Provisional Translation

Digital Society Promotion Standard Guidelines DS-920

The Guideline for Japanese Governments' Procurements and Utilizations of Generative AI for the sake of Evolution and Innovation of Public Administration

May 27, 2025
Approved by the Council for the Promotion of a Digital Society
Executive Board Meeting

[Positioning of this Document]

Normative

A document specifying the rules to be adhered to regarding the development and management of government information systems.

[Keywords]

Generative AI, Large Language Models (LLM), Policy for the Utilization of Generative AI in Government, AI Governance Framework (Generative AI Projects, High-Risk Generative AI, Advanced AI Utilization Advisory Board, Chief AI Officer (CAIO), Risk Management in the Procurement and Utilization of Generative AI (Planning, Procurement, Development and Operation, Utilization, Addressing Risk Cases Particular to Generative AI Systems)

[Outline]

This guideline aims to boost the use and secure risk management of generative AI in the Japanese Government, by preparing propelling measures and setting proper rules for the Japanese Government's governance, procurement, and utilization of generative AI.

Revision History

Date of Revision	Revised Section	Details of Revision
May 27, 2025	-	・First Edition

Table of Contents

1 Introduction

1.1 Background

AI-related technologies are developed day by day, with their utilization rapidly advanced in both public and private sectors in ways that foster innovation in industry and address social issues.

Under these circumstances, the G7 Summit was held in Japan in 2023 aiming to promote safe, secure, and trustworthy AI. The G7 Summit, chaired by Japan, concluded "The Hiroshima Process International Guiding Principles for Organizations Developing Advanced AI System",[1] "The Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI Systems"[2] and "The Hiroshima Process International Guiding Principles for All AI Actors".[3] AI governance is actively discussed in multinational frameworks such as the United Nations, the Council of Europe and the OECD. Furthermore, government bodies in various countries are also actively promoting the use of AI, while managing potential risks and setting rules to ensure proper AI governance across government operations.

To respond promptly and flexibly to social changes by embracing the use of new technologies, the Japanese Government has been taking measures to promote the safe and secure use of AI. This includes the publication of the AI Guidelines for Business Ver 1.1 (by the Ministry of Internal Affairs and Communications; Ministry of Economy, Trade and Industry on November 22, 2024. Hereinafter referred to as the AI Guidelines for Business),[4] which aims to support voluntary efforts by businesses and other entities.

The Priority Plan for the Advancement of a Digital Society (approved by the Cabinet on June 21, 2024) stated that AI would create a virtuous circle to accelerate innovation and that it is necessary to manage various risks associated with AI, including generative AI, and to ensure a safe and secure environment. The plan also stated that rules serving as guardrails to ensure the safety and security of AI use are also necessary, for the sake of promoting innovation as well.[5]

Moreover, ministries and agencies are considering utilizations of generative AI in

[1] Hiroshima Process International Guiding Principles for Organizations Developing Advanced AI System
https://www.mofa.go.jp/files/100573471.pdf
[2] Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI Systems
https://www.mofa.go.jp/files/100573473.pdf
[3] Hiroshima Process International Guiding Principles for All AI Actors
https://www.soumu.go.jp/hiroshimaaiprocess/pdf/document03_en.pdf
[4] AI Guidelines for Business Ver 1.1
https://www.soumu.go.jp/main_content/001002576.pdf
[5] Priority Plan for the Advancement of a Digital Society
https://www.digital.go.jp/en/policies/priority-policy-program

different tasks and works. The Digital Agency hosts AI Ideathon and Hackathons, which aim to solve administrative issues by using AI, and implements various projects to experiment generative AI system utilizations. Through these initiatives, use cases are discovered and verifications are carried out by trial environments, for achieving practical uses of AI across the government.

This guideline aims to boost uses and secure risk management of generative AI[6] in the Japanese Government, by setting scheme for AI governance, framework for sharing best practices, and the considerations regarding risks associated with the procurement and utilization of generative AI within the government. This guideline also shows a scheme for totally enhancing functionality, quality, and cost-effectiveness of generative AI systems utilized by the government. This guideline is formulated for the uses by national government staffs, in a manner consistent and compatible with existing guidelines, such as the AI Guidelines for Business and the "Common Standards for Cybersecurity Measures for Government Agencies and Related Agencies," [7] while taking into consideration the regulatory trends of foreign governments in relation to AI.

1.2 Positioning of this Guideline

This guideline is positioned as one of the documents to be adhered to as a normative standard within the Digital Society Promotion Standard Guidelines.[8]

1.3 Definition of Terms

The terms in this guideline conform with the glossary of the standard guideline group unless otherwise specified in Table 1 and within this guideline.

Table 1: Definition of terms 1

Term	Meaning
Artificial Intelligence (AI)	An abstract concept, which includes AI systems (defined below) themselves or software or programs that perform machine learning. (Source: AI Guidelines for Business, P.9)

[6] The initial target of this guideline is text generative AI. For more information, refer to Section 2.2.2 Targeted Generative AI.
[7] Common Standards for Cybersecurity Measures for Government Agencies and Related Agencies https://www.nisc.go.jp/eng/pdf/kijyunr5-en.pdf
[8] Digital Society Promotion Standard Guidelines https://www.digital.go.jp/en/resources/standard_guidelines

Term	Meaning
Generative AI	A general term representing AI developed from an AI model that can generate texts, images, programs, etc. (Source: AI Guidelines for Business, P.10)
AI System	A system (such as a machine, robot, and cloud system) that works at various levels of autonomy during the use process and incorporates a software element that has a learning function. (Source: AI Guidelines for Business, P.9)
Generative AI System	Government Information Systems that comprise generative AI (targeted by this guideline) as a component.[9] (In accordance with Guide to Evaluation Perspectives on AI Safety (Version 1.01) by Japan AI Safety Institute, P.9)[10]
AI model	A model incorporated into an AI system and acquired through machine learning using training data. It produces prediction results in accordance with the input data. (Source: AI Guidelines for Business, P.10)
Large Language Models (LLM)	A language model that treats the probability of occurrence of sentences and words as a deep learning model, built using a very large amount of training data. (Source: Guidelines for Quality Assurance of AI-based Products and Services by Consortium of Quality Assurance for Artificial-Intelligence-based Products and Services, 10-1)[11]
AI Governance	The design and operation of technological, organizational, and social systems by stakeholders for the purpose of managing risks posed by the use of AI at levels acceptable to stakeholders and maximizing their positive impact (benefit). (Source: AI Guidelines for Business, P.10)
Risk cases particular to generative AI	A condition where risks inherent to a generative AI system have materialized, or where signs or events indicating the potential for such risks are observed, which may have significant impacts. (For more information, see Section 6.7 Addressing Risk Cases

[9] The form of government information systems may be cloud-based or on-premises.

[10] Guide to Evaluation Perspectives on AI Safety (Version 1.01)
https://aisi.go.jp/assets/pdf/ai_safety_eval_v1.01_en.pdf

[11] Guidelines for Quality Assurance of AI-based Products and Services
https://www.qa4ai.jp/download/

Term	Meaning
	Particular to Generative AI Systems)

2 Purpose and Scope of this Guideline

2.1 Purpose of this Guideline

The purpose of this guideline is to realize the three “Basic Philosophies” set forth in the “Social Principles of Human-Centric AI,” formulated by the Japanese Government in March 2019, in the procurement and utilization process of generative AI within the government. The three Philosophies are: (1) Dignity: A society that has respect for human dignity, (2) Diversity and Inclusion: A society where people with diverse backgrounds can pursue their own well-being, and (3) Sustainability: A sustainable society.

This guideline serves as a guardrail to boost the use of generative AI, aiming to achieve steady evolution of safe and secure use of generative AI by the Japanese Government, thereby realizing benefits such as:

1. Efficient and effective achievement of administrative objectives
2. Enhanced planning capabilities
3. Enhanced information gathering and analysis capabilities
4. Enhanced quality of policies, documents, and analyses developed by the government
5. Improved function and convenience of existing government information systems using generative AI
6. Enhanced functionality, quality, and cost-effectiveness of the entire generative AI utilized by the government
7. Enhanced international competitiveness and the industrial development in Japan’s AI sector
8. Enhancement of AI safety and realization of international interoperability
9. Strengthened data governance within the government

2.2 Scope

2.2.1 Information Systems Targeted by this Guideline

This guideline applies to government information systems that incorporate as components the generative AI specified in “2.2.2 Generative AI Covered by this Guideline”. However, this guideline does not apply to government information systems that handle specially designated secrets (as defined in Article 3, Paragraph 1 of the Act on the Protection of Specially Designated Secrets, Act No. 108 of 2013), critical economic security information (as defined in Article 3, Paragraph 1 of the Act on the

Protection and Utilization of Critical Economic Security Information, Act No. 27 of 2024), or information requiring classification as confidential documents according to the Guidelines on the Management of Administrative Documents (determined by the Prime Minister; first edition published on April 1, 2011). Additionally, this guideline does not apply to government information systems handling confidential information related to national security, the maintenance of public safety and order, as well as information that may potentially become confidential.

Incorporated Administrative Agencies and Designated Corporations[12] are also expected to follow this guideline when procuring and utilizing generative AI. Furthermore, local public entities are expected to refer to this guideline as needed.

2.2.2 Generative AI Targeted by this Guideline

The generative AI subject to this guideline comprises text-generating AI[13] that includes large language models (LLM) as components. (For AI systems generating both text and images, this guideline applies solely to the text generation aspect of them.)

Additionally, in terms of AI systems that generate images or videos, AI capable of performing advanced tasks (such as AI agents), and other types of AI, this guideline may be revised to cover them as needed, considering the situation of utilizations within the government and the status of domestic and international rule developments.

2.2.3 Intended Audience of this Guideline

This guideline is intended for national government staff involved in the procurement and utilization of generative AI. The types of staff assumed as readers are categorized in Table 2.

[12] Refers to "Designated Corporations," as stipulated in Article 13 of the Basic Act on Cybersecurity (Act No. 104 of 2014)

[13] For the use of AI systems and services other than text-generating AI, which are not covered by this guideline, it is desirable to refer to the AI Guidelines for Business (which cover all types of AI including non-text generating AI) and this guideline (note that this is written mainly on text-generating AI), and to implement appropriate risk measures based on these guidelines to promote utilization at each ministry or agency.

Table 2 Types of Intended users of these guidelines [14]

Types of Staff	Description	Specific Examples of the Staff
Chief AI Officer (CAIO)	A person responsible for formulating and promoting policies for the utilization of generative AI for the evolution and innovation of public administration in ministries and agencies, overseeing the utilization status and risk management within the entire organization.	Officials equivalent of Chief Information Officer or Deputy Chief Information Officer.
Planners	Individuals who plan the utilization of new generative AI, define what the operational tasks require for generative AI systems, and promote procurement, development, and utilization of them.	Government staff in departments or teams responsible for planning and procuring the utilization of generative AI for operational tasks (e.g., staff responsible for departments overseeing generative AI systems, staffs in departments planning and procuring generative AI systems, PJMO staff, etc.).
Developers	Individuals who construct generative AI systems, including the model, system infrastructure, and input/output functions of generative AI, by developing generative AI models and algorithms, collecting data (including purchases), preprocessing, and training/verifying AI models in accordance with the plan.	(In cases where development is conducted internally) Government staff responsible for developing the generative AI systems mentioned on the left (including PJMO staff).
Providers	Individuals who provide services to the	Government staff

[14] For systems provided by the Digital Agency as common features, the roles of planners, providers, and users may extend across both the Digital Agency and other ministries and agencies. However, in this case, it is necessary to clearly define the boundaries of responsibility and ensure that all parties collaborate in implementing risk management measures.

Types of Staff	Description	Specific Examples of the Staff
	government or the public by incorporating generative AI models into applications, products, existing systems, or administrative utilization processes.	responsible for operating generative AI systems utilized by government staff or the public (including PJMO staff).
Users[15]	Individuals using generative AI systems within public administrations.	Government staff using generative AI systems in general administrative tasks and various public administration fields.

Table 3 Terminology Comparison between this Guideline and the AI Guidelines for Business [16]

Guidelines	AI Guidelines for Business
Chief AI Officer (CAIO)	Business Executive Officers, including Executives
Planners	AI Developers or AI Providers
Developers	AI Developers
Providers	AI Providers
Users	AI Business Users

*Businesses that provide generative AI systems to the government under contracts are not directly subject to this guideline. Instead, government staff acting as Planners and Providers are required to ensure compliance with this guideline and actions based on it throughout procurement procedures, contracts with these businesses, supervision of contracted businesses, and cooperation with generative AI system providers.

[15] Even though this guideline is not directly applied to the users, they are required to comply with the rules related to generative AI utilization formulated by the Chief AI Officer (CAIO) and the utilization rules for each generative AI system formulated by planners, taking this guideline into account. (For more details, refer to "6.6 Matters to be Addressed by Users of Generative AI Systems in Government")

[16] Because this guideline is intended for national government uses and the AI Guidelines for Business mainly targets the private sector, meanings of these corresponding words are not always exactly the same.

2.2.4 Effective Date of this Guideline

The complete application of this guideline to government information systems shall be to generative AI systems procured and utilized from the fiscal year 2026 onward (including procurement procedures such as planning and public notices conducted before the end of March 2026 for the fiscal year 2026 projects). Alignment with this guideline shall also be requested for generative AI systems procured and utilized in fiscal year 2025.

Considering the advancement of generative AI utilization across various ministries and agencies, initiatives related to "4. Boosting the Use of AI and Establishing Structures for Strengthening and Promoting AI Governance" shall also be initiated from the fiscal year 2025.

This guideline evolves and integrates the framework of the Japanese Government's proper grasp of generative AI as established by the “Agreement on the Use of Generative AI such as ChatGPT (Version 2.1),” from the perspective of promoting both risk management and utilization. This guideline will replace the previous agreement.

3 Policy for the Government’s Utilization of Generative AI

3.1 Government Policy for utilizations of Generative AI

Utilizations of generative AI in the government involve risks such as information leakages and generation of inappropriate expressions. On the other hand, utilizations of generative AI have potentials of realizing efficiency and sophistication of various administrative tasks and procedures, which can significantly advance the evolution and innovation of public administration, including reforms of work style and improvements in public services. Furthermore, it is crucial for the government to take the lead in utilizing AI in order to promote its safe and secure uses across society and enhance international competitiveness of Japan's AI industry.

To this end, each ministry or agency shall actively consider integrating generative AI into their operations while undertaking the following measures:

(1) Each ministry or agency shall work to strengthen AI governance by such means as establishing a framework for the control and supervision of AI systems, for example, by appointing a Chief AI Officer (CAIO).

à Refer to “4. Boosting the Use of AI and Establishing Structures for Strengthening and Promoting AI Governance.”

(2) All individuals involved in the procurement and utilization of generative AI within each ministry or agency shall understand both the benefits and risks of generative AI.

à Refer to “5. Boosting the Use of Generative AI with an Understanding of Benefits and Risks.”

(3) Individuals involved in the procurement and utilization of generative AI within each ministry or agency shall understand measures for mitigating the risks associated with generative AI. They should implement appropriate risk countermeasures and enhance the effectiveness of generative AI utilizations by improving the quality of generative AI systems and optimizing methods of utilizing them.

à Refer to “6. Government Rules for the Procurement and Utilization of Generative AI.”

When undertaking the above measures, in order to steadily promote the utilization of generative AI throughout the government, firstly, each ministry or agency shall swiftly implement generative AI utilizations in areas considered to have lower risk, such as internal administrative tasks.

Secondly, even for generative AI utilizations that may pose relatively high risks (refer to “3.2 Approach to High-Risk Generative AI Utilization”), initiatives that contribute to the evolution and innovation of public administration shall be supported in ways that such generative AI utilizations are realized in as safe and effective as possible manner by taking appropriate risk countermeasures.

