

Appendix B: Relationship between risk sources and measure requirements

■Functions/Assumed Security Incidents/Risk Sources/Measure Requirements in the First Layer

#	Function	Assumed security incident	Risk sources			Measure Requirement	Measure Requirement ID
			Threat	Vulnerability ID	Vulnerability		
1_1	Establishing the organizational risk management system effective in normal times and appropriately operating it.	Data that must be protected is leaked from an area managed by the organization	- Malware infection that takes advantage of a data storage system's vulnerability - Injection attack exploiting incomplete input validation (e.g. SQL injection, XSS) - Communication interception on the network - Physical intrusion by an unauthorized person into areas that need to be protected - Identity spoofing using a stolen ID/password of a proper user - Internal fraud by an authorized user	L1_1_a_ORG	[Organization] - Security risks are not managed in accordance with appropriate procedures, and other organizations needed are not involved in risk management.	The organization understands its mission and uses it to inform cybersecurity risk management decisions.	CPS.GV.OC-01
						The organization identifies strategic opportunities (positive risks for the organization), clarifies their characteristics, and integrates them into organizational cybersecurity risk deliberations.	CPS.GV.RM-08
						The organization establishes supply chain risk management programs, strategies, objectives, policies, and processes, and operates them upon agreement with organizational stakeholders.	CPS.GV.SC-01
						The organization establishes cybersecurity roles and responsibilities for suppliers and partners, communicates them internally and externally, and coordinates adjustments as necessary.	CPS.GV.SC-02
						The organization integrates cybersecurity supply chain risk management into its cybersecurity and enterprise risk management, risk assessment, and improvement processes.	CPS.GV.SC-03
						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.	CPS.GV.SC-04
						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.	CPS.GV.SC-05
						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.	CPS.GV.SC-06
						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.	CPS.GV.SC-10
			L1_1_a_PEO	[People] - People are not fully aware of the security or safety risks that may concern them.		The organization establishes roles, responsibilities, and authorities related to its cybersecurity risk management and communicates them within the organization.	CPS.GV.RR-02
						The organization continuously improves security training and education programs for its personnel and designated contacts at critical partner organizations.	CPS.ID.IM-03
						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.	CPS.PR.AT-01
						[People] - The security or safety risks that involve people are not managed adequately.	CPS.GV.OC-02
							CPS.GV.RM-06
							CPS.GV.RR-01
						The organization establishes roles, responsibilities, and authorities related to its cybersecurity risk management and communicates them within the organization.	CPS.GV.RR-02
						The organization incorporates security-related matters (e.g., revoking access privileges and screening employees) into measures that address role changes resulting from personnel transfers.	CPS.GV.RR-05
						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.	CPS.GV.PO-01
						The organization periodically reviews its security policies and updates them as necessary, based on changes in requirements, threats, technology, and the organization's mission.	CPS.GV.PO-02
			L1_1_a_COM	[Components] - The security status of components and the status of network connections are not managed appropriately (e.g. Inventory of assets, monitoring).		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.	CPS.ID.AM-01
						The organization develops and appropriately manages communication network diagrams and data flow diagrams within the organization.	CPS.ID.AM-02
						The organization develops and appropriately manages inventories of external information systems connected to its organizational assets.	CPS.ID.AM-03
						The organization manages systems, hardware, software, services, and data throughout their entire lifecycle, from acquisition to disposal.	CPS.ID.AM-06
						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.	CPS.DE.CM-02
			L1_1_a_SYS	[System] - The organization has not implemented technical measures considering risks, or cannot confirm such implementation.		The organization establishes its risk appetite and risk tolerance, and communicates them across the organization.	CPS.GV.RM-03
						The organization identifies vulnerabilities in its assets and manages them by linking them to the corresponding assets.	CPS.ID.RA-01
						- 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.	CPS.ID.RA-03
						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.	CPS.ID.RA-04
						- 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.	CPS.ID.RA-06
						The organization assesses the risk impact posed by significant organizational changes and security requirement exceptions, and records and manages the results.	CPS.ID.RA-07

#	Function	Assumed security incident	Risk sources			Measure Requirement	Measure Requirement ID
			Threat	Vulnerability ID	Vulnerability		
					[System] - Vulnerabilities that should be handled are left unaddressed in the system.	The organization identifies vulnerabilities in its assets and manages them by linking them to the corresponding assets.	CPS.ID.RA-01
						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).	CPS.ID.RA-02
						The organization periodically scans its IoT devices, servers, and related assets to identify vulnerabilities requiring remediation.	CPS.DE.CM-06
						The organization develops a vulnerability remediation plan and remediates component vulnerabilities in accordance with the plan.	CPS.PR.PS-08
						The organization applies security-critical updates for IoT devices, servers, and related assets in a timely manner using managed tools while appropriately recording history.	CPS.PR.PS-09
						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.	CPS.PR.PS-10
					[System] - Settings in the system where the data to be protected is stored are not secure.	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).	CPS.PR.PS-06
						The organization prevents the installation and execution of unauthorized software.	CPS.PR.PS-07
					[System] - Regarding access to stored information, a request sender is not identified / authenticated in a manner suited to the level of confidentiality of such information.	The organization establishes and implements procedures to issue, manage, verify, revoke, and audit identities and credentials for authorized components, people, and procedures.	CPS.PR.AA-01
						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).	CPS.PR.AA-02
						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.	CPS.PR.AA-03
						The organization protects, transmits, receives, and verifies information regarding authenticated entities (ID assertions).	CPS.PR.AA-04
					[System] - The organization does not take physical security measures such as access control and monitoring of areas where its IoT devices and servers are installed,	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.	CPS.PR.AA-07
						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.	CPS.PR.IR-02
						The organization implements appropriate physical access settings, logging, and monitoring, commensurate with the criticality of IoT devices, servers, and related assets.	CPS.DE.CM-05
					[System] - The system has no mechanism for detecting and handling any abnormality related to security as soon as it arises.	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.	CPS.PR.PS-11
						The organization monitors networks and network services to properly detect security events.	CPS.DE.CM-01
						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.	CPS.DE.CM-02
						The organization monitors communications with external service providers to properly detect security events.	CPS.DE.CM-03
						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.	CPS.DE.CM-04
						The organization verifies the integrity and authenticity of information received from cyberspace prior to operation.	CPS.DE.CM-07
						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.	CPS.DE.CM-08
						As part of its monitoring operations, the organization periodically tests and validates whether functions detecting security events operate as intended.	CPS.DE.CM-09
						The organization analyzes potential security events to understand their details.	CPS.DE.AE-01

