

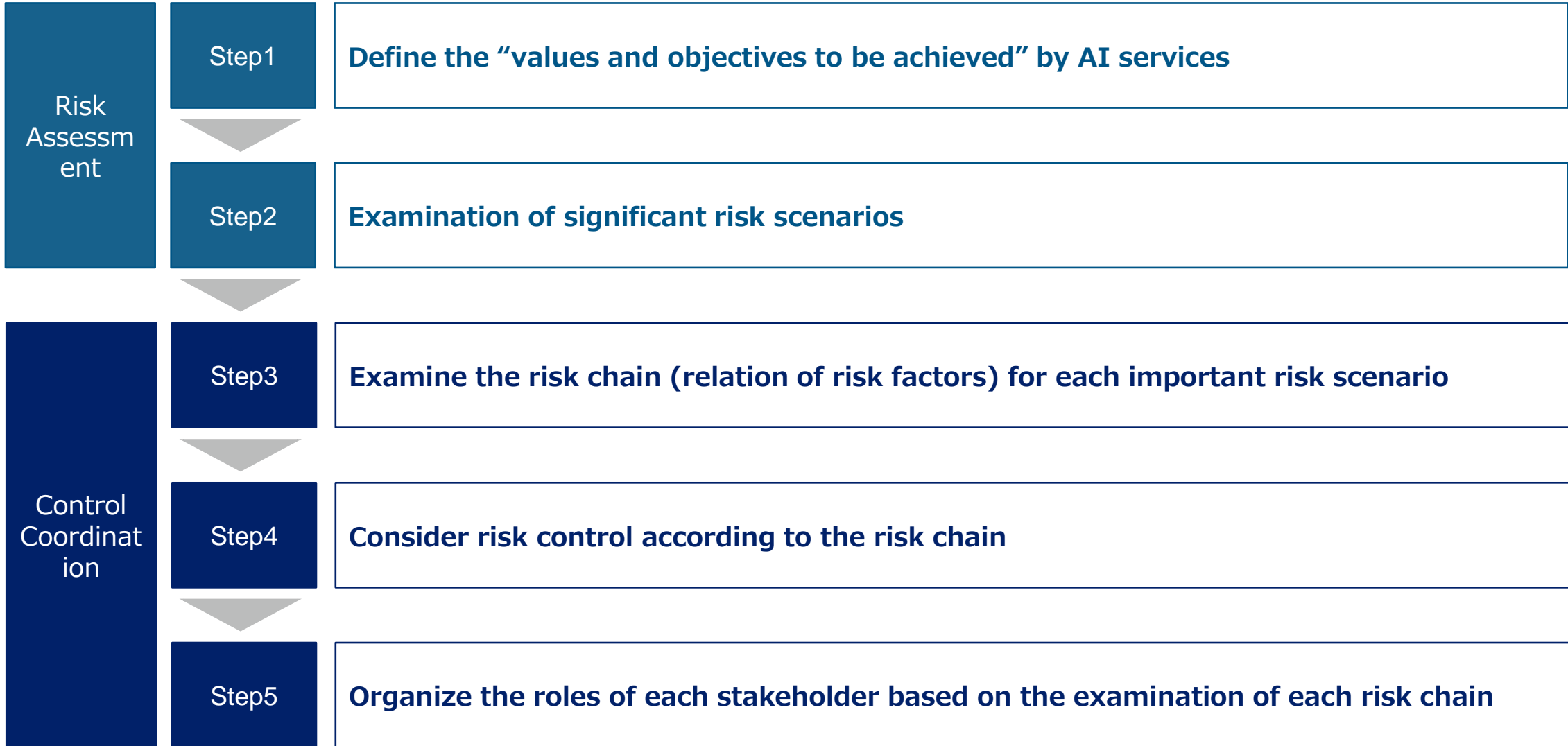
Risk Assessment & Control Coordination for AI services : Case02 Unstaffed Convenience Store



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

How to operate the RCModel

- Risk Assessment & Control Coordination -





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/>



東京大学未来ビジョン研究センター
Institute for Future Initiatives

Research

Education

People

News

Events

Publications

How to use Risk Chain Model

[Risk Chain Model \(RCModel\) Guide Ver1.0](#)

Case Study

*These are fictional case studies below and don't raise issues or assure for any company or AI service.

[Case01.Recruitment AI \(2021/07\)](#)

Case Study



Case02 : Unstaffed Convenience Store

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

We present an unstaffed convenience store wherein an artificial intelligence (AI) system calculates the purchase price items as they are picked up by customers who then can pay with electronic money as they leave. The AI service is provided by Co. J, which manages convenience store chains in Japan. This system’s image recognition capability was developed by Co. X.

[Values & Objectives]

- **Provision of 24 h/day, 365 days/year service (target: unstaffed operation at any time, mainly in rural areas; unstaffed operation at midnight in metropolitan areas)**
 - **It is difficult for stores in metropolitan areas to manage a large number of incidental operations (e.g., mail and utility bills) and inventory management operations during the day.**
- **Maintaining customer satisfaction**
- **Improvement of profit per store (e.g., reduction of personnel expenses)**
- **Service provision in underpopulated areas**

Co. X, the developer, provides the following system:

- Head Office) A management system for product master data, etc. The server is installed in the cloud environment owned by Co. X.
- Store) A monitor that displays the learned AI models and sensor actuator amounts.

Co. J provides actual stores, store facilities, payment terminals, and incorporates learned AI models, sensors, actuators, and monitors developed by Co. X. In case of trouble (e.g., error in settlement amounts) related to customers, Co. J’s customer center will take preliminary measures. Product data (e.g., images and prices) are registered and maintained by Co. J’s management system.

