Advancing AI Audits for Enhanced AI Governance

AI Audit Study Group, AI Governance Project
Technology Governance Policy Research Unit
Institute for Future Initiatives, The University of Tokyo

東京大学未来ビジョン研究センター

Institute for Future Initiatives
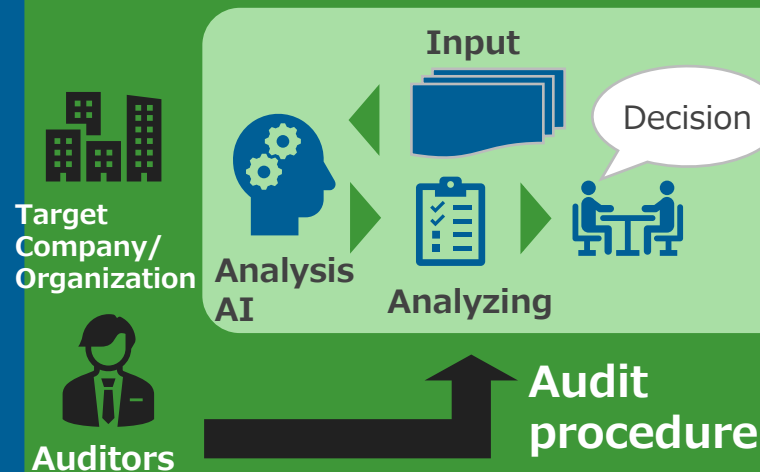The University of Tokyo

Agenda

Our target is Audit for AI. Not AI used in audit

The premise of wording "AI Audit" in our policy recommendation
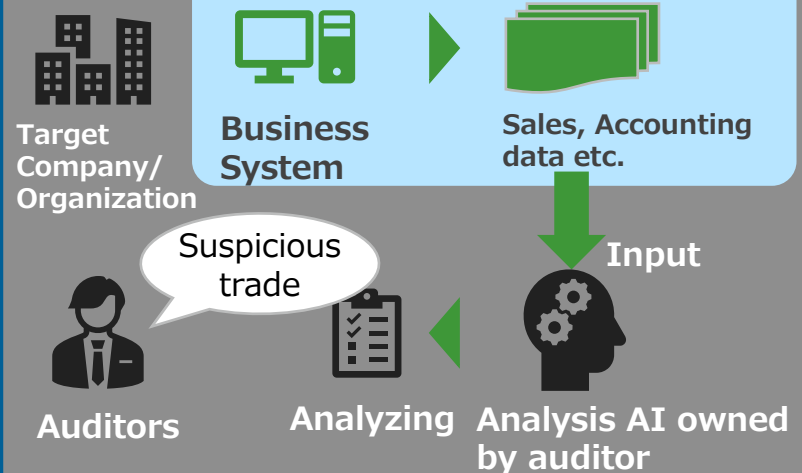

AI Audit - **Topics in the context of AI and Audit**

Audit for AI
- **Perform Audit procedures for AI services and systems**

Target Company/Organization

Auditors

Analysis AI

Input

Decision

Analyzing

Audit procedure

Our target

AI Used in Audit
- **Using AI service or system in our current audit procedures**

Target Company/Organization

Business System

Sales, Accounting data etc.

Auditors

Suspicious trade

Analyzing

Input

Analysis AI owned by auditor

Out of our scope

1. The Need for Summarizing AI Audit Issues

Without common understanding, misunderstanding occurs

1. The Need for Summarizing AI Audit Issues

Alex: AI audit is to perform audit procedures efficiently and effectively with using AI technology

Bob: I want to discuss internal audit for our sensor using deep learning technology to confirm excess or not certain threshold.

Chris: Our bank client introduced machine learning model for their loan execution judgement. We plan to external audit for their internal controls.

- If they discuss AI audit, including audit procedures and timing, it doesn't work properly. In order to have effective discussion, we have to be on the same page and clarify what we are discussing.

