cameras or by any other means. - The organization requires personnel in charge to accompany a visitor into the area where the organization's assets that must be protected are directly accessible (e.g., an office) in order to monitor the visitor's behavior. - If the above physical security measures are difficult to implement for components such as IoT devices and servers that may be critical to the organization's operation because they are in a remote location or for any other reasons, the organization considers using tamper-resistant equipment (CPS.PR.PS-02) or taking any other appropriate measures to enhance the physical security properties of the equipment itself.	O/S	○ (In addition to the following, 03.10.02 Monitoring Physical Access a,b)			○ (6.4.1.1)	-
			<Basic> - If the organization is unable to control access to, or provide video surveillance service for, the areas that should allow only limited physical access because of issues of costs and other reasons, it takes alternative manual measures, such as having an employee in charge accompany visitors on the premises. - The organization implements physical security measures to control access to designated areas in the facility that are not accessible to the general public. - The organization verifies the access authority of the personnel before permitting the physical access and collects and manages the records of entry and exit.	O/S	○ (03.10.07 Physical Access Control b.)				-
CPS.DE.CM-06	The organization periodically scans its IoT devices, servers, and related assets to identify vulnerabilities requiring remediation.	L1_1_a_SYS L2_1_a_ORG L2_1_c_ORG L3_3_d_SYS L3_1_a_SYS L3_3_a_SYS	<High-Advanced> - The organization conducts vulnerability scan at planned timings such as planned stopping so as not to adversely affect the operation of the system managed by the organization. And then, identify and list vulnerabilities that exist in the system owned by the organization. - When using tools to conduct vulnerability scan, the organization should use tools that can quickly update the vulnerability database of the system being diagnosed. - The organization updates the vulnerabilities targeted for inspection in vulnerability scans (scan definitions) periodically, or whenever new vulnerabilities are identified or reported. - The organization implements a system for authorizing privileged access to the relevant system components in connection with the specified vulnerability scanning.	O	-	-	○ (A.8.8)	○ (6.3.2.1)	-
			<Advanced> - The organization periodically reviews the operating systems and firmware of network devices installed at the internet boundary to identify any vulnerabilities with a CVSS base score of 7.0 or higher. - The organization has its systems and applications scanned for vulnerability regularly, or when any newly-found weaknesses that affect the systems and/or applications are reported. - The organization uses a tool for vulnerability scanning. Applying the standard methods that meet the following means automates parts of the vulnerability management process. - List defects in the platform and software, and wrong setups. - Format a checklist and test procedure. - Assess the impact of the vulnerability. - The organization shares information obtained from vulnerability scans and related assessments with administrators of other systems within the organization, and identifies similar vulnerabilities existing in other information systems. [Reference] Japan Vulnerability Notes (https://jvn.jp/) and other sources of information are available for reference to obtain information regarding vulnerability. Also, CVSS (https://www.ipa.go.jp/security/vuln/scap/cvssv3.html , explained by IPA) could be used as a referential indicator to evaluate the impact level of vulnerability.	O/S	○ (In addition to the following, 03.11.02 Vulnerability Monitoring and Scanning a.)	-		-	-
			<Basic> - The organization regularly has its systems and applications scanned for vulnerability.	O	○ (03.14.01 Flaw Remediation a.)	-		-	-

- Examples of security measures for each of the High Advanced, Advanced, and Basic levels are stated for implementing measure requirements described in Part III. To implement High Advanced-level measures, there is a need to include not only High Advanced-level measures but also Advanced- and Basic-level measures.

- The level of a measure is determined according to the costs in implementing/operating the measure, the scope of the measure (e.g., whether the scope is applied only to the organization or other related organizations), etc., based on management measures stratified into levels.

- The subject that implements measures is classified as “S” (implemented by a system through technical means), as “O” (implemented by an organization (e.g., by people through non-technical means)), and as “O/S” (implemented by both a system and an organization).

- In describing the examples of security measures, reference is made to major security documents and other relevant materials (shown as “Reference Guidelines” in the table).

- The measures described in this section are just examples and do not deny other implementation methods. Use this document as a reference for risk management according to the characteristics of the business of each organization, the results of the risk analyses, etc.