To this end, each ministry or agency shall proactively promote the utilization of generative AI in ways that contribute to the evolution and innovation of public administration, while conducting risk assessments tailored to specific use cases. Regarding generative AI utilization that are likely to pose high risks, they shall report the content of projects, risk mitigation measures, and quality assurance plans to the “Advanced AI Utilization Advisory Board.” The “Advanced AI Utilization Advisory Board” will provide advice considering status of internal and external AI utilizations in governments, including cases of best practice, development of rules, and establishment of evaluation methods for generative AI systems.

Furthermore, each ministry or agency shall make efforts to identify utilization methods that contribute to the evolution and innovation of public administration and improve the functionality, quality, and cost-effectiveness of the entire generative AI system they use within each ministry or agency. As necessary, they shall effectively leverage the functions of the aforementioned “Advanced AI Utilization Advisory Board” and the “AI Consultation Desk,” which will be mentioned later.

3.2 Approach to High-Risk Generative AI Utilization

The Chief AI Officer (CAIO) of each ministry or agency shall conduct risk assessments tailored to specific utilization cases in collaboration with planners and appropriately determine the risk classification (including whether the cases are likely to be high-risk).

When determining risk classification, the Chief AI Officer (CAIO) of each ministry or agency shall make the final decision in collaboration with planners based on the results of “[Appendix 1] High-Risk AI Project Finder” (hereinafter referred to as the “High-Risk AI Project Finder”). The High-Risk AI Project Finder indicates the risk classification aligned with the risk axes presented in Table 4.

In cases where it is determined that a utilization case of generative AI system is likely to be classified as high-risk, the Chief AI Officer (CAIO) should report the case to the

"Advanced AI Utilization Advisory Board." (*Even if it is determined that a utilization case is not likely to be classified as high-risk, consultation with the Digital Agency is possible, as necessary)

Table 4: Risk Axes and Approach

Risk Axes	Description	Viewpoints
A: Scope and types of users	The degree of risk and its extent of its impact vary depending on the scope of generative AI with which to be procured/utilized. Services utilized outside government ministries and agencies, in a manner accessible from the public, are considered to pose higher risks compared to utilization by government staff within ministries and agencies. Additionally, even when used within ministries and agencies, if the service is utilized across multiple ministries and agencies, the impact range will become larger when risk is actualized; therefore, it is essential to take these factors into account.	(1) Used by citizens, etc. outside ministries and agencies (2) Used by government staff etc. within and across multiple ministries and agencies (e.g., utilization in a common government system) (3) Used by government staff etc. within a single ministry
B: Characteristics of operations using generative AI	Risks will be higher when utilizing generative AI for operations where errors could potentially have significant impacts, such as operations substantially affecting the fundamental rights and safety of citizens, operations involving confidential policy fields, operations impacting human life, physical well-being, and citizen's property, operations requiring qualifications, and operations necessitating high levels of accountability.	(1) Used in operations where errors could potentially have significant impacts (2) Not used in operations where errors could potentially have significant impacts

Risk Axes	Description	Viewpoints
C: Presence of confidential information or personal data in training generative AI, etc.	In the utilization of generative AI, there are risks associated with the training data and the data input into prompts. If confidential information or personal data is included in the training data or data input into prompts, the risk is considered to be higher.	(1) Confidentiality class-2 level information or personal data is stored or used for training by the generative AI system (2) Confidentiality class-2 level information or personal data is handled but not stored or used for training by the generative AI system (3) Confidentiality class-2 level information or personal data is not handled
D: Utilization involving the judgment by government staff on output results	The output results of generative AI are not always accurate. Therefore, risks are considered to be higher when the operation is designed to utilize generative AI without involving judgment by government staff on the output results.	(1) Utilized without government staff's judgment on the appropriateness of the generative AI system's output (2) Utilized with government staff's judgment on the appropriateness of the generative AI system's output

*Examples of cases that are highly likely to be classified as high-risk

The following examples illustrate cases that are highly likely to be classified as high-risk. These cases are not necessarily assessed solely by a single risk axis in Table 4. Instead, it is important to evaluate the risk classification from a total perspective of different viewpoints, as presented in the "High-Risk AI Project Finder." (Also refer to "How to Read the High-Risk AI Project Finder" below).

- (Example 1) A generative AI system provided outside ministries and agencies, used for operations where its malfunctions, etc. could substantially affect the rights and safety of citizens.
  <A: Scope and types of users: (1) / B: Characteristics of operations using generative AI: (1) in Table 4, Figure 1-3 → Potentially high-risk >
- (Example 2) Cases where personal data is used, and the utilization is assumed in operations that impact human life, physical well-being, and citizen's property, which may pose a risk of infringing upon rights.
  < C: Presence of confidential information or personal data in training, etc. (1) or (2), B: Characteristics of operations using generative AI (1) in Table 4, Figure 1-3 → Potentially high-risk >

*How to use the “High-Risk AI Project Finder”

The "High-Risk AI Project Finder" is a tool designed to provide a simplified suggestion of whether a case is "likely to be classified as high-risk" or "unlikely to be classified as high-risk" by responding to questions related to the four risk axes mentioned above. (Refer to “Figure 1 [Image Before Filling out the List] High-Risk AI Project Finder,” “Figure 2 [Image After Filling out the List] High-Risk AI Project Finder.”)

Figure 1: [Image Before Filling out the List] High-Risk AI Project Finder

Date of Entry	
Affiliation (Ministry/Department, etc.)	
System Name	
Name of the Person Entering the Form	

Risk Assessment Result	Please fill in the “Response” column in the table below.

■High-Risk AI Project Finder Checklist

Please verify the following checklist and fill out the response section based on assumptions at the planning stage.

Viewpoints	Checklist	Options	Response	Comments (Free Text)
A. Scope and Types of Users	Which of the following best describes the scope of uses?	(1) Used by citizens, etc. outside ministries and agencies (2) Used by government staff etc. within and across multiple ministries and agencies (e.g., utilization of generative AI in a common government system) (3) Used by government staff etc. within a single ministry (4) Undetermined at the planning stage		
B. Characteristics of Operations Using Generative AI	Which of the following best describes impacts in case of errors in the uses of the generative AI ?	(1) Used in operations where errors could potentially have significant impacts* (2) Not used in operations where errors could potentially have significant impacts (3) Undetermined at the planning stage *Operations substantially affecting the fundamental rights and safety of citizens, operations involving sensitive policy fields, operations impacting human life, physical well-being, and citizen's property, operations requiring qualifications, and operations necessitating high level of accountability.		
C. Presence of Confidential Information or Personal Data in Training Generative AI, etc.	Which of the following best describes the data and its handling in the project?	(1) Confidentiality class-2 level information or personal data is stored or used for training (2) Confidentiality class-2 level information or personal data is handled but not stored or used for training by the generative AI system (3) Confidentiality class-2 level information or personal data is not handled (4) Undetermined at the planning stage		
D. Utilization Involving the Judgment by Government Staff on Output Results	Which of the following best describes the operations in relation to the utilization of output results in administrative operations?	(1) Utilized without government staff's judgment on the appropriateness of the generative AI system's output (2) Utilized with government staff's judgment on the appropriateness of the generative AI system's output (3) Undetermined at the planning stage		

Figure 2: [Image After Filling out the List] High-Risk AI Project Finder

Date of Entry	YYYY/MM/DD
Affiliation (Ministry/Department, etc.)	○○Agency ○○
System Name	○○○○
Name of the Person Entering the Form	○○ ○○

Risk Assessment Result	Unlikely to be classified as "High-Risk"

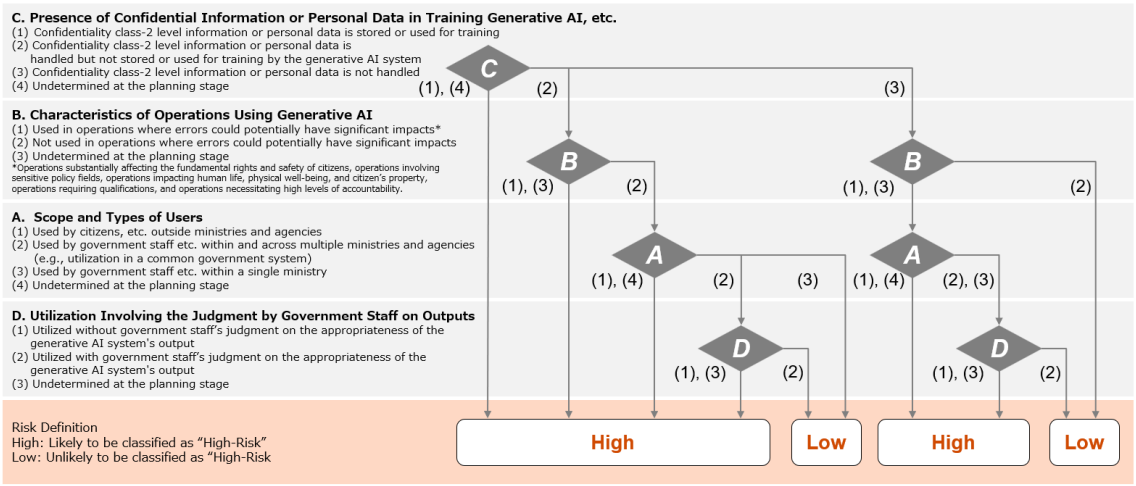
■High-Risk AI Project Finder Checklist

Please verify the following checklist and fill out the response section based on assumptions at the planning stage.

Viewpoints	Checklist	Options	Response	Comments (Free Text)
A. Scope and Types of Users	Which of the following best describes the scope of uses?	(1) Used by citizens, etc. outside ministries and agencies (2) Used by government staff etc. within and across multiple ministries and agencies (e.g., utilization of generative AI in a common government system) (3) Used by government staff etc. within a single ministry (4) Undetermined at the planning stage	2	○○○○○○○○
B. Characteristics of Operations Using Generative AI	Which of the following best describes impacts in case of errors in the uses of the generative AI ?	(1) Used in operations where errors could potentially have significant impacts* (2) Not used in operations where errors could potentially have significant impacts (3) Undetermined at the planning stage *Operations substantially affecting the fundamental rights and safety of citizens, operations involving sensitive policy fields, operations impacting human life, physical well-being, and citizen's property, operations requiring qualifications, and operations necessitating high level of accountability.	2	○○○○○○○○
C. Presence of Confidential Information or Personal Data in Training Generative AI, etc.	Which of the following best describes the data and its handling in the project?	(1) Confidentiality class-2 level information or personal data is stored or used for training (2) Confidentiality class-2 level information or personal data is handled but not stored or used for training by the generative AI system (3) Confidentiality class-2 level information or personal data is not handled (4) Undetermined at the planning stage	2	○○○○○○○○
D. Utilization Involving the Judgment by Government Staff on Output Results	Which of the following best describes the operations in relation to the utilization of output results in administrative operations?	(1) Utilized without government staff's judgment on the appropriateness of the generative AI system's output (2) Utilized with government staff's judgment on the appropriateness of the generative AI system's output (3) Undetermined at the planning stage	2	○○○○○○○○

Note that the "High-Risk AI Project Finder" is designed to facilitate the high-risk assessment based on the responses provided and in accordance with the following flow. (Refer to "Figure 3 Risk Judgment Logic.")

Figure 3: Risk Judgment Logic



4 Establishing Frameworks for Boosting Utilizations of AI and Strengthening and Promoting AI Governance

4.1 Establishing Frameworks for Boosting the Use of AI and Establishing AI Governance Structures across the Government

4.1.1 Holding the Advanced AI Utilization Advisory Bord and Operating the AI Consultation Desk

To effectively and safely promote generative AI projects across the government, the "Advanced AI Utilization Advisory Board," will be held, consisting of experts with advanced knowledge of AI rules, utilizations, risk management, and cybersecurity (assumingly including both private sector and government experts). The Digital Agency will operate the secretariat office.

The "Advanced AI Utilization Advisory Board" will be also participated by the Digital Agency and the AI Safety Institute (AISI) as board and secretariat members to operate effectively, leveraging their expertise and capabilities.

"The Advanced AI Utilization Advisory Board" will have the following roles:

- Recognizing the procurement and utilization status of generative AI in each ministry or agency
- Providing advice on evaluation and risk mitigation related to the procurement and utilization of generative AI systems by each ministry or agency, which are highly likely to be classified as high-risk
- Identifying and disseminating best practices for the procurement and utilization of generative AI in each ministry or agency
- Providing advice for identifying risk cases particular to generative AI systems in each ministry or agency and preventing their recurrence
- Providing advice on the effective utilization of generative AI in each ministry or agency, as well as on the improvement of functionality, quality, and cost-effectiveness of generative AI systems. This advice also includes listing and introducing experts and government staff with advanced knowledge and extensive experiences of AI utilization
- Considering revisions of this guideline

The "Advanced AI Utilization Advisory Board" will review the guideline in collaboration with relevant ministries and agencies, considering the overall trends in generative AI policies across the government as well as the operational status of this

guideline. The Digital Agency shall convene the "Council of Chief AI Officers (CAIO) " as a liaison meeting for relevant ministries and agencies, provide briefings on discussions from the “Advanced AI Utilization Advisory Board,” and offer necessary information on the utilization and governance status of generative AI in each ministry or agency.

Moreover, the Digital Agency will operate an "AI Consultation Desk," accepting questions and consultations from ministries and agencies regarding the procurement and utilization of generative AI and the operation of this guideline.

The "AI Consultation Desk" will receive inquiries and consultations from ministries and agencies in the government and provide necessary supports and advice from technical and professional perspectives to promptly realize effective utilizations of generative AI, including:

- Inquiries regarding the content of the guideline
- Consultations on methods and technical aspects for improving the efficiency of administrative tasks and enhancing administrative services by utilizing generative AI
- Consultations on cases where it is unclear whether generative AI systems will be classified as high-risk AI
- Other consultations on points to consider for risk reduction in the planning and procurement of generative AI systems

Furthermore, the Digital Agency will establish a scheme where AI experts and responsible staff of the Digital Agency as necessary collaborate with information technology specialists dispatched by the Digital Agency to ministries and agencies, in providing support for the utilization of generative AI in projects conducted by each ministry or agency.

4.1.2 Checks under the Control and Supervision by the Digital Agency

In accordance with Article 4, Paragraph 2, Item 17 of the Act on the Establishment of the Digital Agency (Act No. 36 of 2021), the Digital Agency, as part of its control and supervision (centralized project management role), which is to oversee the development and management of national information systems, shall check the planned implementation of generative AI systems and the status of risk management measures for these systems within each ministry or agency. This information will be shared properly with the “Advanced AI Utilization Advisory Board.”

4.2 Development of AI Governance Frameworks within Each Ministry or Agency

4.2.1 Appointment of Chief AI Officers (CAIO) in Each Ministry or Agency

Each ministry or agency shall establish schemes for the control and supervision of generative AI systems throughout their lifecycle, including checks on procurements and contracts based on this guideline.

Specifically, each ministry or agency shall appoint a Chief AI Officer (CAIO) to centrally manage generative AI systems in terms of planning, handling of administrative data, procurement, utilization, and operation, as well as risk cases particular to generative AI, enabling initiatives related to the proper procurement and utilization of generative AI.

The Chief AI Officer (CAIO) shall proactively promote the utilization of generative AI in the operations of each ministry or agency. Serving as a central authority for establishment and implementation of AI governance within each ministry or agency, the CAIO shall monitor generative AI systems, ensure comprehensive risk management, handle risk cases particular to generative AI systems, conduct trainings to enhance AI literacy among government staff, and decide whether reports to the Advisory Board are necessary.