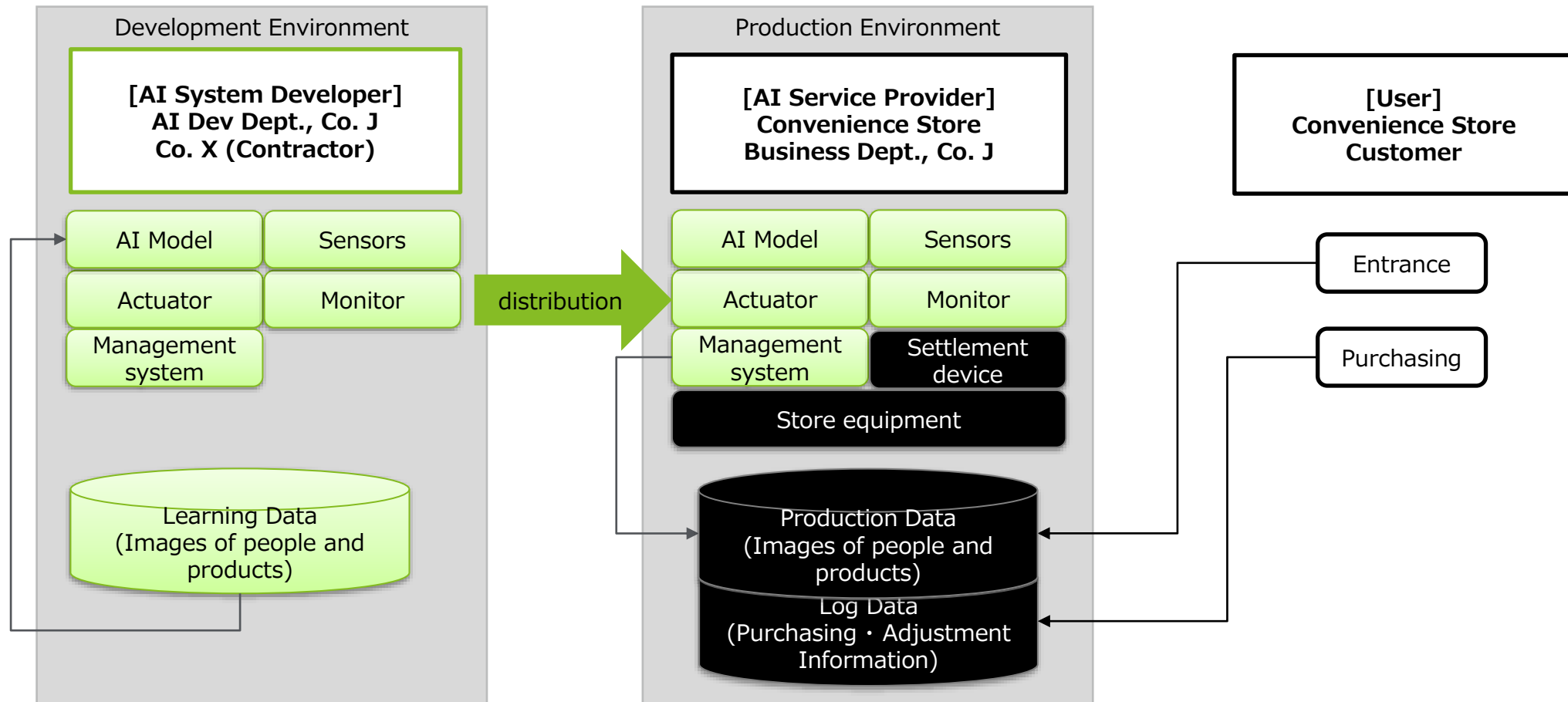
The AI model is operated independently by distributing the learned model to each store. There is no incremental learning in the AI model, but when an update is distributed from Co. X, Co. J will apply it. Each store has information on the AI system with people and product data for a certain period (i.e., 3 months). It is possible to confirm information of false recognitions within this period. After a certain period, data are automatically deleted from the store. If it is considered that the AI’s predictive performance is significantly deteriorated, Co. J will contact Co. X to request improvement of the AI system, as necessary.



Case02 : Unstaffed Convenience Store

- System Overview -

AI System	AI Dev Dept., Co. J and Co. X (contractor)	AI system including image recognition for unstaffed sales operations
AI Service Provider	Convenience Store Business Dept., Co. J + store	Provision of services as convenience stores
User	Convenience Store Customer	Shopping at a convenience store



Case02 : Unstaffed Convenience Store

- Input & Output -

[Input Data]

Data	Purpose	Collection Method	Data Manager	Including Privacy Data
Learning data of product (image)	Learning	Collected by Co. X(contractor). If necessary, Co. J will provide it.	Co. X (development environment of Co. X)	None
Learning data of people (images)	Learning	Collected by Co. X(contractor). If necessary, Co. J will provide it.	Co. X (development environment of Co. X)	Yes (image data of people)
Production data of product (images)	Production	Co. J collects images from suppliers and registers it in the management system.	Convenience Store Business Dept., Co. J (management server of Co. J)	None
Production data of people (image)	Production	Get it at any time with a camera at a convenience store.	Convenience Store Business Dept., Co. J (store encrypted in the system installed at each store)	Yes (customer image data)

[Output]

Users	Convenience store customer
Output	Price of the products (to print the receipt, the amount of money and tax is shown for each item.)
Output Method	To display information related to the price of merchandise on a monitor. When the convenience store user confirms the merchandise and performs settlement processing, a receipt is output from the terminal. When there is an error in the merchandise, the user corrects it on the screen.
Expected Accuracy	Correct rate: 93.3% (1120/1200) *In general, the number of users is expected to be 1,200 per day, and the maximum number of users who can deal with problems is expected to be about 80 per day.
User judgment	Yes
Output of evidence information	The monitor displays the recognized product line and price.
Safety Risk	No
Connection with external system	No
Users	Convenience store customer



Risk Assessment



Risk Assessment

- Examination of significant risk scenarios -

Values & Objectives		Service Requirement			Risk No.	Risk Scenario	
1	24/7 service (open late at night by unstaffed operation)	1-1	Precision performance	<ul style="list-style-type: none"> Accuracy Stable system operation Security 	R001	Unstable performance	Convenience store operations are stopped due to deterioration of AI's predictive performance
					R002	System failure	AI service stopped caused by system failure
		1-2	Responding to changes in store environments and products handled	<ul style="list-style-type: none"> Image recognition Relearning Data management 	R003	Changes in the store environment	AI misidentifies products and customers due to changes in the store environment (e.g., weather, brightness, and cleaning conditions)
					R004	Changes of customer appearance	AI misidentifies customers due to customer behavior (e.g., hats, glasses, and jackets)
					R005	Changes of product	AI predictions cannot keep up with new products and packaging changes
2	Maintaining Customer Satisfaction	2-1	Consumer support	<ul style="list-style-type: none"> User interface 	R006	Modify by user	Product recognition is incorrect, but the user cannot correct it
					R007	Non-service operations (1) (incidental business)	Convenience store operations (mail, utilities, printing, and ATM), which are not covered by AI services, are not maintained
		2-2	Maintenance of the store environment	-	R008	Non-service operations (2) (Inventory)	Because there is no restocking or inventory, stores lose customers or sell defective products
					R009	Non-service operations (3) (Environment)	The hygienic environment in the store is not maintained and it may cause lose customers
3	Improve profit per store (e.g., reduction of personnel expenses)	3-1	Adequate cost	-	R010	Excess costs	Operation costs are exceeded
		3-2	loss prevention	<ul style="list-style-type: none"> User interface 	R011	Abuse by the user	Losses due to using correction function by malicious customers
4	Service provision in underpopulated areas	4-1	Localization	<ul style="list-style-type: none"> Relearning 	R012	Expansion of services	When opening a store in a new country or region, the predictive performance of AI cannot respond to changes in customer base or products
5	Corporate social responsibility	5-1	Compliance with laws and regulations	<ul style="list-style-type: none"> Accuracy Data protection 	R013	Age verification	Age verification is not properly conducted when selling alcohol, cigarettes, etc
					R014	Leakage of privacy data	Violation of the Personal Information Protection Act by mishandling personal information (e.g., user's image and purchase record)
		5-2	Compliance with ethics	<ul style="list-style-type: none"> Accuracy 	R015	Fairness	Produces unfair predictions for specific countries/regions/races/genders/ages