- <u>**This report is intended to summarize the issues related to AI auditing and to establish a common foundation for discussing critical issues among the parties concerned.**</u>

2. Issues Related to AI Audits

Introduce several issues related to AI audits for discussion

2. Issues Related to AI Audits

The necessity for AI auditing	Currently, there is no regulation to mandatory require AI audit in Japan. However, people have much concerns for AI audit to use AI service safely
AI Audit Proof Propositions	We use the term "proof propositions" to describe what should be considered audit topics when conducting an audit. Considering AI specific concerns, it's hard to address them with only current standards / criteria.
AI Audit Scope	The AI systems and services' audit scope can be classified into two categories: auditing individual AI services and systems and auditing the internal controls implemented in organizations that provides AI services
Timing of AI Audits	We classifies the AI lifecycle into four phase: (1)new development, (2)functional change or additional development, (3)operation and (4)disposal. Identified audit timing based on audit categories.
AI Audit Practitioner Requirement	The AI audit practitioner requirements are presented from the perspectives of (1) expertise requirements, (2) independence requirements, (3)organizational requirements, and (4) legal responsibilities of the auditor.
AI auditing Parties and Organizations Involved	Auditors and audited companies are not the only parties involved in auditing AI services and systems. We organized relevant parties with charts.

Traditional audit proof propositions are not enough to cover all AI audit specific needs

2. Issues Related to AI Audits – AI Audit Proof Propositions #1

Examples of audit proof propositions of traditional service and system audit

	Proof Propositions	Standard / Criteria example
IT audit in part of financial statement audit	Risks arising from the use of IT are appropriately reduced to reflect their financial status on financial statements accurately and completely (Accuracy and Completeness). (*)	International Standard on Auditing (ISA) 315
SOC2 report assurance	Security / Availability / Process Integrity / Confidentiality / Privacy	Trust Service Criteria
Internal audit	Governance process, risk management and control validity and effectiveness	International Standards for the Professional Practice of Internal Auditing(IPPF) Japanese system audit standard

Part of them can be used for AI audit but not enough to cover all AI audit specific needs

(*)Management assertions like existence and completeness are applicable for entire financial statement audit proof propositions. However, we listed accuracy and completeness of the process as a representative of automated control assertion in this table.

Common understanding are needed because our discussion are much different based on AI audit specific proof propositions

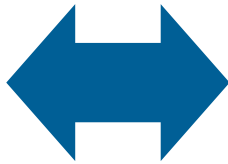## 2. Issues Related to AI Audits – AI Audit Proof Propositions #2

Proof Propositions that are unique to AI audit (Example)

AI Principle

Items frequently appear in various guidelines

Consumer fears in using AI service

etc.

Proof Propositions	Explanation
Fairness	• Is there any inappropriate bias in the output results of the AI system, etc.? • It is required to have a common understanding of the definition of fairness beforehand.
Transparency	• Can the output results of the AI system be reproduced, and can the training data and feature values be explained, etc.?
Safety	• Is there any possibility that the AI system may harm the user? If a problem occurs, does the system properly transition to a halted state etc.? • Hardware in which AI systems are embedded should also be considered.
Security	• Can attacks on training data be prevented or detected? • Can production input data that intentionally induce inappropriate output be prevented etc.?
Privacy	• Can individuals refuse to attribute data they do not wish to share? • Can erroneous personal assessments be corrected in a timely and appropriate manner etc.?

- Audit procedures and criteria are much different depending on each proof propositions. Hence, Common understanding are needed in auditing and discussion.

- Only current standards / criteria are not enough to cover all proof propositions.

Expected AI audit scope are different depending on the background

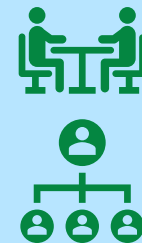## 2. Issues Related to AI Audits – AI Audit Scope #1