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measure	Reference Guidelines				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 Annex A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.DE.CM-07	The organization verifies the integrity and authenticity of information received from cyberspace prior to operation.	L1_1_a_SYS L1_1_b_SYS L1_1_b_DAT L2_2_a_COM L3_3_d_SYS L3_3_a_DAT	<High-Advanced> - The organization introduces the concept of “whitelisting” for data entry in order to specify known items and systems considered trustworthy as the sources of input data, and the format allowed for the input data. - The information system and the industrial control system protect the authenticity of communications sessions.	O/S	○ (03.13.15 Session Authenticity)	-	-	○ (11.2.16.1)	-
			<Advanced> - The information system uses an integrity verification tool to detect any unauthorized changes that are made to communication data transmitted from IoT devices and servers. - IoT devices and servers that are acknowledged as critical to the organization’s operations begin communication with other IoT devices only after the devices are mutually authenticated successfully so that the source of data is always clear.	S	-	-	-	-	○ (SR 1.2)
			<Basic> - N/A	-	-	-	-	-	-
CPS.DE.CM-08	The organization deploys IoT devices that detect anomalies or suspend operations by comparing commanded operations with actual operational outcomes. The organization verifies that information received from cyberspace does not contain malicious code and remains within permissible operating parameters prior to execution.	L1_1_a_SYS L1_3_a_SYS L2_2_a_COM L2_2_a_SYS L3_3_d_SYS L3_3_a_DAT	<High-Advanced> - The information system detects exploit code that attacks unknown vulnerabilities by installing on endpoints (especially, IoT devices and servers with various functions) detection and restoration software using technologies of behavioral detection of malware. - The information system automatically updates the logic to detect malicious code through an IDS/IPS. - IoT devices, or systems that contain these devices, examine information output from software programs or applications to see if it matches the expected content in order to prepare for certain attacks that may have a consequence different from a normally expected outcome (e.g., command injection).	S	-	-	○ (A 8.7)	-	○ (SR 3.2)
			<Advanced> - To prevent malware infection via email, the organization performs malware checks at email gateways, email servers, and other relevant points. - To verify the safety of files received from external sources, the organization establishes mechanisms to execute real-time scanning with anti-malware software or verify safety in a virtual environment. - The information system detects exploit code by installing on endpoints (IoT devices, servers, and so on) detection/restoration software using technologies of pattern matching of malware. - The organization considers implementing whitelist-type malware protection for IoT devices with limited functions. * Especially regarding IoT devices and control devices, OS to which anti-malware software can be applied may not be used. It is desirable for the organization to confirm whether devices to be introduced are compatible with anti-malware software at the phase of procurement and to select compatible ones. If it is difficult to procure devices compatible with anti-malware software, it is desirable to take alternative measures such as introducing/strengthening a malware detection mechanism on a network.	S	-	-		○ (9.3.2.1)	
			<Basic> - The organization installs anti-malware software on all personal computers and servers connected to the information system network, defines device-specific scanning scopes and frequencies, and executes scans. - Information system and industrial control system verify the effectiveness of input data by checking whether the data conforms to a specified format or content.	O/S	○ (03.14.02 Malicious Code Protection a.)	-		-	○ (SR 3.5)
CPS.DE.CM-09	As part of its monitoring operations, the organization periodically tests and validates whether functions detecting security events operate as intended.	L1_1_a_SYS L1_3_a_SYS	<High-Advanced> - The organization introduces known and harmless test cases to its systems to test its mechanism for detecting malware. - The organization regularly tests the mechanism it uses for intrusion detection monitoring. The frequency of the test depends on the type of tool the organization uses and the way the tool is installed. - The organization conducts a trend analysis examining the latest information about threats, vulnerabilities, and assessments of security management measures carried out several times in order to determine whether the activities for continuous monitoring need any correction.	O	-	-	-	-	○ (SR 3.3, SR 6.2)
			<Advanced> - The organization establishes and manages a procedure for a regular review of its system monitoring activities to see if they conform to the organization's risk management strategy and the order of priority for actions to handle risks. - The organization calculates the percentages of false detections and false negatives when correlation analysis of information pertaining to the security of network devices or endpoints is conducted, thereby checking the validity of the detection mechanism regularly.	O	-	-	-	-	○ (SR 6.2)
			<Basic> - N/A	-	-	-	-	-	-
CPS.DE.AE-01	The organization analyzes potential security events to understand their details.	L1_1_a_SYS L3_3_d_SYS L3_1_a_SYS L3_3_a_SYS	Common among <High-Advanced> and <Advanced> - To detect known malicious and suspicious activities, the organization continuously monitors log events using tools such as Security Information and Event Management (SIEM). - The organization periodically reviews log events manually for devices and systems where automated monitoring cannot be performed sufficiently. - The organization uses cybersecurity software to generate alerts and delivers them to the Security Operations Center (SOC), incident response personnel, and incident response tools. - The information system automatically reports confirmed incidents through detection mechanisms. - The organization uses log analysis tools to generate reports on analytical findings. - The organization enables incident response personnel and other authorized personnel to have continuous access to log analysis results.	O/S	○ (03.03.05 Audit Record Review, Analysis, and Reporting a.)	○ (AU-06, CA-07, IR-04, SI-04, PM-15, PM-16)	○ (A.8.15)	○ (6.3.2.1, 12.2.7.1)	○ (SR 6.2)
			<Basic> - N/A	-	-	-	-	-	-

- Examples of security measures for each of the High Advanced, Advanced, and Basic levels are stated for implementing measure requirements described in Part III. To implement High Advanced-level measures, there is a need to include not only High Advanced-level measures but also Advanced- and Basic-level measures.

