RRI Questionniare (Ver.1.0)

NIST CSF		Countermeasure ID	RRI requirements	Evidence example	Maturity Level		
					1 Partial. documented.	2 Use risk information (approved or operated by the organization's security officer).	3 A mechanism that can be applied repeatedly has been built, and PDCA is being executed.
Identify	AM-1	CPS.AM-1 (Asset Management)	Document and manage appropriately the list of hardware and software, and management information (e.g. name of asset, version, network address, name of asset manager, license information) of components in the system in the organization.	Name, version, network address, person responsible for management, license information, usage, scope of use, and system account owner of the equipment and software comprising the system. Installation and security status of the equipment. Disposal methods, information necessary for recovery in the event of malfunctions including failures, dependencies of other systems, list of assets including network configuration diagrams and their approval, and revision approval history.	The securiy officer of the organization identifies and makes lists of assets.	The organization's Chief information security officer has approved the list of identified assets. The organization manages and implements the approved documents.	The organization's security officers and Chief information security officer regularly review, update, and maintain the asset list.
	GV-1 GV-2	CPS.GV-1 (Governance)	Develop and announce security policies, define roles and responsibilities for security across the organization and other relevant parties (Suppliers) .	History of security policy development and approval, and approval of revisions to the security policy. Describe the security roles and responsibilities of the organization and other relevant organizations (e.g., contractors), and any arrangements for security with contractors in the security policy.	The security officer of the organization has developed (documented) a security policy.	The organization's Chief information security officer has approved and implemented the security policy. The organization manages and implements the approved documents.	The organization's security officers and Chief information security officer regularly review, update, and maintain security policies.
	RA-1	CPS.RA-1 (Risk Assessment)	Analyze the vulnerability of the organization's assets and document the result.	Documents that identify vulnerabilities of major assets listed.	The security officer of the organization has identified and documented the vulnerabilities of some identified assets.	The organization's Chief information security officer has approved documentation that identifies all vulnerabilities of the identified assets. The organization manages and implements the approved documentation.	The organization's security officers and Chief information security officers regularly review, update, and maintain documentation that identifies all vulnerabilities of identified assets.
	RM-1	CPS.RM-1 (Risk Management Strategy)	Establish and manage the cyber security risk management process by appropriate relevant parties within the organization.	Cyber security risk management plan (including implemetation records, the result reports of implementation and approval flows).	The secuirty officer of the organization documents the cyber security risk management plan and records of implementation status for its own organization and subcontractors.	The organization's Chief information security officer has approved the documentation of the cyber security risk management plan and implementation status records of the organization and its subcontractors. The organization manages and implements the approved documentation.	The organization's security officers and Chief information security officers regularly review, update, and maintain documentation of cyber security risk management plans and records of implementation status for their own organization and contractors.

	SC-1	CPS.SC-1 (Supply Chan Risk Management)	Establish and manage the supply chain risk management process by appropriate relevant parties within the organizationin.	Contracts with Suppliers (security must be considered in the contract.)	The security officer of the organization has documented standards for security-related measures that take into account the lifecycle of the business relationship.	The organization's Chief information security officer has documented and agrees with business partners on the criteria for security-related measures that take into account the lifecycle of the business relationship.	The organization's security officers and Chief information security officer regularly review, update, and maintain standards for security measures that take into account the lifecycle of the business relationship. Changes are agreed upon with existing business partners.
Protect	AC-1	CPS.AC-1 (Identify Management & Access Control)	Issue, manage, validate, revoke, and audit Identification (ID) and authentication information (credential) for authorized devices, people, and processes executed.	Identification (ID) and authentication information (credential) issuance, management, verification, revocation, and audit records for authorized devices, people, and processes executed.	The organization (security officer) has documented the list of IDs and certificates of authorized devices/equipment, users, and processes, as well as their issuance, management, verification, revocation, and audit records.	The organization's Chief information security officer has approved the list of IDs and certificates for authorized devices and equipment, users, and processes, as well as their issuance, management, verification, cancellation, and audit records. The organization manages and implements the approved documentation.	The organization's security officers and Chief information security officer regularly review, update, and maintain a list of IDs and certificates for authorized devices and equipment, users, and processes, as well as issuance, management, verification, cancellation, and audit records.
	AT-1 AT-2	CPS.AT-1 (Awareness &Training)	Provide appropriate training and education to all individuals in the organization so that they can understand assigned roles and responsibilities to prevent from or respond to security incidents.	A list of roles and responsibilities regarding cyber security for all relevant personnel of the organization (executives, employees, temporary employees, and contractor employees). Training and education plans and implementation records for all relevant personnel.	・The security officer of the organization has documented a list of roles and responsibilities for cybersecurity of all parties involved in the organization. ・The organization's security officer has documented the plans and implementation records of training and education for all relevant personnel.	・The organization's chief security officer has approveed a list of roles and responsibilities for cybersecurity for all parties in the organization. The organization manages and implements the approved documentation. ・The organization's security officer has approved training and education plans and implementation records for all relevant personnel. The organization manages and implements the approved documentation.	・The organization's security officers and Chief information security officer regularly review, update, and maintain a list of roles and responsibilities for cybersecurity for all relevant personnel in the organization. ・The organization's security officers and Chief information security officer regularly review, update, and maintain training and education plans and implementation records for all relevant personnel.
	DS-1	CPS.DS-1 (Data Security)	Agree in advance on security requirements for protection of information,if the organization exchanges protected information with other organizations.	NDA between organizations; a document that defines the information to be protected ;information exchange methods and its implementation.;Access control methods and its mplemention.	The security offier of organizations has NDAs when exchanging information that needs to be protected between organizations.	The organization's chief security officer has documented and systematized the definitions of the information to be protected, the means of information exchange and its implementation, and the access control methods.	The organization's security officers and chief security officer regularly review, update, and maintain definitions of information to be protected, information exchange methods and their implementation, and access control methods.