The Chief AI Officer (CAIO) shall assume the AI-related roles, within the duties of the Chief Information Officer responsible for the comprehensive and strategic digitalization promotion of public administration in the organization. Thus, it is expected that the Chief AI Officer (CAIO) will be a government staff of the level equivalent to the " Chief Information Officer" or the "Deputy Chief Information Officer" assisting the Chief Information Officer within each ministry or agency.[17]

4.2.2 Report to the Advanced AI Utilization Advisory Board

The Chief AI Officer (CAIO) of each ministry or agency shall compile an ongoing comprehensive overview list of the operational status of generative AI systems within each ministry or agency, as well as their utilization status within government administration. They shall report on this status list to the "Advanced AI Utilization Advisory Board" on a regular basis, approximately once per quarter.

Moreover, in collaboration with planners, the Chief AI Officer (CAIO) of each ministry or agency shall conduct appropriate risk assessments during the planning of generative AI utilization projects, as outlined in "3 Government Policy for the Use of

[17] The Chief AI Officer (CAIO) may also be concurrently held by the "Chief Digital Officer" or "Deputy Chief Digital Officer" in each ministry or agency.

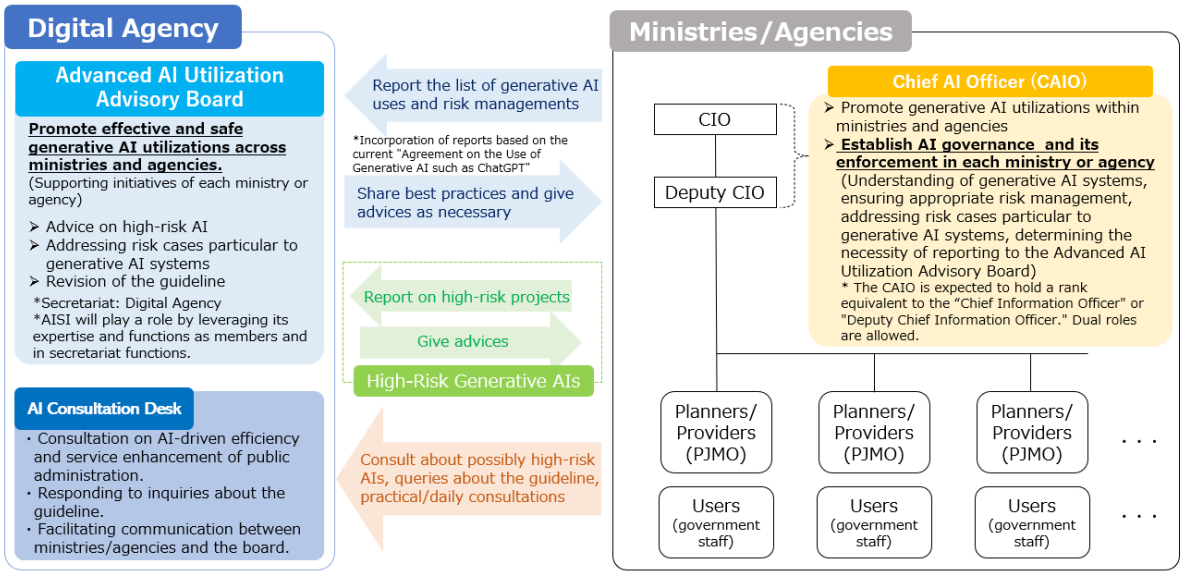
Generative AI." For generative AI systems that are likely to be classified as high-risk, the Chief AI Officer (CAIO) shall report the project's details, objectives, risk mitigation measures, and quality assurance plans during operation etc., to the Advanced AI Utilization Advisory Board.

Furthermore, not only during project planning but also throughout development, release, and post-launch, if there is a possibility that the project may be classified as high-risk due to changes in circumstances, or if the use of generative AI was not recognized at the time of planning but is recognized at the time of release or post-development and is found carrying a potential high-risk classification, the said report shall be made to the Advanced AI Utilization Advisory Board accordingly.

The determination of whether generative AI utilization falls under high-risk shall be based on risk assessment is made by each ministry or agency, with the Chief AI Officer (CAIO) having the final decision-making authority. However, if requested by the Advanced AI Utilization Advisory Board, each ministry or agency should provide necessary reports on the relevant project. (Refer to Figure 4: Overview of the Government's Framework Related to AI Procurement and Utilization.[18])

[18] In cases where information security is anticipated to be involved in risk assessment of generative AI systems, collaboration with the Chief Information Security Officer (CISO) will be undertaken as needed to determine whether the generative AI poses a high-risk.

Figure 4: Overview of the Government's Framework Related to AI Procurement and Utilization



5 Boosting the Use of Generative AI with an Understanding of Benefits and Risks

5.1 Benefits of Generative AI

AI Guidelines for Business outline the benefits of AI utilization as follows.

> There are a variety of benefits from AI use, and they have been enhancing as technologies are advanced.
>
> AI business actors can use AI to create value. The following can be expected as the result of AI use:
>
> - Reduction of operation costs
> - Creation of new products and services that accelerate innovation in existing business
> - Renovation of organization
>
> Furthermore, it is conceivable that AI is applied to various fields (agriculture, education, healthcare, manufacturing, transportation, etc.) and various deployment models (cloud service, on-premise system, cyber-physical system, etc.) are used.

In the government sector, the utilization of generative AI is expected to bring benefits as shown in Table 5. These benefits are expected to expand further as generative AI advances rapidly.

Each ministry or agency should understand these benefits and proactively incorporate generative AI into their operations moving forward.

Additionally, to accelerate the utilization within the government, the Digital Agency will work with other ministries and agencies to conduct technical trials envisioning actual use cases and promote the creation of use cases through initiatives such as "AI Ideathon and Hackathon," etc.

Table 5: Examples of benefits expected from government utilization of AI

Purpose of introducing generative AI	Example of benefits
Efficient and effective achievement of public administration goals	Generative AI can be used to create a draft of a specified content. By simply making minor adjustments and corrections to AI-generated text as needed, it enables the rapid creation of greeting messages, emails, and key points of documents.
	Generative AI can be used to quickly grasp the key points of long and complex texts such as meeting minutes. Even complex

Purpose of introducing generative AI	Example of benefits
	contents or long texts can be summarized instantly, allowing users to quickly understand the main ideas of the text.
	Generative AI can be used to translate Japanese texts into English, significantly reducing the time required for translation. Additionally, by translating back into Japanese, users can check the accuracy to a certain degree.
Enhancement of planning skills	Generative AI can be used to generate ideas that help efficiently create proposals by exploring and expanding upon ideas presented by the generative AI. This facilitates the organization of new insights and thoughts on designated themes, making the conceptualization of proposals more accessible.
Enhancement of information gathering and analysis capabilities	Generative AI can be used to investigate documents such as past cases within government ministries and agencies. By reducing the amount of work required, it will be possible to answer inquiries without exceeding deadlines.
Enhancement of the quality of government policies, documents, analyses, etc.	Generative AI can be used to create articles for social media about the information on events held by the government. Multiple article ideas are proposed, and the best parts of each can be combined to create a more refined article.
	Generative AI can be used to evaluate and analyze the text created before consulting with others. This preliminary AI-generated review provides constructive feedback before a supervisor points out areas for improvement, ultimately enhancing the quality of reports.
	Generative AI can be used to examine issues and propose countermeasures for submitted reports for enhancing effectiveness. The findings and countermeasures proposed by the generative AI are specific and multifaceted, offering useful feedback to improve the quality of the report.
Improvement of the functionality	By using generative AI in the classification and search tasks of inquiries, it is expected that the classification and search

Purpose of introducing generative AI	Example of benefits
and convenience of existing government information systems by using generative AI	accuracy of existing government information systems are expected to be improved.

5.2 Risks Associated with Generative AI

AI Guidelines for Business provide the following examples as risks associated with AI.

Table 6: Examples of risks in AI Guidelines for Business

Risk classification (Example)		Examples of AI risk cases and their descriptions
Technical Risks[19]	**Risks during the learning and input stages**	**Attacks on AI systems such as data poisoning attack** There are risks such as the mixing of fraudulent data into training data, cyber-attacks targeting the applications themselves, and attacks through prompts, which could intentionally manipulate the output of AI, resulting in adverse effects.
	Risks during the output stage	**Biased outputs, discriminatory outputs, and inconsistent outputs** AI may amplify discrimination due to biased training data, etc.
		Incorrect outputs due to hallucinations and other issues Generative AI gives plausible answers that are not actually factual.
	Risks during the post-	**Black-boxing and inadequate explanations of decisions** The black-box nature of AI's decisions can hinder accountability at times of emergencies. Furthermore, AI

[19] Risks primarily associated with AI systems.

Risk classification (Example)		Examples of AI risk cases and their descriptions
	responses stage	systems with complex mechanisms may pose increased challenges in maintenance and troubleshooting.
Societal Risks[20]	**Risks related to ethics and law**	**Inappropriate uses of personal data** There is a risk of using personal information without obtaining proper consent, thereby lacking transparency in utilizing personal data.
		Occurrence of accidents related to lives, etc. In contexts like autonomous driving, there is concern about large-scale accidents caused by AI malfunctions. Additionally, the generation of codes for machines using generative AI can result in erroneous or inefficient codes, leading to performance decline or accidents.
		Discrimination in triage AI may introduce bias when determining priorities, compromising fairness. In medical settings, this could pose a threat to life.
		Excessive dependence Over-reliance on AI in critical decision-makings, such as personnel recruitment, may lead to accountability issues and criticisms for companies. There are also reports of users developing psychological dependence on generative AI-driven chatbots.
		Misuse There are concerns about AI being used for fraudulent purposes.
	Risks related to economic activities	**Infringement of intellectual property rights, etc.** AI-generated output may infringe on others' intellectual property rights, as evidenced by collective lawsuits from multiple artists.[21]
		Financial Loss

[20] Existing risks that may also arise in AI or be amplified by AI.

[21] Regarding initiatives that are considered desirable for reducing the risks involved in the relations between copyright and generative AI, and for preserving and exercising one's own rights, it is necessary to take actions based on the "Checklist and Guidance on AI and Copyright" (July 31, 2024; by the Copyright Division, Agency for Cultural Affairs).

Risk classification (Example)		Examples of AI risk cases and their descriptions
		Companies may face financial liability, such as damage compensation claims, if their AI outputs significantly infringe on others' rights.
		Leak of confidential information There is a risk of personal and confidential information being input as prompts and subsequently leaked through AI outputs. This is particularly concerning when integrating external services with internal data, which requires caution against unintentional leaks or data tampering.
		Unemployment of workers The introduction of AI raises concerns about unemployment risks and widening disparities.
		Concentration of data and profits There is a concern that data and profits may become concentrated among a few AI developers. In countries with minority languages, lack of high-performing AI for their native language is worried.
		Infringement of qualifications, etc. The use of AI in fields requiring legal or medical licenses and qualifications carries the risk of violating industry-specific licenses and exclusive rights.
	Risks related to the information space	**Distribution and diffusion of disinformation and misinformation** There are concerns about the manipulation of information and public opinion through the dissemination of misinformation and deepfakes generated by AI.
		Negative influence on democracy In electoral activities, there is concern about the use of AI to generate and spread false/misleading information or deepfakes about other candidates.
		Filter bubble and echo chamber phenomena This issue arises in recommendation systems on social media, where individuals are surrounded only by information they wish to see, with views that align solely with their own

Risk classification (Example)		Examples of AI risk cases and their descriptions
		thoughts being displayed, leading to the amplification of extreme views.
		Loss of diversity and inclusion If the entire society uses the same AI models in the same way, there is a risk of homogenized opinions and responses, leading to a loss of diversity. In financial trading, the use of common algorithms may increase market instability.
		Reproduction of bias Continued acceptance of generative AI outputs without critical evaluation may amplify biases in existing information, perpetuating and expanding unfair or discriminatory outputs.
	Risks related to the environment	**Energy consumption and environmental load** The development and expansion of AI use will require large amounts of electricity, which will increase the burden on the environment.

In the procurement and utilization of generative AI within the government, it is necessary to be mindful of the risks described above. As for the government, it is also essential to take into consideration the following risks, for example:

- The risk of generating information or expressions that deviate from political neutrality and appropriateness, when using generative AI in policy-related tasks
- The risk of increased costs and the risk of bias becoming entrenched due to reliance on a single model
- The risk of making incorrect or counter-national statements by directly utilizing the output of generative AI that does not sufficiently consider the language, culture and historical background
- The risk of utilizing generative AI in operations, leading to the reasoning of administrative decisions being unclear or untraceable, thereby failing to fulfill accountability to the public regarding administrative processes
- The risk of increased unnecessary costs due to vendor lock-in
- The risk of spreading illegal or harmful information due to incorrect responses when using generative AI for legally binding translations or inquiries

Each ministry or agency must advance the utilization and risk management of generative AI at the same time, being mindful not only of the benefits but also of these risks.

6 Government Rules for the Procurement and Utilization of Generative AI

6.1 Overview of Measures to be Addressed for Procurement and Utilization of Generative AI in the Government

6.1.1 Measures to be Addressed Based on Various Laws, Regulations, and Guidelines

(1) In the procurement and utilization of generative AI, it is required to comply with laws, regulations and guidelines related to the government information systems such as "Digital Society Promotion Standard Guidelines," "Common Standards for Cybersecurity Measures for Government Agencies and Related Agencies," "Agreement on the Procurement Policy and Procedures for Goods and Services of the Government Regarding IT Procurement," and "Guidelines on the Act on the Protection of Personal Information (For Administrative Organs, etc.)"

(2) Regarding generative AI systems targeted by this guideline, when procuring cloud services that deal with confidential information, it is required to adhere to the utilization principles of the Information System Security Management and Assessment Program (ISMAP). Selections must be made in principle from the ISMAP Cloud Service List or the ISMAP-LIU Cloud Service List, and measures specified in this guideline must be implemented separately. In other words, since measures required to address risks particular to generative AI systems need to be taken in accordance with this guideline, it is important to note that even if a service is selected from the ISMAP Cloud Service List or the ISMAP-LIU Cloud Service List, compliance with this guideline is still required.

(3) When utilizing cloud-service based generative AI systems in operations, which are offered to a large, unspecified number of users and accessible merely by agreeing to standard terms and conditions or rules, etc., it is in principle prohibited to deal with confidential information. Even if confidential information is not handled, it is necessary to take risks into consideration and determine an available scope of operations in advance. For individual uses, adherence to the usage procedures is required, whereby the approver[22] must assess the application details from the planner regarding the purpose of use (operation details) and the scope of users, then subsequently determine the permissibility of the uses. Additionally, it is essential to supervise the usage status.

[22] The official who reviews and approves applications for exceptional measures.

(4) For operational uses of generative AI in the government agencies, taking into account the "Notice Regarding the Operational Use of Generative AI such as DeepSeek" (Secretariat for the Meeting for the Promotion of a Digital Society Executive Committee, February 6, 2025),[23] it is essential to fully recognize the potential risks (*) associated with service uses, even when procurement actions are not involved. It is also necessary to seek advice from the National Center of Incident Readiness and Strategy for Cybersecurity, to make an appropriate judgment, considering the intent of the "Agreement on the Procurement Policy and Procedures for Goods and Services of the Government Related to IT Procurement."
*For example, if server equipment is located overseas, local laws and regulations may apply, and data may be censored or seized by the local governments and authorities.

(5) Government staff involved in the procurement and utilization of generative AI must undertake initiatives based on the "AI Guidelines for Business, Part 2, C. Common Guiding Principles."