- The level of a measure is determined according to the costs in implementing/operating the measure, the scope of the measure (e.g., whether the scope is applied only to the organization or other related organizations), etc., based on management measures stratified into levels.

- The subject that implements measures is classified as “S” (implemented by a system through technical means), as “O” (implemented by an organization (e.g., by people through non-technical means)), and as “O/S” (implemented by both a system and an organization).

- In describing the examples of security measures, reference is made to major security documents and other relevant materials (shown as “Reference Guidelines” in the table).

- The measures described in this section are just examples and do not deny other implementation methods. Use this document as a reference for risk management according to the characteristics of the business of each organization, the results of the risk analyses, etc.

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measure	Reference Guidelines				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 Annex A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.DE.AE-02	The organization accurately identifies security incidents by implementing procedures to correlate security events and analyze them against external threat information.	L2_1_a_ORG	<High-Advanced> - The organization carries out policy tuning (management of signatures to apply) and maintenance for devices such as IDS, IPS, and SIEM. - The organization creates custom signatures used for sensors on its own. - In order to properly detect security events that are likely to adversely affect the organization, the organization collects and analyzes logs of edge devices such as IoT devices in addition to the logs of devices presented in <Advanced>, if possible.	O	-	○ (AU-06, CA-07, IR-04, IR-05, IR-08, PM-16, RA-03, SI-04)	-	○ (12.2.7.1)	-
			<Advanced> - The organization refers to risk assessment results and, considering the following angles, establishes what to monitor in correlation analysis. Furthermore, it is desirable that correlation analysis includes logs from interfaces where data is exchanged with other organizations. - The scope of systems to monitor - Which device logs should be collected for analysis - The organization securely shares asset inventory information with responsible personnel and incorporates it into detection mechanisms and operational processes. - The organization securely shares the latest threat intelligence with responsible personnel and incorporates it into detection mechanisms and operational processes. - By integrating the latest threat intelligence into log analysis tools, the organization improves detection accuracy and identifies threat actors, their tactics, and indicators of compromise. - It is desirable that the organization should monitor mainly logs of the devices listed below for real-time analysis to appropriately detect security events highly likely to have an adverse effect on its own organization. This will require the handling of many different logs. Hence, it is necessary to normalize logs to store them in the same database or to use SIEM for efficient analysis. It is also advisable to handle information about network flows if it is available. - Logs and network flows from network devices, e.g., firewalls - Logs from security devices, e.g., IPS/IDS - Access logs of web servers - Logs from various systems, e.g., Active Directory; DNS - Logs related to users' terminals [Reference] For details on the various tasks performed by security response organizations (SOC/CSIRT), it is advised to refer to documents such as "Textbook for Security Response Organizations (SOC/CSIRT)" - Utilization Functions, Roles, Personnel Skills, and Maturity of the X.1060 Framework -" (ISOG-J, October 2025).	O	○ (03.03.05 Audit Record Review, Analysis, and Reporting c.)		○ (A.5.7)		-
			<Basic> - The organization checks each notice from firewalls and endpoint security products in order to identify security events that may have an adverse impact on the organization.	O	-		-		-
CPS.DE.AE-03	The organization identifies the impact of security events, including the adverse effects on relevant external organizations.	L1_3_a_COM	<High-Advanced> - The organization adopts an automatic mechanism for quantifying and monitoring the form, scale, and cost of a security event that has occurred. - The organization has its security measure organizations (SOC/CSIRT) analyze the functions of the malware, or program, or script that is placed by an attacker if any is found in a security event that has occurred. - The organization constructs a hypothesis about the profile of the attacker (e.g., his/her organization; the purpose of the organization's activities).	O/S	-	○ (PM-09, PM-11, PM-18, PM-28, PM-30)	-	-	-
			<Advanced> - Designated personnel independently estimate the magnitude and scope of impact of security events. - The organization uses tools such as SIEM to estimate the magnitude and scope of impact of security events, and reviews the estimation results to make them more accurate. - The organization works with IPA, JPCERT/CC, the industry's ISAC, and a security vendor to collect information, thereby interlinking and sharing information about threats and vulnerability to obtain a whole picture of the security event. - The organization requests an external security vendor to analyze the functions of programs or scripts placed by malware or an attacker if any is found in a security event that has occurred.	O	-		-	-	-
			<Basic> - N/A		-	-		-	-
CPS.DE.AE-04	The organization establishes criteria for determining whether a security event constitutes an incident, and declares an incident when the criteria are met.	-	<High-Advanced> - The organization uses an automated mechanism designed to help track security events and collect and analyze information about threats and vulnerability related to incidents, so that it applies the findings to classification (triage) of security events.	O	-	○ (IR-04, IR-08)	○ (A.5.25)	-	-
			<Advanced> - The organization defines security incident levels and the scope for each level within the company, and communicates them to officers, employees, contingent workers, and seconded personnel. - When detecting suspicious authentication attempts through authentication server log monitoring, or upon receiving alerts from network devices or services equipped to detect and block unauthorized access in real time, the organization analyzes and determines the appropriate incident level based on the predefined security incident levels and scope.	O	-			-	-
			<Basic> - The organization analyzes network device logs and alerts, and when a suspicious event is discovered by personnel or administrators of the security department, determines whether that event constitutes a security incident based on established criteria. - The organization takes into account events and anomalies specific to industrial control systems when determining whether a security event constitutes an incident. - The organization specifies security events that must be reported, considering the level of the impact the security event has. [Reference] For example, SP 800-61 Rev. 3 (NIST, 2025) is available for reference when an organization decides on a measure of the severity of the impact of a security event.	O	-			-	-