AI Audit - **Topics in the context of AI and Audit**

Audit for AI - **Perform Audit procedures for AI services and systems**

Auditing AI services and systems

Audits of internal controls in organizations that provide AI services and systems
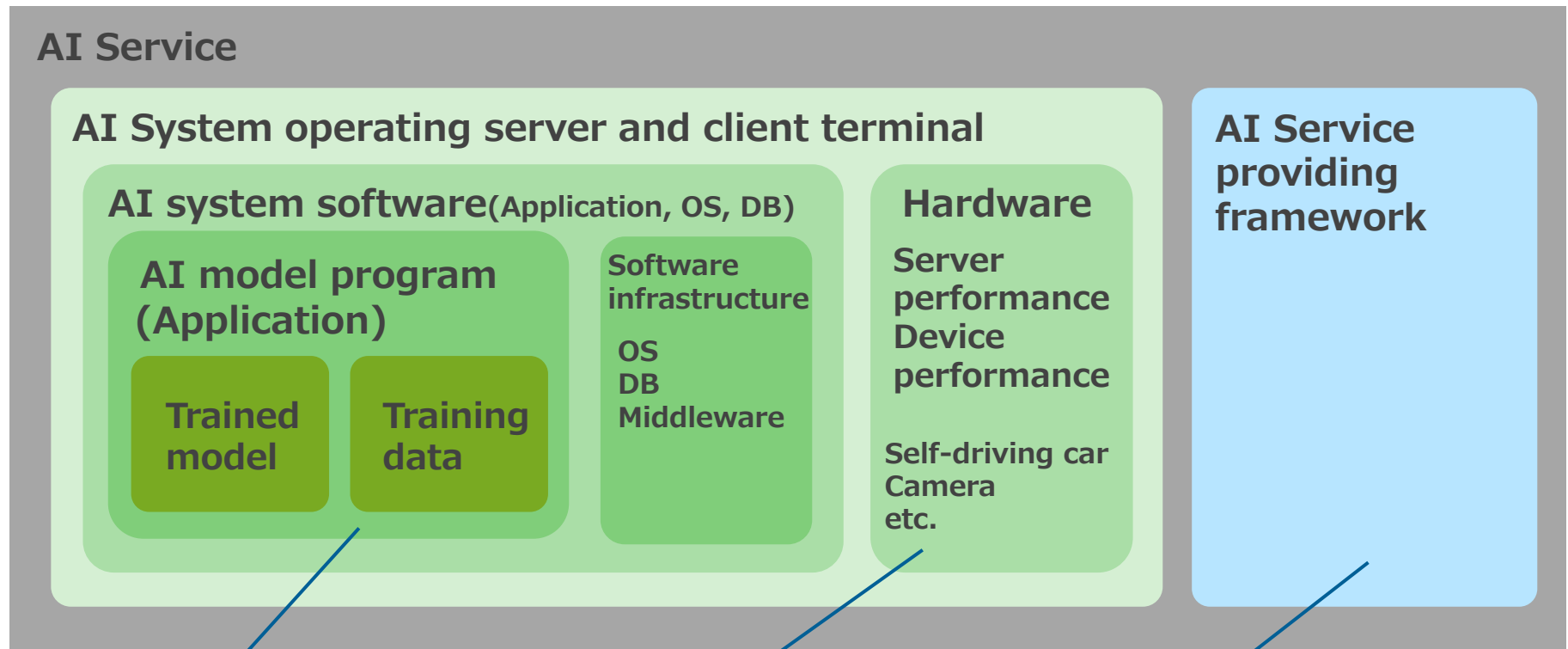
Mixed approach is acceptable

AI Used in Audit
- Using AI service or system in our current audit procedures
- (Example) Detecting suspicious trades from numerous trade data
- Out of our scope

Auditing AI services and systems

2. Issues Related to AI Audits – AI Audit Scope #2

AI Service

AI System operating server and client terminal

AI system software(Application, OS, DB)

AI model program (Application)

Trained model

Training data

Software infrastructure

OS
DB
Middleware

Hardware

Server performance
Device performance

Self-driving car
Camera
etc.

**AI Service providing framework**

Need to expand traditional application audit such as audit for data governance, algorithm auditing etc.

In addition to traditional issues like server hardware performance and physical security, need to consider device performance which is close to AI output accuracy and performance.

- **Appropriate disclosure about using AI for users**
- **Appropriate explanation about collected information**

Need to consider service providing framework too.

