RCM
RiskChainModel

Risk Assessment & Control Coordination for AI services :
Case04 Defect Detection AI

Institute for Future Initiatives, The University of Tokyo
Technology Governance Research Unit
AI Governance Project

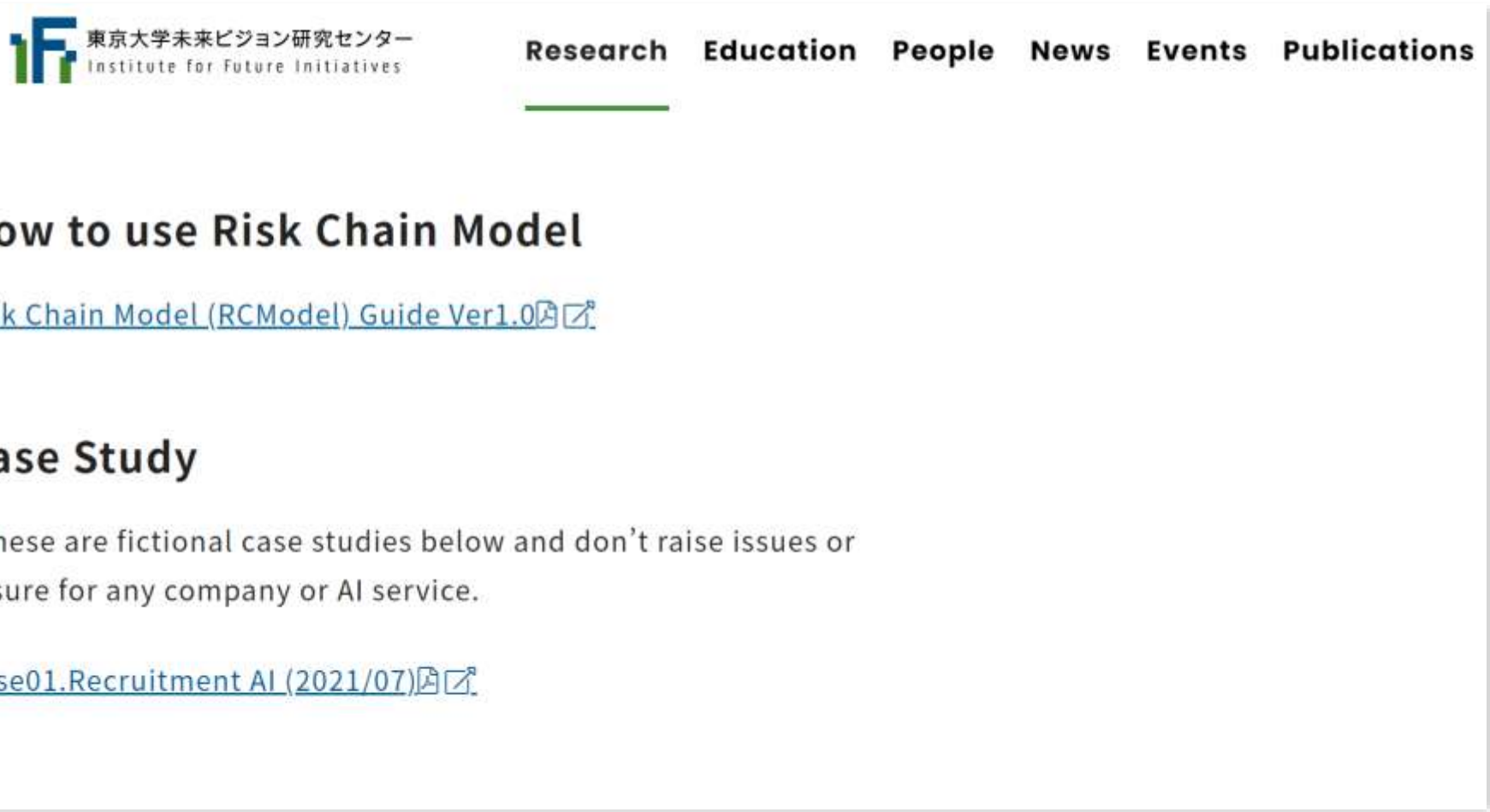
How to operate the RCModel
- Risk Assessment & Control Coordination -

Risk Assessment	Step1	Define the “values and objectives to be achieved” by AI services
	Step2	Examination of significant risk scenarios
Control Coordination	Step3	Examine the risk chain (relation of risk factors) for each important risk scenario
	Step4	Consider risk control according to the risk chain
	Step5	Organize the roles of each stakeholder based on the examination of each risk chain

Guide book and Case Studies of Risk Chain Model

AI Service and Risk Coordination Study Group

https://ifi.u-tokyo.ac.jp/en/projects/ai-service-and-risk-coordination/



RCM
RiskChainModel

Case Study

Case04 : Defect Detection AI

- Define the “values and objectives to be achieved” by AI services -

Step1

This defect detection system uses a generative adversarial network: a deep-learning image generation and identification model. Conventionally, inspection of finished products (industrial parts) is conducted visually; therefore, a large labor cost is required. Therefore, we incorporated the automatic inspection of finished products by applying deep learning to the production line.

This identifies defects on the surface of finished products (industrial parts) produced at the companies’ plant at Co. A. Because the number of defective products identified in the factory is extremely small compared with the total number of finished products that are normally shipped, models that generate images different from finished products and that that correctly identify normal products are utilized. The deep-learning model was developed by Co. B.

[Values & Objectives]

- **Maintaining inspection quality**
- **Increased production volume due to faster inspection**
- **Reduction of labor cost for inspection**
- **Corporate social responsibility**

[Flow of Actual Operations using AI Services]

① The finished product is inspected immediately after production using this model.