- Examples of security measures for each of the High Advanced, Advanced, and Basic levels are stated for implementing measure requirements described in Part III. To implement High Advanced-level measures, there is a need to include not only High Advanced-level measures but also Advanced- and Basic-level measures.

- The level of a measure is determined according to the costs in implementing/operating the measure, the scope of the measure (e.g., whether the scope is applied only to the organization or other related organizations), etc., based on management measures stratified into levels.

- The subject that implements measures is classified as “S” (implemented by a system through technical means), as “O” (implemented by an organization (e.g., by people through non-technical means)), and as “O/S” (implemented by both a system and an organization).

- In describing the examples of security measures, reference is made to major security documents and other relevant materials (shown as “Reference Guidelines” in the table).

- The measures described in this section are just examples and do not deny other implementation methods. Use this document as a reference for risk management according to the characteristics of the business of each organization, the results of the risk analyses, etc.

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measure	Reference Guidelines				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 Annex A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.RS.MA-01	To clarify response actions, priorities, and remediation scope following the occurrence of a security incident, the organization predefines and implements response procedures (security operation processes) for the organization, people, components, and systems after detecting an incident.	L1_3_a_PEO L1_3_a_PRO L1_3_b_PRO L1_3_c_PRO L2_1_a_PRO L2_1_b_PRO L2_1_c_SYS L2_1_d_SYS L2_2_a_PRO	<High-Advanced> - The organization incorporates detection capability into its incident response capability to detect unauthorized changes that are made to the settings and security, such as unauthorized privilege escalation. - The organization establishes mechanisms to automatically create and assign tickets in its ticket management system when specific types of alerts occur, and defines operational procedures for these mechanisms. - The organization assumes the course of action for security incidents of the supply chain and prepares a procedure that adjusts incident responses between the organization and other organizations that are concerned with the supply chain. - The organization assumes the course of action for security incidents of the supply chain and implements tests that adjust incident responses with other organizations that are concerned with the supply chain. [Reference] Examples of security incidents in the supply chain include compromises of system components, IT products, development processes, developers, distribution processes, and warehouse facilities.	O	-	○ (CP-01, CP-02, IR-01, IR-08, PL-02, SA-04, SA-09, SR-02, SR-03, SR-08)	○ (A.5.24)	○ (12.2.8.1)	-
			<Advanced> - The organization defines and documents its own roles and responsibilities as well as those of suppliers in incident response. - In addition to the security operation processes defined in the Basic level, the organization includes the following in its workflow: - Track and record incident status, response actions, evidence, and other relevant information. - Determine whether the occurrence of the incident and the status of the response need to be reported to external organizations. - The organization establishes mechanisms to track and manage incident response (such as a ticket management system), and defines procedures to manually create tickets and assign responsible personnel upon detecting indicators of compromise. - The organization adjusts the incident response process of an external service provider that contains important features in order to continue its business, as well as adjusting the organization's incident response process to meet the incident response requirements. - The organization tests the incident response process that requires cooperation between the organization and external service providers.	O	-			○ (12.2.8.1)	-
			<Basic> - The organization documents established security incident response procedures as an incident response plan and communicates this plan to its stakeholders. - When operating industrial control systems, the organization incorporates safety and containment considerations specific to industrial control systems into the development of its incident response plan. - The organization establishes reporting formats for security incidents. - The organization develops and manages a process of security operation it should follow when a security incident arises that it must address. The process is structured in line with a series of response phases consisting of discovery and reporting, initial response, investigation and response, recovery, and final reporting, and it is advisable to include the following examples: - Response procedure for the person who received the incident report - Instructions and orders, and how to prioritize actions in an emergency; - Incident response; - Incident impact assessment and damage analysis; - Information gathering, selecting information that the organization needs; - Communication and announcement to relevant internal personnel; - Communication with relevant external organizations; - The system (especially, industrial control system) shuts down, issues an alert to the administrator, or takes other fail-safe actions if any abnormality (e.g., malfunction) occurs in IoT devices or servers. [Reference] In examining response procedures for security incidents, the "Incident Handling Manual" (JPCERT/CC, 2021), SP 800-61 Rev. 3 (NIST, 2025), and "Creating an Incident Response Manual" (JPCERT/CC, 2015) are available for reference.	O/S	○ (03.06.01 Incident Handling, 03.06.05 Incident Response Plan a.)			○ (8.2.4.1, 12.2.2.1, 12.2.8.1)	○ (SR 3.7)
CPS.RS.MA-02	The organization verifies that events reported as security incidents are not false positives or duplicate reports, and validates their legitimacy as incidents.	L1_3_a_PEO	Common among <High-Advanced> and <Advanced> - The organization conducts an initial review of incident reports to determine whether they constitute security events that require incident response. - The organization tracks the status of all ongoing security incidents and verifies their validity.	O	○ (03.06.02 Incident Monitoring, Reporting, and Response Assistance b.)	○ (IR-04, IR-05, IR-06)	○ (A.5.25)	○ (12.2.8.1)	-
			<Basic> - N/A	-	-	-	-	-	-
CPS.RS.MA-03	The organization classifies and prioritizes detected security incidents based on the severity of impact, entry route, and other factors.	L1_3_a_PEO	<High-Advanced> - The organization uses an automated mechanism designed to help track security incidents and collect and analyze information about threats and vulnerability related to incidents, so that it applies the findings to classification (triage) of security incidents.	O	-	○ (IR-04, IR-05, IR-06)	-	○ (12.2.8.1)	-
			<Advanced> - The organization further reviews and classifies security incidents based on incident type (e.g., data breaches, ransomware, DDoS, and account compromise). - The organization determines response priorities based on the scope, anticipated impact, severity, and urgency of the security incident, as well as recovery objectives of the affected targets among other factors. - For ongoing security incidents, the organization selects a security incident response strategy by balancing the need for rapid recovery against the need to observe threat actor behaviors and conduct more detailed investigations.	O	-		-		-
			<Basic> - N/A	-	-	-	-	-	-

