Overview of the RRI Questionnaire

【What is the RRI Questionnaire?】

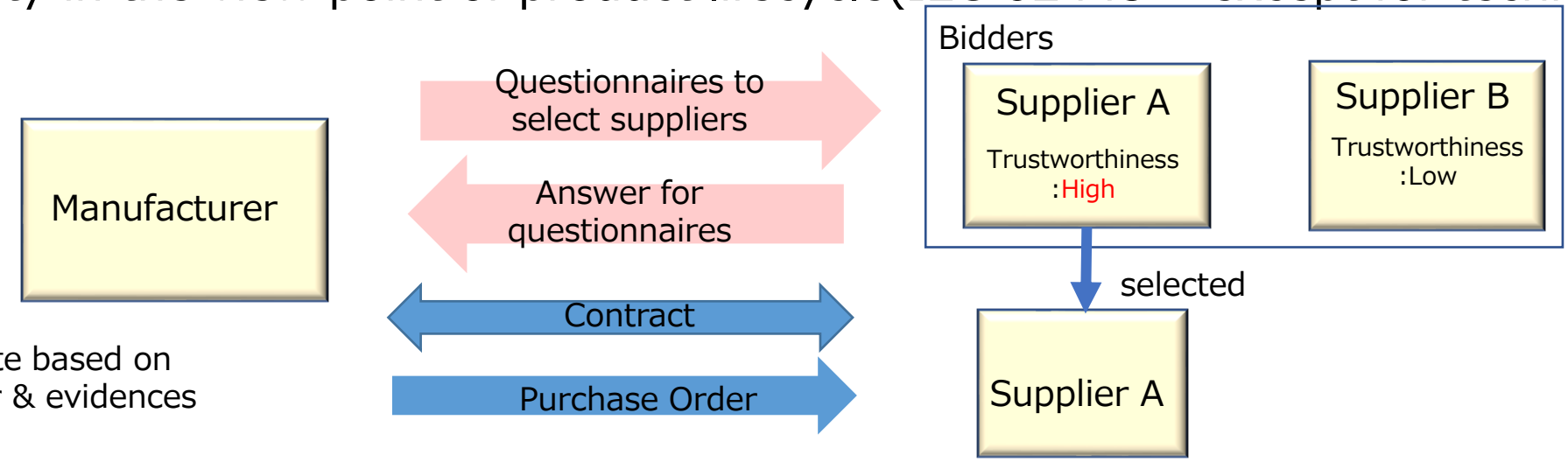
- A simple assessment of the level of security (Trustworthiness) that buyers, regardless of size or industry, expect from suppliers during procurement by answering 25 questions.
- Self-assess the status of security measures taken and measure the maturity level of the current security status of the organization prior to contracting. (Questions were developed based on METI CPSF and IEC624432-1,2-4,4-1)
- Buyers can compare the security status of suppliers' organizations before signing a contract.

Scope & Use case ~Security questionnaires for suppliers~

- A template for security requirements in the supply chain as baseline to select supplier before contract, being applied across sectors of manufacturing industry.

(Any specific regulation (Electricity, automobile, defense etc.) follows these rules)

- Questioner: Procurement department for manufacturer
- Answerer: Bidder for development department
- The answer for the questionnaires would be useful for the Manufacturer to determine "the supplier's trustworthiness" and "how supplier's in the value chain have the same trustworthiness level"
- Focus on Organization security（METI/CPSF, NIST/CSF,ISMS）and industrial control system security in the view point of product lifecycle(IEC 62443 ＊except for technical requirements)



✓ Evaluate based on answer & evidences

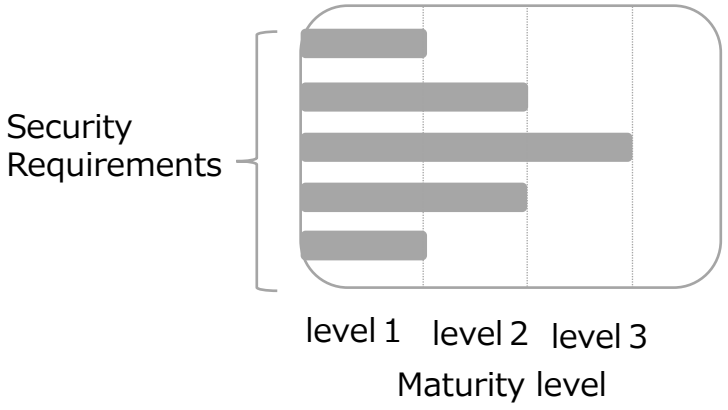
Use case of profile (Answer of questionnaire)