Risk Assessment & Control Summary

Step5

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

Values & Objectives	Risk No.	Risk Scenario	Uncertainty	Environmental change	Caused by user	RC	Control Summary		
							AI System	AI service provider	User
1 24/7 service (open late at night by unstaffed operation)	R001	Unstable performance	○			●	Accuracy of model predictions	Validate model Relearn AI model	
	R002	System failure					Stable system operation	Fallback operations by staff	
	R003	Changes in the store environment	○	○		●	Camera maintenance Image denoising Robustness	Store management(cleaning) Product display and correction function	Alerting users Use of the correction function
	R004	Changes of customer appearance	○		○	●	Learning data Robustness Cooperation in case of loss of object	Remote customer service	Announcement to the user Self-checkout service
	R005	Changes of product	○	○		●	Learning Data Prediction performance Stable system operation	Model development process Receipt validation	
2 Maintaining Customer Satisfaction	R006	Modify by user	○		○	●	Basis of decision	Correction function Remote customer service	Use of the correction function
	R007	Non-service operations (1) (incidental business)						Design and implementation of store operations	
	R008	Non-service operations (2) (Inventory)						Design and implementation of store operations	
	R009	Non-service operations (3) (Environment)						Design and implementation of store operations	
3 Improve profit per store (e.g., reduction of personnel expenses)	R010	Excess costs						Cost management	
	R011	Abuse by the user			○	●	Store usage information	Validate Corrected Data Response to subsequent requests, etc.	Alerting users
4 Service provision in underpopulated areas	R012	Expansion of services	○	○		●	System environment Individual models	Individual target accuracy Monitoring model Development team	
5 Corporate social responsibility	R013	Age verification	○		○	●	Data management Age verification process	Reminder to users, internal verification, and corrective actions	Understanding of user responsibility Appropriate purchase
	R014	Leakage of privacy data					Data protection	Compliance	
	R015	Fairness	○			●	Data bias Model generalization	Review fairness Relearning	

Organization

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

J Co) Top Management

- Values and objectives
- Approve risk controls

J Co) Legal Dept.

- Education on legal compliance
- Claims against malicious users

J Co) Internal Audit Dept.

- Review prediction accuracy
- Review fairness

Consumer Affairs Agency

- AI Service Provider - J Co) Convenience Store Business Dept.

Set business objectives

- Setting target accuracy by area
- Cost management
- Design of store operations

PJ management

- Development process
- Development system
- Performance monitoring
- Validate corrected data

Preparing related functions

- Product display and correction function
- Collaborative processing at the time of loss of object
- Age verification process

J Co) AI Dev Dept. & X Co. (Contractor)

- Predictive performance
- Model generalization
- Model robustness
- Ensuring learning data
- Adjusting data bias
- Output of decision basis
- Securing data by area
- Model development by area

J Co) IT Dept.

- Image noise correction
- Development environment based on the number of models
- Verifiability
- Protecting and securing data

J Co) Convenience Store

- Ancillary business of the store
- Store inventory management
- Store cleaning
- Alerting to users
- Fallback operations by staff

J Co) Customer Service

- Support desk
- Remote customer service

- User - Convenience Store Users

- Understanding of user responsibility
- Appropriate purchase
- Use of the correction function
- Self-checkout service



Control Coordination



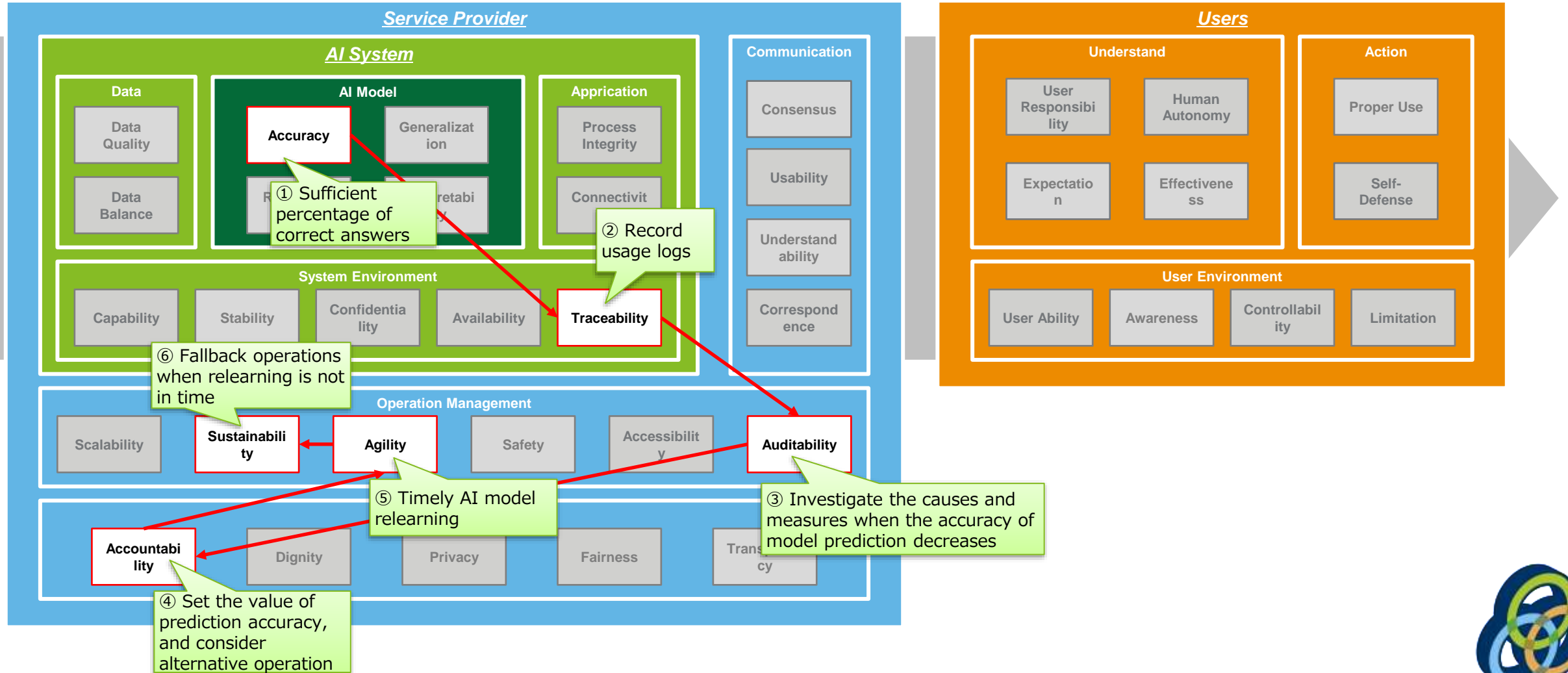
Control Coordination

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

R001

Unstable performance

Convenience store operations are stopped due to deterioration of AI's predictive performance



Risk Control

- Consider risk control according to the risk chain -

R001

Unstable performance

Convenience store operations are stopped due to deterioration of AI's predictive performance

Risk Control		
AI system (AI Dev Dept., Co. J & Co. X (Contractor))	AI Service Provider (Convenience Store Business Dept., Co. J)	User (Customer)
<p>① [Accuracy] Ensuring a sufficient percentage of models correct when learning (Co. X)</p> <p>② [Traceability] Saving log information of customer and purchase information (IT Dept., Co. J)</p>	<p>③ [Auditability] Investigation of causes and countermeasures for deterioration in model prediction accuracy (Convenience Store Business Dept., Co. J)</p> <p>④ [Accountability] Review of the expected value that is sufficient and technically appropriate for the performance of the service, and study of alternative operation methods and systems for fallback operation (Convenience Store Business Dept., Co. J)</p> <p>⑤ [Agility] Requesting relearning of AI models to ensure sufficient accuracy (Convenience Store Business Dept., Co. J)</p> <p>⑥ [Sustainability] When relearning cannot be done in time, fallback operation by staff (Convenience Store Business Dept., Co. J / Stores)</p>	