Table 7: Overview of the AI Guidelines for Business "Part 2, C. Common Guiding Principles"

1. Human-centric	(1) Human dignity and autonomy of individuals
	(2) Paying attention to manipulations by AI on decision-making and emotions
	(3) Countermeasures against disinformation, etc.
	(4) Ensuring diversity/inclusion
	(5) Providing user support
	(6) Ensuring sustainability
2. Safety	(1) Taking into consideration the lives, bodies, properties and minds of humans and the environment
	(2) Proper use (of AI)
	(3) Proper training
3. Fairness	(1) Consideration for bias in technologies forming AI models
	(2) Intervention by decisions made by humans
4. Privacy protection	(1) Protection of privacy across AI systems and services in general

[23] Notice Regarding the Operational Use of Generative AI such as DeepSeek
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/d2a5bbd2-ae8f-450c-adaa-33979181d26a/e7bfeba7/20250206_councils_social-promotion-executive_outline_01.pdf

5. Ensuring security	(1) Security measures relevant to AI systems and services
	(2) Consideration for the latest trends
6. Transparency	(1) Ensuring verifiability
	(2) Providing relevant stakeholders with information
	(3) Reasonable and truthful support
	(4) Improving explainability and interpretability for relevant stakeholders
7. Accountability	(1) Improving traceability
	(2) Explaining conformity to common guiding principles
	(3) Designation of responsible persons
	(4) Sharing responsibilities among actors
	(5) Specific actions for stakeholders
	(6) Documentation
8. Education/literacy	(1) Ensuring AI literacy
	(2) Education and reskilling
	(3) Support for stakeholders
9. Ensuring fair competition	-
10. Innovation	(1) Promoting open innovation, etc.
	(2) Consideration for interconnectivity and interoperability
	(3) Providing information appropriately

6.1.2 Measures to be Addressed Based on this Guideline

(1) The government staff involved in the procurement and utilization of generative AI shall take appropriate measures for "6.2 Measures to be Addressed by Chief AI Officers (CAIO) of Generative AI Systems in the Government," "6.3 Measures to be Addressed by Planners of Generative AI Systems in the Government," "6.4 Measures to be Addressed by Developers of Generative AI Systems in the Government," "6.5 Measures to be Addressed by Providers of Generative AI Systems in the Government," "6.6 Measures to be Addressed by Users of Generative AI Systems in the Government," And "6.7 Addressing Risk Cases Particular to Generative AI Systems" as stipulated in this guideline, respectively.

(2) However, various patterns can be anticipated in the implementation of generative AI systems. For instance, when classifying the implementations based on

"whether individual development is conducted" and "what type of contract is made," the following categorization can be a basis for applying this guideline to cases:

Type A: The generative AI system is used without conducting individual development, by agreeing to standard terms and conditions or rules, etc. (In principle, it is assumed that confidential information is not handled.)

Type B: The generative AI system is used without conducting individual development, with individual contracts concluded in addition to agreeing to standard terms and conditions or rules, etc.

Type C: Individual development of the generative AI system is conducted, and individual contract is concluded.

In cases that fall under Type A, it is generally assumed that the uses of the generative AI system do not involve handling of confidential information. Therefore, it should be verified whether it is unnecessary to establish requirements in the procurement specifications or contract based on the "Procurement Check Sheet" and "Contract Check Sheet" defined in "6.3.2 Measures to be Addressed during the Procurement of Generative AI Systems." This includes ensuring that there are no issues such as the presence of terms and conditions conflicting with the details in the "Procurement Check Sheet" and "Contract Check Sheet." (If there are requirements that need to be fulfilled, consider procuring in the form of Type B or Type C.)

In cases that fall into Type B or Type C, it is necessary to consider the balance between risks and countermeasures, for each measure to be addressed in a way to that the measure is neither insufficient nor excessive, by taking the following perspectives into account:

・Project phase, such as whether it is in the Proof of Concept (PoC) stage or in the development stage in production environment

(e.g., implementing all measures in check sheets during the PoC stage may result in excessive countermeasures.)

・Risk classification, such as whether the use is potentially high-risk or not

(e.g., for potential high-risk uses, additional measures in relation to check sheets tailored to the use case may be necessary)

・Nature of use cases

(e.g., in cases where using generative AI system for searching a large number of

documents within government offices, basic requirements such as "output control of harmful information" or "prevention of output or manipulation of false/incorrect information " in the Procurement Check Sheet may not be necessary.)

Accordingly, depending on specific generative AI system projects, it is essential to consider the aforementioned implementation types, project phases, risk levels, and the nature of use cases. Considering the preceding section (paragraph (1) of "6.1.2 Measures to be Addressed Based on this Guideline"), it is necessary to assess the balance between risks and countermeasures and to determine the required level of each measure, and to selectively incorporate or expand requirements and agreed terms as appropriate.

6.2 Measures to be Addressed by Chief AI Officers (CAIO) of Generative AI Systems in the Government

6.2.1 Development of Rules within Each Ministry or Agency

The Chief AI Officer (CAIO) of each ministry or agency shall develop the following rules to outline the (1) policy for generative AI uses within each ministry or agency, and (2) policy for addressing risk cases particular to generative AI systems. These rules shall be revised as needed based on revisions of this guideline as well as latest trends and the utilization status of generative AI.

(1) Rules for Users of Generative AI Systems

In order to boost proper uses of generative AI within each ministry or agency, the Chief AI Officer (CAIO) shall develop a rule for the users (government staff) of generative AI systems in each ministry or agency based on "[Appendix 2] Model User Rule for Generative AI," considering following matters:

- Indispensable knowledge that government staff and other users should have before using generative AI systems, as well as important points to consider for handling confidential information
- Key points to be considered by government staff when utilizing generative AI, including (i) uses of the generative AI systems within the scope of specified utilization purposes (as described in the utilization rules for each generative AI system) and (ii) accountability and risk mitigation of the operations by the use of AI-generated outputs
- Appropriate handling of documents for official duties created by using

generative AI.

- Matters to be reported to the Chief AI Officer (CAIO) in the event of risk cases particular to generative AI

etc.

(2) Rules for Addressing Risk Cases Particular to Generative AI Systems
The Chief AI Officer (CAIO) shall develop rules for addressing risk cases particular to generative AI systems.
(Refer to "6.7 Addressing Risk Cases Particular to Generative AI Systems" for details)

6.2.2 Ensuring AI Governance within Each Ministry or Agency

The Chief AI Officer (CAIO) ensures AI governance by undertaking the actions outlined in (1) and (2) below.

(1) The Chief AI Officer (CAIO) shall establish an AI governance framework within each ministry or agency and continuously ensure proper AI governance in the ministry or agency. (Refer to "4.2 Development of AI Governance Frameworks within Each Ministry or Agency " for details.)

(2) The Chief AI Officer (CAIO) shall take necessary measures to ensure that the procurements and utilizations of generative AI systems are conducted based on this guideline within each ministry or agency. In this regard, the Chief AI Officer (CAIO) formulates and revises relevant rules of the ministry or agency in accordance with this guideline, disseminates this guideline and the utilization rules for generative AI systems of the ministry or agency, and conducts training sessions (such as giving heads-up regarding input data and hallucinations).

6.3 Measures to be Addressed by Planners of Generative AI Systems in the Government

6.3.1 Measures to be Addressed during the Planning Stage of Generative AI Systems

Planners of generative AI systems should undertake the measures listed below during the planning stage of generative AI systems. To maximize the benefits of generative AI, it is desirable for planners to proceed with deliberations by leveraging both knowledge of administrative tasks and knowledge of generative AI system aspects at the time of planning. Therefore, planners should make efforts to establish schemes where experts in the both areas can collaborate in the planning of these generative AI systems.

(1) Planners should clearly define the purpose of what they aim to achieve or solve by using the generative AI system and set appropriate goals of the project.

(2) Planners should conduct an environment/risk analysis for the use case, while also considering methods to minimize risks and developing quality assurance plans throughout the operation of the generative AI system.

(3) For the control and supervision by the Digital Agency, planners should report on the implementation schedule of generative AI systems, results of risk analysis, risk countermeasures, handling of public administration data, and other relevant matters.

(4) For generative AI systems that are likely to pose high risks, planners should collaborate with the Chief Artificial Intelligence Officer (CAIO) in reporting the project's purpose, risk mitigation measures, and quality assurance plans throughout their operational period to the Advanced AI Utilization Advisory Board, as stated in "4.2.2 Reporting to the Advanced AI Utilization Advisory Board."

(5) In anticipation of expanding the uses of generative AI within the government, it is important to optimize generative AI systems across the government through data linkage between systems within government agencies, shared use of generative AI systems across ministries and agencies, and the formation of joint projects and common systems. For instance, actively utilizing generative AI systems provided on common functions such as the Government Cloud can potentially enhance cost-effectiveness, ensure security, and facilitate integration with operational systems. Therefore, planners should also consider the utilization of such services provided as common functions in the government when starting new generative AI system projects. (*)

*Based on the law related to the Government Cloud (Bill to Amend Part of Act on the Advancement of Government Administration Processes that Use Information and Communications Technology, Act No. 4 of 2025), national administrative organs are obligated to consider as an option to utilize the Government Cloud when developing information systems relevant to the execution of their own administrative tasks.

When contemplating the development or renewal of systems combined with generative AI, it is necessary to consider whether it is possible to efficiently secure a generative AI environment by constructing the system on the Government Cloud and utilizing its packages or tools.

For further details on specific approaches to utilization methods, please refer to "Basic Considerations for the Utilization of Government Cloud."

6.3.2 Measures to be Addressed during the Procurement Phase of Generative AI Systems

(1) Planners should refer to "[Appendix 3] Procurement Check Sheet (for Generative AI Systems)" (hereinafter referred to as the "Procurement Check Sheet") (*) and include, in procurement specifications, the requirements (stated in the “Procurement Check Sheet”) for service providers and the generative AI systems. Additionally, based on the results of the risk analysis and other relevant factors, planners should consider adding any necessary requirement items not listed in the “Procurement Check Sheet.”

*The "Procurement Check Sheet" was formulated by referring to the AI Guidelines for Business and the "Guide to Evaluation Perspectives on AI Safety (Version 1.01)"[24] published by AISI, among others. The “Procurement Check Sheet” organizes the requirements for procuring generative AI systems, along with examples and details of measures to meet these requirements, and examples of supporting information of them. The following perspectives are included; AI governance of generative AI suppliers, appropriate input/output and data handling, ensuring quality of LLMs and services including prevention of the output including false/incorrect information, responding appropriately to risks particular to generative AI systems, ensuring proper handling for public use cases (i.e. including indication that the output is generated by generative AI), protection of personal information and intellectual property, assurance of security and explainability, and more. By referring to the "Procurement Check Sheet," key points for procuring generative AI systems can be checked. Therefore, it is advisable to refer to it when determining what items are to be included in the specifications, whether its supporting information should be submitted, and what information should be submitted. Since the "Procurement Check Sheet" includes only requirements particular to the “procurement of generative AI systems,” it is necessary to also refer to the content of the "Digital Government Promotion Standard Guidelines," and the annex "Procurement

[24] This guideline refers to the "Guide to Evaluation Perspectives on AI Safety (Version 1.01)." Any amendments in response to revisions to the latest "Guide to Evaluation Perspectives on AI Safety (Version 1.01)" will be considered in future revisions of this guideline.

Specification Template" of the "Digital Government Promotion Standard Guidelines Practical Guidebook" to prepare procurement specifications.

*How to Read the Procurement Check Sheet”

(Refer to “Figure 5: Image of ‘Procurement Check Sheet’ Requirements”)

Figure 5: Image of “Procurement Check Sheet” Requirements

Classification of Items for Evaluation and Selection

Requirements

Classification	Evaluation Viewpoints No.	Evaluation Viewpoints	Classification of Items for Evaluation and Selection	Req. No.	Note: Items in this column are requirements for service providers, whch are intended to be included in procurement specifications for generative AI systems. Note: The degree of requirement level of each item and selection/additon of items are to be considerd, taking into account the project type, the project stage, the project's risk level, etc., as stated in "6.1.2 Measures to be Addressed Based on this Guideline." Requirements
Requirements on Organizational Matters	1	Compliance with the Common Guiding Principles of the AI Guidelines for Business	Basic Requirements	1	To be able to declare the capability of understanding, comprehending and complying the Common Guiding Principles of the AI Guidelines for Business.
	2	Establishment of AI Governance	Basic Requirements	2	AI governance* is applied in developments and operations of generative AI systems. *A control mechanism/operation mechanism to maximize the positive impact of AI, while managing AI-related risks at an acceptable level.
	3	Understanding of Trends in the AI Industry and Latest Technologies	Basic Requirements	3	Grasping trends in the AI industry and latest technologies to improve quality and explainability in the development and operation of generative AI systems.
	4	Response to Information Security Incidents and Risk Cases Risk Cases Particular to Generative AI Systems	Basic Requirements	4	Having response frameworks and procedures for information security incidents and risk cases particular to generative AI systems (limited to those within the service provider's scope of responsibility), including cooperation responding to users' reports about the insidents in services that your business have developed and is operating.
	5	Enhancement of Education/Literacy Regarding Generative AI for Stakeholders	Basic Requirements	5	Taking necessary actions to enhance literacy about generative AI for staff or sections involved in the development and operation of generative AI systems.
Requirements on Development/ Implementation Processes	6	Handling of Data	Basic Requirements	6	Properly suprevise the handlings of inputs, outputs, or processed data within generative AI systems.
	7	Assurance of Outputs Quality	Basic Requirements	7	Taking proper actions to meet the expected quality standards of generative AI systems.
	8	Avoidance of Vendor Lock-In	Basic Requirements	8	To be able to explicitly describe information on LLMs being used, including version information.
			Optional Additional Requirements (Optional Criteria)	9	To be able to provide disclosure or share information to the planner to a reasonable extent, in order to make sure that parts of the prompts or parameters entered into generative AI systems are not concealed.
			Optional Additional Requirements (Optional Criteria)	10	Having technology to offer features such as saving past chat histories, registering prompts as templates, and exporting such data.
			Optional Additional Requirements (Optional Criteria)	11	Having technology to select or combine the optimal LLM from multiple options, considering that each LLM has characteristics that lead to different functions and behavior, when the primary purpose is not to use of a specific model.
	9	Consideration of Proper Updates to Generative AI Systems	Basic Requirements	12	Mitigate risks from viewpoints particular to generative AI with regard to major system updates or migrations.
	10	Cultural/Linguistic Considerations	Optional Additional Requirements (Optional Criteria)	13	Making outputs from generative AI systems align with the Japanese linguistic and cultural environment.
	11	Environmental Considerations	Optional Additional Requirements (Optional Criteria)	14	Developing and providing environmentally conscious generative AI systems.

Among the "Requirements," those deemed essential for government agencies to include in the procurement of generative AI systems are designated as "Basic Requirements" (as indicated in the "Classification of Items for Evaluation and Selection" column of the “Procurement Check Sheet”).

Requirements labeled as "Basic Requirements" should be included as mandatory criteria in principle for applicants during procurement. Requirements designated as “Optional Additional Requirements (Optional

Criteria)" are perspectives considered beneficial to take into account if necessary and are intended to serve as optional criteria in the procurement evaluation process.

As a reference information for the Procurement Check Sheet, the "Reference of Requirements" sheet provides "Example of Measures", "Detailed Example of Measures," and "Examples of Supporting Information," which serve as examples of measures to fulfill the requirements. These examples will be reviewed and updated flexibly in consideration of changes in technological trends and the business environment.

(2) When adopting a comprehensive evaluation method or competitive proposal method, planners should reflect these requirements into the evaluation criteria as necessary.

(3) To foster the growth of domestic startups in the generative AI business, leveraging "public procurement" is crucial. Therefore, planners should evaluate digital startups in the procurement related to generative AI systems in accordance with the "Implementation Guidelines for Evaluation Systems in Procurement for Information Systems for Expanding Opportunities for Digital Startups to Enter the Public Procurement" (approved by the Council for the Promotion of a Digital Society Executive Board Meeting on January 15, 2024). Furthermore, when considering SaaS-based generative AI systems or services provided by companies to support such systems' implementation, the "Digital Marketplace"[25] operated by the Digital Agency can be utilized. By leveraging the "Digital Marketplace," rapid implementation can be achieved, and diverse businesses, including small and medium-sized enterprises and start-ups, will find it easier to access the public procurement market. Active utilizations of this "Digital Marketplace" are encouraged for the sake of accelerating fair competitions.