- Examples of security measures for each of the High Advanced, Advanced, and Basic levels are stated for implementing measure requirements described in Part III. To implement High Advanced-level measures, there is a need to include not only High Advanced-level measures but also Advanced- and Basic-level measures.

- The level of a measure is determined according to the costs in implementing/operating the measure, the scope of the measure (e.g., whether the scope is applied only to the organization or other related organizations), etc., based on management measures stratified into levels.

- The subject that implements measures is classified as “S” (implemented by a system through technical means), as “O” (implemented by an organization (e.g., by people through non-technical means)), and as “O/S” (implemented by both a system and an organization).

- In describing the examples of security measures, reference is made to major security documents and other relevant materials (shown as “Reference Guidelines” in the table).

- The measures described in this section are just examples and do not deny other implementation methods. Use this document as a reference for risk management according to the characteristics of the business of each organization, the results of the risk analyses, etc.

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measure	Reference Guidelines				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 Annex A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.RS.MA-04	Once a security incident is declared, the organization executes incident response in accordance with predefined procedures, coordinating with other relevant organizations such as business partners.	L1_3_b_PEO L1_3_c_ORG	<High-Advanced> - The organization interlinks information regarding threats and vulnerabilities with how individual security incidents have been handled so as to improve its understanding of the situations.	O	-	○ (In addition to the following, SR-06)	-	○ (12.2.8.1)	-
			<Advanced> - The organization prepares internal resources for incident handling assistance (e.g., help desk; CSIRT). These resources offer advice and support related to security incident handling and reporting for system users of the information system and industrial control system, and are an integral part of organizational ability to handle incidents. - The organization designates a lead incident handler for each incident. - The organization examines the results of correlation analysis and other data to accurately detect security incidents requiring action, and takes action in accordance with the security operation process. - The organization requests response assistance from external incident response contractors. - The organization determines an alternative processing site in case the availability of its primary processing site has been compromised by a security incident. - The organization designates an alternative processing site away from its primary processing site in order to mitigate the vulnerability to the same threats. - The organization sets forth in the service agreement that if its primary processing function becomes unavailable, certain operations are moved to resume at the alternative processing site within the recovery time objective that the organization specifies in order to ensure that it continues to perform its critical missions and operational functions. - To support incident response, the organization executes business continuity plans, disaster recovery plans, and other relevant plans as necessary.	O	-				-
			<Basic> - If any security incident that requires handling is found, the organization reports it promptly to relevant organizations such as IPA and JPCERT/CC in order to receive advice about providing assistance in handling, identifying how the incident has occurred, analyzing the tactic, and preventing any recurrence.	O	-	○ (CP-01, IR-01, IR-06, IR-07, IR-08, PM-31, RA-03, RA-05, RA-07, SA-04, SA-09, SR-02, SR-03, SR-05, SR-08)			-
CPS.RS.MA-05	The organization takes appropriate actions for components (products) suspected of having quality defects, such as those produced using equipment damaged during a security incident.	L1_3_b_COM	Common among <High-Advanced> and <Advanced> - The organization provides an overview of a security incident for relevant external entities including business partners and end users, and collects detailed information about damage inflicted by the incident. - The organization coordinates actions related to recovery and post-incident processing with relevant external entities involved in the supply chain. It is advisable to identify the items for handling in accordance with the approaches included in CPS.ID.AM-07 and CPS.ID.AM-08. - The organization coordinates actions related to recovery and post-incident processing with relevant external entities involved in the supply chain. An example of these actions is recalling items produced when a security incident in the production system has occurred.	O	-	-	-	○ (12.2.8.1)	-