#	Function	Assumed security incident	Risk sources			Measure Requirement	Measure Requirement ID
			Threat	Vulnerability ID	Vulnerability		
				L1_1_a_DAT	[Data] - Classification concerning protection of data managed in own organization is not clear.	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.	CPS.PR.DS-01
					[Data] - Data protection at a predefined level of confidentiality is not implemented.	The organization protects the confidentiality, integrity, and availability of data-at-rest.	CPS.PR.DS-02
						The organization protects the confidentiality, integrity, and availability of data-in-transit.	CPS.PR.DS-03
						The organization protects the confidentiality, integrity, and availability of data-in-use.	CPS.PR.DS-04
						The organization performs routine backups of data (e.g., component configurations and operational data), protects backup data, and tests restoration capabilities.	CPS.PR.DS-06
						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.	CPS.RS.AN-01
						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.	CPS.RS.AN-02
				L1_1_a_PRO	[Procedure] - Appropriate procedures for security risk management have not been established.	The organization defines risk management objectives and agrees on them with relevant stakeholders.	CPS.GV.RM-01
						The organization develops a cybersecurity strategy to ensure effective cybersecurity risk management.	CPS.GV.RM-02
						The organization establishes its risk appetite and risk tolerance, and communicates them across the organization.	CPS.GV.RM-03
						The organization formulates policies regarding risk response options and their operations, and shares them within the organization.	CPS.GV.RM-05
						The organization standardizes methodologies for assessing, documenting, classifying, and prioritizing cybersecurity risks, and shares them within the organization.	CPS.GV.RM-07
						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.	CPS.GV.PO-01
						The organization periodically reviews its security policies and updates them as necessary, based on changes in requirements, threats, technology, and the organization's mission.	CPS.GV.PO-02
						The organization establishes supply chain risk management programs, strategies, objectives, policies, and processes, and operates them upon agreement with organizational stakeholders.	CPS.GV.SC-01
						The organization establishes cybersecurity roles and responsibilities for suppliers and partners, communicates them internally and externally, and coordinates adjustments as necessary.	CPS.GV.SC-02
						The organization integrates cybersecurity supply chain risk management into its cybersecurity and enterprise risk management, risk assessment, and improvement processes.	CPS.GV.SC-03
						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.	CPS.GV.SC-05
						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.	CPS.GV.SC-09
						The organization establishes and implements procedures to be followed upon the termination of contracts with partners and other parties.	CPS.GV.SC-11
		Data that must be protected is tampered with in an area managed by the organization		L1_1_b_ORG	[Organization] - Security risks are not managed in accordance with appropriate procedures, and other organizations needed are not involved in risk management.	The organization understands its mission and uses it to inform cybersecurity risk management decisions.	CPS.GV.OC-01
						The organization identifies strategic opportunities (positive risks for the organization), clarifies their characteristics, and integrates them into organizational cybersecurity risk deliberations.	CPS.GV.RM-08
						The organization establishes supply chain risk management programs, strategies, objectives, policies, and processes, and operates them upon agreement with organizational stakeholders.	CPS.GV.SC-01
						The organization establishes cybersecurity roles and responsibilities for suppliers and partners, communicates them internally and externally, and coordinates adjustments as necessary.	CPS.GV.SC-02
						The organization integrates cybersecurity supply chain risk management into its cybersecurity and enterprise risk management, risk assessment, and improvement processes.	CPS.GV.SC-03
						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.	CPS.GV.SC-04
						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.	CPS.GV.SC-05
						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.	CPS.GV.SC-06
						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.	CPS.GV.SC-10
				L1_1_b_PEO	[People] - People are not fully aware of the security or safety risks that may concern them.	The organization establishes roles, responsibilities, and authorities related to its cybersecurity risk management and communicates them within the organization.	CPS.GV.RR-02
						The organization establishes and maintains lines of communication across the organization regarding cybersecurity risks, including risks posed by partners and other third parties.	CPS.GV.RM-06
						The organization continuously improves security training and education programs for its personnel and designated contacts at critical partner organizations.	CPS.ID.IM-03
						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.	CPS.PR.AT-01

#	Function	Assumed security incident	Risk sources			Measure Requirement	Measure Requirement ID	
			Threat	Vulnerability ID	Vulnerability			
					[People] - The security or safety risks that involve people are not managed adequately.	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.	CPS.GV.OC-02	
					Organizational senior management is responsible and accountable for cybersecurity risk, fostering a culture that is risk-aware, ethical, and continually improving.	CPS.GV.RR-01		
					The organization establishes roles, responsibilities, and authorities related to its cybersecurity risk management and communicates them within the organization.	CPS.GV.RR-02		
					The organization incorporates security-related matters (e.g., revoking access privileges and screening employees) into measures that address role changes resulting from personnel transfers.	CPS.GV.RR-05		
					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.	CPS.GV.PO-01		
					The organization periodically reviews its security policies and updates them as necessary, based on changes in requirements, threats, technology, and the organization's mission.	CPS.GV.PO-02		
					L1_1_b_COM	[Components] - The security status of components that compose information systems and Industrial control systems and the status of network connections are not managed appropriately (e.g. Inventory of assets, monitoring).	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.	CPS.ID.AM-01
							The organization develops and appropriately manages communication network diagrams and data flow diagrams within the organization.	CPS.ID.AM-02
							The organization develops and appropriately manages inventories of external information systems connected to its organizational assets.	CPS.ID.AM-03
							The organization manages systems, hardware, software, services, and data throughout their entire lifecycle, from acquisition to disposal.	CPS.ID.AM-06
							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.	CPS.DE.CM-02
					L1_1_b_SYS	[System] - The organization has not implemented technical measures considering risks, or cannot confirm such implementation.	The organization establishes its risk appetite and risk tolerance, and communicates them across the organization.	CPS.GV.RM-03
							The organization identifies vulnerabilities in its assets and manages them by linking them to the corresponding assets.	CPS.ID.RA-01
			- 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.	CPS.ID.RA-03				
			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.	CPS.ID.RA-04				
			- 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.	CPS.ID.RA-06				
			The organization assesses the risk impact posed by significant organizational changes and security requirement exceptions, and records and manages the results.	CPS.ID.RA-07				
			[System] - Settings in the system where the data to be protected is stored are not secure.	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).		CPS.PR.PS-06		
				The organization prevents the installation and execution of unauthorized software.		CPS.PR.PS-07		
			[System] - Regarding access to stored information, a request sender is not identified / authenticated in a manner suited to the level of confidentiality of such information.	The organization establishes and implements procedures to issue, manage, verify, revoke, and audit identities and credentials for authorized components, people, and procedures.		CPS.PR.AA-01		
				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).		CPS.PR.AA-02		
				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.		CPS.PR.AA-03		
				The organization protects, transmits, receives, and verifies information regarding authenticated entities (ID assertions).		CPS.PR.AA-04		
			[System] - The system does not have a mechanism to quickly detect and respond to anomalies on the network (eg, spoofing, message tampering)	The organization monitors networks and network services to properly detect security events.		CPS.DE.CM-01		
				The organization monitors communications with external service providers to properly detect security events.		CPS.DE.CM-03		
				The organization verifies the integrity and authenticity of information received from cyberspace prior to operation.		CPS.DE.CM-07		