(4) Planners should refer to the "[Appendix 4] Contract Check Sheet (for Generative AI Systems)" (hereinafter referred to as the "Contract Check Sheet") (*) and consider including key considerations for the procurement of generative AI systems in the contract or procurement specifications. Additionally, based on the results of the risk analysis and other relevant factors, planners should consider adding any necessary items not listed in the "Contract Check Sheet."

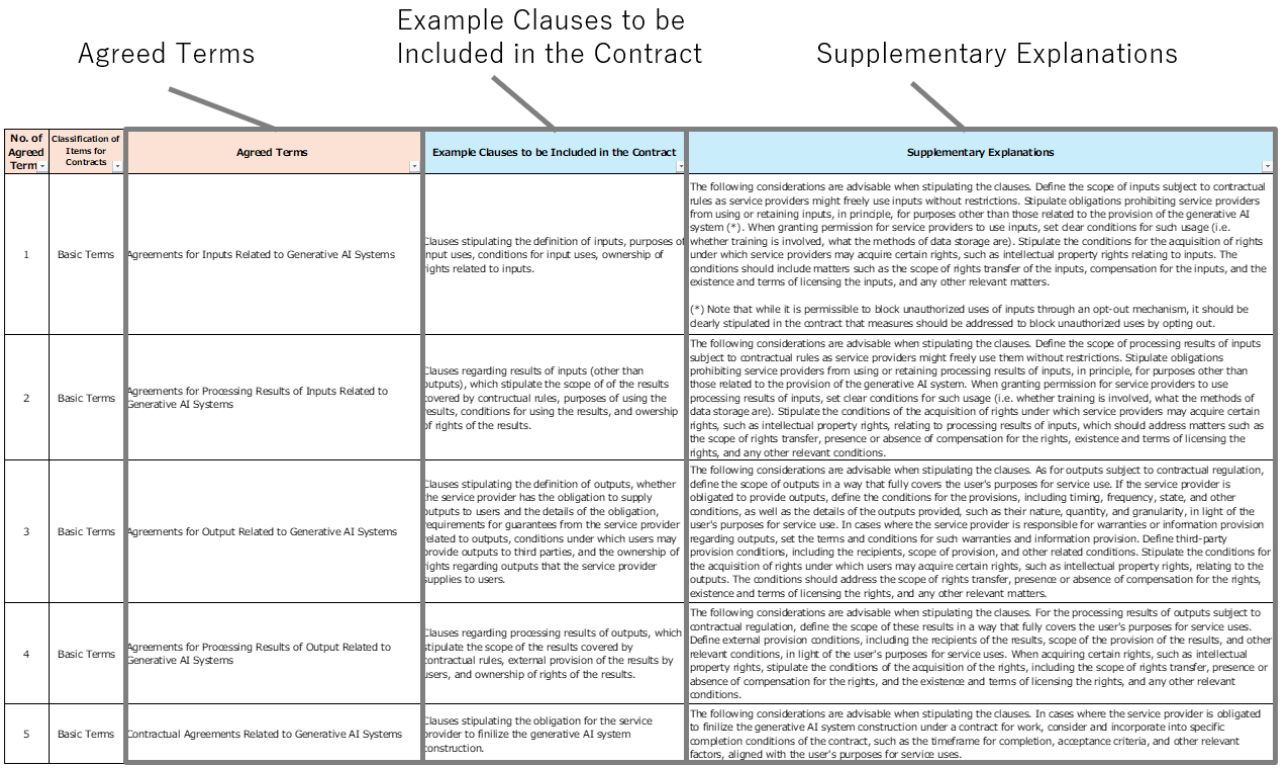
[25] Digital Market Place https://www.dmp-official.digital.go.jp/

*The “Contract Check Sheet” was formulated by referring to the AI Guidelines for Business, the Ministry of Economy, Trade and Industry's “Checklist for Contracts Regarding AI Utilization and Development,” and the “Guidelines for Contracts Regarding the Use of AI and Data,” among others. The “Contract Check Sheet” organizes items that need to be confirmed at the time of contracting in the procurement process of generative AI systems, including ownership of rights concerning inputs of generative AI systems, the scope of provider obligations, ownership of intellectual property rights related to outputs, the scope of provider obligations in response to risk cases particular to generative AI systems, the scope of provider obligations regarding the maintenance of expected quality standards and environmental considerations, and other matters. By referring to the “Contract Check Sheet,” key points to be considered in contracts during the procurement process of generative AI systems can be checked. Therefore, it is advisable to refer to it when deciding on clauses to be included in contracts or procurement specifications. Note that the “Contract Check Sheet” only lists items particular to contracts related to the “procurement of generative AI systems.”

*How to Read the “Contract Check Sheet”

(Refer to “Figure 6: Image of ‘Contract Check Sheet’ Agreed Terms”)

Figure 6: Image of “Contract Check Sheet” Agreed Terms



No. of Agreed Term	Classification of Items for Contracts	Agreed Terms	Example Clauses to be Included in the Contract	Supplementary Explanations
1	Basic Terms	Agreements for Inputs Related to Generative AI Systems	Clauses stipulating the definition of inputs, purposes of input uses, conditions for input uses, ownership of rights related to inputs.	The following considerations are advisable when stipulating the clauses. Define the scope of inputs subject to contractual rules as service providers might freely use inputs without restrictions. Stipulate obligations prohibiting service providers from using or retaining inputs, in principle, for purposes other than those related to the provision of the generative AI system (*). When granting permission for service providers to use inputs, set clear conditions for such usage (i.e. whether training is involved, what the methods of data storage are). Stipulate the conditions for the acquisition of rights under which service providers may acquire certain rights, such as intellectual property rights relating to inputs. The conditions should include matters such as the scope of rights transfer of the inputs, compensation for the inputs, and the existence and terms of licensing the inputs, and any other relevant matters. (*) Note that while it is permissible to block unauthorized uses of inputs through an opt-out mechanism, it should be clearly stipulated in the contract that measures should be addressed to block unauthorized uses by opting out.
2	Basic Terms	Agreements for Processing Results of Inputs Related to Generative AI Systems	Clauses regarding results of inputs (other than outputs), which stipulate the scope of of the results covered by contractual rules, purposes of using the results, conditions for using the results, and owership of rights of the results.	The following considerations are advisable when stipulating the clauses. Define the scope of processing results of inputs subject to contractual rules as service providers might freely use them without restrictions. Stipulate obligations prohibiting service providers from using or retaining processing results of inputs, in principle, for purposes other than those related to the provision of the generative AI system. When granting permission for service providers to use processing results of inputs, set clear conditions for such usage (i.e. whether training is involved, what the methods of data storage are). Stipulate the conditions of the acquisition of rights under which service providers may acquire certain rights, such as intellectual property rights, relating to processing results of inputs, which should address matters such as the scope of rights transfer, presence or absence of compensation for the rights, existence and terms of licensing the rights, and any other relevant conditions.
3	Basic Terms	Agreements for Output Related to Generative AI Systems	Clauses stipulating the definition of outputs, whether the service provider has the obligation to supply outputs to users and the details of the obligation, requirements for guarantees from the service provider related to outputs, conditions under which users may provide outputs to third parties, and the ownership of rights regarding outputs that the service provider supplies to users.	The following considerations are advisable when stipulating the clauses. As for outputs subject to contractual regulation, define the scope of outputs in a way that fully covers the user's purposes for service use. If the service provider is obligated to provide outputs, define the conditions for the provisions, including timing, frequency, state, and other conditions, as well as the details of the outputs provided, such as their nature, quantity, and granularity, in light of the user's purposes for service use. In cases where the service provider is responsible for warranties or information provision regarding outputs, set the terms and conditions for such warranties and information provision. Define third-party provision conditions, including the recipients, scope of provision, and other related conditions. Stipulate the conditions for the acquisition of rights under which users may acquire certain rights, such as intellectual property rights, relating to the outputs. The conditions should address the scope of rights transfer, presence or absence of compensation for the rights, existence and terms of licensing the rights, and any other relevant matters.
4	Basic Terms	Agreements for Processing Results of Output Related to Generative AI Systems	Clauses regarding processing results of outputs, which stipulate the scope of the results covered by contractual rules, external provision of the results by users, and ownership of rights of the results.	The following considerations are advisable when stipulating the clauses. For the processing results of outputs subject to contractual regulation, define the scope of these results in a way that fully covers the user's purposes for service uses. Define external provision conditions, including the recipients of the results, scope of the provision of the results, and other relevant conditions, in light of the user's purposes for service uses. When acquiring certain rights, such as intellectual property rights, stipulate the conditions of the acquisition of the rights, including the scope of rights transfer, presence or absence of compensation for the rights, and the existence and terms of licensing the rights, and any other relevant conditions.
5	Basic Terms	Contractual Agreements Related to Generative AI Systems	Clauses stipulating the obligation for the service provider to finilize the generative AI system construction.	The following considerations are advisable when stipulating the clauses. In cases where the service provider is obligated to finilize the generative AI system construction under a contract for work, consider and incorporate into specific completion conditions of the contract, such as the timeframe for completion, acceptance criteria, and other relevant factors, aligned with the user's purposes for service uses.

Terms to be aligned with the service provider at the time of contracting are set as "Agreed Terms" (as indicated in the " Agreed Terms " column of the “Contract Check Sheet”). “Agreed Terms" should, in principle, be considered for inclusion in the contract or procurement specifications.

The "Example Clauses to be Included in the Contract" and "Supplementary Explanations" provide sample clauses content and supplementary explanations for incorporating agreed terms into contracts. Planners should select and incorporate these in the contract or procurement specifications as necessary, considering the features of the generative AI system being procured, project specifics, and risk evaluation results.

Column: SBIR Program (Small/Startup Business Innovation Research)

SBIR (Small/Startup Business Innovation Research)[26] is a program aiming at supporting startups.

This program facilitates research and development by startups and other organizations, smooth social implementation of the outcomes of the research and development, and in turn, fosters innovation in our country.

Under the SBIR program, two types of grants are awarded: “Specific New Technology Grants” and “Designated Grants.”

1) Specific New Technology Grants

Specific New Technology Grants refer to the grants and commissioned funds for research and development within each ministry or agency, which include research and development-type startups as eligible recipients. Target amounts are set for grants to research and development-type startups and measures to increase such grants are prescribed.

2） Designated Grants

Designated Grants are a subset of the above-mentioned Specific New Technology Grants, wherein the government sets research and development tasks based on policy needs. These were newly established in fiscal year 2025 as part of the reforms of rules.

In the field of AI, including generative AI, "startups" often possess cutting-edge knowledge and technology.

For this reason, when ministries and agencies operating Designated Grants compile topics addressing policy challenges and procurement needs, it is advisable to actively consider AI-related themes.

Additionally, specific support measures have been implemented to ensure that small and medium-sized enterprises receiving Specific New Technology Grants under the SBIR program can generally participate in all government procurement bids, regardless of their bidding qualification grade or past delivery performances.

[26] SBIR Program (Small/Startup Business Innovation Research)
https://www8.cao.go.jp/cstp/openinnovation/sbirseido/sbirseido.html

6.3.3 Measures to be Addressed during the Preparation Stage Before the Construction/Release of Generative AI Systems

Planners of generative AI systems should undertake the following processes prior to the system release.

(1) Verification of Stable Operation

- Based on the intended purpose and functions, create test scenarios for input/output verification, test the input/output, and confirm that the system operates stably and meets the expected quality standards. (*)

  (Example: In the case of individual development, check for any prohibited outputs within the domain, the presence of inappropriate generation or bias (social biases such as prejudices and discrimination based on race, ethnicity, gender, etc.), and adopt diverse/independent internal and external testing methods such as red teaming, to ensure fulfilling requirements in the specifications for generative AI systems.)

  *If it is difficult to create scenarios solely by planners, consult with users and developers. For systems intended for public uses, the individuals conducting operation checks may include citizens. Verification and improvement of data (such as training data and test data) may be conducted not only by planners but also by service providers (including generative AI system providers), as contractual responsibilities.

(2) Promotion of Proper Use

- Establish utilization rules and usage methods for each generative AI system and inform them to the users of the generative AI systems (referring to internal users within ministries and agencies, as well as the citizens when the generative AI system is provided to them; the same applies hereinafter).

  (Examples: Purpose and scope of generative AI use, available generative AI environments, types of data permissible for use, conditions/procedures/usage methods, recommended and prohibited practices related to utilization, and other things users should be informed of based on specifics of the generative AI system)

- Provide important information and points to consider when utilizing generative AI systems in a manner that is easily understandable and accessible for the users of the generative AI systems.

  (Examples: Purpose and the scope of generative AI use, appropriate/inappropriate uses, technical features, foreseeable risks and

mitigation plans, operational status, verification results of acceptance tests, details/status/recovery measures of risk cases particular to generative AI systems that have occurred, data collection policies, training methods, system architecture, data processing procedures, emergency contact information/inquiry desks, etc.)

- Provide users of the generative AI system information about the purpose and usage methods (including model constraints) of the systems being used.
  (Examples: Availability of data upload, upper limits of numbers of prompt token, response speed, etc.)
- Inform users of the generative AI systems that their information may be collected by the systems.
  (Examples: Login histories, prompts and output results, etc. collected to fulfill appropriate oversight / accountability / investigation responsibilities of the usage status)

6.4 Measures to be Addressed by Developers of Generative AI Systems in the Government

In the government sector, the development of generative AI systems is carried out primarily through outsourcing to service providers. Therefore, the requirements for developers are included in requirements for procurement applicants in specifications and contracts, as detailed in "6.3 Measures to be Addressed by Planners of Generative AI Systems in the Government."

In cases where government staff themselves engage in the development of generative AI, they are expected to undertake the initiatives stated in "Part 3 Matters Related to AI Developers " of the AI Guidelines for Business.

6.5 Measures to be Addressed by Providers of Generative AI Systems in the Government

Providers of generative AI systems should undertake the following processes after the releases of the systems.

(1) System Operation

- Monitor to ensure that the output of the generative AI system meets expected quality standards and does not produce inappropriate generations nor biases.
  (Examples: Conduct sample checks of usage logs such as prompts and output

results when available, regularly monitor inputs and outputs, and verify the decision rationale to ensure they are not biased nor based on a specific cultural background. Conduct surveys of users and analyze the actual utilization situation to check whether inappropriate generation or bias has not occurred.)

- Regularly verify that the generative AI system is being used for appropriate purposes and that they are not being used in ways out of purposes.
  (Examples: Conduct sample checks of usage logs such as prompts and output results when available, ensuring that no input has been made that appears to be in anticipation of outputs unrelated to task operations. Conduct surveys of users and analyze actual utilization situations to evaluate the adherence to intended usage of the system.)
- Check whether there is no improper handling of personal information, nor any leakage of personal/confidential information, nor violation of privacy.
  (Example: Conduct sample checks of usage logs such as prompts and output results when available, detect if there are any cases where personal data is suspected to be used for an unintended purpose, if confidential information beyond the expected input range of the generative AI systems is included in the input, and if privacy has been violated. Conduct surveys of users and analyze the actual utilization situation to check if similar incidents have occurred.)
- Stay updated on the latest risks associated with generative AI systems (including diversified attack methods) and trends in their countermeasures, and implement necessary measures to address them.
  (Example: Regularly review reports of information security incidents (as defined in JIS Q 27000:2019), examples of risk cases particular to generative AI systems, and reports on vulnerabilities in developer models, in order to execute necessary actions.)
- Conduct reviews to assess usefulness and identify issues concerning the input-output aspects of the generative AI system, informing users of them as necessary.
  (Example: Evaluate the system's inputs, outputs, and decision rationale in order to share with users effective usage methods to make the most of usefulness and provide caution to prepare for potential issues. Conduct surveys of users and analyze the actual utilization situation by asking users to share information about usefulness and issues of the system.)