Audits of internal controls in organizations that provide AI services and systems

2. Issues Related to AI Audits – AI Audit Scope #3

AI service and system
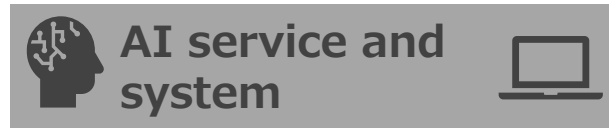
Organization that provide AI services and systems
- Management, User division and system developing or operation team

**Structure
Policy**

**Rule
Guideline**

**Daily operation
Following rule**

Entity level control for entire organization

**AI utilize policy
Education structure etc.**

Individual work level control
Test and approval before release
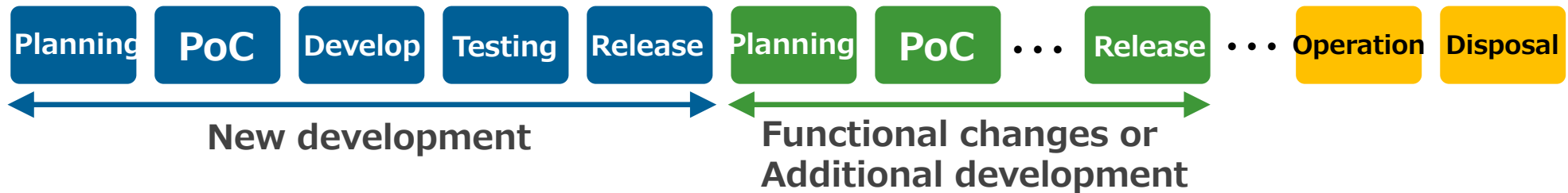**Confirmation for training data validity
etc.**

Design and operate each control

Framework like COSO and COBIT

(*)COSO : Internal control framework from by Committee of Sponsoring Organizations of the Treadway Commission
COBIT : Entity information and technology framework by ISACA and ITGI

Need to AI specific consideration when determine audit timing

2. Issues Related to AI Audits – Timing of AI Audits

AI life cycle

| Planning | PoC | Develop | Testing | Release | Planning | PoC | ... | Release | ... | Operation | Disposal |

New development · **Functional changes or Additional development**

Issues around timing of AI audits

> Performance updates with continuous training
> - Performance and accuracy may differ between the AI output results at the timing of the audit procedure and AI output results when such results are used.
>
> Timing difference based on audit scope and auditor
> - Timing differs depending on audit scope (AI services / systems or internal control) and auditor (internal audit or external audit).
> - In providing AI services, the appropriateness of the service itself and the appropriateness of decisions on whether or not development is necessary are also important issues. Therefore, external audits that include the planning and PoC phases may be considered necessary.

In addition to AI specific knowledge as requirement, AI auditor certification and organization accreditation should be considered

2. Issues Related to AI Audits – AI Audit Practitioner Requirements

|	Expertise requirements	Independence requirements
Internal audit External audit	• An understanding of audit theory, industry knowledge related to the audited company and the services it provides, and knowledge and experience in IT areas not limited to AI. • Deep AI specific technical knowledge, and ethical, cultural, legal, and regulatory expertise. New certification program should be considered too. • The requirements for those conducting AI audits are very high, and an individual is unlikely to possess all the skills and experience required for AI auditing.	• As with traditional audits, AI audits must be conducted by independent practitioners and organizations that have no conflict of interest with the audited company or department. • Independence requirements are defined for both external and internal audits.
	Organizational Requirements	**Legal responsibility of the auditor**
External audit	• The organization conducting the audit must meet certain quality and independence standards. • The certification and accreditation system for the organization, as well as the organization and its role in conducting monitoring, must be considered. • Notably, the audit results conducted by an organization that does not meet these standards may not credibly reflect the actual situation.	• The scope of AI audit practitioner's legal liability with due care. • If the responsibility of AI audit practitioners is too burdensome, very few would be willing to conduct the audits. • The need for exemption requirement or insurance system to protect AI audit practitioners

Many internal and external parties are relevant to audit, assurance and certification for AI