#	Function	Assumed security incident	Risk sources			Measure Requirement	Measure Requirement ID
			Threat	Vulnerability ID	Vulnerability		
				L1_1_b_PRO	[Procedure] - Appropriate procedures for security risk management have not been established.	The organization defines risk management objectives and agrees on them with relevant stakeholders.	CPS.GV.RM-01
						The organization develops a cybersecurity strategy to ensure effective cybersecurity risk management.	CPS.GV.RM-02
						The organization establishes its risk appetite and risk tolerance, and communicates them across the organization.	CPS.GV.RM-03
						The organization formulates policies regarding risk response options and their operations, and shares them within the organization.	CPS.GV.RM-05
						The organization standardizes methodologies for assessing, documenting, classifying, and prioritizing cybersecurity risks, and shares them within the organization.	CPS.GV.RM-07
						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.	CPS.GV.PO-01
						The organization periodically reviews its security policies and updates them as necessary, based on changes in requirements, threats, technology, and the organization's mission.	CPS.GV.PO-02
						The organization establishes supply chain risk management programs, strategies, objectives, policies, and processes, and operates them upon agreement with organizational stakeholders.	CPS.GV.SC-01
						The organization establishes cybersecurity roles and responsibilities for suppliers and partners, communicates them internally and externally, and coordinates adjustments as necessary.	CPS.GV.SC-02
						The organization integrates cybersecurity supply chain risk management into its cybersecurity and enterprise risk management, risk assessment, and improvement processes.	CPS.GV.SC-03
						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.	CPS.GV.SC-05
						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.	CPS.GV.SC-09
						The organization establishes and implements procedures to be followed upon the termination of contracts with partners and other parties.	CPS.GV.SC-11
				L1_1_b_DAT	[Data] - Data are not protected enough in communication paths.	The organization protects the confidentiality, integrity, and availability of data-in-transit.	CPS.PR.DS-03
					[Data] - Data being handled have no mechanism to detect falsification.	The organization protects the confidentiality, integrity, and availability of data-at-rest.	CPS.PR.DS-02
						The organization protects the confidentiality, integrity, and availability of data-in-transit.	CPS.PR.DS-03
						The organization protects the confidentiality, integrity, and availability of data-in-use.	CPS.PR.DS-04
						The organization maintains, updates, and manages data provenance, including data sources and processing history, throughout the entire lifecycle.	CPS.PR.DS-05
						The organization verifies the integrity and authenticity of information received from cyberspace prior to operation.	CPS.DE.CM-07
		The system dealing with the data of its own organization stops due to a denial of service attack, ransomware infection etc..	- DoS attacks on computer equipment and communication devices (e.g., servers) that comprise a system - Malware infection exploiting security vulnerabilities in the system - Transmission of jamming waves	L1_1_c_ORG	[Organization] - Security risks are not managed in accordance with appropriate procedures, and other organizations needed are not involved in risk management.	The organization understands its mission and uses it to inform cybersecurity risk management decisions.	CPS.GV.OC-01
						The organization identifies strategic opportunities (positive risks for the organization), clarifies their characteristics, and integrates them into organizational cybersecurity risk deliberations.	CPS.GV.RM-08
						The organization establishes supply chain risk management programs, strategies, objectives, policies, and processes, and operates them upon agreement with organizational stakeholders.	CPS.GV.SC-01
						The organization establishes cybersecurity roles and responsibilities for suppliers and partners, communicates them internally and externally, and coordinates adjustments as necessary.	CPS.GV.SC-02
						The organization integrates cybersecurity supply chain risk management into its cybersecurity and enterprise risk management, risk assessment, and improvement processes.	CPS.GV.SC-03
						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.	CPS.GV.SC-04
						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.	CPS.GV.SC-05
						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.	CPS.GV.SC-06
						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.	CPS.GV.SC-10
				L1_1_c_PEO	[People] - People are not fully aware of the security or safety risks that may concern them.	The organization establishes roles, responsibilities, and authorities related to its cybersecurity risk management and communicates them within the organization.	CPS.GV.RR-02
						The organization continuously improves security training and education programs for its personnel and designated contacts at critical partner organizations.	CPS.ID.IM-03
						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.	CPS.PR.AT-01

#	Function	Assumed security incident	Risk sources			Measure Requirement	Measure Requirement ID	
			Threat	Vulnerability ID	Vulnerability			
					[People] - The security or safety risks that involve people are not managed adequately.	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.	CPS.GV.OC-02	
					Organizational senior management is responsible and accountable for cybersecurity risk, fostering a culture that is risk-aware, ethical, and continually improving.	CPS.GV.RR-01		
					The organization establishes roles, responsibilities, and authorities related to its cybersecurity risk management and communicates them within the organization.	CPS.GV.RR-02		
					The organization incorporates security-related matters (e.g., revoking access privileges and screening employees) into measures that address role changes resulting from personnel transfers.	CPS.GV.RR-05		
					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.	CPS.GV.PO-01		
					The organization periodically reviews its security policies and updates them as necessary, based on changes in requirements, threats, technology, and the organization's mission.	CPS.GV.PO-02		
					L1_1_c_COM	[Components] - The security status of components that compose information systems and Industrial control systems and the status of network connections are not managed appropriately (e.g. Inventory of assets, monitoring).	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.	CPS.ID.AM-01
					The organization develops and appropriately manages communication network diagrams and data flow diagrams within the organization.	CPS.ID.AM-02		
					The organization develops and appropriately manages inventories of external information systems connected to its organizational assets.	CPS.ID.AM-03		
					The organization manages systems, hardware, software, services, and data throughout their entire lifecycle, from acquisition to disposal.	CPS.ID.AM-06		
					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.	CPS.DE.CM-02		
					L1_1_c_SYS	[System] - The organization has not implemented technical measures considering risks, or cannot confirm such implementation.	The organization establishes its risk appetite and risk tolerance, and communicates them across the organization.	CPS.GV.RM-03
			The organization identifies vulnerabilities in its assets and manages them by linking them to the corresponding assets.	CPS.ID.RA-01				
			- 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.	CPS.ID.RA-03				
			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.	CPS.ID.RA-04				
			- 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.	CPS.ID.RA-06				
			The organization assesses the risk impact posed by significant organizational changes and security requirement exceptions, and records and manages the results.	CPS.ID.RA-07				
			[System] - Communications to IoT devices, servers, etc. are not properly controlled.	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).	CPS.PR.AA-02			
			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.	CPS.PR.AA-03				
			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).	CPS.PR.PS-06				
			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).	CPS.PR.IR-01				
			[System] - The system does not cope with physical interference (e.g. jamming waves) to IoT devices and servers.	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.	CPS.PR.AA-07			
			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 uninterrupted power supplies, fire protection equipment, and flood protection measures.	CPS.PR.IR-02				
			[System] - A system that contains IoT devices does not have adequate resources (i.e., processing capacity, communication bandwidths, and storage capacity)	The organization implements mechanisms to achieve requirements for the continuous operation of systems and services under normal and adverse conditions.	CPS.PR.IR-03			
			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.	CPS.PR.IR-04				

#	Function	Assumed security incident	Risk sources			Measure Requirement	Measure Requirement ID
			Threat	Vulnerability ID	Vulnerability		
				L1_1_c_PRO	[Procedure] - Appropriate procedures for security risk management have not been established.	The organization defines risk management objectives and agrees on them with relevant stakeholders.	CPS.GV.RM-01
						The organization develops a cybersecurity strategy to ensure effective cybersecurity risk management.	CPS.GV.RM-02
						The organization establishes its risk appetite and risk tolerance, and communicates them across the organization.	CPS.GV.RM-03
						The organization formulates policies regarding risk response options and their operations, and shares them within the organization.	CPS.GV.RM-05
						The organization standardizes methodologies for assessing, documenting, classifying, and prioritizing cybersecurity risks, and shares them within the organization.	CPS.GV.RM-07
						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.	CPS.GV.PO-01
						The organization periodically reviews its security policies and updates them as necessary, based on changes in requirements, threats, technology, and the organization's mission.	CPS.GV.PO-02
						The organization establishes supply chain risk management programs, strategies, objectives, policies, and processes, and operates them upon agreement with organizational stakeholders.	CPS.GV.SC-01
						The organization establishes cybersecurity roles and responsibilities for suppliers and partners, communicates them internally and externally, and coordinates adjustments as necessary.	CPS.GV.SC-02
						The organization integrates cybersecurity supply chain risk management into its cybersecurity and enterprise risk management, risk assessment, and improvement processes.	CPS.GV.SC-03
						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.	CPS.GV.SC-05
						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.	CPS.GV.SC-09
						The organization establishes and implements procedures to be followed upon the termination of contracts with partners and other parties.	CPS.GV.SC-11
		Security measures that satisfy the legal requirements for a system cannot be implemented	All threats	L1_2_a_ORG	[Organization] - The organization is unaware of legal systems with which it should comply, or it has not developed, or is not operating internal rules that conform to the legal systems.	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.	CPS.GV.OC-02
				L1_2_a_PEO	[People] - People are unaware of legal systems with which it should comply, or they do not follow internal rules that conform to the legal systems.	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.	CPS.PR.AT-01
				L1_2_a_COM	[Components] - The type of components that must receive certain protection under a legal system is not provided with the required level of protection.	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.	CPS.GV.OC-02
						The organization utilizes products that implement appropriate security measures to ensure the trustworthiness of sensing data by preserving measurement availability and integrity.	CPS.PR.PS-03
				L1_2_a_SYS	[System] - The type of system that must receive certain protection under a legal system is not provided with the required level of protection.	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.	CPS.GV.OC-02
				L1_2_a_PRO	[Procedure] - Established internal procedures are not designed to ensure compliance with laws and regulations.	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.	CPS.GV.OC-02
				L1_2_a_DAT	[Data] - The type of data that must receive certain protection under a legal system is not provided with the required level of protection.	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.	CPS.GV.OC-02
						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.	CPS.PR.DS-01
1_2	Continuing the business of the organization appropriately even when a security incident occurs.	The organization's security incidents prevent their business from continuing properly	All threats	L1_3_a_ORG	[Organization] - The organization has not established a framework for accurately detecting security incidents.	The organization establishes roles, responsibilities, and authorities related to its cybersecurity risk management and communicates them within the organization.	CPS.GV.RR-02
						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.	CPS.GV.RR-03
						The organization allocates necessary resources commensurate with its cybersecurity strategy, roles, responsibilities, and policies.	CPS.GV.RR-04
						The organization applies lessons learned from the analysis of detected events such as alerts and logs, to continuously improve security event detection processes.	CPS.ID.IM-05
				[Organization] - The organization has not established a framework for accurately handling security incidents.		The organization establishes roles, responsibilities, and authorities related to its cybersecurity risk management and communicates them within the organization.	CPS.GV.RR-02
						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.	CPS.GV.RR-03
						The organization allocates necessary resources commensurate with its cybersecurity strategy, roles, responsibilities, and policies.	CPS.GV.RR-04
						The organization incorporates lessons learned from responses to security incidents to continuously improve its incident response plan.	CPS.ID.IM-06