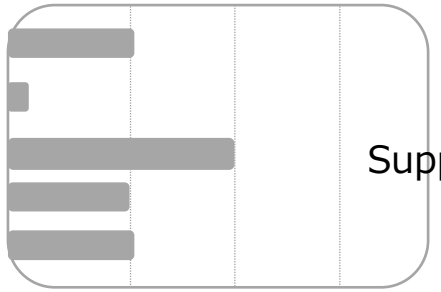
Supplier

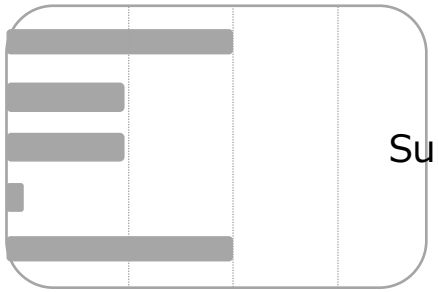
Answer from supplier=Supplier's capability

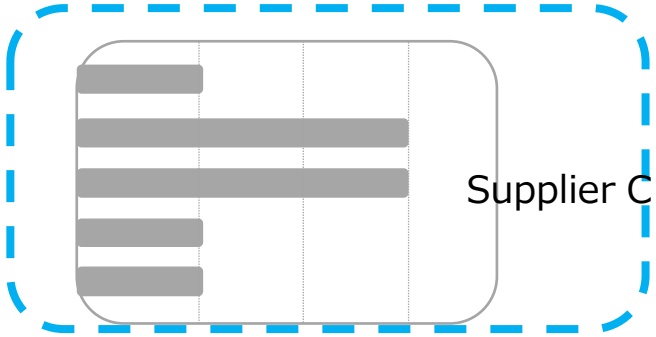
Manufacturer

Expected level for trustworthiness profile
= requirement

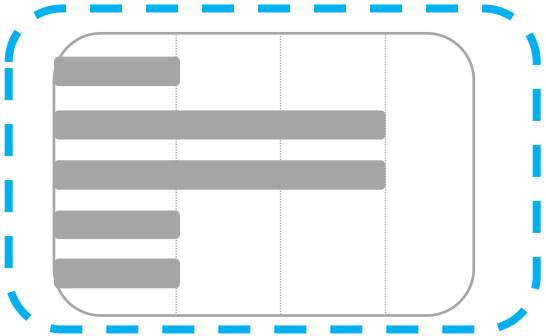








Selected supplier



Supplier C

Maturity level for Trustworthiness

◆ Check maturity level by two axes
①Management – layer process
Processes achieved by high-level management side
(Policies and procedures referred by senior managers)
②Operation-layer process
Security processes achieved by manufacturing and production side
(Policies and procedures referred by personnel in fields)

Partial

Level1

①Management
・Partially implemented by organization level

②Operation
・Documented

Risk Informed

Level2

①Management
・Implemented by organization and got approval by a chief security officer

②Operation
・Documented and developed

Repeatable

Level3

①Management
・Implemented, reviewed and adapted by organization
・Got approval by a chief security officer

②Operation
・Documented, developed
・Reviewed, updated

The contents and the amount of evidences are developed

Risk management process is developed

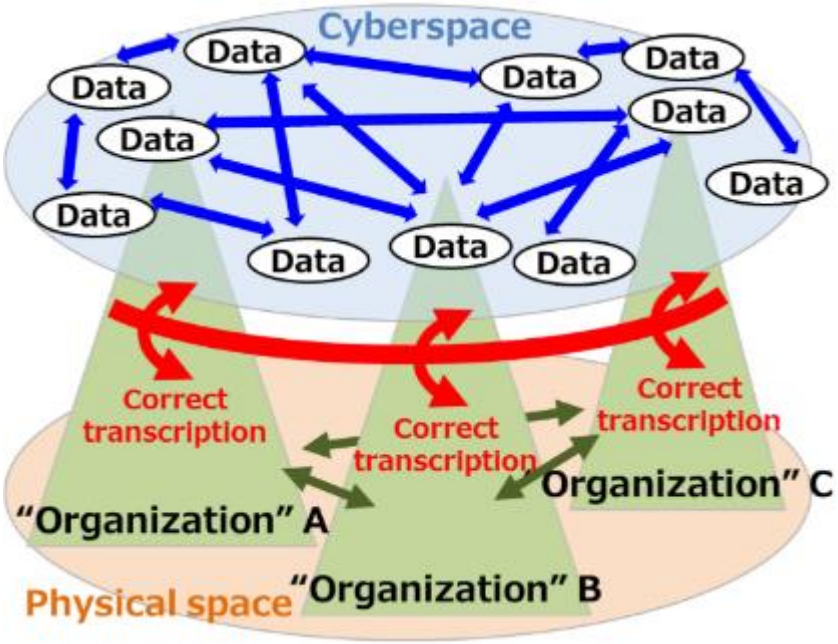
Selected requirements in RRI questionnaire from CPSF

I . Why we had chosen METI CPSF (Cyber Physical Security Framework) as baseline:

- CPSF provides cybersecurity requirements focused on communications between companies and/or organizations categorized as 3 levels,
- The 1st layer ,The 2nd layer, The 3rd layer and six elements (organization, people, component, data, procedure and system).