			<Basic> - The organization considers stating what to do with components produced after the incident in the business continuity plan or emergency response plan, taking into account the type of the organization's business. Note that the business continuity plan or emergency response plan may not be for security incidents.	O	-	-	-		-
CPS.RS.MA-06	The organization determines the initiation of recovery based on predetermined criteria, taking into account the characteristics of the security incident and the impact of recovery activities on business operations.	L1_3_a_PEO	Common among <High-Advanced> and <Advanced> - The organization considers the potential for business disruption arising from incident recovery activities. - The organization collects and preserves all relevant security incident data and metadata (e.g., data source and acquisition date and time) in accordance with evidence preservation principles and the chain of custody, and ensures their integrity.	O	-	○ (IR-04, IR-08)	-	○ (12.2.8.1)	-
			<Basic> - N/A	-	-	-	-	-	-
CPS.RS.AN-01	The organization collects data and metadata related to security incidents (including the history of actions taken during incident response), preserves their integrity, and retains them in a state where acquisition sources, timestamps, and related provenance can be referenced.	L1_1_a_DAT L3_1_a_DAT L3_3_d_SYS	Common among <High-Advanced> and <Advanced> - The organization collects and preserves all relevant security incident data and metadata (e.g., data source and acquisition date and time) in accordance with evidence preservation principles and the chain of custody, and ensures their integrity.	O	○ (03.06.02 Incident Monitoring, Reporting, and Response Assistance a.)	○ (AU-07, IR-04, IR-06)	○ (A.5.28)	-	-
			<Basic> - N/A	-	-	-	-	-	-
CPS.RS.AN-02	After a security incident occurs, the organization conducts digital forensics to identify the root cause. In doing so, it preserves records of the investigation process in a tamper-resistant manner.	L1_1_a_DAT L3_1_a_DAT L3_3_d_SYS	<High-Advanced> - The information system provides a procedure for processing an audit record regarding critical security incidents.	O	-	○ (In addition to the following, AU-07)	○ (A.5.28)	-	-
			<Advanced> - The organization establishes procedures for identifying, collecting, acquiring, and saving proof according to the medium, device, and the state of the device (e.g., whether it is switched on or off). - It is desirable that the organization should retain the following evidence after the occurrence of any serious security incident: - Incident identification data (e.g., location of occurrence, date and time of occurrence, serial number on the items, host name, MAC address, and IP address) - Title, name, and contact information of the person who collected and processed the evidence, as well as the processing date and time (including time zone) - Activity logs of incident responders and personnel performing response operations - The organization organizes the chronological flow of events that occurred during the incident and identifies the assets and resources involved in each event. - The organization identifies the vulnerabilities, threats, and threat actors directly or indirectly involved in the incident. - The organization analyzes the incident and identifies the root cause at the system level. - The organization uses tools and other means to inspect other targets potentially affected by the incident, in order to confirm indicators of compromise and evidence of ongoing unauthorized activities. - The organization reviews information from deception techniques to gain additional insight regarding attacker behavior.	O	-			○ (12.2.8.1)	-
			<Basic> - The organization establishes and manages procedures for identifying, collecting, acquiring, and saving data that may serve as proof.	O	-	○ (IR-04, IR-06, SI-02)			-

- Examples of security measures for each of the High Advanced, Advanced, and Basic levels are stated for implementing measure requirements described in Part III. To implement High Advanced-level measures, there is a need to include not only High Advanced-level measures but also Advanced- and Basic-level measures.

- The level of a measure is determined according to the costs in implementing/operating the measure, the scope of the measure (e.g., whether the scope is applied only to the organization or other related organizations), etc., based on management measures stratified into levels.

- The subject that implements measures is classified as “S” (implemented by a system through technical means), as “O” (implemented by an organization (e.g., by people through non-technical means)), and as “O/S” (implemented by both a system and an organization).

- In describing the examples of security measures, reference is made to major security documents and other relevant materials (shown as “Reference Guidelines” in the table).

- The measures described in this section are just examples and do not deny other implementation methods. Use this document as a reference for risk management according to the characteristics of the business of each organization, the results of the risk analyses, etc.