(2) System Maintenance

- Encourage service providers to make decisions regarding the improvement of

generative AI models as necessary.
(Example: Reevaluate biases among various technological components within the generative AI model and propose improvements if bad changes are identified based on the evaluation results.)

- Consider and address vulnerabilities, in compliance with the " Common Standards for Cybersecurity Measures for Government Agencies and Related Agencies" and implement necessary actions.
  (Example: If vulnerabilities inherent to a generative AI system's programs are detected, consider and carry out measures such as patching or model updates.)

(3) Addressing Risk Cases Particular to Generative AI Systems
（Refer “6.7 Addressing Risk Cases Particular to Generative AI Systems” for details）

6.6 Measures to be Addressed by Users of Generative AI Systems in the Government

Users are required to comply with the rules in accordance with this guideline. The rules to be complied with are the utilization rules of generative AI systems established by each ministry or agency (see “6.2 Measures to be Addressed by Chief AI Officers (CAIO) of Generative AI Systems in the Government”), as well as the utilization rules for each generative AI system (see “6.3.3 Measures to be Addressed during the Preparation Stage Before the Construction/Release of Generative AI Systems).

6.7 Addressing Risk Cases Particular to Generative AI Systems

Even if all measures to address the risks, mentioned above, are implemented, it is not possible to eliminate risks entirely. Therefore, it is essential for each ministry or agency to prepare measures to be addressed in the event that risks become apparent, alongside taking measures to mitigate risks. Due to the nature of generative AI systems, there is a possibility of specific risk cases unique to these systems in relation to their output results. The following are examples of risk cases particular to generative AI systems.

- Generative AI has produced output that could pose significant social issues, such as biases or discrimination related to race, gender, culture, etc.
- Generative AI has generated aggressive or dangerous content.
- Generative AI has output information that is factually incorrect (hallucination), and users have used such information, leading to their disadvantages or harm to the users or third parties.
- Users have unintentionally generated content similar to existing works by using

generative AI, potentially leading to issues such as copyright infringement. As a result, users have received requests for removal or other actions from the rights holders of the relevant works.

As measures against risk cases particular to generative AI systems, etc., government staff in each ministry or agency should implement the following.

(1) The Chief AI Officer (CAIO) should establish procedures for responding to risk cases particular to generative AI systems based on this guideline.

(2) If a risk case particular to generative AI systems occurs, the Chief AI Officer (CAIO) and the provider of the generative AI should take the lead in taking appropriate measures, taking into consideration the degree of severity and impact.

(3) To enhance the ability to respond to risk cases particular to generative AI systems across the government, the Advanced AI Utilization Advisory Board (Secretariat) should aggregate knowledge regarding such cases. To this end, the Chief AI Officer (CAIO) must report to the Advanced AI Utilization Advisory Board (Secretariat) both upon the occurrence and after addressing risk cases particular to generative AI systems. The Advanced AI Utilization Advisory Board (Secretariat) will provide advice to ministries and agencies as needed regarding the risk cases.

(4) There is a possibility of incidents including the nature of both information security incidents and risk cases particular to generative AI systems (e.g., the training data of generative AI systems may be contaminated by cyber attackers, reducing the accuracy of the model and making it more likely to generate prejudiced outputs). Under such circumstances, it is necessary to ensure appropriate coordination between the response frameworks of both information security incident and risk cases particular to generative AI systems, or to collaborate by leveraging the expertise of both frameworks. The basic protocol for this case is to follow the procedures defined by each ministry or agency for handling information security incidents.

In the event of a risk case particular to such generative AI systems, it is important to consider requesting necessary data from relevant business operators and conducting necessary audits to ensure appropriate responses (in order to ensure that these are handled appropriately, consider incorporating these measures

into contracts with the business operators related to generative AI systems).

(5) In the event of incidents such as personal information leaks related to generative AI systems, appropriate measures must be taken by following the procedures defined by each ministry or agency. In such situations, there must be proper coordination between the personal information protection response framework and the response framework of risk cases particular to generative AI systems.

7 Future Approaches

Because technologies related to generative AI systems are advancing day by day, procurements and utilizations of generative AI systems by the government may face unanticipated new risks. Therefore, the government will continue to review rules on procurement and utilization of generative AI in a timely manner.

The approach to introducing provenance verification[27] for generative AI involving images and videos etc. procured by the government will be continuously examined, taking into consideration the state of AI utilization within the government and trends in international discussions, etc.

Additionally, in fiscal year 2025, we will assess how to optimize generative AI systems across the government through data linkage between generative AI systems within government agencies, shared uses of systems between ministries and agencies, and the formation of joint projects and common systems. These assessments and considerations will be reflected in future revisions of the rules.

End of Document

[27] Technology that enables content to be tagged in a verifiable manner, indicating by whom, when, and how it was created, as well as any modifications made.

Date of Entry	
Affiliation (Ministry/Department, etc.)	
System Name	
Name of the Person Entering the Form	

Appendix 1

Provisional Translation

Risk Assessment Result	Please fill in the “Response” column in the table below.

■High-Risk AI Project Finder Checklist

Please verify the following checklist and fill out the response section based on assumptions at the planning stage.

Viewpoints	Checklist	Options	Response	Comments (Free Text)
A. Scope and Types of Users	Which of the following best describes the scope of uses?	(1) Used by citizens, etc. outside ministries and agencies (2) Used by government staff etc. within and across multiple ministries and agencies (e.g., utilization of generative AI in a common government system) (3) Used by government staff etc. within a single ministry (4) Undetermined at the planning stage		
B. Characteristics of Operations Using Generative AI	Which of the following best describes impacts in case of errors in the uses of the generative AI ?	(1) Used in operations where errors could potentially have significant impacts* (2) Not used in operations where errors could potentially have significant impacts (3) Undetermined at the planning stage *Operations substantially affecting the fundamental rights and safety of citizens, operations involving sensitive policy fields, operations impacting human life, physical well-being, and citizen’s property, operations requiring qualifications, and operations necessitating high level of accountability.		
C. Presence of Confidential Information or Personal Data in Training Generative AI, etc.	Which of the following best describes the data and its handling in the project?	(1) Confidentiality class-2 level information or personal data is stored or used for training (2) Confidentiality class-2 level information or personal data is handled but not stored or used for training by the generative AI system (3) Confidentiality class-2 level information or personal data is not handled (4) Undetermined at the planning stage		
D. Utilization Involving the Judgment by Government Staff on Output Results	Which of the following best describes the operations in relation to the utilization of output results in administrative operations?	(1) Utilized without government staff’s judgment on the appropriateness of the generative AI system's output (2) Utilized with government staff’s judgment on the appropriateness of the generative AI system's output (3) Undetermined at the planning stage		

***How to Use the "High-Risk Project Finder"**

The "High-Risk AI Project Finder" is a tool designed to provide a simplified suggestion of whether a case is "likely to be classified as high-risk" or "unlikely to be classified as high-risk" by responding to questions related to the four risk axes mentioned below. The judgement logic follows the flow outlined below.

[Image Before Filling out the List]

Date of Entry	
Affiliation (Ministry/Department, etc.)	
System Name	
Name of the Person Entering the Form	

Risk Assessment Result	Please fill in the “Response” column in the table below.

■High-Risk AI Project Finder Checklist
Please verify the following checklist and fill out the response section based on assumptions at the planning stage.

Viewpoints	Checklist	Options	Response	Comments (Free Text)
A. Scope and Types of Users	Which of the following best describes the scope of uses?	(1) Used by citizens, etc. outside ministries and agencies (2) Used by government staff etc. within and across multiple ministries and agencies (e.g., utilization of generative AI in a common government system) (3) Used by government staff etc. within a single ministry (4) Undetermined at the planning stage		
B. Characteristics of Operations Using Generative AI	Which of the following best describes impacts in case of errors in the uses of the generative AI ?	(1) Used in operations where errors could potentially have significant impacts* (2) Not used in operations where errors could potentially have significant impacts (3) Undetermined at the planning stage *Operations substantially affecting the fundamental rights and safety of citizens, operations involving sensitive policy fields, operations impacting human life, physical well-being, and citizen's property, operations requiring qualifications, and operations necessitating high level of accountability.		
C. Presence of Confidential Information or Personal Data in Training Generative AI, etc.	Which of the following best describes the data and its handling in the project?	(1) Confidentiality class-2 level information or personal data is stored or used for training (2) Confidentiality class-2 level information or personal data is handled but not stored or used for training by the generative AI system (3) Confidentiality class-2 level information or personal data is not handled (4) Undetermined at the planning stage		
D. Utilization Involving the Judgment by Government Staff on Output Results	Which of the following best describes the operations in relation to the utilization of output results in administrative operations?	(1) Utilized without government staff's judgment on the appropriateness of the generative AI system's output (2) Utilized with government staff's judgment on the appropriateness of the generative AI system's output (3) Undetermined at the planning stage		

[Image After Filling out the List]

Date of Entry	YYYY/MM/DD
Affiliation (Ministry/Department, etc.)	○○Agency ○○
System Name	○○○○
Name of the Person Entering the Form	○○ ○○

Risk Assessment Result	Unlikely to be classified as "High-Risk"

■High-Risk AI Project Finder Checklist
Please verify the following checklist and fill out the response section based on assumptions at the planning stage.

Viewpoints	Checklist	Options	Response	Comments (Free Text)
A. Scope and Types of Users	Which of the following best describes the scope of uses?	(1) Used by citizens, etc. outside ministries and agencies (2) Used by government staff etc. within and across multiple ministries and agencies (e.g., utilization of generative AI in a common government system) (3) Used by government staff etc. within a single ministry (4) Undetermined at the planning stage	2	○○○○○○○○
B. Characteristics of Operations Using Generative AI	Which of the following best describes impacts in case of errors in the uses of the generative AI ?	(1) Used in operations where errors could potentially have significant impacts* (2) Not used in operations where errors could potentially have significant impacts (3) Undetermined at the planning stage *Operations substantially affecting the fundamental rights and safety of citizens, operations involving sensitive policy fields, operations impacting human life, physical well-being, and citizen's property, operations requiring qualifications, and operations necessitating high level of accountability.	2	○○○○○○○○
C. Presence of Confidential Information or Personal Data in Training Generative AI, etc.	Which of the following best describes the data and its handling in the project?	(1) Confidentiality class-2 level information or personal data is stored or used for training (2) Confidentiality class-2 level information or personal data is handled but not stored or used for training by the generative AI system (3) Confidentiality class-2 level information or personal data is not handled (4) Undetermined at the planning stage	2	○○○○○○○○
D. Utilization Involving the Judgment by Government Staff on Output Results	Which of the following best describes the operations in relation to the utilization of output results in administrative operations?	(1) Utilized without government staff's judgment on the appropriateness of the generative AI system's output (2) Utilized with government staff's judgment on the appropriateness of the generative AI system's output (3) Undetermined at the planning stage	2	○○○○○○○○

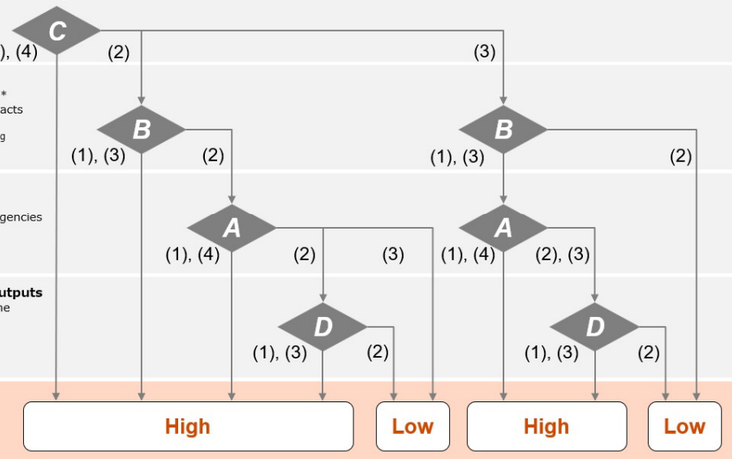
【Judgement Logic】 [High]=[Likely to be classified as "High-Risk"], [Low]=[Unlikely to be classified as "High-Risk"]

C. Presence of Confidential Information or Personal Data in Training Generative AI, etc.
(1) Confidentiality class-2 level information or personal data is stored or used for training
(2) Confidentiality class-2 level information or personal data is handled but not stored or used for training by the generative AI system
(3) Confidentiality class-2 level information or personal data is not handled
(4) Undetermined at the planning stage

B. Characteristics of Operations Using Generative AI
(1) Used in operations where errors could potentially have significant impacts*
(2) Not used in operations where errors could potentially have significant impacts
(3) Undetermined at the planning stage
*Operations substantially affecting the fundamental rights and safety of citizens, operations involving sensitive policy fields, operations impacting human life, physical well-being, and citizen's property, operations requiring qualifications, and operations necessitating high levels of accountability.

A. Scope and Types of Users
(1) Used by citizens, etc. outside ministries and agencies
(2) Used by government staff etc. within and across multiple ministries and agencies (e.g., utilization in a common government system)
(3) Used by government staff etc. within a single ministry
(4) Undetermined at the planning stage

D. Utilization Involving the Judgment by Government Staff on Outputs
(1) Utilized without government staff's judgment on the appropriateness of the generative AI system's output
(2) Utilized with government staff's judgment on the appropriateness of the generative AI system's output
(3) Undetermined at the planning stage



Risk Definition
High: Likely to be classified as “High-Risk”
Low: Unlikely to be classified as “High-Risk

Provisional Translation

Appendix 2

Ministry of ○○ Rules for Users of Generative AI Systems（Model Ver1.0）

Month Date, Year

1. Purpose for Formulating These Rules

The purpose for formulating these rules is to stipulate matters that staff of the Ministry of ○○ must adhere to and consider when using generative AI systems, in order to promote the proper utilization of generative AI by the staff, based on the "Guideline for Japanese Governments' Procurements and Utilizations of Generative AI for the sake of Evolution and Innovation of Public Administration."

2. Rules for Users of Generative AI Systems

Users of generative AI systems must comply with the following rules: (1) Rules Before Use* and (2) Rules During Use.

(*) Please also refer to the "Notice Regarding the Operational Use of Generative AI such as DeepSeek (Administrative Notice)."[1]

(1) Rules Before Use

- Understand that while various benefits are expected by utilizing generative AI, there are also risks such as the leakage of confidential information and hallucinations. (For details on benefits and risks of generative AI, refer to "5 Boosting the Use of Generative AI with an Understanding of Benefits and Risks" in the "Guideline for Japanese Governments' Procurements and Utilizations of Generative AI for the sake of Evolution and Innovation of Public Administration.")
- Understand the usage methods, security considerations, and the accuracy/risk level of outputs from generative AI explained by the planners or providers of the generative AI system (government staff who operate generative AI systems used by other government staff or citizens; the same applies hereinafter). (Example: Before using generative AI, ensure understanding of the environment in which generative AI can be used, conditions for the uses, rules, contact information for consultation, and response measures for information security incidents (as defined in JIS Q

[1] Notice Regarding the Operational Use of Generative AI such as DeepSeek (Administrative Notice) (Japanese version)
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/d2a5bbd2-ae8f-450c-adaa-33979181d26a/e7bfeba7/20250206_councils_social-promotion-executive_outline_01.pdf

27000:2019) and for risk cases particular to generative AI systems.)