2. Issues Related to AI Audits – AI auditing Parties and Organizations Involved
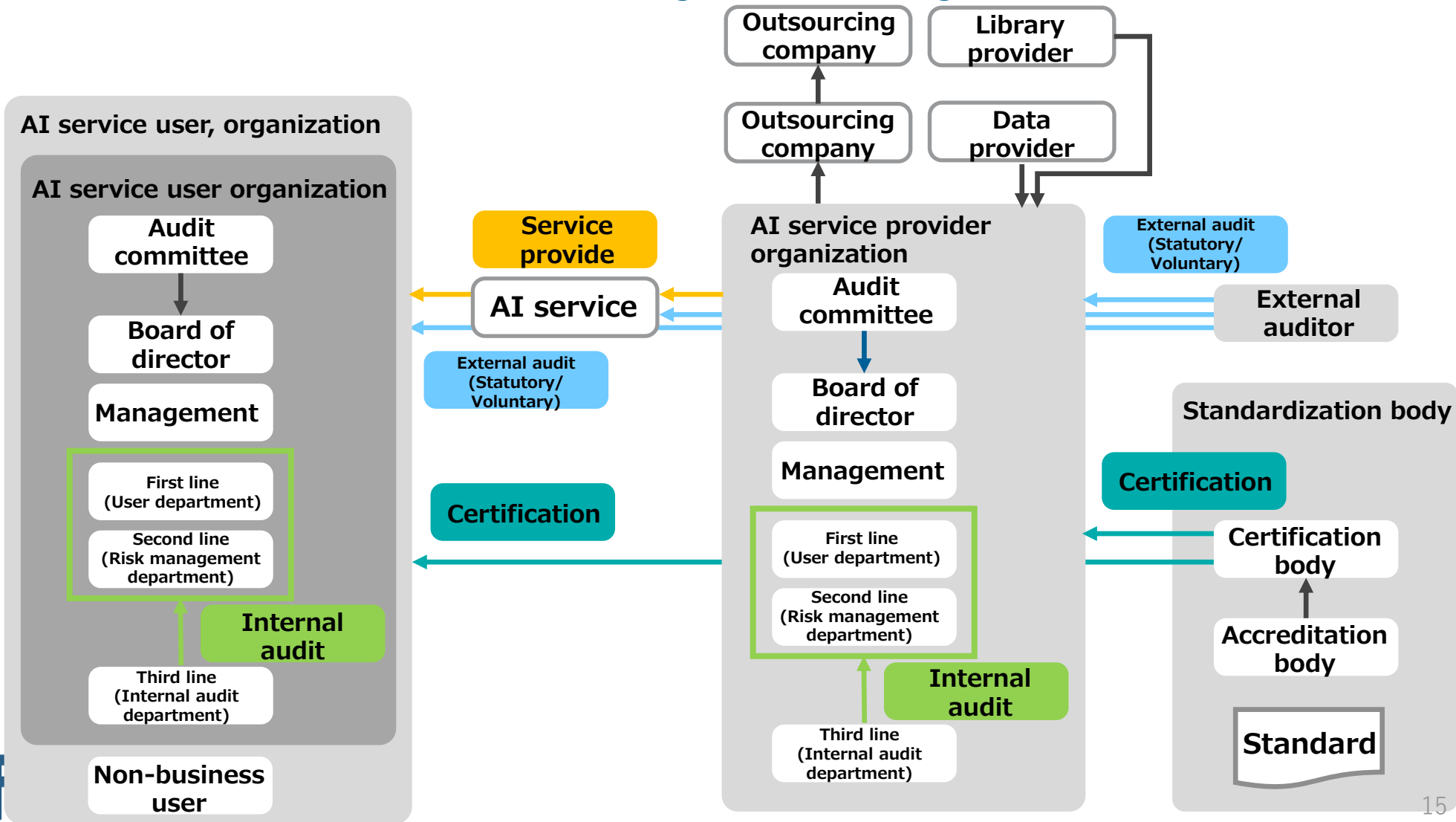
Many internal and external parties are relevant to audit, assurance and certification for AI