- CPSF provides informative references of other standards (e.g. NIST CSF and IEC 62443) on each requirement and this information supports our tasks.

- CPSF is enterprise-wide security framework and security requirements are described for each entity in a company.



The Cyber/Physical Security Framework (CPSF)
https://www.meti.go.jp/english/press/2019/pdf/0418_001a.pdf

The 1st layer (Connections between organizations in physical space)
The 2nd layer (Mutual connections between cyberspace and physical space)
The 3rd layer (Connections in cyberspace)

Selected requirements in RRI questionnaire from CPSF

II. How we had prioritized requirements and selected 17 requirements is:

- Security requirements that we have already achieved in our companies.
- Security requirements that we require for product/system suppliers at least.
- Security controls in operation, management processes and organization.

(Technical security controls are out of scope because they depend on products)

- High(Policy)-level security requirements in the security risk management process.

RRI質問票の要求事項（CPSFから選定）

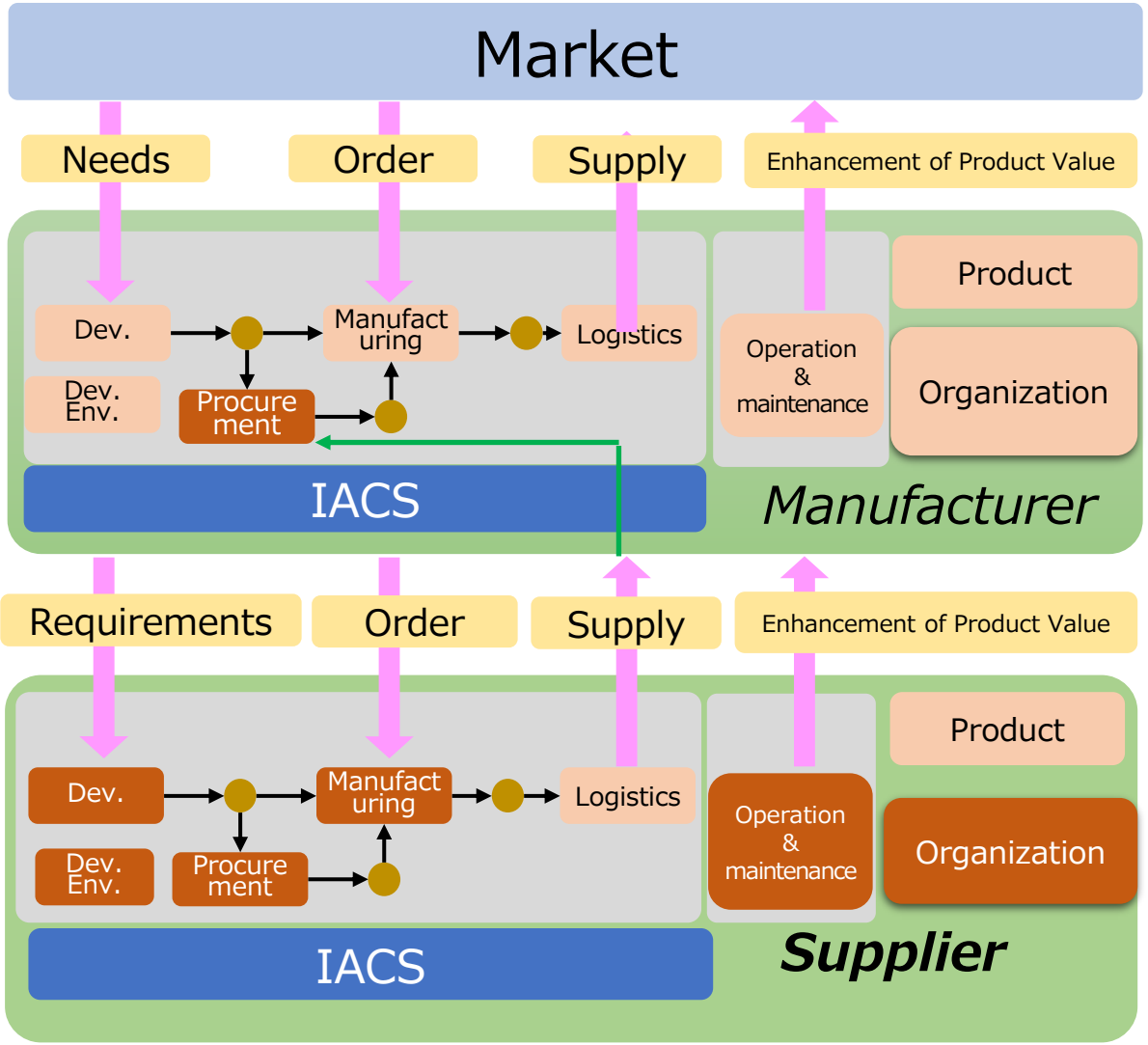
The total number of requirements in CPSF are 104