#	Function	Assumed security incident	Risk sources			Measure Requirement	Measure Requirement ID
			Threat	Vulnerability ID	Vulnerability		
				L1_3_a_PEO	[People] - People are unable to take appropriate action when a security incident arises.	The organization incorporates lessons learned from responses to security incidents to continuously improve its incident response plan.	CPS.ID.IM-06
						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.	CPS.PR.AT-01
						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.	CPS.PR.AT-02
						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.	CPS.RS.MA-01
						The organization verifies that events reported as security incidents are not false positives or duplicate reports, and validates their legitimacy as incidents.	CPS.RS.MA-02
						The organization classifies and prioritizes detected security incidents based on the severity of impact, entry route, and other factors.	CPS.RS.MA-03
						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.	CPS.RS.MA-06
						The organization develops and implements rules governing internal communication and external disclosure after the occurrence of a security incident.	CPS.RS.CO-01
						Based on established rules, the organization escalates incidents to executive decision-makers within the organization and relevant external entities as necessary.	CPS.RS.CO-02
						The organization minimizes the spread of damage from security incidents, eradicating causes or mitigating adverse impacts.	CPS.RS.MI-01
			L1_3_a_COM		[Components] - The scope of the organization's business (e.g., products) damaged by a security incident cannot be identified.	The organization establishes identification methods to ensure traceability according to the importance of the components it produces within the supply chain.	CPS.ID.AM-07
						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.	CPS.ID.AM-08
						The organization identifies the impact of security events, including the adverse effects on relevant external organizations.	CPS.DE.AE-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.	CPS.RS.AN-03
			L1_3_a_SYS		[System] - Devices or other tools for accurately detecting security incidents are not installed or not correctly operated.	The organization applies lessons learned from the analysis of detected events such as alerts and logs, to continuously improve security event detection processes.	CPS.ID.IM-05
						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.	CPS.PR.PS-11
						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.	CPS.DE.CM-08
						As part of its monitoring operations, the organization periodically tests and validates whether functions detecting security events operate as intended.	CPS.DE.CM-09
			L1_3_a_PRO		[Procedure] - The organization has not developed internal procedures for security incident handling.	The organization incorporates lessons learned from responses to security incidents to continuously improve its incident response plan.	CPS.ID.IM-06
						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.	CPS.RS.MA-01
						The organization develops and implements rules governing internal communication and external disclosure after the occurrence of a security incident.	CPS.RS.CO-01
					[Procedure] - Security incidents are not treated in the business continuity plan. This means a highly hazardous security incident hinders the organization's business continuity when it occurs.	The organization incorporates lessons learned from responses to security incidents to continuously improve its business continuity plan or emergency response plan.	CPS.ID.IM-07
						The organization incorporates security incidents into its business continuity plan or emergency response plan, which defines response policies and procedures for natural disasters.	CPS.RC.RP-01
						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.	CPS.RC.CO-02
						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.	CPS.RC.CO-03
			L1_3_a_DAT		[Data] - Data necessary to continue the business at the time of the security incident has not been properly backed up, or has been backed up but does not function properly.	The organization performs routine backups of data (e.g., component configurations and operational data), protects backup data, and tests restoration capabilities.	CPS.PR.DS-06
						The organization verifies the integrity of backups and other recovery assets prior to use.	CPS.RC.RP-04

#	Function	Assumed security incident	Risk sources			Measure Requirement	Measure Requirement ID
			Threat	Vulnerability ID	Vulnerability		
		Other relevant organizations cannot continue their business properly due to the organization's security incidents	All threats	L1_3_b_ORG	[Organization] - The organization is unclear about how its components, systems, and/or data have been working with other organizations in cyberspace.	The organization develops and appropriately manages communication network diagrams and data flow diagrams within the organization.	CPS.ID.AM-02
						The organization develops and appropriately manages inventories of external information systems connected to its organizational assets.	CPS.ID.AM-03
					[Organization] - The organization is unclear about how it has been working with other organizations (e.g., suppliers) in physical space.	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.	CPS.GV.OC-03
						The organization establishes cybersecurity roles and responsibilities for suppliers and partners, communicates them internally and externally, and coordinates adjustments as necessary.	CPS.GV.SC-02
						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.	CPS.GV.SC-04
						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.	CPS.GV.SC-05
				L1_3_b_PEO	[People] - People in other organizations are unable to take appropriate action when the organization has a security incident.	The organization establishes cybersecurity roles and responsibilities for suppliers and partners, communicates them internally and externally, and coordinates adjustments as necessary.	CPS.GV.SC-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.	CPS.PR.AT-02
						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.	CPS.RS.MA-04
				L1_3_b_COM	[Components] - A security incident causes damage to components (products) and/or services.	The organization takes appropriate actions for components (products) suspected of having quality defects, such as those produced using equipment damaged during a security incident.	CPS.RS.MA-05
						The organization establishes identification methods to ensure traceability according to the importance of the components it produces within the supply chain.	CPS.ID.AM-07
					[Components] - The organization does not retain the records of components (products) (e.g., dates of manufacture, identification numbers, and delivery destinations) delivered to/from the organization.	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.	CPS.ID.AM-08
				L1_3_b_PRO	[Procedure] - Procedures for security incident handling in cooperation with other relevant organizations have not been developed.	The organization establishes cybersecurity roles and responsibilities for suppliers and partners, communicates them internally and externally, and coordinates adjustments as necessary.	CPS.GV.SC-02
						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.	CPS.RS.MA-01
		The organization's security incidents prevent the business of other relevant organizations from continuing properly	All threats	L1_3_c_ORG	[Organization] - The organization is unclear about how its components, systems, and/or data have been working with other organizations in cyberspace.	The organization develops and appropriately manages communication network diagrams and data flow diagrams within the organization.	CPS.ID.AM-02
						The organization develops and appropriately manages inventories of external information systems connected to its organizational assets.	CPS.ID.AM-03
					[Organization] - The organization is unclear about how it has been working with other organizations (e.g., suppliers) in physical space.	The organization establishes cybersecurity roles and responsibilities for suppliers and partners, communicates them internally and externally, and coordinates adjustments as necessary.	CPS.GV.SC-02
						The organization incorporates lessons learned from responses to security incidents to continuously improve its incident response plan.	CPS.ID.IM-06
						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.	CPS.PR.AT-02
						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.	CPS.RS.MA-04
				L1_3_c_PEO	[People] - People in the organizations are unable to take appropriate action when other organizations have a security incident.	The organization establishes roles, responsibilities, and authorities related to its cybersecurity risk management and communicates them within the organization.	CPS.GV.RR-02
						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.	CPS.PR.AT-01
						The organization continuously improves security training and education programs for its personnel and designated contacts at critical partner organizations.	CPS.ID.IM-03
				L1_3_c_PRO	[Procedure] - Procedures for security incident handling in cooperation with other relevant organizations have not been developed.	The organization establishes cybersecurity roles and responsibilities for suppliers and partners, communicates them internally and externally, and coordinates adjustments as necessary.	CPS.GV.SC-02
						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.	CPS.RS.MA-01