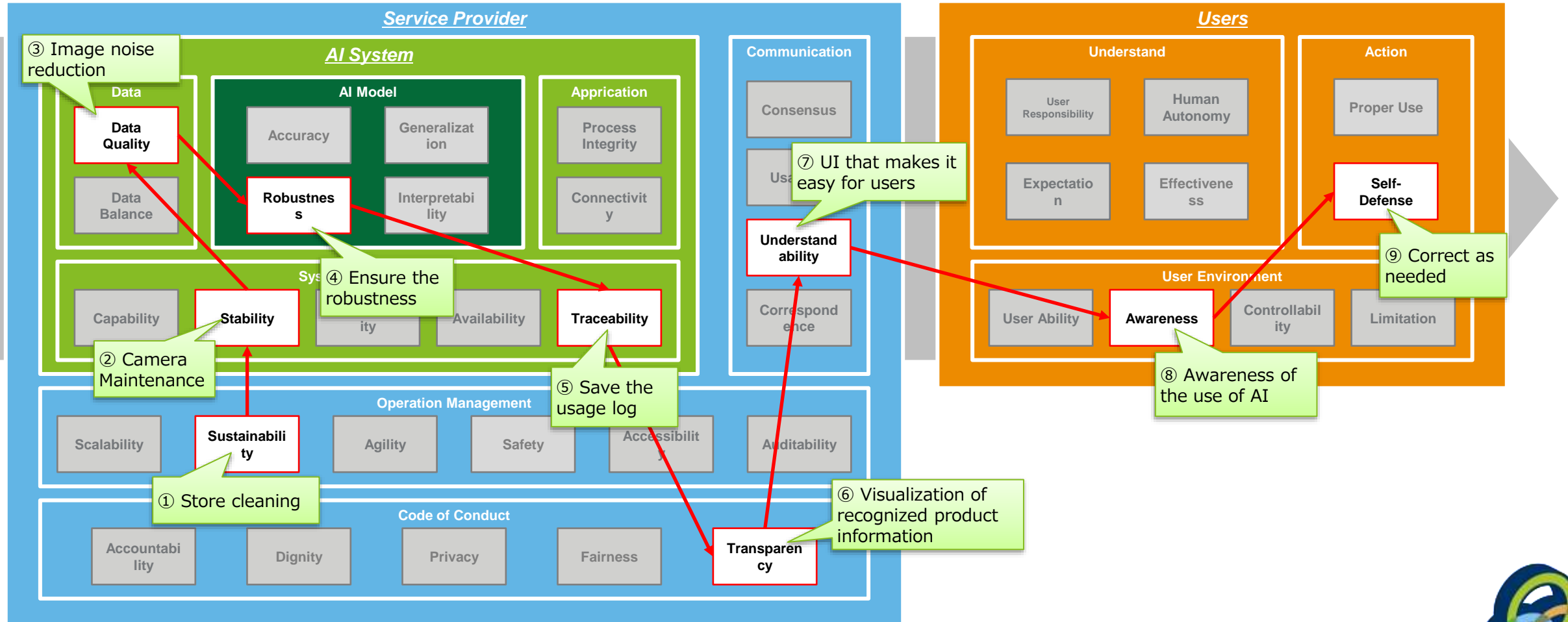
Control Coordination

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

R003

Changes in the store environment

AI misidentifies products and customers due to changes in the store environment (e.g., weather, brightness, and cleaning conditions)



Risk Control

- Consider risk control according to the risk chain -

R003

Changes in the store environment

AI misidentifies products and customers due to changes in the store environment (e.g., weather, brightness, and cleaning conditions)

Risk Control		
AI system (AI Dev Dept., Co. J & Co. X (Contractor))	AI Service Provider (Convenience Store Business Dept., Co. J)	User (Customer)
<p>② [Stability] Monitoring and maintenance of cameras in stores (IT Dept., Co. J)</p> <p>③ [Data Quality] Degradation of real image data by noise reduction, etc (AI Dev Dept., Co. J)</p> <p>④ [Robustness] Learning to increase model robustness (Co. X)</p> <p>⑤ [Traceability] Saving log information of customer and purchase information (IT Dept., Co. J)</p>	<p>① [Sustainability] Store management (cleaning) in accordance with the Manual (Stores)</p> <p>⑥ [Transparency] Visualize product information for users (Convenience Store Business Dept., Co. J)</p> <p>⑦ [Understandability] Design UI for product information and correction function that users can easily understand (Convenience Store Business Dept., Co. J)</p>	<p>⑧ [Awareness] In stores, alert customers to the possibility of product recognition errors (Stores)</p> <p>⑨ [Self-Defense] If there is misidentification of the product, use the correction function to purchase correctly (Customer)</p>



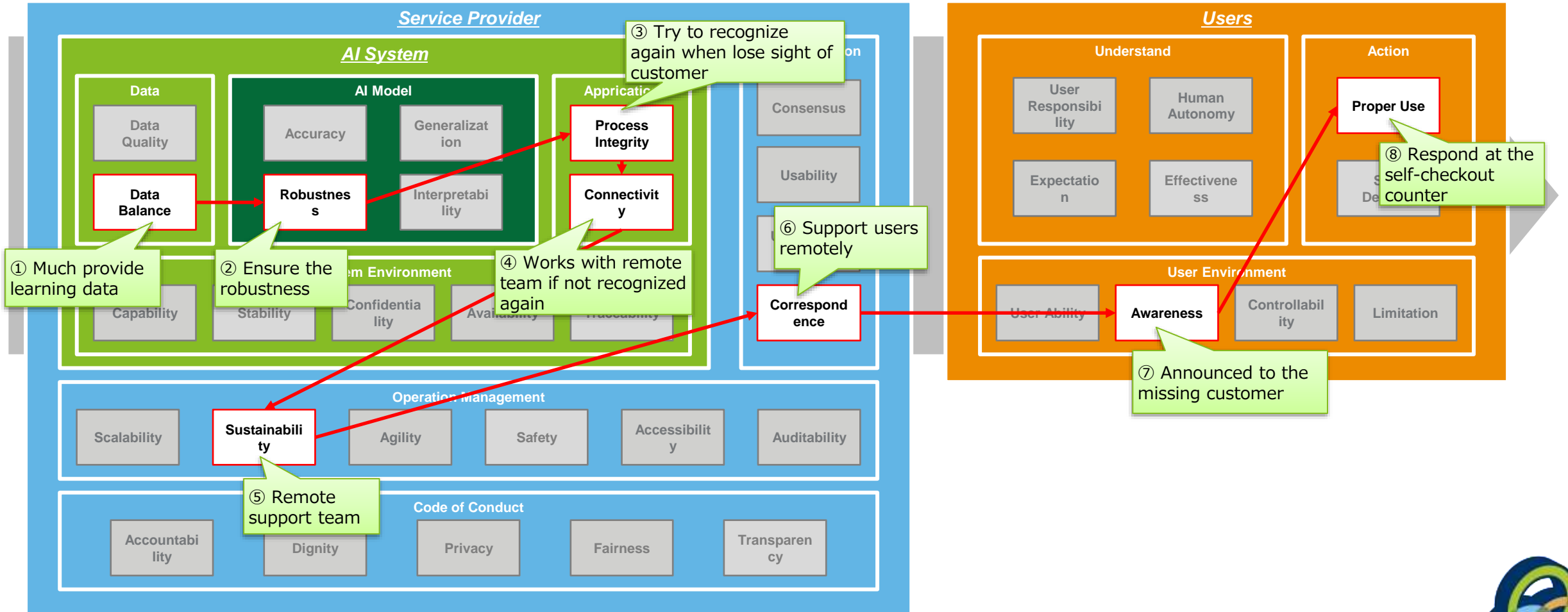
Control Coordination

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

R004

Changes of customer appearance

AI misidentifies customers due to customer behavior (e.g., hats, glasses, and jackets)