2. Issues Related to AI Audits – AI auditing Parties and Organizations Involved
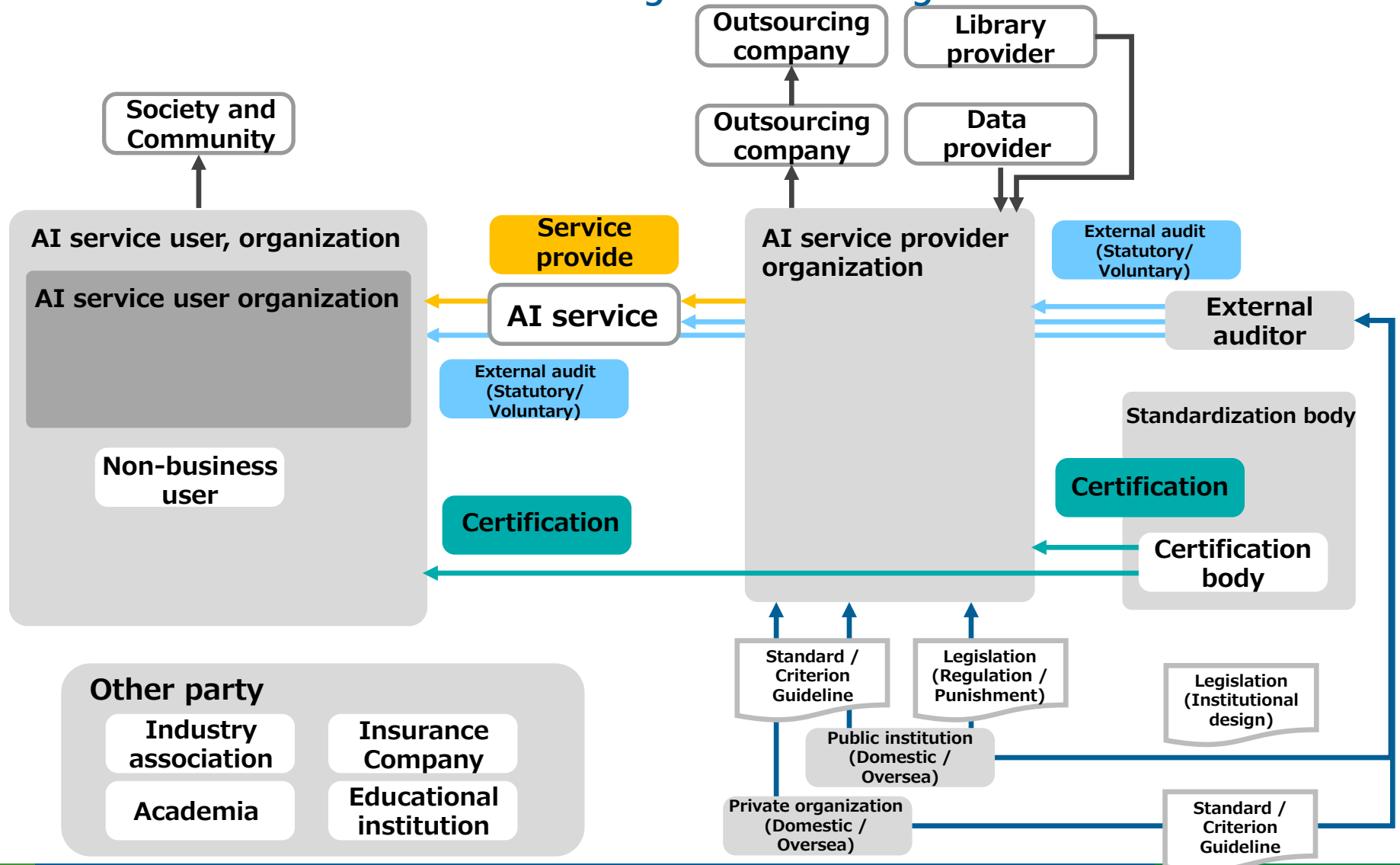
3. Factors that make AI Audits Difficult

Complicated technical, institutional, and social factors make auditing AI services and systems difficult

