METI
Ministry of Economy, Trade and Industry

Reference Material A: List of actions

Main action categories

Legend: O Organizational measures
L Legal measures
T Technical measures

Monitoring	Identify suspicions or early indications of risk occurrence	O Identifying early signs caused by laws/regulations (e.g., policy consideration) O Identifying early signs caused by the private enterprise (e.g., suspicious behavior)
	Identifying whether risk has occurred	O Understanding number of risk occurrences and track record (e.g., number of law enforcement cases/internal occurrences, etc.)
Pre-response	Prevention/ reduction of the probability of risk occurrence	O Guideline development, storage location/service selection, alternative data/operation, etc. L Conclusion of a contract for data sharing and usage T Access restrictions, take-out controls, prevention of unauthorized access
	Reduction of impact when occurring	O Guideline development, ensuring accountability and transparency L Conclusion of a contract for data sharing and usage T Data protection and encryption
Post-response	Protective measures Pursuit of liability	O Assess the impact of risk, initiate initial response L Protective measures and liability enforcement based on contracts or applicable laws
	Prevention of recurrence	O Review of internal operations, business partners, and services used L Review of contracts T Review and identification of issues in technical measures

List of actions/measures: Monitoring 1/2

Legend: O Organizational measures
L Legal measures
T Technical measures

Category 1	Category 2	Subject of action	E.g. of measures
Identify suspicions or early indications of risk occurrence	O Identifying early signs caused by laws/regulations	Own company	(Especially in the legislative phase), grasp the content of the regulation and timing of its enforcement as part of regulation study • Contact the legal department of the head office/local subsidiary • Use/refer to websites of government agencies and think tanks in each country (Ministries, JICA, etc.) • Exchange and gather information within the community (industry associations, etc.) • Participate in study webinars and opinion-gathering events by government and legislative bodies • Consult with experts (law firms, etc.)
			(Especially after enforcement) Check for changes in regulations and future updates • Same as the above
	O Identifying early signs caused by the private enterprise	Own company	Check/monitor for signs of risk within the company • Detect abnormal behavior of PCs/devices, check logs – Access from/to IP addresses/devices not normally used, abnormal network traffic, large file downloads/uploads, log deletions/changes, etc. • Check compliance with information handling policies and employee working conditions – Collection/disposal of materials, restrictions on access/ projection, restrictions on bringing in and using personal USBs and memories, etc. – Frequent entry/exit outside working hours, unusually long overtime hours vs. the workload, etc.
		Business partners/ service providers	Check the security level of business partners/service providers • Check the data handling policy of business partners/service providers – Storage (location, system) , confidentiality, data access rights, scope of disclosure, etc. • Check the status of data protection measures at business partners/service providers (certification, etc.)
			Check for signs of risk at business partners • Request periodic reports from business partners – Status of information storage and data sharing/utilization, disposal reports, etc. – Changes to the policy for handling provided data, and expected impact, etc.

List of actions/measures: Monitoring 2/2

Legend: O Organizational measures
L Legal measures
T Technical measures

Category 1	Category 2	Subject of action	E.g. of measures
Identifying whether risk has occurred	O Understanding number of risk occurrences and track record (law enforcement cases)	Own company	Check for enforcement and track record of relevant laws/regulations • Contact the legal department of the head office/local subsidiary • Exchange and gather information within the community (industry associations, etc.) • Consult with experts (law firms, etc.)
			Check the content of precedents, when a trial is held • Check the court information for each country • Consult with experts (law firms, etc.)
	O Understanding number of risk occurrences and track record (internal occurrences)	Own company	Check the number of incidents in the company • Aggregate and share the number of incidents, including violations of internal data use rules unauthorized accesses and leaks by employees
		Business partners/ service providers	Check the number of incidents in business partners/service providers • Receive reports on violations of contracts, unauthorized use or leakage by employees to confirm the occurrence situation