Risk Control

- Consider risk control according to the risk chain -

R004

Changes of customer appearance

AI misidentifies customers due to customer behavior (e.g., hats, glasses, and jackets)

Risk Control		
AI system (AI Dev Dept., Co. J & Co. X (Contractor))	AI Service Provider (Convenience Store Business Dept., Co. J)	User (Customer)
<p>① [Data Balance] Improve learning data to respond to changes in people's appearance (AI Dev Dept., Co. J)</p> <p>② [Robustness] Learning to increase model robustness (Co. X)</p> <p>③ [Process Integrity] When a customer is lost, an attempt is made to associate the customer with a newly identified person (AI Dev Dept., Co. J)</p> <p>④ [Connectivity] When a customer is completely lost, a support request is automatically notified to the remote team together with the previous images (AI Dev Dept., Co. J)</p>	<p>⑤ [Sustainability] Deploy a remote customer support team (Convenience Store Business Dept., Co. J / Remote Support Team, Co. J)</p> <p>⑥ [Correspondence] Remote support for lost customer (Remote Support Team, Co. J)</p>	<p>⑦ [Awareness] makes in-store announcements and calls for remote support for lost customer (Remote Support Team, Co. J)</p> <p>⑧ [Proper Use] Use self-checkout to make purchases (Customer)</p>



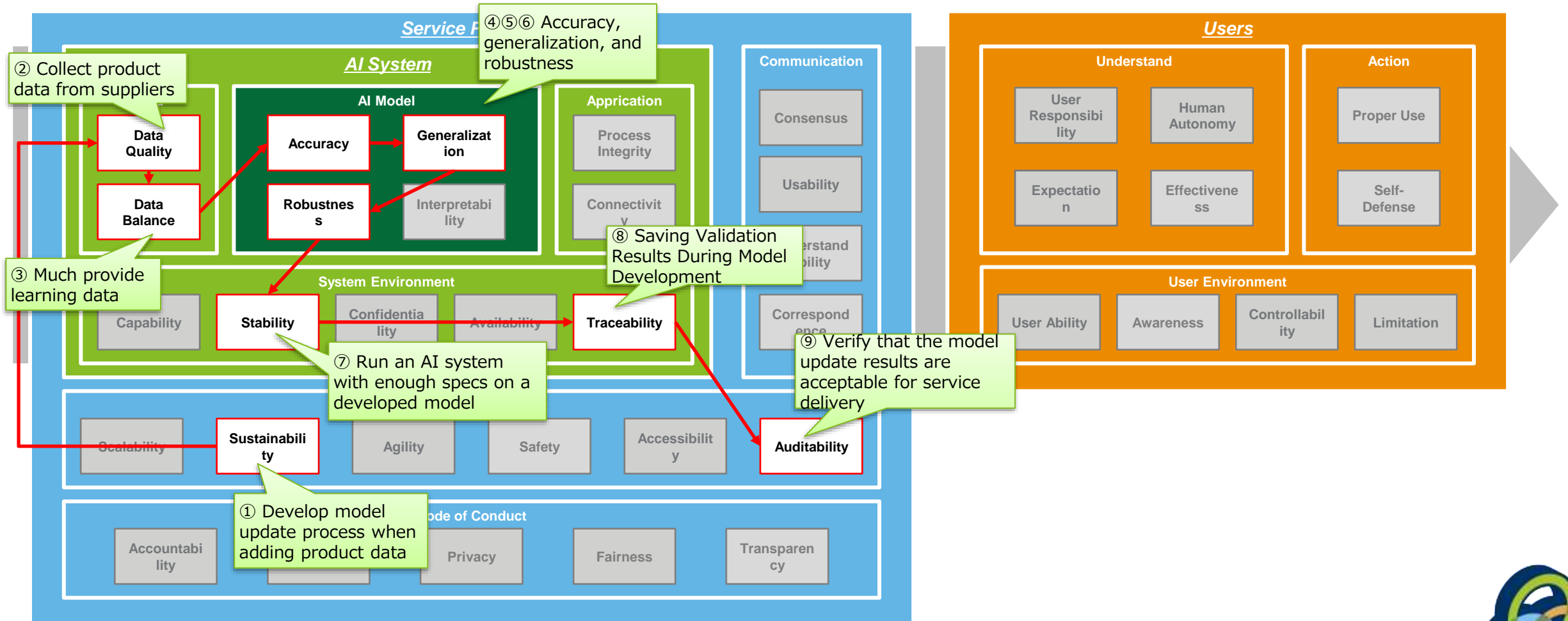
Control Coordination

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

R005

Changes of product

AI predictions cannot keep up with new products and packaging changes



Risk Control

- Consider risk control according to the risk chain -

R005

Changes of product

AI predictions cannot keep up with new products and packaging changes

Risk Control		
AI system (AI Dev Dept., Co. J & Co. X (Contractor))	AI Service Provider (Convenience Store Business Dept., Co. J)	User (Customer)
<p>② [Data Quality] Obtain accurate product information from suppliers (Convenience Store Business Dept., Co. J / AI Dev Dept., Co. J)</p> <p>③ [Data Balance] Improve learning data to respond to changes in the appearance of products (Co. X)</p> <p>④ [Accuracy] Ensuring sufficient recognition accuracy for products to be sold (Co. X)</p> <p>⑤ [Generalization] Ensures generalization performance including data other than added products (Co. X)</p> <p>⑥ [Robustness] Learning to increase model robustness (Co. X)</p> <p>⑦ [Stability] When using the updated model, ensure the response required for service provision to the AI system (IT Dept., Co. J)</p> <p>⑧ [Traceability] Saving verification results during model development (AI Dev Dept., Co. J / Co. X)</p>	<p>① [Sustainability] Define the model development process by adding and updating product data (Convenience Store Business Dept., Co. J / AI Dev Dept., Co. J)</p> <p>⑨ [Auditability] Verify that the model update results are acceptable for service provision (Convenience Store Business Dept., Co. J)</p>	