- Understand in advance that input and output results from the generative AI system need to be provided to the system's provider when necessary. (Example: Upon request from the Project Management Office (PJMO), if the data is accessible, submit the input data or prompts, output results, and the data provision methods/format, etc.)
- When utilizing cloud-service based generative AI systems in operations, which are offered to a large, unspecified number of users and accessible merely by agreeing to standard terms and conditions or rules, etc., it is in principle prohibited to deal with confidential information. (As an exception, handling of confidential information requires approval from the Information Security Officer in accordance with the information security policy of the Ministry of ○○.) Even if confidential information is not involved, when utilizing cloud-service based generative AI systems in operations, which are offered to a large, unspecified number of users and accessible merely by agreeing to standard terms and conditions or rules, etc., obtaining approval for its utilization is necessary according to the information security policy of the Ministry of ○○. Furthermore, even if confidential information is not involved, it is necessary to understand that if, for instance, server equipment is located overseas, where local laws and regulations may apply, and data may be censored or seized by the local governments and authorities.

(2) Rules During Use

1. Rules Regarding Input Data or Prompts

- Appropriately utilize generative AI systems within the scope of their intended purpose, considering the risks that may arise from misunderstanding or errors by users. (Examples: Utilize the generative AI system in accordance with the usage methods explained by the provider of the generative AI system and refer to its manuals as necessary. Avoid utilizing the generative AI system for purposes outside the scope explained by the provider.
- When inputting prompts containing personal information into the generative AI system, confirm in advance whether the input is permissible, and ensure that the utilization or provision of personal information is minimal and necessary for the intended purpose. (Example: Properly determine whether users can input prompts including personal information by checking the privacy policy or rules for users stipulated by the generative AI system provider of the Ministry of ○○ before using the generative AI system. If unsure, use prompts that do not contain personal information.)

- If administrative organs, etc. input prompts containing retained personal information into a generative AI system and the relevant personal information retained in the system is handled for the purposes different from outputting responses to the relevant prompt, the administrative organ may be in violation of the regulations prescribed in the Act on the Protection of Personal Information (Act No. 57 of 2003). Therefore, when entering such prompts, ensure that the provider of the generative AI system does not utilize the retained personal information for machine learning or any other improper purposes.
- Input accurate and up-to-date data. (Example: Since inaccurate inputs can lead to incorrect responses, users should check whether the information, such as its premise, is accurate or not before inputting data into the generative AI.)

2. Rules Regarding the Utilization of Generated Outputs

- Recognize that decisions made based on outputs from generative AI should be accountable. (Example: Users ensure that they can explain about the generated outputs before utilizing them in their operational tasks. If necessary, rephrase the outputs into expressions that the users can explain by themselves.)
- Make responsible decisions regarding the uses of generative AI outputs in operations. (Example: Users themselves should determine whether it is appropriate to utilize the outputs of generative AI in operations, taking into consideration the biases that can be included in input data, prompts or outputs. If users are unsure whether it is appropriate or not, do not utilize the outputs in operations.)
- Ensure accuracy, rationale, and factuality of the outputs, taking into consideration the level of associated risks.
- Ensure there are no issues regarding safety, fairness, objectivity, or neutrality of the outputs. Be sure to edit, omit, or correct any problematic expressions. (Example: Confirm that there is no use of discriminatory words or expressions that violate ethics, infringe third-party's rights such as copyrights, or do harm to / adversely impact on the life, body, or property of third parties.)
- Properly deal with documents for official duties created by using generative in accordance with the Public Records and Archives Management Act (Act No. 66 of 2009).[2]
- Promptly report to the Chief AI Officer (CAIO) at xxx@xxx.go.jp upon detecting

[2] Regarding the handling of documents formulated by using generative AI, the "Notification Regarding Creation and Management of Administrative Documents Using Digital Technologies" (issued by the Director of the Records and Archives Management Division, the Cabinet Office, on February 14, 2025) states that "documents formulated by staff of administrative organs by using AI in their official duties (such as draft minutes of councils) are regarded as administrative documents if they are retained for organizational use by the administrative organs. However, it is important to undergo necessary verifications to ensure the accuracy of these documents."

significant risk cases particular to generative AI systems. (Example: Generative AI outputs results contain prejudice or discrimination related to race, gender, or culture that could pose major social issues.)

3. Contact Information

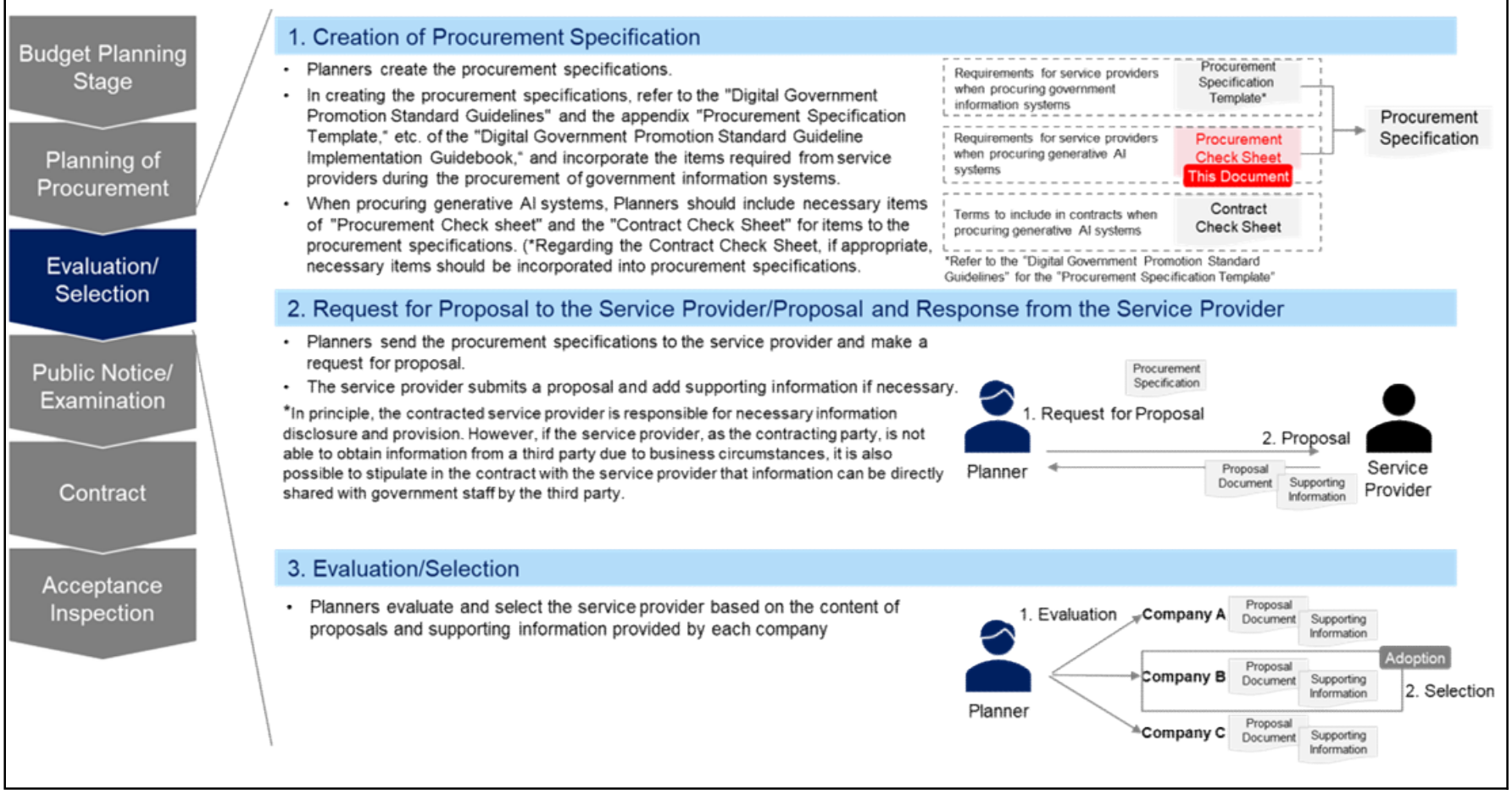
For inquiries regarding these rules, contact the ○○ (Representative) of the Ministry of ○○ (yyy@yy.go.jp). For inquiries about various generative AI systems, contact the representatives of the respective generative AI system provider. (In cases independent reporting rules are set for the use of specific generative AI systems, comply with those rules.)

End of Document

Overview of this Check Sheet

Provisional Translation | **Appendix 3**

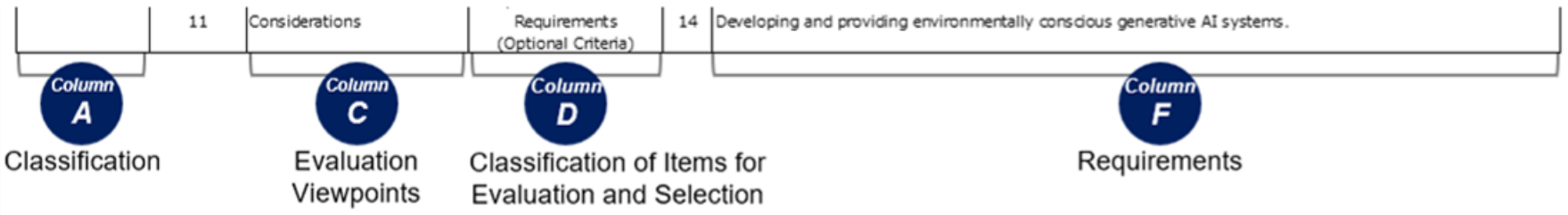
This check sheet organizes the items for evaluating and selecting service providers when procuring generative AI systems.
Planners should refer to this check sheet when creating procurement specifications for procuring generative AI systems. (Also refer to "[Appendix 4] Contract Check Sheet (for Generative AI Systems).” If appropriate, these items should be included in procurement specifications.)
However, this check sheet only includes terms specific to the "procurement of generative AI systems" that require particular attention. Therefore, it is necessary to also refer to the content of the "Digital Government Promotion Standard Guidelines" and the appendix "Procurement Specification Template" of the "Digital Government Promotion Standard Guideline Implementation Guidebook" when creating the procurement specification.
In this check sheet, "[Appendix 3] Procurement Check Sheet (for Generative AI Systems)" is referred to as the "Procurement Check Sheet" and "[Appendix 4] Contract Check Sheet (for Generative AI Systems)” is referred to as the "Contract Check Sheet."



Structure of this Check Sheet

■"Procurement Check Sheet" Sheet

Classification	Evaluation Viewpoints No.	Evaluation Viewpoints	Classification of Items for Evaluation and Selection	Req. No.	Note: Items in this column are requirements for service providers, which are intended to be included in procurement specifications for generative AI systems. Note: The degree of requirement level of each item and selection/addition of items are to be considerd, taking into account the project type, the project stage, the project's risk level, etc., as stated in "6.1.2 Measures to be Addressed Based on this Guideline." Requirements
Requirements on Organizational Matters	1	Compliance with the Common Guiding Principles of the AI Guidelines for Business	Basic Requirements	1	To be able to declare the capability of understanding, comprehending and complying the Common Guiding Principles of the AI Guidelines for Business.
	2	Establishment of AI Governance	Basic Requirements	2	AI governance* is applied in developments and operations of generative AI systems. *A control mechanism/operation mechanism to maximize the positive impact of AI, while managing AI-related risks at an acceptable level.
	3	Understanding of Trends in the AI Industry and Latest Technologies	Basic Requirements	3	Grasping trends in the AI industry and latest technologies to improve quality and explainability in the development and operation of generative AI systems.
	4	Response to Information Security Incidents and Risk Cases Risk Cases Particular to Generative AI Systems	Basic Requirements	4	Having response frameworks and procedures for information security incidents and risk cases particular to generative AI systems (limited to those within the service provider's scope of responsibility), including cooperation responding to users' reports about the insidents in services that your business have developed and is operating.
	5	Enhancement of Education/Literacy Regarding Generative AI for Stakeholders	Basic Requirements	5	Taking necessary actions to enhance literacy about generative AI for staff or sections involved in the development and operation of generative AI systems.
Requirements on Development/ Implementation Processes	6	Handling of Data	Basic Requirements	6	Properly suprevise the handlings of inputs, outputs, or processed data within generative AI systems.
	7	Assurance of Outputs Quality	Basic Requirements	7	Taking proper actions to meet the expected quality standards of generative AI systems.
	8	Avoidance of Vendor Lock-In	Basic Requirements	8	To be able to explicitly describe information on LLMs being used, including version information.
			Optional Additional Requirements (Optional Criteria)	9	To be able to provide disclosure or share information to the planner to a reasonable extent, in order to make sure that parts of the prompts or parameters entered into generative AI systems are not concealed.
			Optional Additional Requirements (Optional Criteria)	10	Having technology to offer features such as saving past chat histories, registering prompts as templates, and exporting such data.
			Optional Additional Requirements (Optional Criteria)	11	Having technology to select or combine the optimal LLM from multiple options, considering that each LLM has characteristics that lead to different functions and behavior, when the primary purpose is not to use of a specific model.
	9	Consideration of Proper Updates to Generative AI Systems	Basic Requirements	12	Mitigate risks from viewpoints particular to generative AI with regard to major system updates or migrations.
	10	Cultural/Linguistic Considerations	Optional Additional Requirements (Optional Criteria)	13	Making outputs from generative AI systems align with the Japanese linguistic and cultural environment.
		Environmental	Optional Additional		

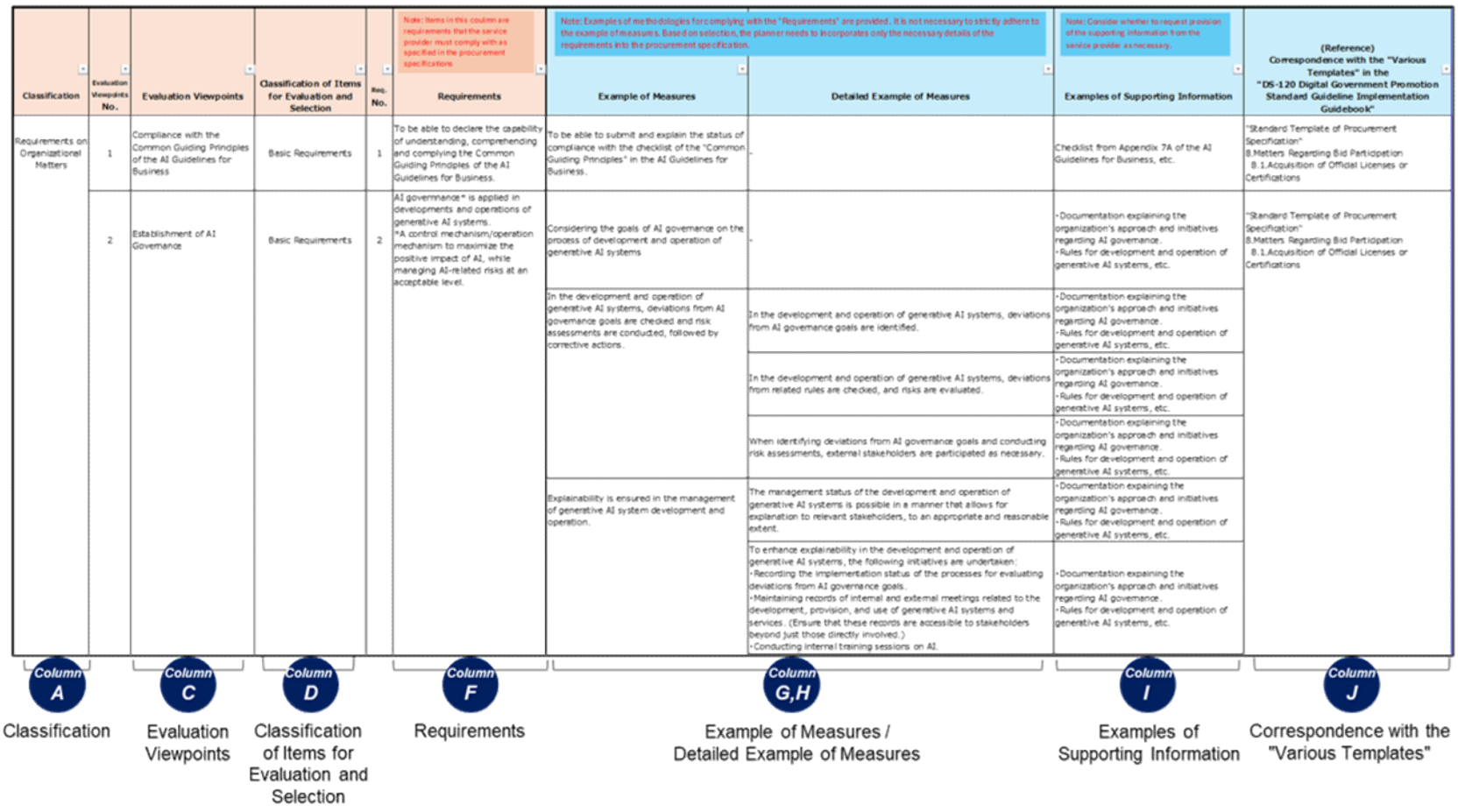


【Column A: Classification】
As a broad framework for evaluating service providers, the "Requirements on Organizational Matters," "Requirements on Development/Implementation Processes," and "Basic Functional Requirements of the Generative AI System" are established. This column distinguishes "Column C: Evaluation Viewpoints" and "Column F: Requirements."