② If the model determines that the product is appropriate, the process proceeds to manual inspection to determine the number of samples according to the accuracy rate of the model.

③ If the model determines that the product is defective, a manual inspection is performed, and if there is a problem, the product is discarded. If there is no problem, the product is sent to the packaging process.

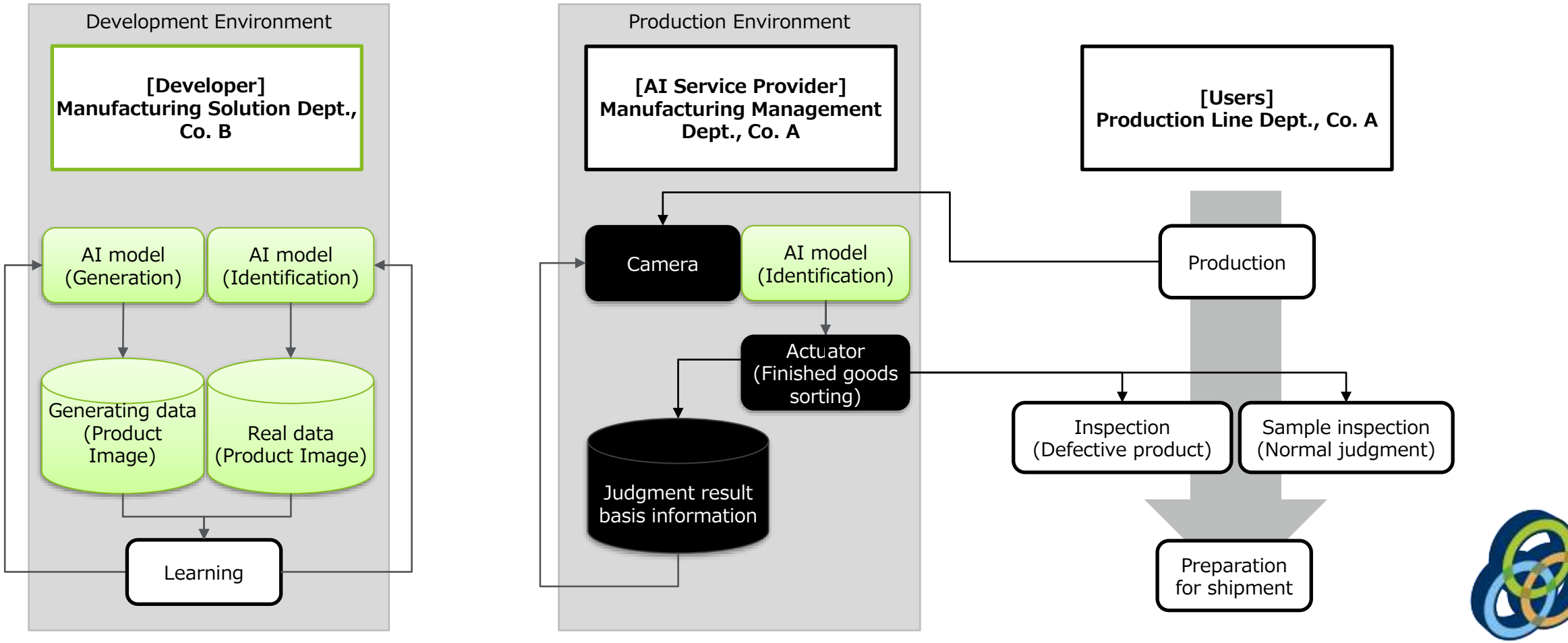
The performance of the model is evaluated using accuracy, precision, and recall. The precision is especially important, and if the precision of the sample inspection is significantly reduced, the model should be relearned.

Model creation and learning are conducted in the learning environment of Co. B. Models are created for each product; however, in the case of minor changes to extant products, older models may be used as a prelearning model. If there is a tendency for the accuracy to deteriorate significantly after operation, although sequential learning is not performed, Co. A will request Co. B perform additional learning and relearning.

Case04 : Defect Detection AI

- System Overview -

AI System	Manufacturing Solution Dept., Co. B	Developing AI System (includes AI model)
AI Service Provider	Manufacturing Management Dept., Co. A	Distribution normal and abnormal products
User	Production Line Dept., Co. A	Sample inspection is performed if AI is judged to be normal, and inspection is performed if AI is judged to be abnormal



Case04 : Defect Detection AI

- Input & Output -

[Input Data]

Data	Purpose	Collection Method	Data Manager	Including Privacy Data
Product data (image)	Learning	Receiving samples of parts from Industry Co. A and photographing image data	Manufacturing Solution Dept., Co. B	None
Product data (image)	Production	In the Manufacturing line, after the production process, photographs are taken and put into the model (automatic).	Manufacturing Management Dept., Co. A (Internal Cloud Environment)	None

[Output]

Users	Person in charge of inspection at the manufacturing line of Co. A
Output	The binary classification of whether the product is normal/abnormal, and the highlight of the focused part of the image (explanatory information)
Output Method	The finished product is classified in the manufacturing line according to the AI judgment result. Images (including explanatory information) of the parts judged to be abnormal can be stored and checked on the monitor in the factory
Expected Accuracy	The accuracy rate, precision, and recall rate are used Accuracy of 99% or more in principle
User judgment	Yes (human inspection process)
Output of evidence information	Highlight areas of interest in the image
Safety Risk	Yes (risk of shipping defective products)
Connection with external system	No
Users	Person in charge of inspection at the manufacturing line of Co. A