List of actions/measures: Pre-response[1] 1/3

Legend: Ⓞ Organizational measures
Ⓛ Legal measures
Ⓣ Technical measures

Category 1	Category 2	Subject of action	E.g. of measures
Prevention/ reduction of the probability of risk occurrence	Ⓞ Guideline development	Own company	Define guidelines/policies for data sharing/utilization in the company • Definition/determination of confidential/secret data, scope of access, data handling and disclosure
			Raise internal awareness of international data governance • Disseminate guidelines and policies (company regulations, training, etc.)
	Ⓞ Storage location/service selection	Own company	Identify the location of data storage and where critical data is stored • Confirm internal/external storage location, confidentiality and security level of each critical data
			Review/select data storage locations and recipients/service providers for data with risk concerns • Select storage locations and services with lower risks • Restrict data transfers to specific countries to avoid being subject to government access
			Decentralize critical data and keep it at multiple locations • (If cross-border transfer is not restricted), duplicate and store data in multiple domestic and international locations
	Ⓞ Alternative data/operations	Own company	When the use of specific data is restricted, consider operations without it • Use alternative data • Omit or simplify processes that use specific data in operations
	Ⓞ Compliance and response to regulatory requirements and exceptions	Own company	Check regulatory requirements and determine response as needed • Check requirements (building a local data center, domestic operation system, etc.) • Determine whether to respond based on business benefits and inevitability after considering feasibility in technology, human resources, and cost
			Comply with requirements/conditions for exceptional measures • Check and comply with conditions of exceptional measures (e.g., conditional cross-border transfer restrictions)

[1] For more information on "pre-responses" for data management, such as the guideline development, please refer to the readers and guides in the "Data Spaces Academy" of the Information-technology Promotion Agency (IPA), as supplementary information to the manual https://www.ipa.go.jp/digital/data/data-spaces-academy.html

List of actions/measures: Pre-response 2/3

Legend: Ⓞ Organizational measures
Ⓛ Legal measures
Ⓣ Technical measures

Category 1	Category 2	Subject of action	E.g. of measures
Prevention/ reduction of the probability of risk occurrence	Ⓛ Conclusion of a contract for data sharing and usage	Own company	Conclude confidentiality agreements with employees • Conclude nondisclosure agreements with employees who handle confidential/secret data, or require them to submit a written pledge (upon joining the company, resignation or termination of a contract, or transferring during employment)
		Business partners	Conclude contracts with business partners on data handling and use • Conclude agreements on data handling conditions and authority (confidentiality obligations, scope and purpose of data to be used, audit compliance, handling of derivative data and IP rights, restriction of data scope, etc.) – For details of the items, refer to the model agreement in the “Contract guidelines for the use of AI and data[1]” and “Data collaboration platform rules Ver. 1.0[2]” (METI) • (For mandatory data disclosure), agree as a distributor/manufacturer on the scope of third-party disclosure, rights and conditions of data acquisition and provision, etc., with buyers of equipment • (For data localization), check and consider using Intra Group Data Transfer Agreements (IGDTAs) that incorporate provisions that comply with the cross-border transfer regulations of multiple countries
		Service providers	Conclude contract with service providers on data handling and use • Conclude agreement on data handling conditions and authority (e.g., target data processing, processing methods/restrictions on processors/rights to use processed data, IP rights)
			Confirm/define the terms of use of platform services • Confirm the scope of data use in the PF service (setting and managing the sharing destination for each type of data), obligations/responsibilities of the PF service providers, and obligations/rights of the data recipients

[1] https://www.meti.go.jp/policy/mono_info_service/connected_industries/sharing_and_utilization/20200619002.pdf
[2] https://www.meti.go.jp/policy/mono_info_service/digital_architecture/model_kiyaku.pdf