	IP-1	CPS.IP-1 (Information Protection Process & Procedures)	Initial configuration of assets and configuration changes to assets are managed based on security principles.	Documentation which describes initial configuration procedures and Configuration change procedures for assets. Security principles need to be defined (e.g. configuraion that achive least priviledge principle)	The security officer of the organization has documented initial configuration procedures and configuration change management process operating procedures.	The organization's chief information security officer implements and operates the initial configuration procedures and configuration change management process operational procedures.	The organization's security officers and chief information security officer regularly review, update, and maintain operational initial configuration procedures and configuration change control process operating procedures.
	IP-11	CPS.IP-9 (Information Protection Process & Procedures)	Include items concerning security in personnel processes such as recruitment and transfer of personnel. Manage the access rights of personnel.	A document which describes procedures for account creation, deletion, and access rights granting and deletion.	The security officer of the organization has documented operational procedures for account creation, deletion, and access rights granting and deletion.	The organization's chief information security officer has approved the operational procedures for account creation, deletion, and access rights granting and deletion. The organization manages and implements the approved documents.	The organization's security officers and chief information security officer regularly review, update, and maintain operational procedures for account creation, deletion, and access rights granting and deletion.
	MA-1	CPS.MA-1 (Maintenance)	Maintenance of system components is performed with approved tools and history is taken.	List of system components requiring maitanace(including security updates) ; implementation plans, procedures, and implementation records for maintenance.	The organization (security officer) has documented the list of assets to be updated, security update implementation plan, procedures, and implementation records.	The organization's chief information security officer has approved the list of assets to be security updated, security update implementation plan, procedures, and implementation records. The organization implement based on the approved plan.	The organization's security officers and chief information security officer regularly review, update, and maintain the list of assets to be security updated, the security update implementation plan, procedures, and implementation records.
	MA-2	CPS.MA-2 (Maintenance)	Maintenance of the components of the delivered system is performed with approved tools and history is taken.	List of system components requiring maitanace(including security updates) ; implementation plans, procedures, and implementation records for maintenance.	The security officer of the organization has documented the list of assets to be updated, security update implementation plan, procedures, and implementation records.	The organization's chief information security officer has approved the list of assets to be security updated, security update implementation plan, procedures, and implementation records. The organization implement based on the approved plan.	The organization's security officer and chief information security officer regularly review, update, and maintain the list of assets to be security updated, the security update implementation plan, procedures, and implementation records.
Detect	AE-1	CPS.AE-1 (Anomalies & Events)	Identify the routine network operation and the flow of information between people and systems during the operation.	Data flow diagrams Documentation of operation specifications and equipment communication specifications.	The security officer of the organization has established and documented procedures to identify and control the flow of information across all devices connected to the organization's network.	The organization's chief information security officer identifies and manage the flow of information for all devices connected to the network in the organization.	The organization's security officer and chief information security officer regularly review, update, and maintain procedures to identify and control the flow of information across all devices connected to the organization's network.
	AE-2	CPS.AE-2 (Anomalies & Events)	Establish a organization to detect, analyze, and respond to security events.	Documentation that shows the security manager (CISO) and security response organization (SOC/CSIRT) structure.	A chief information security officer is appointed in the organization.	A chief information security officer has been appointed within the organization, and a security response organization system has been established.	The organization's security officer and chief information security officer coordinate information with external security response organizations.