*CPSF:Cyber/Physical Security Framework (CPSF)
https://www.meti.go.jp/english/press/2019/0418_001.html

METI/CPSF		NIST/CSF	
Category name	Acronym	Related category of NIST Cybersecurity Framework Ver. 1.1	
Asset Management	CPS.AM	ID.AM (Asset Management)	Identity
Business Environment	CPS.BE	ID.BE (Business Environment)	
Governance	CPS.GV	ID.GV (Governance)	
Risk Assessment	CPS.RA	ID.RA (Risk Assessment)	
Risk Management	CPS.RM	ID.RM (Risk Management Strategy)	
Supply Chain Risk Management	CPS.SC	ID.SC (Supply Chain Risk Management)	
Identity Management,Authentication, and Access Control	CPS.AC	PR.AC (Identity Management and Access Control)	Protect
Awareness and Training	CPS.AT	PR.AT (Awareness and Training)	
Data Security	CPS.DS	PR.DS (Data Security)	
Information Protection Processes and Procedures	CPS.IP	PR.IP (Information Protection Processes and Procedures)	
Maintenance	CPS.MA	PR.MA (Maintenance)	
Protective Technology	CPS.PT	PR.PT (Protective Technology)	
Anomalies and Events	CPS.AE	DE.AE (Anomalies and Events)	Detect
Security Continuous Monitoring	CPS.CM	DE.CM (Security Continuous Monitoring)	
Detection Processes	CPS.DP	DE.DP (Detection Processes)	
Response Planning	CPS.RP	RS.RP (Response Planning) RC.RP (Recovery Planning)	Respond/ Recovery
Communications	CPS.CO	RS.CO (Communications) RC.CO (Communications)	
Analysis	CPS.AN	RS.AN (Analysis)	
Mitigation	CPS.MI	RS.MI (Mitigation)	
Improvements	CPS.IM	RS.IM (Improvements) RC.IM (Improvements)	

4 domains
17 items

Additional requirements



*IACS(Industrial Automation and Control System)
*Dev.(Development)
*Env.(Environment)

Selected category for questionnaire

I . We added additional requirements

-development,
-development environment,
-procurement,
-Operation & maintenance(O&M)
-Production equipment

from the view point of product life cycle.
e.g.) IEC 62443 2-1,2-4,4-1

Additional requirements

II. How we had selected additional requirements is

-already implemented by us

-appropriate to request the requirements to suppliers

-not technical but managing/operational

-not too specific but moderately general

Additional requirements

ECM development process	IEC 62443-4-1 SM	Include security management requirements in the product development process.
Development environment	IEC 62443-4-1 SM	Manage product development environment according to security requirements.
	IEC 62443-4-1 SM	Confirm that the source code and data contents of the product are maintained correctly.
Procurement	IEC 62443-2-4 SP.02	Present documentations that ensure the security level of the products and services provided.
O&M	IEC 62443-4-1 SG	Provide manuals to securely set up and make the equipment robust.
	IEC 62443-4-1 SG	Provide manuals for secure use and disposal of equipment.
Production equipment	IEC 62443-2-4 SP.01.01, SP.01.02	Manage construction of production equipment according to security requirements.
	IEC 62443-2-1	Manage operation of production equipment according to security requirements.

◆ ***This requirement is added because it will become important when production facilities are connected to IT networks within the company in the Connected Industry in the near future.***

Questionnaire in-practice- Example

Category			Governance
Security requirement			Develop and announce security policies, define roles and responsibilities for security across the organization and other relevant parties (Suppliers) .
Example : Answer	evidence		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.
	Maturity level	1	The security officer of the organization has developed (documented) a security policy.
			☐Implemented ☐Planned to be implemented ☐Not applicable
		2	The organization's Chief information security officer has approved and implemented the security policy. The organization manages and implements the approved documents.
			☐Implemented ☐Planned to be implemented ☐Not applicable
		3	The organization's security officers and Chief information security officer regularly review, update, and maintain security policies.
			☐Implemented ☐Planned to be implemented ☐Not applicable