RCM
RiskChainModel

Risk Assessment

Risk Assessment

- Examination of significant risk scenarios -

Step2

Values & Objectives		Service Requirement			Risk No.	Risk Scenario	
1	Maintaining of inspection quality	1-1	Precision performance	■ Accuracy ■ Robustness	R001	Unstable performance	Defective products are shipped, or many normal products are judged as defective due to deterioration of AI prediction performance
					R002	Impact by noise	Noise is mixed into the image and the accuracy of AI judgment deteriorates
		1-2	Adopting the changes in environment	■ Robustness ■ IoT	R003	Change in product specifications	Identification accuracy is significantly reduced due to changes in product specifications
					R004	Changes in the IoT	Appropriate judgment cannot be made due to changes in image specifications (e.g., resolution, pixels, and format) due to changes in the imaging device
		1-3	Protection from external attacks	■ Robustness ■ Security	R005	Security protection	Performance cannot be maintained due to abnormal input of learning data or model changes caused by external attacks
2	Increased production volume due to faster inspection	2-1	Inspection speed	■ Performance	R006	Insufficient inspection speed	Inspection speed of AI service is too slow to handle the expected production volume
		2-2	Alternative operation in the event of an error	–	R007	Stopping a process when an error occurs	When an abnormality occurs due to deterioration of AI performance, etc., it is impossible to switch to manual inspection, etc., which interferes with production planning
3	Reduction of labor cost for inspection	3-1	Appropriate detection level	■ Accuracy	R008	Excessive inspection	Excessive inspection results in increased verification costs on the human side and excessive waste
		3-2	Clarity of the evidence for judgment	■ Explainability ■ Easy-to-understand expression	R009	Excessive AI dependence	There is no doubt at all about the judgment of AI, and a lot of defective products are delivered to customers as the sample inspection becomes a mere facade
4	Corporate social responsibility	4-1	Accountability	■ Process description ■ Verifiability	R010	Response to quality audits	Inability to provide appropriate explanations when subjected to quality audits
					R011	Investigation at the time of trouble	When an external explanation is required due to the occurrence of abnormality or trouble, the cause and preventive measures cannot be considered and explained
		4-2	Data protection	■ Data protection	R012	Process anxiety	Leakage of AI inspection results spread false fears about decisions at specific products and factories

Risk Assessment&Control Summary

- Organize the roles of each stakeholder based on the examination of each risk chain -

Step5

Values & Objectives		Risk No.	Risk Scenario	Uncertainly	Environmental change	Caused by user	RC	Control Summary		
								AI System	AI service provider	User
1	Maintaining of inspection quality	R001	Unstable performance	○			●	Ensuring a sufficient accuracy rate Saving usage logs	Verification of prediction performance Relearning	Alternative operation
		R002	Impact by noise	○			●	Camera specification definition Image noise correction Robustness of the model	Maintenance of the shooting environment Relearning	
		R003	Change in product specifications	○	○		●	Ensuring Learning Data performance of the model Securing the execution environment	Model update process Arrangements at the time of specification change Model performance verification	Information linkage for specification changes
		R004	Changes in the IoT	○	○		●	*Same as R002	*Same as R002	*Same as R002
		R005	Security protection					Security management	Investigation and improvement of causes	
2	Increased production volume due to faster inspection	R006	Insufficient inspection speed					Performance maintenance	Performance monitoring	
		R007	Stopping a process when an error occurs	○		○	●	*Same as R008	*Same as R008	*Same as R008
3	Reduction of labor cost for inspection	R008	Excessive inspection	○			●	Output of rationale information Alert upon overdetection	Defining discovery levels Overdetection monitoring Relearning	Relearning decision
		R009	Excessive AI dependence	○		○	●	Output of rationale information Saving log information	Verifying AI errors of judgment Relearning	Sample inspection of normal products Relearning decision
4	Corporate social responsibility	R010	Response to quality audits	○			●	Recording understanding data Record of model performance Saving log information	Organize information to be disclosed Rights management Audit response	
		R011	Investigation at the time of trouble	○				Saving log information	System operation monitoring Fault handling	Manual alternative operation
		R012	Process anxiety					Data protection	Education on professional ethics	Education on professional ethics

Organization

- Organize the roles of each stakeholder based on the examination of each risk chain -

Step5

Co. A) Top Management

- Values and objectives
- Approve risk controls

Co. A) Quality Management Dept.

- Organize information to be disclosed

Co. A) Internal Audit Dept.

- Internal audit
- Response to external audit

- AI Service Provider -
Co. A) Manufacturing Managementl Dept.

Development:
- Camera specification definition
- Model Update Process
- Verifying the updated model

Utilization:
- Image noise correction
- Maintenance of the shooting environment
- Setting and monitoring the detection level
- Verification of prediction performance
- Relearning
- Performance monitoring

Co. B) Manufacturing Solution Dept.

- Sufficient accuracy rate
- Sufficient learning Data
- Model robustness
- Information of evidence for judgment
- Alert function for overdetection

Co. A) IT Dept.

- Recording of usage logs
- Execution environment
- Performance maintenance

- User -
Co. A) Production Line Dept.

- Sample inspection
- Alternative operation
- Linkage of product specification changes
- Relearning decision