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measure	Reference Guidelines				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 Annex A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.RS.AN-03	Based on the full scope of the security incident and the inferred intent of the threat actor, the organization assesses the impact on society as a whole, including the organization itself and relevant external organizations.	L1_3_a_COM	<High-Advanced> - The information system adopts an automatic mechanism for quantifying and monitoring the form, scale, and cost of a security incident that has occurred. - The organization constructs a hypothesis about the profile of the attacker (e.g., his/her organization; the purpose of the organization's activities).	O	-	○ (IR-04, IR-08, RA-03, RA-07)	-	-	-
			<Advanced> - The organization works with IPA, JPCERT/CC, the industry's ISAC, and a security vendor to collect information, thereby interlinking and sharing information about threats and vulnerability to obtain a whole picture of the security incident.	O	-		-	-	-
			<Basic> - N/A	-	-	-	-	-	-
CPS.RS.CO-01	The organization develops and implements rules governing internal communication and external disclosure after the occurrence of a security incident.	L1_3_a_PRO L1_3_a_PEO	Common among <High-Advanced> and <Advanced> - The organization notifies its human resources department when insider fraud occurs within its operations. - The organization notifies business partners and customers about the incident in accordance with contractual requirements and organizational notification procedures. - The organization notifies relevant authorities and competent ministries of incidents based on criteria defined in the incident response plan and upon obtaining senior management approval. - The organization voluntarily shares information regarding attacker TTPs with the Information Sharing and Analysis Center (ISAC) after removing all sensitive information.	O	-	○ IR-04, IR-06, IR-07, SR-03, SR-08)	-	○ (12.2.8.1)	-
			<Basic> - The organization defines contact directories along with reporting and information-sharing routes for internal and external entities (including relevant authorities and competent ministries) during a security incident. - The organization develops and manages rules regarding publishing of information after a security incident that cover the following: - What information should be published? - Timing of publishing of the information; - Who is in charge of publishing the information? - The process for publishing the information. - The organization shares incident cases and their countermeasures with internal departments at least annually and when major security incidents occur internally or externally.	O	○ (03.06.05 Incident Response Plan a.)		○ (A.5.5)		-
CPS.RS.CO-02	Based on established rules, the organization escalates incidents to executive decision-makers within the organization and relevant external entities as necessary.	L1_3_a_PEO	Common among <High-Advanced> and <Advanced> - The organization regularly reports the status of major incidents to senior management. - The organization coordinates with designated internal and external stakeholders to manage incident escalation or severity upgrades.	O	○ (03.06.02 Incident Monitoring, Reporting, and Response Assistance c.)	○ (IR-04, IR-05, IR-06, IR-07)	-	○ (12.2.8.1)	-
			<Basic> - N/A	-	-	-	-	-	-
CPS.RS.MI-01	The organization minimizes the spread of damage from security incidents, eradicating causes or mitigating adverse impacts.	L1_3_a_PEO	<High-Advanced> - The organization minimizes the number of users who can use the system administrator's authority as necessary in an emergency to mitigate the damage caused by the security incident. - The organization prevents even system administrators from stopping critical services and protected processes through the server as necessary to mitigate the damage caused by security incidents. - The organization uses an automated mechanism for assisting with the process of security incident handling. - The information system automatically transitions compromised terminals to a remediation VLAN.	O/S	-	○ (IR-04)	-	○ (12.2.8.1)	-
			<Advanced> - Cybersecurity technologies (e.g., antivirus software) and cybersecurity capabilities embedded in other technologies (e.g., operating systems and network infrastructure devices) automatically execute containment responses. - The organization enables third parties (e.g., internet service providers and managed security service providers) to execute containment actions on behalf of the organization. - Cybersecurity technologies and capabilities embedded in other technologies (e.g., operating systems and network infrastructure devices) automatically execute eradication actions. - The organization enables incident response personnel to manually select and execute eradication actions. - The organization enables third parties (e.g., managed security service providers) to execute eradication actions on its behalf.	O/S	-		-		-
			<Basic> - The organization (or its members) takes courses of action to reduce security incidents (e.g., shutting down the system; cutting off the system from a wired/wireless network; cutting off a modem cable; disabling certain functions) in accordance with prescribed procedures.	O	-		-	○ (8.2.5.1, 12.2.8.1)	-
CPS.RC.RP-01	The organization incorporates security incidents into its business continuity plan or emergency response plan, which defines response policies and procedures for natural disasters.	L1_3_a_PRO	Common among <High-Advanced> and <Advanced> - The organization will establish a system of business continuity in emergency for information systems, industrial control systems and managers of related processes. This system defines the priority of the system for recovering operation when an event occurs that causes interruption in business continuity. - The organization develops and manages a business continuity plan or an emergency response plan specifically for security incidents with certain characteristics, such as that the damage the incident inflicts is less obvious than that caused by a disaster, making it difficult to specify when the business continuity plan should be carried out, or that identifying the cause of the incident has high priority. - The organization ensures that the business continuity plan or emergency response plan it develops specifically for security incidents goes along with the organization-wide policy on business continuity.	O	-	-	○ (A.5.29)	○ (13.2.1.1)	-
			<Basic> - N/A	-	-	-	-	-	-

- Examples of security measures for each of the High Advanced, Advanced, and Basic levels are stated for implementing measure requirements described in Part III. To implement High Advanced-level measures, there is a need to include not only High Advanced-level measures but also Advanced- and Basic-level measures.