#	Function	Assumed security incident	Risk sources			Measure Requirement	Measure Requirement ID
			Threat	Vulnerability ID	Vulnerability		
1_3	Products or services in physical space are received or shipped with desired quality	A security event occurs in the channel for product / service provisioning, causing unintended quality deterioration such as malfunction of a device.	- Fraudulent falsification by internal or external people with malicious intent - Insertion of a counterfeit that imitates a genuine equipment	L1_1_d_ORG	[Organization] - The organization does not confirm the trustworthiness of products and services at the time of procurement.	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.	CPS.GV.SC-07
						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.	CPS.GV.SC-08
				L1_1_d_PEO	[People] - The organization's staff in charge of procurement are not fully aware of security risks related to procurement.	The organization continuously improves security training and education programs for its personnel and designated contacts at critical partner organizations.	CPS.ID.IM-03
						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.	CPS.PR.AT-01
				L1_1_d_COM	[Components] - Physical protection measures are not sufficiently applied to procured products and services.	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.	CPS.GV.SC-07
						When procuring devices that process sensitive information or have[TN122.1] important functions for its organization, the organization utilizes tamper-resistant devices.	CPS.PR.PS-02
				L1_1_d_PRO	[Procedure] - There is no procedure for confirming the qualification of procured goods at the time of procurement of products and services.	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.	CPS.GV.SC-05
						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.	CPS.GV.SC-06
						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.	CPS.GV.SC-07

■Functions/Assumed Security Incidents/Risk Sources/Measure Requirements in the Second Layer

#	Function	Assumed security incident	Risk sources		Measure Requirement	Measure Requirement ID	
			Threat	Vulnerability ID			
2_Comm on	Both of the following functions; - Function to read events in physical space and translating them into digital data and sending the data to cyberspace in accordance with certain rules - Function to control components and displaying visualized data based on data received from cyberspace in accordance with certain rules	Unexpected behavior of the IoT device due to unauthorized access to its controls by exploiting a vulnerability results in unpredicted operation	- Malware infection using an attack tool that takes advantage of an IoT device's vulnerability	L2_1_a_ORG	[Organization] - The organization is unclear about the status of the security measures (e.g., software configurations; the status of patches applied) for its IoT devices connecting to information systems and industrial control systems.	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.	CPS.ID.AM-01
						The organization identifies vulnerabilities in its assets and manages them by linking them to the corresponding assets.	CPS.ID.RA-01
						- 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.	CPS.ID.RA-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).	CPS.PR.PS-06
						The organization applies security-critical updates for IoT devices, servers, and related assets in a timely manner using managed tools while appropriately recording history.	CPS.PR.PS-09
						The organization periodically scans its IoT devices, servers, and related assets to identify vulnerabilities requiring remediation.	CPS.DE.CM-06
	</						

#	Function	Assumed security incident	Risk sources			Measure Requirement	Measure Requirement ID
			Threat	Vulnerability ID	Vulnerability		
		Unexpected behavior of the IoT device due to unauthorized access to its controls by impersonation of an authorized user results in unpredicted operation	- Identity spoofing using a stolen ID of a proper host - Unauthorized access that exploits vulnerable protocols with no security means	L2_1_b_ORG	[Procedure] - The response procedure after detecting malfunction of the IoT device is not defined.	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.	CPS.RS.MA-01
					[Organization] - The organization has no mechanism for regularly checking proper use of its network.	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.	CPS.PR.PS-11
						The organization monitors networks and network services to properly detect security events.	CPS.DE.CM-01
						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.	CPS.DE.CM-02
						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.	CPS.DE.CM-04
				L2_1_b_COM	[Components] - Some settings are not robust enough in terms of security (e.g., passwords, ports).	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).	CPS.PR.PS-06
				L2_1_b_SYS	[System] - Access control of communication partners is not robust enough.	The organization establishes and implements procedures to issue, manage, verify, revoke, and audit identities and credentials for authorized components, people, and procedures.	CPS.PR.AA-01
						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).	CPS.PR.AA-02
						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.	CPS.PR.AA-03
						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.	CPS.PR.AA-05
						The organization periodically reviews granted access privileges and remediates unnecessary or excessive permissions.	CPS.PR.AA-06
				L2_1_b_PRO	[Procedure] - No procedure for security settings of an IoT device is established.	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).	CPS.PR.PS-06
					[Procedure] - The response procedure after detecting malfunction of the IoT device is not defined.	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.	CPS.RS.MA-01
		Unauthorized input to the IoT device due to unauthorized access to the system that remotely manages the IoT devices results in unpredicted operation	- Malware infection that takes advantage of a system's vulnerability - Identity spoofing using a stolen ID/password of a proper user - Unauthorized command from system managing IoT device to IoT device	L2_1_c_ORG	[Organization] - The organization is unclear about the status of the security measures (e.g., software configurations; the status of patches applied) for its system that manages IoT devices.	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.	CPS.ID.AM-01
						The organization identifies vulnerabilities in its assets and manages them by linking them to the corresponding assets.	CPS.ID.RA-01
						- 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.	CPS.ID.RA-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).	CPS.PR.PS-06
						The organization applies security-critical updates for IoT devices, servers, and related assets in a timely manner using managed tools while appropriately recording history.	CPS.PR.PS-09
						The organization periodically scans its IoT devices, servers, and related assets to identify vulnerabilities requiring remediation.	CPS.DE.CM-06

#	Function	Assumed security incident	Risk sources		Measure Requirement	Measure Requirement ID				
			Threat	Vulnerability ID	Vulnerability					
				L2_1_c_SYS	[System] - Access control regarding system administration authority is not robust enough.	The organization establishes and implements procedures to issue, manage, verify, revoke, and audit identities and credentials for authorized components, people, and procedures.	CPS.PR.AA-01			
						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).	CPS.PR.AA-02			
						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.	CPS.PR.AA-05			
						The organization periodically reviews granted access privileges and remediates unnecessary or excessive permissions.	CPS.PR.AA-06			
					[System] - Access control regarding system administration authority is not robust enough.	The organization develops a vulnerability remediation plan and remediates component vulnerabilities in accordance with the plan.	CPS.PR.PS-08			
						The organization applies security-critical updates for IoT devices, servers, and related assets in a timely manner using managed tools while appropriately recording history.	CPS.PR.PS-09			
						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.	CPS.PR.PS-10			
					[Procedure] - The response procedure after detecting malfunction of the IoT device is not defined.	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.	CPS.RS.MA-01			
					Functions of IoT devices and communication devices stop due to attacks such as denial-of-service (DoS) attack	- DoS attacks on IoT and communication devices that comprise an IoT system	L2_1_d_SYS	[System] - A system that contains IoT devices does not have adequate resources (i.e., processing capacity, communication bandwidths, and storage capacity)	The organization implements mechanisms to achieve requirements for the continuous operation of systems and services under normal and adverse conditions.	CPS.PR.IR-03
									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.	CPS.PR.IR-04
									[Procedure] - The response procedure after detecting the stopping of the IoT device is not defined.	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.
2_1	Function to control components and displaying visualized data based on data received from cyberspace in accordance with certain rules	Behavior that threatens safety, regardless of the behavior being normal or abnormal	- Command injection by an unauthorized entity - Unacceptable input data from cyberspace - Tampering control signal by malware	L2_2_a_ORG	[Organization] - The organization does not check whether the devices have proper levels of safety functions at the time of procurement.	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.	CPS.GV.SC-05			
						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.	CPS.GV.SC-07			
						The organization utilizes products that implement appropriate security measures to ensure the trustworthiness of sensing data by preserving measurement availability and integrity.	CPS.PR.PS-03			
						The organization deploys IoT devices that implement security safeguards designed for network connectivity.	CPS.PR.PS-04			
				L2_2_a_COM	[Components] - There is no mechanism for verifying data that has been input.	The organization verifies the integrity and authenticity of information received from cyberspace prior to operation.	CPS.DE.CM-07			
						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.	CPS.DE.CM-08			
				L2_2_a_SYS	[System] - Safety instrument is not considered in the system being operated.	- 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.	CPS.ID.RA-03			
						- 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.	CPS.ID.RA-06			
						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.	CPS.DE.CM-08			
				L2_2_a_PRO	[Procedure] - The organization has no established courses of action to take when any of its devices shows a sign of compromising safety.	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.	CPS.RS.MA-01			