Customer of Co. A

RCM
RiskChainModel

Control Coordination

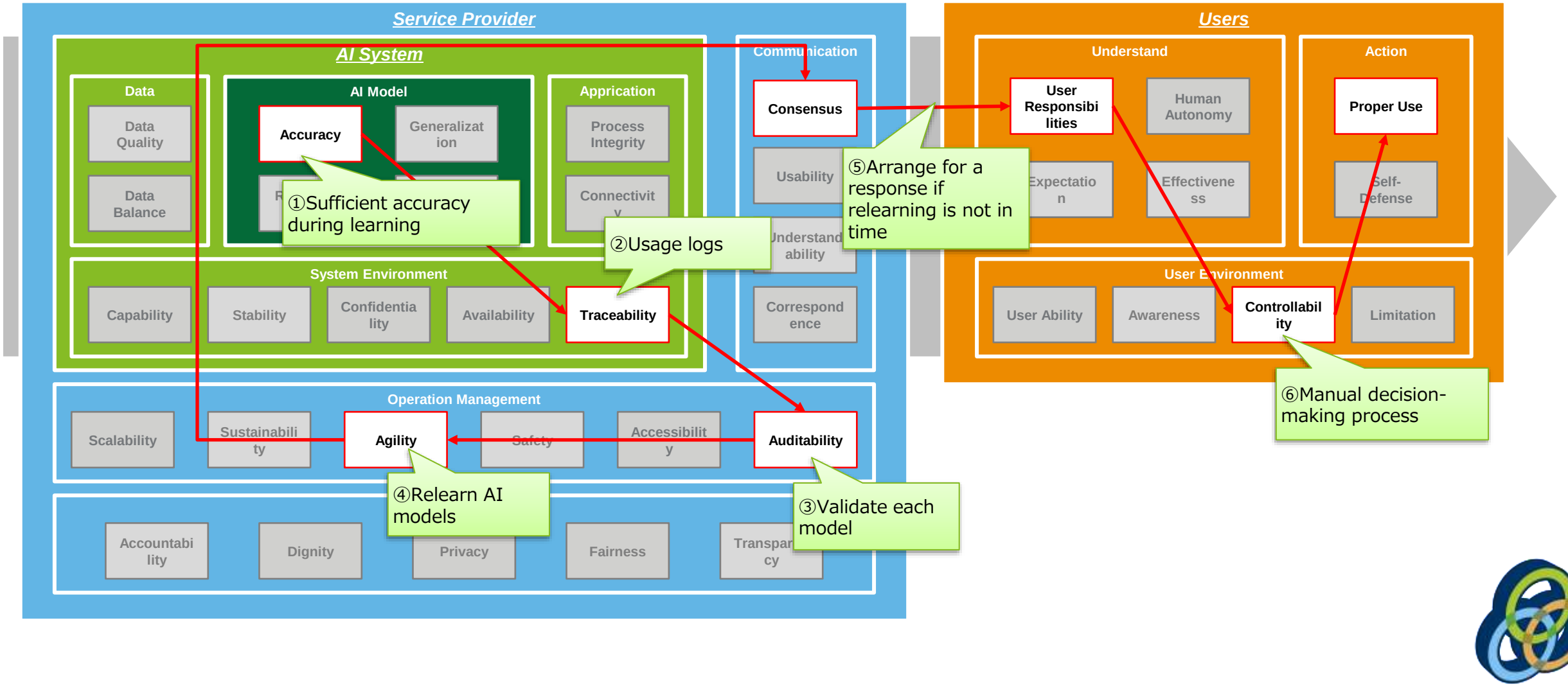
Control Coordination

- Examine the risk chain (relation of risk factors) for each important risk scenario -

Step3

R001

Unstable performance
Defective products are shipped, or many normal products are judged as defective due to deterioration of AI prediction performance



Risk Control

- Consider risk control according to the risk chain -

Step4

R001	**Unstable performance** Defective products are shipped, or many normal products are judged as defective due to deterioration of AI prediction performance

Risk Control		
AI system (Manufacturing Solution Dept., Co. B)	**Service Provider (Manufacturing Management Dept., Co. A)**	**User (Production Line Dept., Co. A)**
①[Accuracy] Ensuring a sufficient accuracy rate of the model when learning (Manufacturing Solution Dept., Co. B) ②[Traceability] Store the AI judgment history (IT Dept., Co. A)	③[Auditability] Examining cause and improvement of model performance when the prediction accuracy of the model deteriorates (Manufacturing Management Dept., Co. A) ④[Agility] Relearning AI model (Manufacturing Management Dept., Co. A) ⑤[Consensus] Agreement on alternative manual operations if relearning is not possible in time (Manufacturing Management Dept., Co. A)	⑤[User Responsibility] Agree on alternative manual operations if relearning is not possible in time (Production Line Dept., Co. A) ⑥[Controllability/Proper Use] Substitute for Alternative manual decision-making (Production Line Dept., Co. A)