3. Factors that make AI Audits Difficult

- Underdevelopment of institutional design for AI audits

- Complexity arising from the scope of audited entities

- Imbalance between demand and supply for AI audits

- Difficulties in Setting Performance Standards for AI Audits

Institutional factors

Technical factors

Social factors
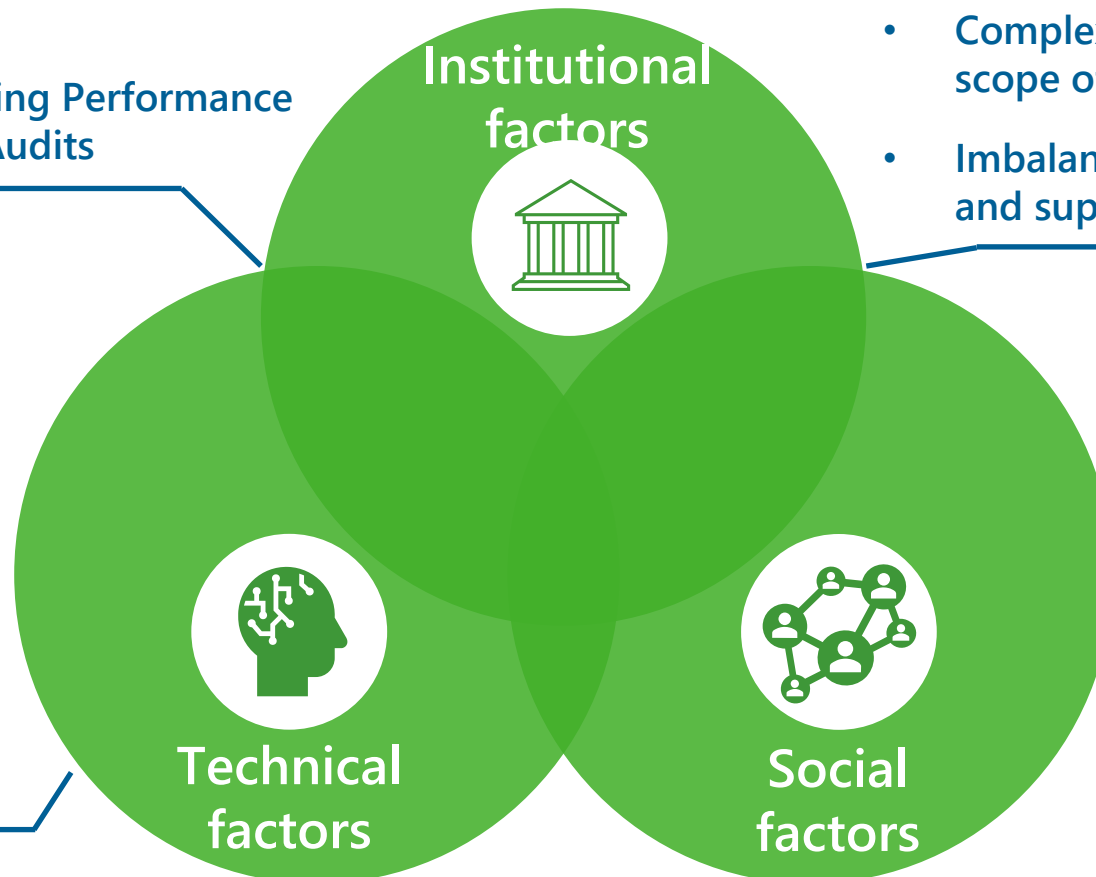
- Complexity of AI Technology

Steady discussion for resolving each factor is necessary to realize AI audit

3. Factors that make AI Audits Difficult

Complexity of AI Technology

- Unlike current IT systems, AI systems are not designed to output pre-defined unique values.
- In the development of AI systems, the logic of decision-making is often black boxed, and it is difficult to verify the logic.
- Some AI services and systems conduct continuous learning. In this case, an evaluation at the time of the audit may differ from an evaluation when the audit results are used.

Underdevelopment of institutional design for AI audits

- AI-specific general standards had not yet been established for audit practitioner requirements and quality management systems.
- No standardized criteria or standards of practice (performance standards) had yet been established for audit procedures, leaving auditors to design their own procedures and judge the audit results.
- There are no unified rules concerning with which domestic and international rules, management, auditors, certification bodies, and other parties must comply.

Difficulties in Setting Performance Standards for AI Audits

- Some proof propositions, including fairness, are difficult to define precisely and difficult to verify.
- Trade-offs can be assumed between the audit's proof propositions. It's difficult to cover multiple audit perspective with one audit procedure.
- When considering the training data governance effectiveness, it's difficult to set sufficiency indicators and potential biases in such data.