#	Function	Assumed security incident	Risk sources		Measure Requirement	Measure Requirement ID		
			Threat	Vulnerability				
2_2	Function to read events in physical space and translating them into digital data and sending the data to cyberspace in accordance with certain rules	Data is tampered with in the communication path between the IoT device and cyberspace	- Man-in-the-middle attack that tamper with data on communication channel.	L2_3_a_ORG	[Organization] - The organization does not check whether the devices have functions to detect and prevent tampering at the time of procurement.	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.	CPS.GV.SC-07	
					When procuring devices that process sensitive information or have[TN122.1] important functions for its organization, the organization utilizes tamper-resistant devices.	CPS.PR.PS-02		
					The organization utilizes products that implement appropriate security measures to ensure the trustworthiness of sensing data by preserving measurement availability and integrity.	CPS.PR.PS-03		
	An unauthorized or tampered-with IoT device connects to the network and transmits incorrect data	- A stolen and illegally modified IoT device connected to a network - Tampering by internal or external people with malicious intent - Tampering with sensor readings, thresholds, and settings	L2_3_b_ORG	[Organization] - The organization is unclear about the status of devices connected to its information system or industrial control system.	The organization evaluates the authenticity and integrity of hardware and software prior to acquisition and deployment, and verifies their integrity during operation.	CPS.PR.PS-01		
					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).	CPS.PR.PS-06		
					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.	CPS.DE.CM-02		
			L2_3_b_PEO	[People] - Physical unauthorized acts to IoT devices by internal or external people can not be prevented.	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.	CPS.PR.AA-07		
					When procuring devices that process sensitive information or have[TN122.1] important functions for its organization, the organization utilizes tamper-resistant devices.	CPS.PR.PS-02		
					The organization implements appropriate physical access settings, logging, and monitoring, commensurate with the criticality of IoT devices, servers, and related assets.	CPS.DE.CM-05		
			L2_3_b_COM	[Components] - The devices used are not anti-tampering, which make it impossible to prevent physical falsification.	When procuring devices that process sensitive information or have[TN122.1] important functions for its organization, the organization utilizes tamper-resistant devices.	CPS.PR.PS-02		
			L2_3_b_SYS	[System] - The organization does not regularly verify the integrity of connected devices.	The organization evaluates the authenticity and integrity of hardware and software prior to acquisition and deployment, and verifies their integrity during operation.	CPS.PR.PS-01		
					The organization monitors networks and network services to properly detect security events.	CPS.DE.CM-01		
				[System] - It is not properly detected that an unauthorized device is connected to the network of the organization.	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.	CPS.DE.CM-02		
					[System] - The organization does not take physical security measures such as access control and monitoring of areas where its IoT devices are installed,	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.	CPS.PR.AA-07	
				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.		CPS.PR.IR-02		
				The organization implements appropriate physical access settings, logging, and monitoring, commensurate with the criticality of IoT devices, servers, and related assets.		CPS.DE.CM-05		
				L2_3_b_DAT	[Data] - The organization has no procedures for deleting data (or making data unreadable) in an IoT device before disposal.	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).	CPS.PR.PS-12	
			An IoT device with low quality is connected to a network, causing failures, transmission of inaccurate data or transmission to unauthorized entity .	- An IoT device with low quality connected to a network - Insertion of a counterfeit that imitates a genuine equipment	L2_3_c_ORG	[Organization] - The organization does not check whether the products are trustworthy at the time of procurement of IoT devices.	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.	CPS.GV.SC-06
							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.	CPS.GV.SC-07
	The organization evaluates the authenticity and integrity of hardware and software prior to acquisition and deployment, and verifies their integrity during operation.	CPS.PR.PS-01						
	[Organization] - The organization does not make certain that the IoT devices and their software are official products (i.e., not falsified).	The organization evaluates the authenticity and integrity of hardware and software prior to acquisition and deployment, and verifies their integrity during operation.				CPS.PR.PS-01		

#	Function	Assumed security incident	Risk sources		Measure Requirement	Measure Requirement ID	
				L2_3_c_SYS	[System] - Network communications (wired or wireless) from unauthorized devices can not be prevented.	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).	CPS.PR.AA-02
						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).	CPS.PR.PS-06
					[System] - The system cannot properly detect and block unauthorized outbound communication from the organization.	The organization monitors networks and network services to properly detect security events.	CPS.DE.CM-01
						The organization monitors communications with external service providers to properly detect security events.	CPS.DE.CM-03
						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.	CPS.DE.CM-04
					[System] - The organization has implemented no mechanism for checking whether the devices to be connected to cyberspace and other official devices are official products.	The organization establishes and implements procedures to issue, manage, verify, revoke, and audit identities and credentials for authorized components, people, and procedures.	CPS.PR.AA-01
						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).	CPS.PR.AA-02
				L2_3_c_PRO	[Procedure] - There is no procedure for checking whether the procured products are reliable at the time of procurement of IoT devices.	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.	CPS.GV.SC-05
						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.	CPS.GV.SC-06
						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.	CPS.GV.SC-07
						The organization evaluates the authenticity and integrity of hardware and software prior to acquisition and deployment, and verifies their integrity during operation.	CPS.PR.PS-01
		Inappropriate measurement occurs due to physical interference with measurement .	Inappropriate acts against transcription function by people with malicious intent	L2_3_d_ORG	[Organization] - The organization does not check whether the products are trustworthy in the measurement security at the time of procurement of IoT devices.	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.	CPS.GV.SC-07
						The organization utilizes products that implement appropriate security measures to ensure the trustworthiness of sensing data by preserving measurement availability and integrity.	CPS.PR.PS-03
					L2_3_d_SYS	[System] - The organization does not take physical security measures such as access control and monitoring of areas where its IoT devices are installed.	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.
						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.	CPS.PR.IR-02
						The organization implements appropriate physical access settings, logging, and monitoring, commensurate with the criticality of IoT devices, servers, and related assets.	CPS.DE.CM-05

■ Functions/Assumed Security Incidents/Risk Sources/Measure Requirements in the Third Layer