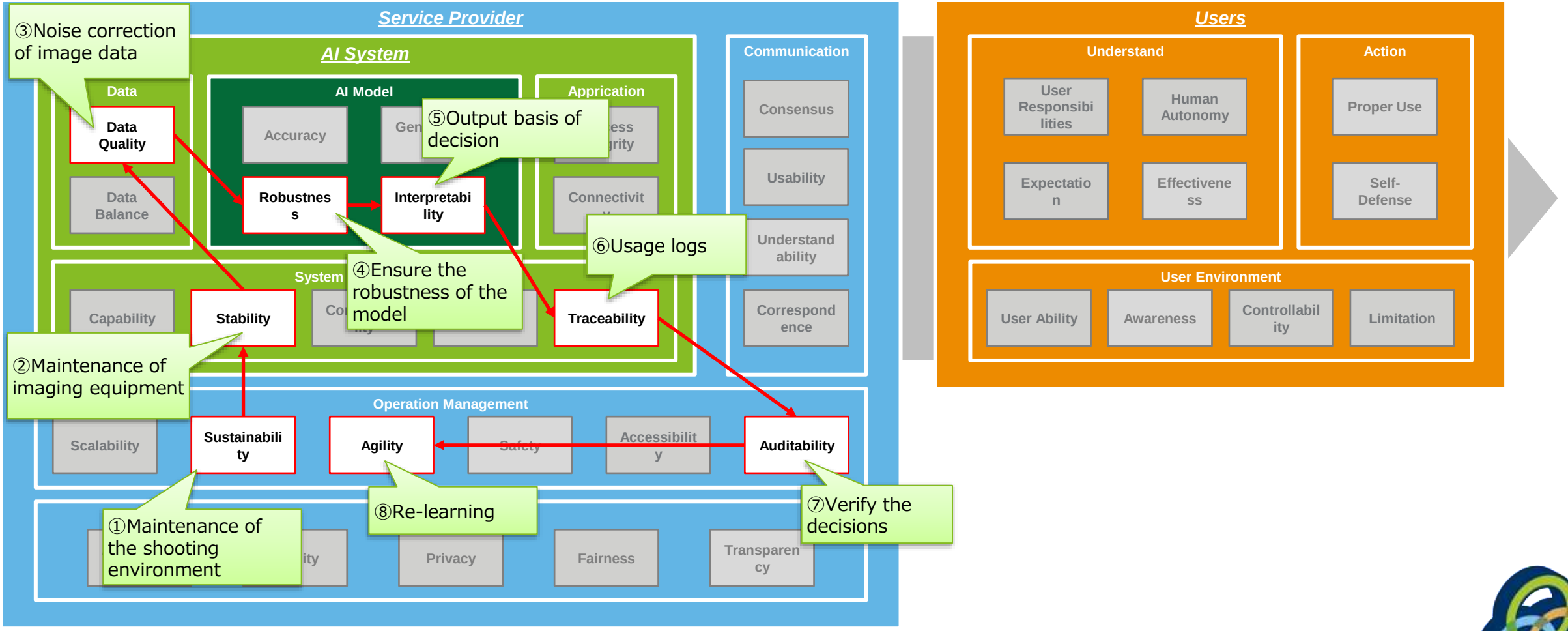
Control Coordination

- Examine the risk chain (relation of risk factors) for each important risk scenario -

Step3

R002

Impact by noise
Noise is mixed into the image and the accuracy of AI judgment deteriorates



Risk Control

- Consider risk control according to the risk chain -

Step4

R002	**Impact by noise** Noise is mixed into the image and the accuracy of AI judgment deteriorates

Risk Control		
AI system (Manufacturing Solution Dept., Co. B)	**Service Provider (Manufacturing Management Dept., Co. A)**	**User (Production Line Dept., Co. A)**
②[Stability] Clarify the required specifications of cameras and maintain them on a regular basis (Manufacturing Management Dept., Co. A / Manufacturing Solution Dept., Co. B) ③[Data Quality] Degradation of image data by noise correction, etc. (Manufacturing Solution Dept., Co. B) ④[Robustness] Learning to enhance the robustness of the model (Manufacturing Solution Dept., Co. B) ⑤[Interpretability] Output basis for the model decision (Manufacturing Solution Dept., Co. B) ⑥[Traceability] Store the AI judgment history (IT Dept., Co. A)	①[Sustainability] Maintain the quality of image information by cleaning and maintaining the shooting environment (Manufacturing Management Dept., Co. A) ⑦[Auditability] Verify the decisions (number of normal and defective items, etc.) and the point of interest in the image (Manufacturing Management Dept., Co. A) ⑧[Agility] Relearning AI model (Manufacturing Management dept., Co. A / Manufacturing Solution Dept., Co. B)	

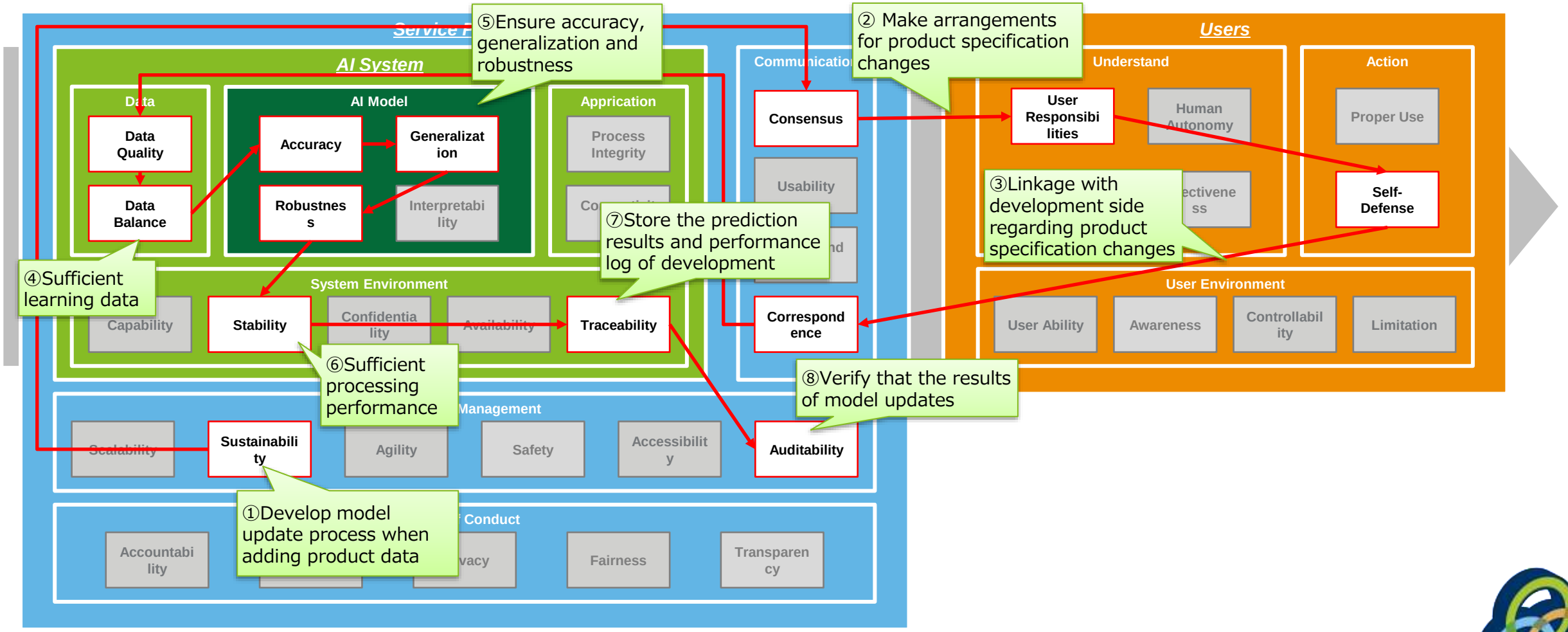
Control Coordination

- Examine the risk chain (relation of risk factors) for each important risk scenario -