Steady discussion for resolving each factor is necessary to realize AI audit

3. Factors that make AI Audits Difficult

Complexity arising from the scope of audited entities

- Because there are many cases that lots of companies are involved in development as our sourcing companies, it's difficult to set audit scope organization. In addition, contractual obligation and audit fee burden issues also should be considered.

- If they prepare models with external library, the correct operation of AI systems is seemed to rely on these function. The audit scope becomes even broader, without the assumption that the functions provided by these libraries are functioning properly.

- If they use third party data collectors and public data providers for training data, these parties should be considered in audit scope.

Imbalance between demand and supply for AI audits

- A huge gap may develop between the requirements of AI audits from society and actual audit result.

- Considering the efforts for performing AI audit, legal responsibility of the auditor and audit fee the auditors receive, they can be imbalanced. In such case, there is little incentive for external auditor to undertake such work.

- Lack of incentives for audited companies to undergo AI audits because there are none or little legally binding regulation with penalty.

To perform AI audits is difficult because of complicated factors. However, considering AI audit demand from expanding AI use cases, discussion in oversea and activities for international rule setting, it's better to proceed discussion as much as we can

4. Future issues and recommendations on AI auditing

We hope that this paper will contribute to realizing responsible AI development and operation by AI system and service companies, and a society in which AI can be used safely and trustfully

4. Future issues and recommendations on AI auditing

1
Development of institutional design for AI audits
Institutional design for AI audits to meet the demands has not been prepared. Considering increasing international demands, further discussion is needed.

2
Training human resources for AI audits
Conducting an AI audit requires diverse expertise with a wide range of skills and experience. To meet the demands, training AI auditors and their new certification should be discussed.

3
Updating AI audits in accordance with technological progress
Technical research related to AI is flourishing around the world, and new services and systems are emerging daily. the AI audit institutional design, standards and methods must be updated to avoid obsolescence.

Our policy recommendation consists of lots of topics

The contents of our paper

Chapter 1	Toward AI Audits that Contribute to AI Governance	Introduction
Chapter 2	Issues Related to AI Audits	Issues
Chapter 3	Factors that make AI Audits Difficult	
Chapter 4	Assumed AI audit case study: Recruitment AI	Practice
Chapter 5	Future issues and recommendations on AI auditing	Summary
Chapter 6	Toward a society that can use AI safely and trustfully	
Appendix	AI Auditing and Generative AI	Appendix

Reference URL

AI監査ガバナンスに資するAI監査の実践に向けて

https://ifi.u-tokyo.ac.jp/news/16814/

Advancing AI Audits for Enhanced AI Governance

https://ifi.u-tokyo.ac.jp/en/news/12034/

About the AI audit study group

This policy recommendation is the result report of the AI Audit Study Group, a study group of the AI Governance Project, a project of the Technology Governance Research Unit of the Institute for Future Initiatives, The University of Tokyo. The AI Audit Study Group started its research activities in June 2022 and consists of the following members.

- Arisa Ema（Associate Professor, Institute for Future Initiatives, The University of Tokyo）

- Ryo Sato（Visiting Researcher, Institute for Future Initiatives, The University of Tokyo / Deloitte Touche Tohmatsu LLC）

- Tomoharu Hase（Visiting Researcher, Institute for Future Initiatives, The University of Tokyo / Deloitte Touche Tohmatsu LLC）

- Masafumi Nakano（Visiting Researcher, Institute for Future Initiatives, The University of Tokyo / The University of Toyo）

- Shinji Kamimura（Deloitte Touche Tohmatsu LLC）

- Hiromu Kitamura（CDLE, AI Legal (NEC) / IRCA (International Register of Certified Auditors) "Japan" Members Supporter）

Acknowledgements

Many people provided valuable advice in the writing of this policy recommendation. Due to time constraints and organizational affiliations, we are unable to include all their names, but acknowledge and thank them for the useful feedback.

The opinions expressed in this presentation are the opinions of this study group and not those of the entities to which members belong.