	CM-1	CPS.CM-1 (Security Continuous Monitoring)	Monitor internal network and external network connection point.	A list of external connection points to the wide area network, a list of allowed communications at the connection points, and the implementation of a firewall.	The security officer of the organization manage all connection points to the wide area network and the communications passing through them.	The organization's chief information security officer controls and monitors all connection points to the wide area network and the communications passing through them.	The organization's security officer and chief information security officer regularly review, update, and maintain all connection points to the wide area network, the communications passing through them, and the means and content of access control and monitoring.
	DP-4	CPS.DP-1 (Detection Process)	Define the roles and responsibilities of security event detection	Documentation describing the roles and responsibilities for incident detection.	The security officer of the organization has documented roles and responsibilities for incident detection.	The organization's chief information security officer has approved documentation describing roles and responsibilities for incident detection. The organization manages and implements the approved documents.	The organization's security officers and chief information security officer regularly review, update, and maintain documentation describing their roles and responsibilities for incident detection.
Respond/ Recover	RP-1	CPS.RP-1 (Detection Process) (Recovery Planning)	Implement the response to detected incidents according to the established response procedure.	Procedures for response to detected incidents (content and priority of response, scope of response, organization, responsible person, and person in charge for each system for response)	The security officer of the organization has documented procedures for responding to detected incidents .	The organization's chief information security officer has approved the response procedures to detected incidents . The organization manages and implements the approved documentation as a playbook.	The organization's security officers and chief information security officer regularly review, update, and maintain procedures for responding to detected incidents.
ECM developme nt process		IEC 62443-4-1 SM	Include security management requirements in the product development process.	A set of security policy documents describing security controls related to the product development process (requirements definition, design, testing, operation, and disposal), and the approval history of their approval and revision.	The security officer of the organization has a documented security policy that describes security controls related to the product development process (requirements definition, design, testing, operation, and disposal).	The organization's chief information security officer has approved a security policy that describes security controls related to the product development process (requirements definition, design, testing, operation, and disposal). The organization manages and implements the approved documents.	The organization's security officers and chief information security officer review, update, and maintain security policies on a regular basis.

Development environment		IEC 62443-4-1 SM	Manage product development environment according to security requirements.	Documents that manage development environment tools for development and design (e.g., Vidual Studio software development tool, CAD tools, Redmine, related hardware, etc.), configuration management lists, etc.	The security officer of the organization has documented a list of documents and configuration to manage a set of development environment tools in development and design (e.g., software development tool Vidual Studio, CAD tools, Redmine, and related hardware).	The organization's chief information security officer has approved a list of documents and configuration to manage a set of development environment tools in development and design (e.g., Vidual Studio software development tools, CAD tools, Redmine, and related hardware). The organization manages and implements the approved documents.	The organization's security officers and chief information security officer regularly review, update, and maintain documentation of the information security management requirements governing the product environment.
		IEC 62443-4-1 SM	Confirm that the source code and data contents of the product are maintained correctly.	Access control in the configuration management list, reflection to the repository after testing, version control (Git, etc.), change management process, etc.	The organization (security officer) has documented configuration management information about the source code and data content of the product.	The organization's chief information security officer has approved documentation of configuration management information regarding product source code and data content. The organization manages and implements the approved documentation.	The organization's security officers and chief information security officer regularly review, update, and maintain documentation of configuration management information regarding product source code and data content.
Procurement		IEC 62443-2-4 SP.02	Present documentations that ensure the security level of the products and services provided.	Inclusion of security-related items in the SLA, and whether security (design, evaluation, configuration, etc.) specifications for the products and services exist at the time of the transaction	The security officer of the organization has documented to assure the security level of procured products and services, explain the security analysis tools and other tools to be used, and explain how to enhance security.	The organization's Chief information security officer has approved documents that assure the security level of procured products and services, describe security analysis tools and other tools to be used, and explain how to enhance security. The organization manages and implements the approved documents.	The organization's security officers and chief information security officer regularly review, update, and maintain documentation that assures the security level of procured products and services, describes the security analysis tools and other tools used, and explains how to enhance security.
		IEC 62443-4-1 SG	Provide manuals to securely set up and make the equipment robust.	A manual or other document that describes how to securely configure and harden the equipment.	The security officer of the organization has documented a manual for secure configuration and robustness of the devices.	The organization's chief information security officer has approved manuals for secure configuration and robustness of equipment. The organization maintains and implements the approved documentation.	The organization's security officer and chief information security officer regularly review, update, and maintain manuals to ensure that equipment is securely configured and robust.

O&M		IEC 62443-4-1 SG	Provide manuals for secure use and disposal of equipment	A manual or other document that describes how to securely use and dispose of the equipment.	The organization (security officer) has documented a manual that contains information on how to seculy use and dispose of equipment.	The organization's chief information security officer has approved a manual that contains information on how to securly use and dispose of equipment. The organization manages and implements the approved documents.	The organization's security officer and chief information security officer regularly review, update, and maintain manuals that contain information on the secure use and disposal of equipment.
Production Equipment		IEC 62443-2-4 SP.01.01, SP.0	Manage construction of production equipment according to security requirements.	When constructing production equipment, a set of documents that define security policies for production equipment elements (systems, components) and the approval history of their approval and revision.	The security officer of the organization has documented a security policy for the elements of production equipment (systems, components), when building production equipment.	The organization's chief information security officer has approved a document that defines the security policy for the elements of production equipment (systems, components), when building production equipment. The organization manages and implements the approved documentation.	The organization's security officer and chief information security officer regularly reviews, updates, and maintains the approved documentation.
		IEC 62443-2-1	Manage operation of production equipment according to security requirements.	When operating production equipment, a set of documents that define security policies for production facility elements (systems, components) and the approval history of their approval and revision.	The security officer of the organization has documented a security policy for the elements of production equipment (systems, components), when operating production equipment.	The organization's chief information security officer has approved a document that defines the security policy for the elements of production equipment (systems, components), when operating production equipment. The organization manages and implements the approved documentation.	The organization's security officer and chief information security officer regularly reviews, updates, and maintains the approved documentation.