Step3

R003

Change in product specifications
Identification accuracy is significantly reduced due to changes in product specifications



Risk Control

- Consider risk control according to the risk chain -

Step4

R003	**Change in product specifications** Identification accuracy is significantly reduced due to changes in product specifications

Risk Control		
AI system (Manufacturing Solution Dept., Co. B)	**Service Provider (Manufacturing Management Dept., Co. A)**	**User (Production Line Dept., Co. A)**
④[Data Quality/Data Balance] Ensuring adequate quantities of new learning data at the correct quality (Manufacturing Solution Dept., Co. B) ⑤ [Accuracy/Generalization/Robustness] Learning models to ensure the accuracy, generalization, and robustness of the model (Manufacturing Solution Dept., Co. B) ⑥[Stability] Ensuring the response required to provide services to the AI system when models are added or updated (IT Dept., Co. A) ⑦[Traceability] Store the prediction results and performance log at training stage (IT Dept., Co. A)	①[Sustainability] Develop a model update process when adding product data (Manufacturing Management dept., Co. A/Manufacturing Solution Dept., Co. B) ②[Consensus] Make arrangements for product specification changes (Manufacturing Management Dept., Co. A/Manufacturing Solution Dept., Co. B) ③[Correspondence] Proceeding with the datCo. Allection and model update process in anticipation of product specification changes (Manufacturing Management Dept., Co. A) ⑧[Auditability] Verify that the model update results are acceptable for service delivery (Manufacturing Management Dept.,Co. A / Manufacturing Solution Dept., Co. B)	②[User Responsibility] Make arrangements for product specification changes (Production Line Dept., Co. A) ③[Self-Defense] Linking information to the development side regarding the schedule of product specification changes (Production Line Dept., Co. A)

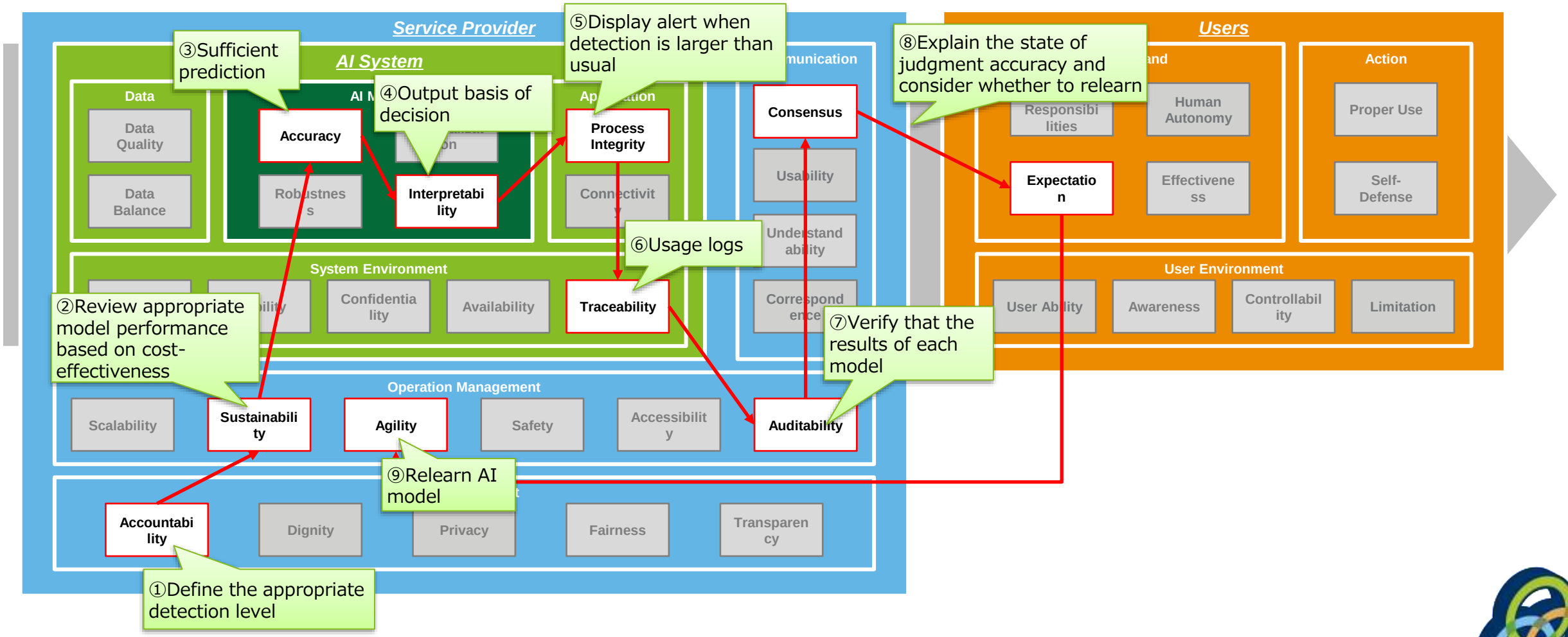
Control Coordination

- Examine the risk chain (relation of risk factors) for each important risk scenario -