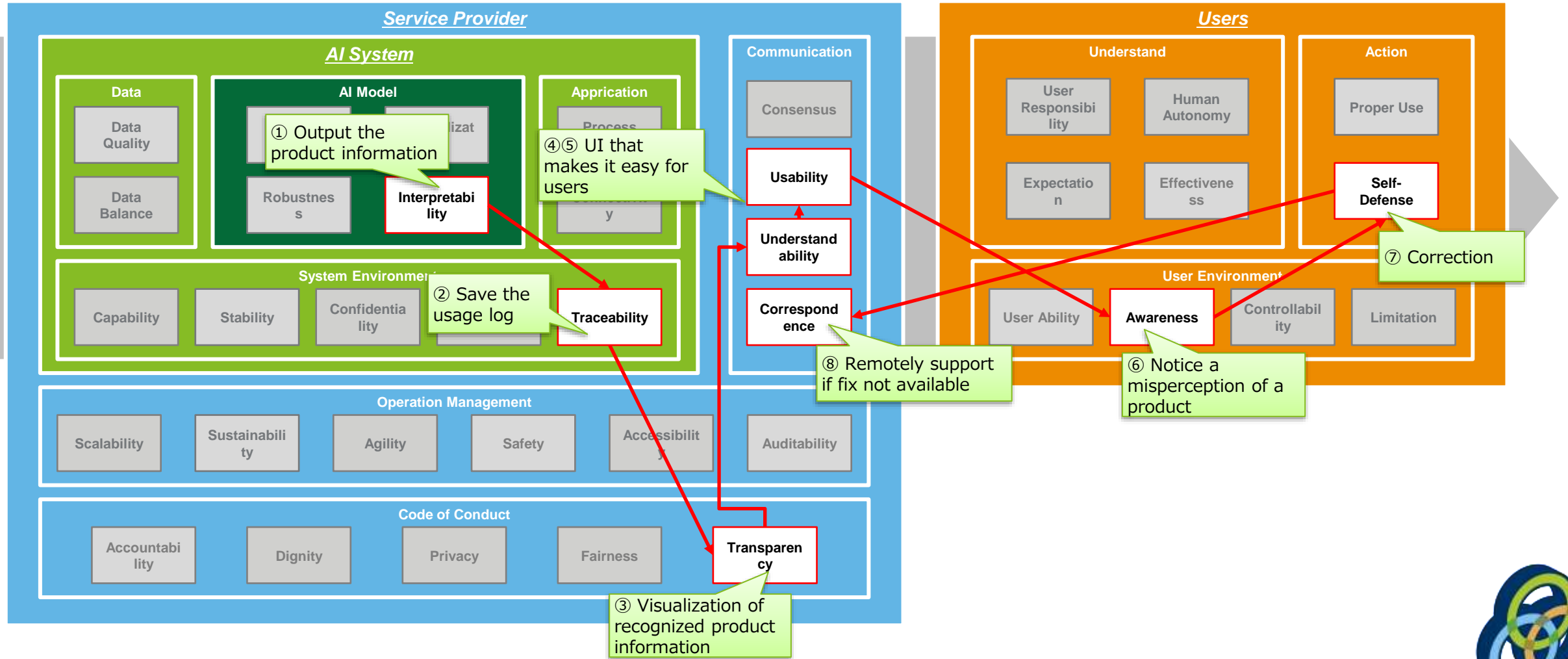
Control Coordination

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

R006

Modify by user

Product recognition is incorrect, but the user cannot correct it



Risk Control

- Consider risk control according to the risk chain -

R006

Modify by user

Product recognition is incorrect, but the user cannot correct it

Risk Control		
AI system (AI Dev Dept., Co. J & Co. X (Contractor))	AI Service Provider (Convenience Store Business Dept., Co. J)	User (Customer)
<p>① [Interpretability] Output the recognized product information from the model (Co. X)</p> <p>② [Traceability] Saving log information of customer and purchase information (IT Dept., Co. J)</p>	<p>③ [Transparency] Visualize product information judged for users (Convenience Store Business Dept., Co. J)</p> <p>④ [Understandability] Design user interface for product information and correction function that users can easily understand (Convenience Store Business Dept., Co. J)</p> <p>⑤ [Usability] Implement user interface of user-friendly modification function (Convenience Store Business Dept., Co. J)</p> <p>⑧ [Correspondence] Remote support for users who cannot correct the problem (Remote Support Team, Co. J)</p>	<p>⑥ [Awareness] Product information recognized so that users may notice the recognition error is output in an easy-to-understand manner (Convenience Store Business Dept., Co. J)</p> <p>⑦ [Self-Defense] Use correction function to correct product information (Customer)</p>



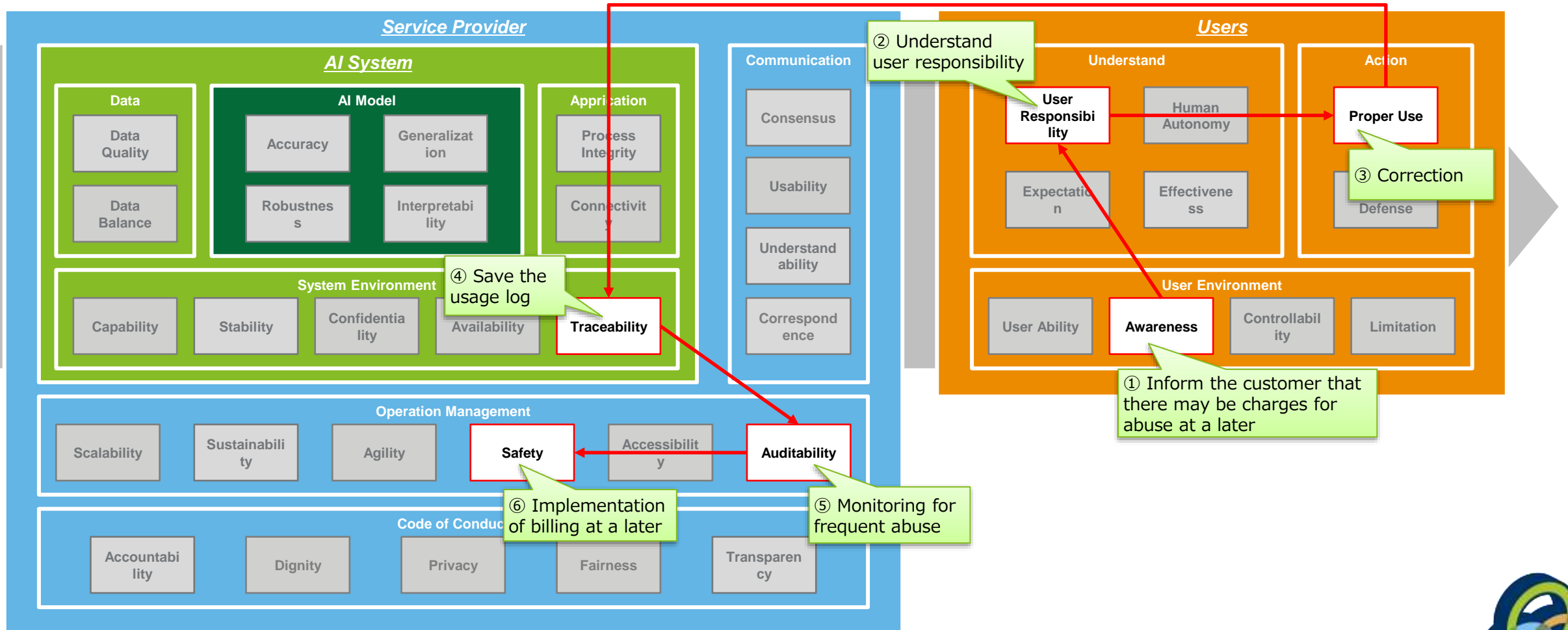
Control Coordination

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

R011

Abuse by the user

Losses due to using correction function by malicious customers



Risk Control

- Consider risk control according to the risk chain -

R011

Abuse by the user

Losses due to using correction function by malicious customers

Risk Control		
AI system (AI Dev Dept., Co. J & Co. X (Contractor))	AI Service Provider (Convenience Store Business Dept., Co. J)	User (Customer)
④ [Traceability] Saving log information of customer and purchase information (IT Dept., Co. J)	⑤ [Auditability] Periodically check for improper revisions by customers (Convenience Store Business Dept., Co. J) ⑥ [Agility] Provide appropriate response to malicious customers (e.g., request at later) (Convenience Store Business Dept., Co. J)	① [Awareness] Tell customers that abuse of the correction function is monitored and can be charged later (Convenience Store Business Dept., Co. J / Stores) ② [User Responsibility] Recognize that you can be charged later by exploiting the remediation feature (Customer) ③ [Proper Use] Use the correction function appropriately (Customer)