#	Function	Assumed security incident	Risk sources		Measure Requirement	Measure Requirement ID							
			Threat	Vulnerability									
3_Comm on	All of the following functions; - Functions to securely send and receive data - Functions to securely process and analyze data - Function to securely store data	- Denial-of-Service (DoS) attacks on computer equipment and communication devices (e.g., servers) that comprise a system	- DoS attack on computing devices such as servers, communication devices, etc. - Transmission of jamming waves	L3_3_b_ORG	[Organization] - The organization does not confirm the trustworthiness of contractor organizations such as data providers or data manipulators/analyzers before and after signing contracts.	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.	CPS.GV.SC-06						
						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.	CPS.GV.SC-07						
						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.	CPS.GV.SC-08						
						The system that handles data stops whether it has been attacked or not.	- Services provided by a system with low quality/trustworthiness	L3_3_c_ORG	[Organization] - The organization does not confirm the trustworthiness of service supplier's organizations, systems, etc. before and after signing contracts.	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.	CPS.GV.SC-06		
										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.	CPS.GV.SC-07		
										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.	CPS.GV.SC-08		
										L3_3_c_SYS	[System] - A system that contains IoT devices does not have adequate resources (i.e., processing capacity, communication bandwidths, and storage capacity)	The organization implements mechanisms to achieve requirements for the continuous operation of systems and services under normal and adverse conditions.	CPS.PR.IR-03
												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.	CPS.PR.IR-04
										Laws and rules that prescribe data protection in cyberspace are violated	- Malware infection that takes advantage of a data storage system's vulnerability - Physical intrusion by an unauthorized entity into the data storage area - Identity spoofing using a stolen ID/password of a proper user	L3_4_a_ORG	[Organization] - Responsibility in the organization for managing data to be protected is not identified.
	[Organization] - The organization is not fully aware of data protection laws and regulations with which it should comply.	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.	CPS.GV.OC-02										
		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.	CPS.PR.DS-01										
	L3_4_a_PEO	[People] - People involved are not fully aware of how the organization's protected data should be handled for security reasons.	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.	CPS.PR.AT-01									
			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.	CPS.PR.AT-02									
	L3_4_a_PRO	[Procedure] - Necessary procedures for handling data are not established.	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.	CPS.PR.DS-01									
			[Procedure] - The organization does not confirm whether the necessary procedures are followed regarding data handling.	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.	CPS.DE.CM-04								
		L3_4_a_DAT	[Data] - Personal data or other important information is distributed among multiple organizations or systems.	The organization develops and appropriately manages inventories of data and metadata in its possession.	CPS.ID.AM-05								
	[Data] - The organization is unaware that the data it handles is the specific type of data that must be protected.			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.	CPS.ID.AM-04								
			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.	CPS.PR.DS-01									
	The security requirements for highly confidential data to be shared only among authorized parties has not been set or met.	- Malware infection that takes advantage of a data storage system's vulnerability - Physical intrusion by an unauthorized entity into the data storage area - Internal fraud by an authorized user - Identity spoofing using a stolen ID/password of a proper user	L3_4_b_ORG	[Organization] - The organization is not fully aware of data protection laws and regulations with which it should comply.	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.	CPS.GV.OC-02							
					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.	CPS.PR.DS-01							
					L3_4_b_PEO	[People] - People involved are not fully aware of how the organization's protected data should be handled for security reasons.	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.	CPS.PR.AT-01					
			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.	CPS.PR.AT-02									

#	Function	Assumed security incident	Risk sources		Measure Requirement	Measure Requirement ID					
			Threat	Vulnerability ID							
				L3_4_b_PRO	[Procedure] - Necessary procedures for handling data are not established.	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.	CPS.PR.DS-01				
					[Procedure] - The organization does not confirm whether the necessary procedures are followed regarding data handling.	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.	CPS.PR.DS-01				
				L3_4_b_SYS	[System] - The system is not designed according to the data confidentiality.	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.	CPS.PR.DS-01				
						The organization protects the confidentiality, integrity, and availability of data-at-rest.	CPS.PR.DS-02				
						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.	CPS.PR.PS-05				
				L3_4_b_DAT	[Data] - Personal data or other important information is distributed among multiple organizations or systems.	The organization develops and appropriately manages inventories of data and metadata in its possession.	CPS.ID.AM-05				
						[Data] - The organization is unaware that the data it handles is the specific type of data that must be protected.	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.	CPS.ID.AM-04			
						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.	CPS.PR.DS-01				
				3_1	Functions to securely process and analyze data	The organization's protected data is leaked from a data processing area managed by a related organization.	- Malware infection that takes advantage of the vulnerability of a data manipulation / analysis system managed by another organization - Physical intrusion by an unauthorized entity into the data manipulation / analysis area managed by another organization - Identity spoofing using a stolen ID/password of a proper user - Protected data has been taken out improperly by another organization's entity	L3_1_b_ORG	[Organization] - The organization does not confirm the safety and trustworthiness of data manipulation / analysis organizations and/or systems before and after signing contracts.	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.	CPS.GV.SC-06
										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.	CPS.GV.SC-07
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.	CPS.GV.SC-08										
L3_1_b_PEO	[People] - The organization does not confirm, before and after signing contracts, the trustworthiness of people in organizations that undertake data manipulation / analysis.	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.	CPS.GV.SC-06								
		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.	CPS.GV.SC-08								
		L3_1_b_DAT	[Data] - The organization's data that must be protected is distributed among multiple organizations at different levels of security.					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.	CPS.GV.SC-05		
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.	CPS.ID.AM-04										
The organization develops and appropriately manages inventories of data and metadata in its possession.	CPS.ID.AM-05										
Improper processed/analyzed results become output due to a malfunction in the data processing/analyzing system		- Malware infection that takes advantage of vulnerability of a data manipulation / analysis system - Unacceptable input data containing code to attack a data manipulation / analysis system						L3_3_d_ORG	[Organization] - The organization does not confirm the safety of data manipulation / analysis organizations and/or systems before and after signing contracts.	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.	CPS.GV.SC-06
										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.	CPS.GV.SC-07
				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.	CPS.GV.SC-08						
				L3_3_d_SYS	[System] - Settings in the system that processes and analyzes data are not secure.	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).	CPS.PR.PS-06				
						[System] - Vulnerabilities that should be handled are left unaddressed in a data manipulation / analysis system.	The organization identifies vulnerabilities in its assets and manages them by linking them to the corresponding assets.	CPS.ID.RA-01			
						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).	CPS.ID.RA-02				
						The organization develops a vulnerability remediation plan and remediates component vulnerabilities in accordance with the plan.	CPS.PR.PS-08				
						The organization applies security-critical updates for IoT devices, servers, and related assets in a timely manner using managed tools while appropriately recording history.	CPS.PR.PS-09				
						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.	CPS.PR.PS-10				
						The organization periodically scans its IoT devices, servers, and related assets to identify vulnerabilities requiring remediation.	CPS.DE.CM-06				

#	Function	Assumed security incident	Risk sources			Measure Requirement	Measure Requirement ID
			Threat	Vulnerability ID	Vulnerability		
					[System] - Data are not protected enough in a system.	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.	CPS.PR.DS-01
					The organization protects the confidentiality, integrity, and availability of data-at-rest.	CPS.PR.DS-02	
					The organization protects the confidentiality, integrity, and availability of data-in-transit.	CPS.PR.DS-03	
					The organization protects the confidentiality, integrity, and availability of data-in-use.	CPS.PR.DS-04	
					The organization performs routine backups of data (e.g., component configurations and operational data), protects backup data, and tests restoration capabilities.	CPS.PR.DS-06	
					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.	CPS.RS.AN-01	
					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.	CPS.RS.AN-02	
					[System] The system does not fully check data that serves as input.	The organization verifies the integrity and authenticity of information received from cyberspace prior to operation.	CPS.DE.CM-07
					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.	CPS.DE.CM-08	
					[System] - The system has no mechanism for detecting and handling any abnormality related to security as soon as it arises.	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.	CPS.PR.PS-11
					The organization monitors networks and network services to properly detect security events.	CPS.DE.CM-01	
					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.	CPS.DE.CM-02	
					The organization monitors communications with external service providers to properly detect security events.	CPS.DE.CM-03	
					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.	CPS.DE.CM-04	
					The organization analyzes potential security events to understand their details.	CPS.DE.AE-01	
3_2	Function to securely store data	A related organization's protected data is leaked from a data storage area managed by the organization.	- Malware infection that takes advantage of the vulnerability of a data storage system managed by another organization - Physical intrusion by an unauthorized entity into the data storage area managed by another organization - Identity spoofing using a stolen ID/password of a proper user - Protected data has been taken out improperly by a malicious entity of the organization	L3_1_a_ORG	[Organization] - Responsibility in the organization for managing data to be protected is not identified.	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.	CPS.ID.AM-04
				L3_1_a_SYS	[System] - Settings in the system storing data to be protected of relevant parties are not secure.	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).	CPS.PR.PS-06
					[System] - Vulnerabilities that should be handled is left unaddressed in the organization's system.	The organization identifies vulnerabilities in its assets and manages them by linking them to the corresponding assets.	CPS.ID.RA-01
						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).	CPS.ID.RA-02
						The organization develops a vulnerability remediation plan and remediates component vulnerabilities in accordance with the plan.	CPS.PR.PS-08
						The organization applies security-critical updates for IoT devices, servers, and related assets in a timely manner using managed tools while appropriately recording history.	CPS.PR.PS-09
						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.	CPS.PR.PS-10
						The organization periodically scans its IoT devices, servers, and related assets to identify vulnerabilities requiring remediation.	CPS.DE.CM-06
					[System] Regarding access to stored information, a request sender is not identified / authenticated in a manner suited to the level of confidentiality of such information.	The organization establishes and implements procedures to issue, manage, verify, revoke, and audit identities and credentials for authorized components, people, and procedures.	CPS.PR.AA-01
						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).	CPS.PR.AA-02
					[System] - The organization does not take physical security measures such as access control and monitoring of areas where its IoT devices and servers are installed.	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.	CPS.PR.AA-07
						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).	CPS.PR.PS-06
						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.	CPS.PR.IR-02