List of actions/measures: Pre-response 3/3

Legend:	
O	Organizational measures
L	Legal measures
T	Technical measures

Category 1	Category 2	Subject of action	E.g. of measures
Prevention/ reduction of the probability of risk occurrence	T Access restrictions/take-out control	Own company	Set access restrictions and controls for each system • Manage access rights, control network traffic, check, monitor, and notify logs for specific systems and their data
			Grant access rights to user IDs, and identify/authenticate appropriate accessors • Limit employees who can operate a particular system by granting access rights to IDs • Identify and authenticate access persons (passwords, IC cards, etc.)
	T Prevention of unauthorized access	Own company	Detect and block unauthorized access from outside • Install firewalls at the connection points with external networks • Update OS and software on devices and keep them up-to-date • Conduct periodic analysis of logs and other data
Reduction of impact when occurring	O Guideline development	Own company	Organize internal escalation routes and actions in case of incidents • Clarify the contact point in the company when an incident is detected • Define where to contact for details, responsibilities, and actions for each event • Define external stakeholders/accountable parties and how and where to contact them
	O Ensuring accountability and transparency	Own company	Ensure transparency to external stakeholders • Communicate the company's information management system and laws with which it complies
	L Conclusion of a contract for data sharing and usage	Business partners/ service providers	Agree with business partners/service providers on responsibility, response/compensation when risks occur • Agree on stakeholder responsibilities, penalties for violations, dispute resolution methods, access to government, and how to respond to legal requests
	T Data protection and encryption	Own company	Make data unavailable to outsiders through encryption • Indicate the origin of data using digital watermarking technology • Protect data using encryption keys and encryption technology • Anonymize data

List of actions/measures: Post-response 1/2

Legend: O Organizational measures
L Legal measures
T Technical measures

Category 1	Category 2	Subject of action	E.g. of measures
Protective measures Pursuit of liability	O Assess the impact of risk, initiate initial response	Own company	Identify actual risks occurred • Clarify responsible departments based on guidelines and company rules • Analyze data logs and identify data leakage routes • Analyze and identify damages and business impact from risks
			Notify and explain to customers, business partners, and other key stakeholders • Notify and publicize the date/time of risk occurrence as soon as possible • Provide explanations of details of the occurrence and the scope of its impact (customer/shareholder briefings, etc.)
	L Protective measures and liability enforcement based on contracts or applicable laws	Own company	Take internal measures against violations within the company • Take internal measures against violations based on company rules or non-disclosure agreements
			Require safeguards based on laws/regulations • Confirm the rights held in the country/region (safeguards under regulations, IP laws, etc.)Confirm consistency with international rules agreed to by that country (WTO agreements, economic partnership agreements, etc.)
		Business partners/ service providers	Take protective measures and pursue liability against business partners/service providers based on contracts • Notify the breach of the contract • Request recovery measures or claims for compensation based on the contract

List of actions/measures: ⚖ Post-response 2/2

Legend: O Organizational measures
L Legal measures
T Technical measures

Category 1	Category 2	Subject of action	E.g. of measures
Prevention of recurrence	O Review of internal operations, business partners, and services used	Own company	Terminate or change internal operations • Clarify the causes of risks for the target operations • Terminate operations or examine check items and processes for the target operations to avoid risks (e.g., double-check the destination of data)
			Terminate or change the services used • Check for alternative services and compare the cost and quality when switching
			Review the scope and method of data provision to business partners • Review the method and scope of data provision by the company to its business partners
			Request business partners to prevent recurrence • Request business partners to consider measures to prevent recurrence, including security improvement and thorough information management and reporting • Receive reports on progress of recurrence prevention measures
	L Review of contract	Own company	Review company guidelines • Add new clauses to the company guidelines based on risk factors/content
		Business partners/ service providers	Review contracts with business partners and service providers • Review contracts with business partners/service providers based on risk factors, etc.
	T Review and identification of issues in technical measures	Own company	Examine technical measures and review responses • Identify risk factors, and the status of internal systems and data management • Study of appropriate technical measures and review existing measures (access restrictions, control of take-out, prevention of unauthorized access, data protection and encryption)