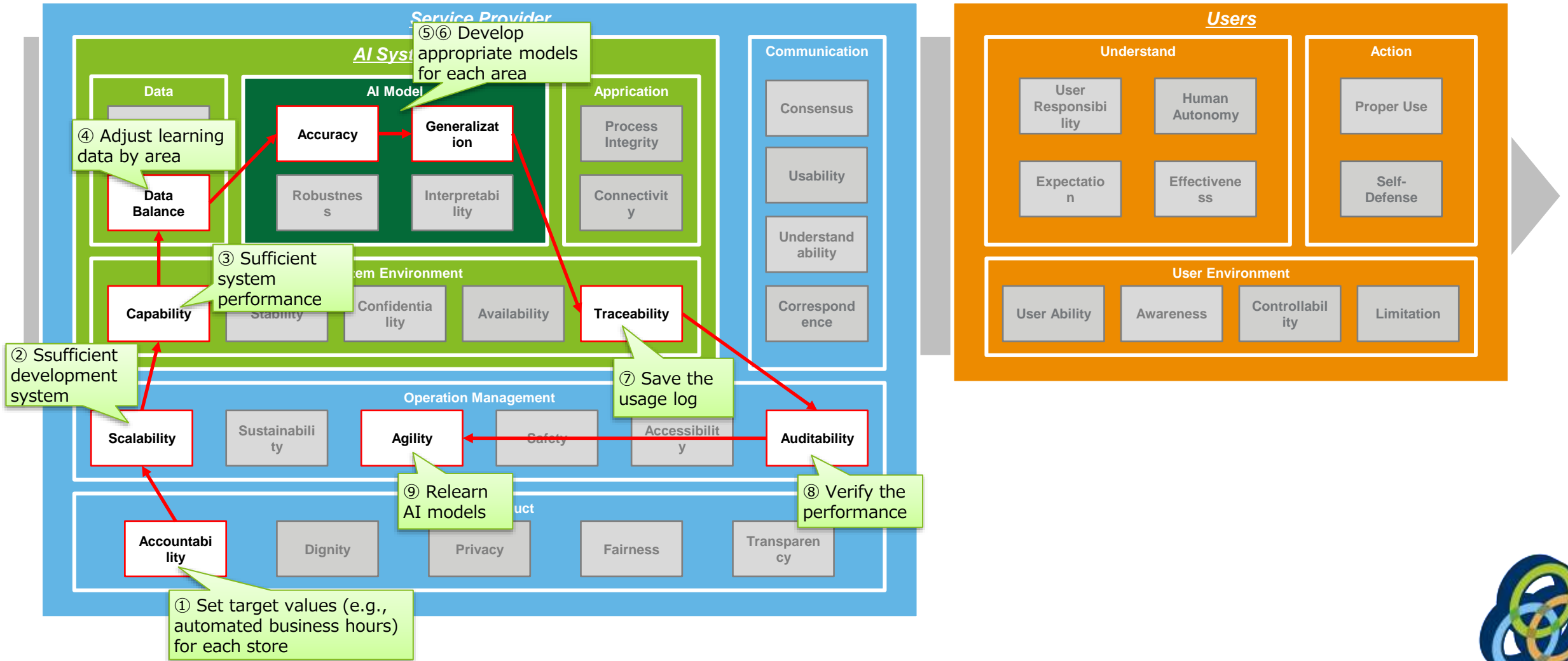
Control Coordination

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

R012

Expansion of services

When opening a store in a new country or region, the predictive performance of AI cannot respond to changes in customer base or products



Risk Control

- Consider risk control according to the risk chain -

R012

Expansion of services

When opening a store in a new country or region, the predictive performance of AI cannot respond to changes in customer base or products

Risk Control		
AI system (AI Dev Dept., Co. J & Co. X (Contractor))	AI Service Provider (Convenience Store Business Dept., Co. J)	User (Customer)
<p>③ [Capability] Prepare an environment that can execute learning models for each region of the store (AI Dev Dept., Co. J)</p> <p>④ [Data Balance] Adjust the percentage of learning data (e.g., users and products) by area (Co. X)</p> <p>⑤ [Accuracy] Develop models with appropriate prediction accuracy for each area (Co. X)</p> <p>⑥ [Generalization] Develop models with appropriate generalization performance for each area (Co. X)</p> <p>⑦ [Traceability] Saving log information of customer and purchase information (IT Dept., Co. J)</p>	<p>① [Accountability] Set appropriate target values (e.g., automated business hours) for each store (Convenience Store Business Dept., Co. J)</p> <p>② [Scalability] Ensuring sufficient development systems to provide services in line with the number of stores (Convenience Store Business Dept., Co. J)</p> <p>⑧ [Auditability] Periodic verification of the performance of each model (Convenience Store Business Dept., Co. J)</p> <p>⑨ [Agility] Requesting relearning of AI models to ensure necessary accuracy (Convenience Store Business Dept., Co. J)</p>	