- The level of a measure is determined according to the costs in implementing/operating the measure, the scope of the measure (e.g., whether the scope is applied only to the organization or other related organizations), etc., based on management measures stratified into levels.

- The subject that implements measures is classified as “S” (implemented by a system through technical means), as “O” (implemented by an organization (e.g., by people through non-technical means)), and as “O/S” (implemented by both a system and an organization).

- In describing the examples of security measures, reference is made to major security documents and other relevant materials (shown as “Reference Guidelines” in the table).

- The measures described in this section are just examples and do not deny other implementation methods. Use this document as a reference for risk management according to the characteristics of the business of each organization, the results of the risk analyses, etc.

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measure	Reference Guidelines				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 Annex A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.RC.RP-02	The organization takes into account critical business functions and the results of cybersecurity risk management when establishing post-incident operational policies.	-	Common among <High-Advanced>, <Advanced> and <Basic> - When defining post-incident operational policies, the organization takes into account the core businesses to be prioritized for continuity and recovery in advance, as well as resources (e.g., relevant organizations, people, components, data, system, etc.) and functions that are critical to operating those businesses.	O	-	○ (IR-01, IR-08, PM-08, PM-09, PM-11)	-	-	-
					-		-		
CPS.RC.RP-03	Upon deciding to initiate the recovery phase, the organization executes recovery based on predetermined recovery plans.	-	Common among <High-Advanced> and <Advanced> - The organization ensures that all personnel responsible for recovery understand the approvals and authorities required to execute recovery actions. - The organization initiates recovery actions during or after the execution of the incident response process. - The organization selects recovery actions based on criteria defined in the incident response plan and available resources. - The organization adjusts recovery actions as appropriate based on reassessments of organizational needs and available resources.	O	-	○ (CP-10, IR-04, IR-08)	-	-	-
				-	-	-	-	-	-
CPS.RC.RP-04	The organization verifies the integrity of backups and other recovery assets prior to use.	L1_3_a_DAT	Common among <High-Advanced> and <Advanced> - Before utilizing assets for recovery, the organization verifies that there are no issues regarding indicators of compromise, file corruption, or other integrity concerns.	O	-	○ (CP-02, CP-04, CP-09)	-	-	-
				-	-	-	-	-	-
CPS.RC.RP-05	The organization verifies the integrity of restored assets, recovers systems and services, and confirms that they are in a normal operational state.	-	Common among <High-Advanced> and <Advanced> - Before putting restored assets into production, the organization confirms that the assets show no signs of compromise and confirms either that the root cause of the incident has been eliminated or that any residual risks have been assessed and the necessary containment or compensating measures have been implemented. - The organization verifies that critical services are restored in the appropriate sequence based on records of business impact and system classification (including service delivery objectives). - The organization monitors the performance of restored systems and verifies that the recovery has been appropriately completed.	O	-	○ (CP-10)	-	-	○ (SR 7.4)
				-	-	-	-	-	-
CPS.RC.RP-06	The organization declares the completion of incident recovery based on predetermined criteria and completes the documentation related to the incident.	-	Common among <High-Advanced> and <Advanced> - The organization prepares a post-incident report that documents incident details, implemented response actions, recovery measures, and lessons learned.	O	-	○ (IR-04, IR-08)	-	-	-
				-	-	-	-	-	-
CPS.RC.CO-01	The organization establishes and maintains rules regarding information exchange aimed at recovery after the occurrence of a security incident.	-	Common among <High-Advanced> and <Advanced> - The organization establishes rules and procedures for reporting and sharing the recovery status of security incidents between the organization and its suppliers. - The organization explains the response actions implemented toward recovery from the incident and the measures for preventing recurrence to internal and external parties.	O	-	○ (CP-01, CP-02, SA-04, SA-09, SR-02, SR-03, SR-08, IR-01, IR-04)	-	-	-
				-	-	-	-	-	-
CPS.RC.CO-02	The organization incorporates provisions to restore public trust and organizational reputation after the occurrence of a security incident into its business continuity plan or emergency response plan.	L1_3_a_PRO	Common among <High-Advanced>, <Advanced> and <Basic> - The organization sets up a single point of contact for the media and business partners requesting information, thereby ensuring consistency in communication with them. - The organization remains aware of the positive side of providing a detailed explanation about damage caused by a security incident while considering the confidentiality of the important information.	O	-	-	-	-	-
CPS.RC.CO-03	The organization specifies within its business continuity or emergency response plans that recovery activities must be communicated to internal and external stakeholders, officers, and management.	L1_3_a_PRO	Common among <High-Advanced> and <Advanced> - The organization provides an overview of a security incident for relevant external entities including the regulatory authorities, business partners, and end users, and collects detailed information about damage inflicted by the incident.	O	-	○ (IR-04, IR-08, SR-08)	-	-	-
				O	-		-	-	-