Step3

R008

Excessive inspection
Excessive inspection results in increased verification costs on the human side and excessive waste



Risk Control

- Consider risk control according to the risk chain -

Step4

R008	**Excessive inspection** Excessive inspection results in increased verification costs on the human side and excessive waste

Risk Control		
AI system (Manufacturing Solution Dept., Co. B)	**Service Provider (Manufacturing Management Dept., Co. A)**	**User (Production Line Dept., Co. A)**
③[Accuracy] Develop models with sufficient prediction (Manufacturing Solution Dept., Co. B) ④[Interpretability] Output basis (the point of interest in the image) for the model decision (Manufacturing Solution Dept., Co. B) ⑤[Process Integrity] Display alert when detection is larger than usual (Manufacturing Solution Dept., Co. B) ⑥[Traceability] Store the AI judgment history (IT Dept., Co. A)	①[Accountability] Define appropriate inspection levels (Manufacturing Management Dept., Co. A) ②[Sustainability] Review appropriate inspection levels (model performance) based on maintenance costs (Manufacturing Management Dept., Co. A) ⑦[Auditability] Verify that the performance of each model and confirm the reason for over-detection (Manufacturing Management Dept., Co. A) ⑧[Consensus] Explain the state of judgment accuracy and consider whether to relearn (Manufacturing Management Dept., Co. A) ⑨[Agility] Relearning AI model (Manufacturing Management Dept., Co. A/Manufacturing Solution Dept., Co. B)	⑧[Expectation] Understand the appropriate detection level and consider whether to relearn (Person in Production Line Dept., Co. A)

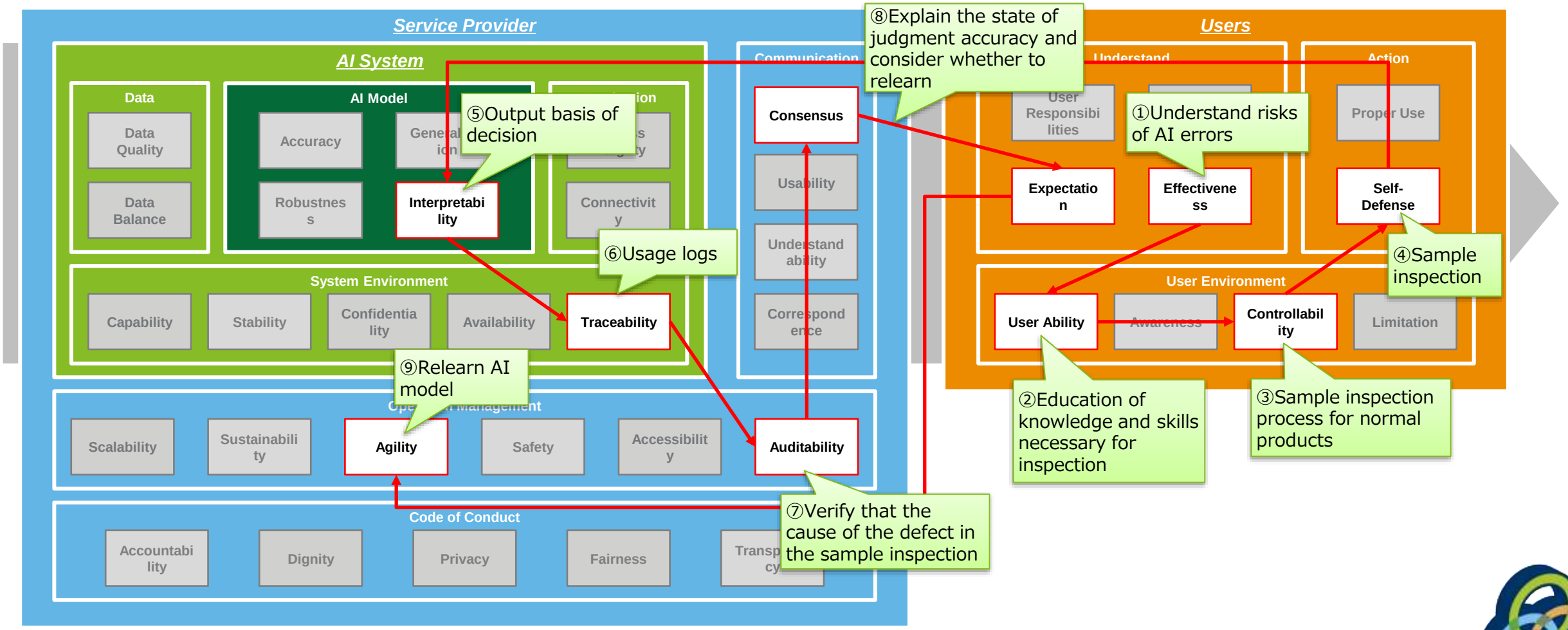
Control Coordination

- Examine the risk chain (relation of risk factors) for each important risk scenario -

Step3

R009

Excessive AI dependence
There is no doubt at all about the judgment of AI, and a lot of defective products are delivered to customers as the sample inspection becomes a mere facade



Risk Control

- Consider risk control according to the risk chain -

Step4

R009	**Excessive AI dependence** There is no doubt at all about the judgment of AI, and a lot of defective products are delivered to customers as the sample inspection becomes a mere facade