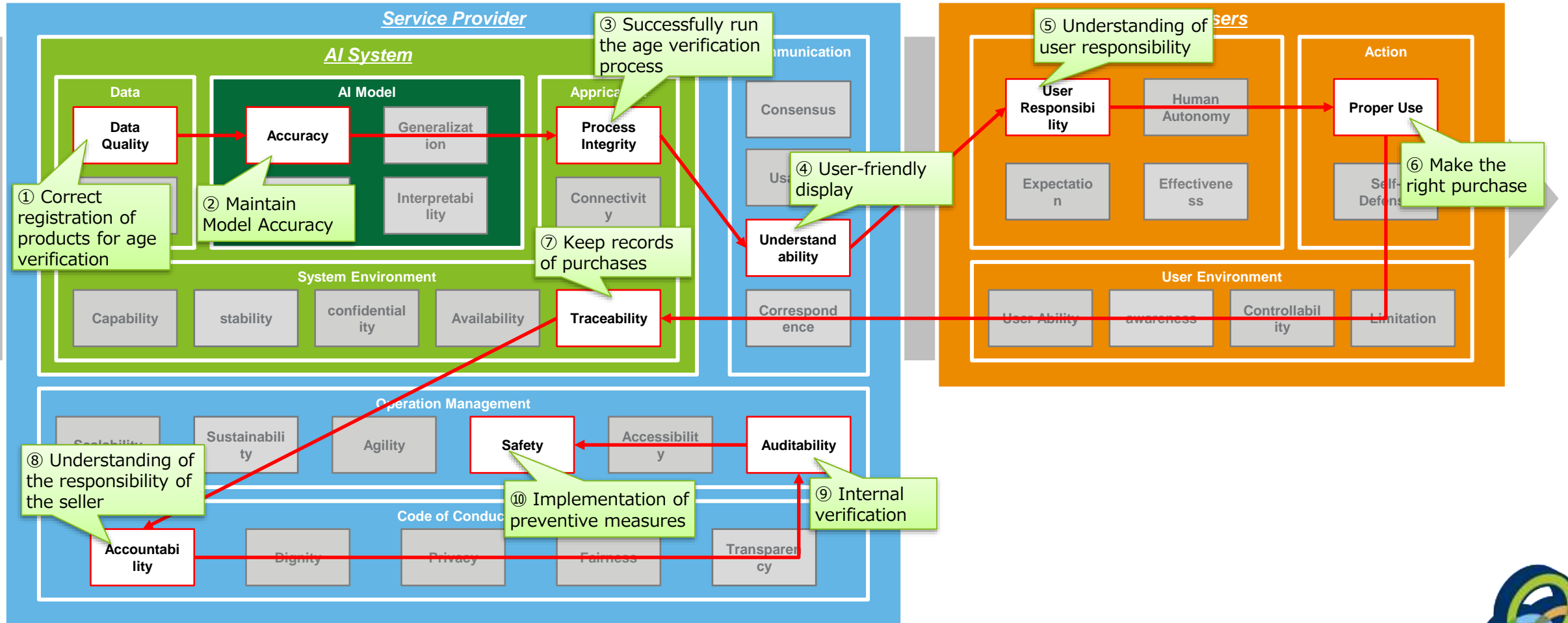
Control Coordination

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

R013

Age verification

Age verification is not properly conducted when selling alcohol, cigarettes, etc



Risk Control

- Consider risk control according to the risk chain -

R013

Age verification

Age verification is not properly conducted when selling alcohol, cigarettes, etc

Risk Control		
AI system (AI Dev Dept., Co. J & Co. X (Contractor))	AI Service Provider (Convenience Store Business Dept., Co. J)	User (Customer)
<p>① [Data Quality] Correct registration of products that requires age verification (Convenience Store Business Dept., Co. J)</p> <p>② [Accuracy] Ensure model accuracy (Co. X)</p> <p>③ [Process Integrity] Perform age verification processing when selecting products that require age verification (AI Dev Dept., Co. J)</p> <p>⑦ [Traceability] Saving log information of customer and purchase information (IT Dept., Co. J)</p>	<p>④ [Understandability] Display products requiring age verification in an easy-to-understand manner (Convenience Store Business Dept., Co. J)</p> <p>⑧ [Accountability] The distributor shall be responsible for educating minors not to sell alcohol or cigarette improperly (Convenience Store Business Dept., Co. J)</p> <p>⑨ [Auditability] Internal verification of purchases of products requiring age verification (including model misrecognition) on a regular basis (Internal Audit Dept., Co. J)</p> <p>⑩ [Safety] If sales of alcohol, cigarette, etc. to minors are frequent, necessary measures (e.g., prohibition of customers from entering the store/relearning models) will be taken (Convenience Store Business Dept., Co. J /legal Dept., Co. J)</p>	<p>⑤ [User Responsibility] Posting that minors are prohibited from using alcohol or cigarette (Stores)</p> <p>⑥ [Proper Use] Make appropriate purchases (Customer)</p>



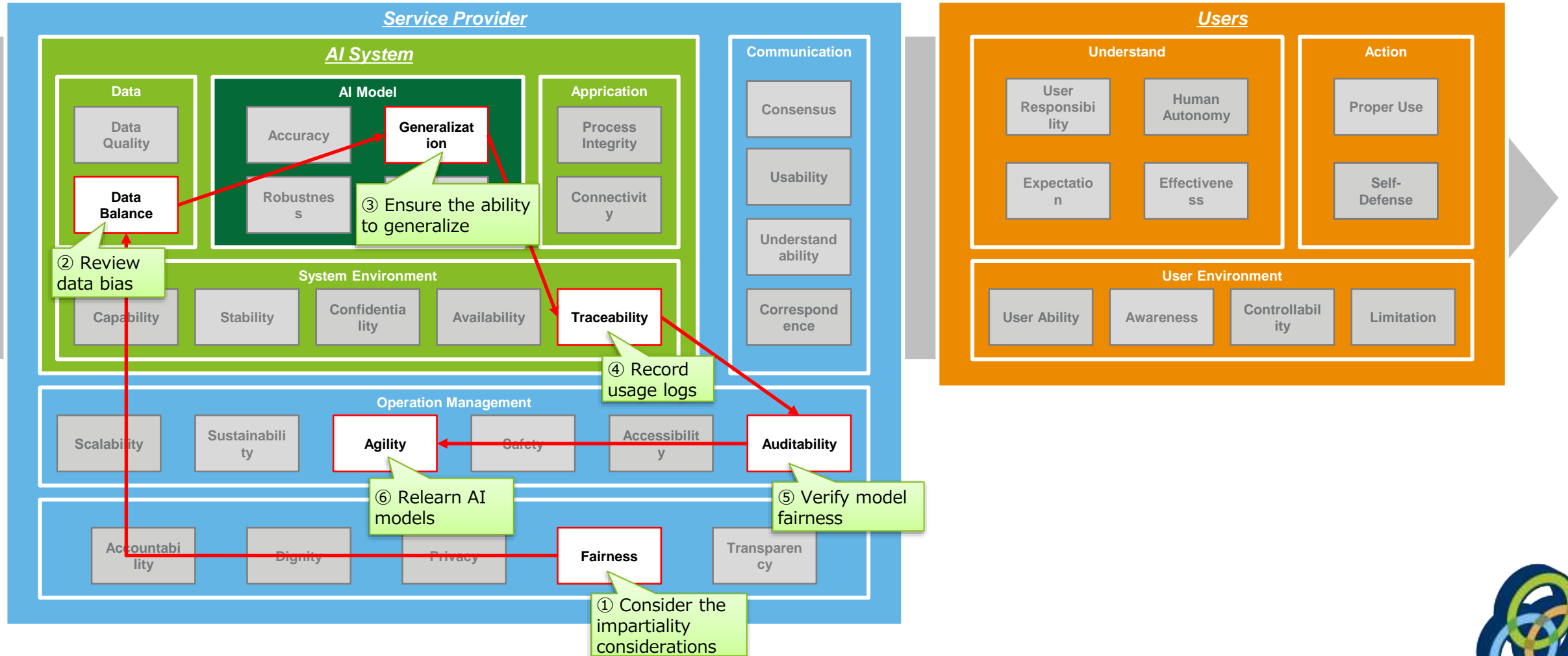
Control Coordination

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

R015

Fairness

Produces unfair predictions for specific countries/regions/races/genders/ages



Risk Control

- Consider risk control according to the risk chain -

R015

Fairness

Produces unfair predictions for specific countries/regions/races/genders/ages

Risk Control		
AI system (AI Dev Dept., Co. J & Co. X (Contractor))	AI Service Provider (Convenience Store Business Dept., Co. J)	User (Customer)
<p>② [Data Balance] Review data bias (Co. X)</p> <p>③ [Generalization] Review the generalization performance of the model (Co. X)</p> <p>④ [Traceability] Saving log information of customer and purchase information (IT Dept., Co. J)</p>	<p>① [Fairness] Defining Fairness Points to Consider (Convenience Store Business Dept., Co. J)</p> <p>⑤ [Auditability] Periodic verification of model fairness (Convenience Store Business Dept., Co. J)</p> <p>⑥ [Agility] Requesting relearning of AI models to ensure fairness (Convenience Store Business Dept., Co. J)</p>	