#	Function	Assumed security incident	Risk sources			Measure Requirement	Measure Requirement ID	
			Threat	Vulnerability ID	Vulnerability			
					[System] - The system has no mechanism for detecting and handling any abnormality related to security as soon as it arises.	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.	CPS.PR.PS-11	
					The organization monitors networks and network services to properly detect security events.	CPS.DE.CM-01		
					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.	CPS.DE.CM-02		
					The organization monitors communications with external service providers to properly detect security events.	CPS.DE.CM-03		
					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.	CPS.DE.CM-04		
					The organization analyzes potential security events to understand their details.	CPS.DE.AE-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.	CPS.RS.MA-01		
					The organization minimizes the spread of damage from security incidents, eradicating causes or mitigating adverse impacts.	CPS.RS.MI-01		
				L3_1_a_PRO	[Procedure] - There is no procedure for confirming levels of confidentiality and necessary security measures regarding data whose management is outsourced from other organizations.	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.	CPS.GV.SC-05	
						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.	CPS.PR.DS-01	
				L3_1_a_DAT	[Data] - Classification concerning protection of data commissioned by relevant parties is not identified.	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.	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.	CPS.PR.DS-01	
					[Data] - Data protection at a predefined level of confidentiality is not implemented.	The organization protects the confidentiality, integrity, and availability of data-at-rest.	CPS.PR.DS-02	
						The organization protects the confidentiality, integrity, and availability of data-in-transit.	CPS.PR.DS-03	
						The organization protects the confidentiality, integrity, and availability of data-in-use.	CPS.PR.DS-04	
						The organization performs routine backups of data (e.g., component configurations and operational data), protects backup data, and tests restoration capabilities.	CPS.PR.DS-06	
						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.	CPS.RS.AN-01	
						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.	CPS.RS.AN-02	
		The organization's protected data is leaked from a data storage area managed by a related organization.		- Malware infection that takes advantage of the vulnerability of a data storage system managed by another organization - Physical intrusion by an unauthorized entity into the data storage area managed by another organization - Identity spoofing using a stolen ID/password of a proper user - Protected data has been taken out improperly by a malicious entity of the organization	L3_1_c_ORG	[Organization] - The organization does not confirm the safeness of data storage organizations and/or systems before and after signing contracts.	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.	CPS.GV.SC-06
							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.	CPS.GV.SC-07
							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.	CPS.GV.SC-08
					L3_1_c_PEO	[People] - The organization does not confirm, before and after signing contracts, the trustworthiness of people in organizations that undertake data manipulation.	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.	CPS.GV.SC-06
							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.	CPS.GV.SC-08
					L3_1_c_DAT	[Data] - The organization's data that must be protected is distributed among multiple organizations at different levels of security.	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.	CPS.GV.SC-05
							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.	CPS.ID.AM-04
							The organization develops and appropriately manages inventories of data and metadata in its possession.	CPS.ID.AM-05

#	Function	Assumed security incident	Risk sources		Measure Requirement	Measure Requirement ID	
			Threat	Vulnerability ID			
		Data in storage is tampered with	- Identity spoofing using a stolen ID/password of a proper user	L3_2_a_DAT	[Data] - Data being stored do not have a mechanism to detect falsifications.	The organization protects the confidentiality, integrity, and availability of data-at-rest.	CPS.PR.DS-02
						The organization maintains, updates, and manages data provenance, including data sources and processing history, throughout the entire lifecycle.	CPS.PR.DS-05
3_3	Functions to securely send and receive data	Data in use is tampered with.	- Identity spoofing using a stolen ID/password of a proper user - Man-in-the-middle attacks to falsify data on communication paths	L3_2_b_DAT	[Data] - Data are not protected enough in communication paths.	The organization protects the confidentiality, integrity, and availability of data-in-transit.	CPS.PR.DS-03
					[Data] - Data being used do not have a mechanism to detect falsifications.	The organization protects the confidentiality, integrity, and availability of data-in-use.	CPS.PR.DS-04
		The system receives inappropriate data from an Organization/People/Component s (due to a spoofing attack etc.).	- Identity spoofing by an unauthorized organization/person/component/system to use an ID of a proper entity - Inappropriate data from authorized components and system that have been tampered with	L3_3_a_ORG	[Organization] - The organization does not confirm the trustworthiness of the data sender organizations such as data providers or data manipulators/analyzers before and after signing the contracts.	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.	CPS.GV.SC-06
						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.	CPS.GV.SC-07
						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.	CPS.GV.SC-08
				L3_3_a_PEO	[People] - A contractor's employees responsible for the outsourced work are not fully aware of how the organization's protected data should be handled for security reasons.	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.	CPS.PR.AT-02
				L3_3_a_SYS	[System] - Vulnerabilities that should be handled is left unaddressed in a data collection / analysis system.	The organization identifies vulnerabilities in its assets and manages them by linking them to the corresponding assets.	CPS.ID.RA-01
						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).	CPS.ID.RA-02
						The organization develops a vulnerability remediation plan and remediates component vulnerabilities in accordance with the plan.	CPS.PR.PS-08
						The organization applies security-critical updates for IoT devices, servers, and related assets in a timely manner using managed tools while appropriately recording history.	CPS.PR.PS-09
						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.	CPS.PR.PS-10
						The organization periodically scans its IoT devices, servers, and related assets to identify vulnerabilities requiring remediation.	CPS.DE.CM-06
						The organization protects the confidentiality, integrity, and availability of data-in-transit.	CPS.PR.DS-03
						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).	CPS.PR.IR-01
						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.	CPS.PR.PS-11
						The organization monitors networks and network services to properly detect security events.	CPS.DE.CM-01
						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.	CPS.DE.CM-02
						The organization monitors communications with external service providers to properly detect security events.	CPS.DE.CM-03
						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.	CPS.DE.CM-04
						The organization analyzes potential security events to understand their details.	CPS.DE.AE-01
						The organization minimizes the spread of damage from security incidents, eradicating causes or mitigating adverse impacts.	CPS.RS.MI-01
				L3_3_a_DAT	[Data] - No mechanism for filtering data sent from the other endpoint of communication is installed or operated.	The organization establishes and implements procedures to issue, manage, verify, revoke, and audit identities and credentials for authorized components, people, and procedures.	CPS.PR.AA-01
						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).	CPS.PR.AA-02
						The organization verifies the integrity and authenticity of information received from cyberspace prior to operation.	CPS.DE.CM-07
						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.	CPS.DE.CM-08