Risk Control		
AI system (Manufacturing Solution Dept., Co. B)	**Service Provider (Manufacturing Management Dept., Co. A)**	**User (Production Line Dept., Co. A)**
⑤[Interpretability] Output basis (the point of interest in the image) for the model decision (Manufacturing Solution Dept., Co. B) ⑥[Traceability] Store the AI judgment history (IT Dept., Co. A)	⑦[Auditability] Verify that the cause of the defect in the sample inspection (Manufacturing Management Dept., Co. A) ⑧[Consensus] Explain the state of judgment accuracy and consider whether to relearn (Manufacturing Management Dept., Co. A) ⑨[Agility] Relearning AI model (Manufacturing Management dept., Co. A/Manufacturing Solution Dept., Co. B)	①[Effectiveness] Understand risks of AI errors (Production Line Dept., Co. A) ②[User Ability] Education of knowledge and skills necessary for inspection (Production Line Dept., Co. A) ③[Controllability] Develop a sample inspection process for normal products in a production line (Person in Production Line Dept., Co. A) ④[Self-Defense] Inspect samples of normal products and exclude defective products (Production Line Dept., Co. A) ⑧[Expectation] Understand the appropriate detection level and consider whether to relearn (Person in Production Line Dept., Co. A)

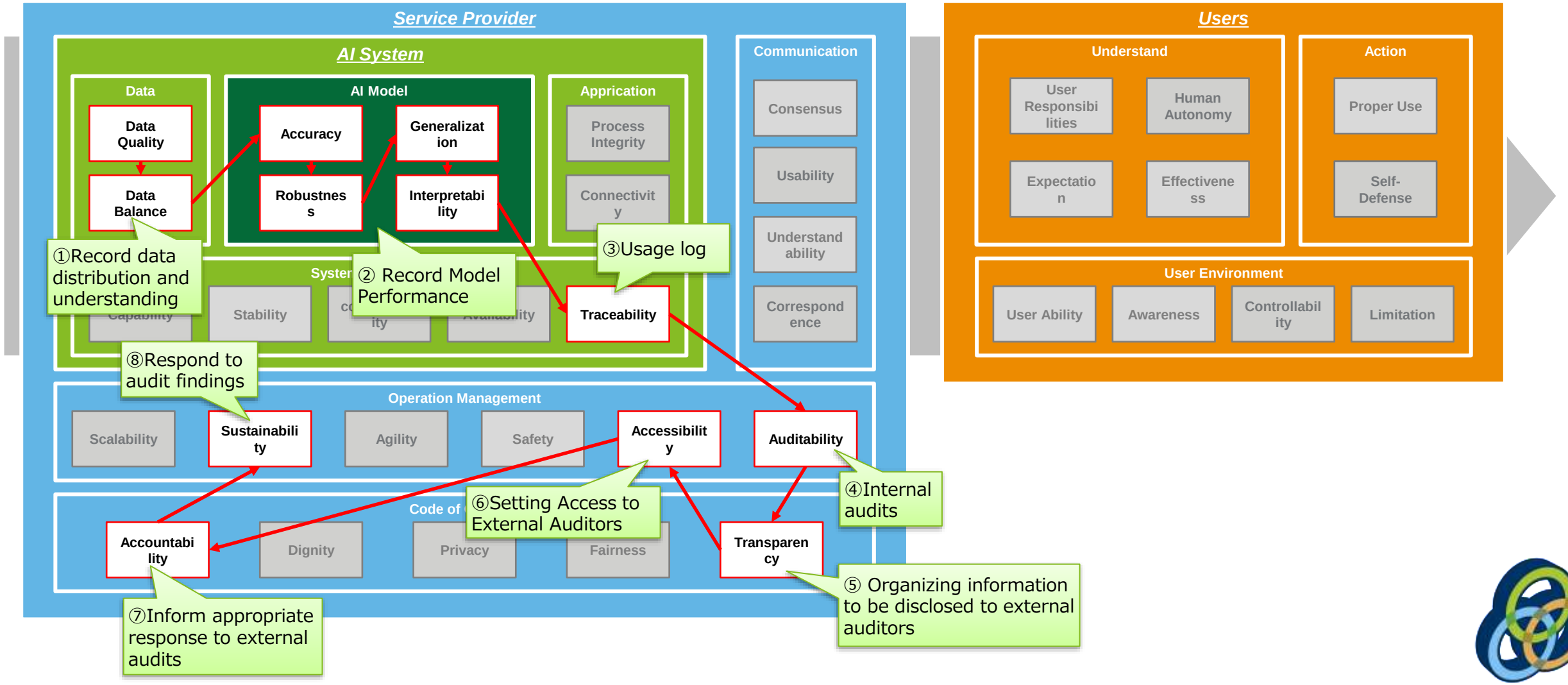
Control Coordination

- Examine the risk chain (relation of risk factors) for each important risk scenario -

Step3

R010

Response to quality audits
Inability to provide appropriate explanations when subjected to quality audits



Risk Control

- Consider risk control according to the risk chain -

Step4

R010	**Response to quality audits** Inability to provide appropriate explanations when subjected to quality audits

Risk Control		
AI system (Manufacturing Solution Dept., Co. B)	**Service Provider (Manufacturing Management Dept., Co. A)**	**User (Production Line Dept., Co. A)**
①[Data Quality/Data Balance] Record data distribution and understanding (Manufacturing Solution Dept., Co. B) ②[Accuracy/Robustness/Generalization/Interpretability] Record the performance of the model (Manufacturing Solution Dept., Co. B) ③[Traceability] Store the AI judgment history (IT Dept., Co. A)	④[Auditability] Conduct internal audits and respond in advance (Manufacturing Management Dept., Co. A) ⑤[Transparency] Organize information to be disclosed to external auditors (Manufacturing Management Dept., Co. A) ⑥[Accessibility] Setting necessary access rights to external auditors (Manufacturing Management Dept., Co. A) ⑦[Accountability] Inform appropriate response to external audits (Manufacturing Management Dept., Co. A) ⑧[Sustainability] Address issues discovered during audits (Manufacturing Management Dept., Co. A)	