【Column C: Evaluation Viewpoints】
This column describes the purposes and viewpoints for complying with the requirements

【Column D: Classification of Items for Evaluation and Selection】
A column for understanding the requirements that are mandatory in principle. Items that are mandatory in principle are marked as "Basic Requirements." Items that are mandatory in principle under certain conditions are marked as "Applicable as Basic Requirements when XX." Viewpoints that are not mandatory in principle but should be considered are marked as "Optional Additional Requirements (Optional Criteria)."

【Column F: Requirements】
Items in this column are requirements for service providers, which are intended to be included in procurement specifications for generative AI systems. The degree of requirement level of each item and selection/additon of items are to be considered, taking into account the project type, the project stage, the project's risk level, etc., as stated in "6.1.2 Measures to be Addressed Based on this Guideline."



Classification	Evaluation Viewpoints No.	Evaluation Viewpoints	Classification of Items for Evaluation and Selection	Req. No.	Requirements (Note: Items in this column are requirements that the service provider must comply with as specified in the procurement specifications)	Example of Measures (Note: Examples of methodologies for complying with the "Requirements" are provided. It is not necessary to strictly adhere to the example of measures. Based on selection, the planner needs to incorporates only the necessary details of the requirements into the procurement specification.)	Detailed Example of Measures	Examples of Supporting Information (Note: Consider whether to request provision of the supporting information from the service provider as necessary.)	(Reference) Correspondence with the "Various Templates" in the "DS-120 Digital Government Promotion Standard Guideline Implementation Guidebook"
Requirements on Organizational Matters	1	Compliance with the Common Guiding Principles of the AI Guidelines for Business	Basic Requirements	1	To be able to declare the capability of understanding, comprehending and complying the Common Guiding Principles of the AI Guidelines for Business.	To be able to submit and explain the status of compliance with the checklist of the "Common Guiding Principles" in the AI Guidelines for Business.	-	Checklist from Appendix 7A of the AI Guidelines for Business, etc.	"Standard Template of Procurement Specification" 8.Matters Regarding Bid Participation 8.1.Acquisition of Official Licenses or Certifications
	2	Establishment of AI Governance	Basic Requirements	2	AI governance* is applied in developments and operations of generative AI systems. *A control mechanism/operation mechanism to maximize the positive impact of AI, while managing AI-related risks at an acceptable level.	Considering the goals of AI governance on the process of development and operation of generative AI systems	-	・Documentation explaining the organization's approach and initiatives regarding AI governance. ・Rules for development and operation of generative AI systems, etc.	"Standard Template of Procurement Specification" 8.Matters Regarding Bid Participation 8.1.Acquisition of Official Licenses or Certifications
						In the development and operation of generative AI systems, deviations from AI governance goals are checked and risk assessments are conducted, followed by corrective actions.	In the development and operation of generative AI systems, deviations from AI governance goals are identified.	・Documentation explaining the organization's approach and initiatives regarding AI governance. ・Rules for development and operation of generative AI systems, etc.	
							In the development and operation of generative AI systems, deviations from related rules are checked, and risks are evaluated.	・Documentation explaining the organization's approach and initiatives regarding AI governance. ・Rules for development and operation of generative AI systems, etc.	
							When identifying deviations from AI governance goals and conducting risk assessments, external stakeholders are participated as necessary.	・Documentation explaining the organization's approach and initiatives regarding AI governance. ・Rules for development and operation of generative AI systems, etc.	
						Explainability is ensured in the management of generative AI system development and operation.	The management status of the development and operation of generative AI systems is possible in a manner that allows for explanation to relevant stakeholders, to an appropriate and reasonable extent.	・Documentation explaining the organization's approach and initiatives regarding AI governance. ・Rules for development and operation of generative AI systems, etc.	
							To enhance explainability in the development and operation of generative AI systems, the following initiatives are undertaken: ・Recording the implementation status of the processes for evaluating deviations from AI governance goals. ・Maintaining records of internal and external meetings related to the development, provision, and use of generative AI systems and services. (Ensure that these records are accessible to stakeholders beyond just those directly involved.) ・Conducting internal training sessions on AI.	・Documentation explaining the organization's approach and initiatives regarding AI governance. ・Rules for development and operation of generative AI systems, etc.	

【Column A: Classification】
As a broad framework for evaluating service providers, the "Requirements on Organizational Matters," "Requirements on Development/Implementation Processes," and "Basic Functional Requirements of the Generative AI System" are established. This column distinguishes "Column C: Evaluation Viewpoints" and "Column F: Requirements."

【Column C: Evaluation Viewpoints】
Describes the purposes and viewpoints for complying with the requirements

【Column D: Classification of Items for Evaluation and Selection】
A column for understanding the requirements that are mandatory in principle. Items that are mandatory in principle are marked as "Basic Requirements." Items that are mandatory in principle under certain conditions are marked as "Applicable as Basic Requirements when XX." Viewpoints that are not mandatory in principle but should be considered are marked as "Optional Additional Requirements (Optional Criteria)."

【Column F: Requirements】
Items in this column are requirements for service providers, which are intended to be included in procurement specifications for generative AI systems. The degree of requirement level of each item and selection/additon of items are to be considered, taking into account the project type, the project stage, the project's risk level, etc., as stated in "6.1.2 Measures to be Addressed Based on this Guideline" of this guideline.

【Column G/Column H: Example of Measures/Detailed Example of Measures】
Examples of methodologies for complying with "Column F: Requirements" are provided. It is not necessary to strictly adhere to the examples of measures. Based on selection, the planner incorporates only the necessary details of the requirements into the procurement specification.

【Column I: Examples of Supporting Information】
Examples of information used to determine whether the requirements are fulfilled are provided. Consider whether to request provision of this information from the service provider if necessary.

【Column J: (Reference) Correspondence with the "Various Templates" in the "DS-120 Digital Government Promotion Standard Guideline Implementation Guidebook"】
This column provides the correspondence of the requirements with the "Digital Government Promotion Standard Guidelines" and the appendix "Procurement Specification Template," "Requirement Definition Document Template"of the "Digital Government Promotion Standard Guideline Implementation Guidebook." When creating the procurement specification, refer to these various templates.

*Regarding example of measures, detailed example of measures, and examples of supporting information, updates to the descriptions will be considered flexibly, taking into account changes in technology and business environments.

How to Use this Check Sheet

・Planners should incorporate necessary items from "Column F: Requirements" into the procurement specification.
  *At that time, refer to "Column D: Classification of Items for Evaluation and Selection." "Basic Requirements" are assumed to be mandatory items to be fulfilled in principle for evaluating and selecting service providers.
  *"Optional Additional Requirements (Optional Criteria)" are not mandatory but are viewpoints that should be considered. If included as evaluation items, they are assumed to be additional factors.
  *Requirements that state "Applicable when used outside of ministries or agencies" or "Applicable when handling personal information," etc., are assumed to be mandatory items to be fulfilled in principle if the project meets the conditions.
  *"Column G/Column H: Example of Measures/Detailed Example of Measures" are literally examples; not necesarily need to be fully satisfied, and adherence to requirements by using the methods other than these examples is acceptable.
  *Additionally, refer to the "Procurement Specification Template" required by the "Digital Government Promotion Standard Guidelines" and include items in it necessary for procuring government information systems.
・Planners should determine the information requested to be provided by the service provider by referring to "Column I: Examples of Supporting Information."
・Planners should distribute the procurement specifications to potential service providers and requests proposals.
・Planners should evaluate and select service providers based on their proposals and responses.

Scope of this Check Sheet

This check sheet applies to systems that incorporate generative AI, as described in "2.2.2 Generative AI Targeted by this Guideline," within the government information systems mentioned in "2.2.1 Information Systems Targeted by this Guideline."

Supplementary Explanation of Terms

・Large Language Model (LLM): A language model that treats the probability of occurrence of sentences and words as a deep learning model, built using a very large amount of training data. (Source: Guidelines for Quality Assurance of AI-based Products and Services by Consortium of Quality Assurance for Artificial-Intelligence-based Products and Services, 10-1)
・Generative AI: A general term representing AI developed from an AI model that can generate texts, images, programs, etc. (Source: AI Guidelines for Business, P.10)
・Generative AI System: Government Information Systems that comprise generative (only the types of generative AI which is targeted by this guideline) as a component. (In accordance with Guide to Evaluation Perspectives on AI Safety (Version 1.01) by Japan AI Safety Institute, P.9)
・Raw Data for Training: Data provided by the user to the provider for input into the generative AI system during training.
・Training Data: Data created by the service provider for training purposes through processing and modification of the raw data (for training) provided by the user.
・Information Security Incidents: Refers to information security incidents as defined in JIS Q 27000:2019.
・Risk Cases Particular to Generative AI Systems: A condition where risks inherent to a generative AI system have materialized, or where signs or events indicating the possible materialization of such risks are observed, which may have significant impacts.

Procurement Check Sheet					
Classification	**Evaluation Viewpoints No.**	**Evaluation Viewpoints**	**Classification of Items for Evaluation and Selection**	**Req. No.**	Note: Items in this column are requirements for service providers, which are intended to be included in procurement specifications for generative AI systems. Note: The degree of requirement level of each item and selection/additon of items are to be considered, taking into account the project type, the project stage, the project's risk level, etc., as stated in "6.1.2 Measures to be Addressed Based on this Guideline." **Requirements**
Requirements on Organizational Matters	1	Compliance with the Common Guiding Principles of the AI Guidelines for Business	Basic Requirements	1	To be able to declare the capability of understanding, comprehending and complying the Common Guiding Principles of the AI Guidelines for Business.
	2	Establishment of AI Governance	Basic Requirements	2	AI governnance* is applied in developments and operations of generative AI systems. *A control mechanism/operation mechanism to maximize the positive impact of AI, while managing AI-related risks at an acceptable level.
	3	Understanding of Trends in the AI Industry and Latest Technologies	Basic Requirements	3	Grasping trends in the AI industry and latest technologies to improve quality and explainability in the development and operation of generative AI systems.
	4	Response to Information Security Incidents and Risk Cases Risk Cases Particular to Generative AI Systems	Basic Requirements	4	Having response frameworks and procedures for information security incidents and risk cases particular to generative AI systems (limited to those within the service provider's scope of responsibility), including cooperation responding to users' reports about the insidents in services that your business have developed and is operating.
	5	Enhancement of Education/Literacy Regarding Generative AI for Stakeholders	Basic Requirements	5	Taking necessary actions to enhance literacy about generative AI for staff or sections involved in the development and operation of generative AI systems.
Requirements on Development/ Implementation Processes	6	Handling of Data	Basic Requirements	6	Properly suprevise the handlings of inputs, outputs, or processed data within generative AI systems.
	7	Assurance of Outputs Quality	Basic Requirements	7	Taking proper actions to meet the expected quality standards of generative AI systems.
	8	Avoidance of Vendor Lock-In	Basic Requirements	8	To be able to explicitly describe information on LLMs being used, including version information.
			Optional Additional Requirements (Optional Criteria)	9	To be able to provide disclosure or share information to the planner to a reasonable extent, in order to make sure that parts of the prompts or parameters entered into generative AI systems are not concealed.
			Optional Additional Requirements (Optional Criteria)	10	Having technology to offer features such as saving past chat histories, registering prompts as templates, and exporting such data.
			Optional Additional Requirements (Optional Criteria)	11	Having technology to select or combine the optimal LLM from multiple options, considering that each LLM has characteristics that lead to different functions and behavior, when the primary purpose is not to use of a specific model.
	9	Consideration of Proper Updates to Generative AI Systems	Basic Requirements	12	Mitigate risks from viewpoints particular to generative AI with regard to major system updates or migrations.
	10	Cultural/Linguistic Considerations	Optional Additional Requirements (Optional Criteria)	13	Making outputs from generative AI systems align with the Japanese linguistic and cultural environment.
	11	Environmental Considerations	Optional Additional Requirements (Optional Criteria)	14	Developing and providing environmentally conscious generative AI systems.
Basic Functional Requirements of the Generative AI System	12	Control of Harmful Output	Basic Requirements	15	Controlling outputs of harmful information by generative AI systems, such as information related to terrorism, crime, or offensive expressions.
	13	Prevention of Misinformation, Disinformation and Manipulation	Basic Requirements	16	Implementing measures to prevent the output of misinformation/disinformation by generative AI systems.
			Applicable as Basic Requirements when used outside of ministries or agencies (For example, used by citizens, etc.)	17	Ensuring that end users can distinguish the output of generative AI systems from information output by humans.
				18	Preventing the undue inducement of generative AI systems on the decision-making of end users.
	14	Fairness and Inclusion	Applicable as Basic Requirements when used outside of ministries or agencies (For example, used by citizens, etc.)	19	Ensuring that the output of generative AI systems does not contain harmful biases and discrimination.
			Basic Requirements	20	Ensuring that the output of generative AI systems is sufficiently readable to all end users.
	15	Addressing Uses for Purpose Other than the Original Intent	Basic Requirements	21	Preventing uses for the purpose other than the original intent and ensuring that even if misuse occurs, no significant harm or disadvantage arises.
	16	Personal Information, Privacy, Intellectual Property	Applicable as Basic Requirements when handling personal information, privacy, and intellectual property	22	Ensuring appropriate handling of personal information collected, processed, and stored by generative AI systems, as well as protecting intellectual property and privacy.
	17	Ensuring Security	Basic Requirements	23	Addressing vulnerabilities across the entire generative AI system and preventing impacts from unauthorized operations.
			Basic Requirements	24	Appropriately implementing security measures throughout the development process of generative AI systems.
	18	Explainability	Basic Requirements	25	Ensuring that the rationale for outputs can be confirmed to a technically reasonable extent.
	19	Robustness	Basic Requirements	26	Ensuring that generative AI systems provide stable outputs in response to inputs.
	20	Data Quality	Basic Requirements	27	Maintaining the data accessed by generative AI systems in an appropriate state.
			Optional Additional Requirements (Optional Criteria)	28	Structuring input data appropriately to enhance the outputs of generative AI systems.
	21	Verifiability	Basic Requirements	29	Making the development and provision processes of generative AI systems verifiable.

Procurement Check Sheet

Classification	Evaluation Viewpoints No.	Evaluation Viewpoints	Classification of Items for Evaluation and Selection	Req. No.	Requirements Note: Items in this coulmn are requirements that the service provider must comply with as specified in the procurement specifications	Example of Measures Note: Examples of methodologies for complying with the "Requirements" are provided. It is not necessary to strictly adhere to the example of measures. Based on selection, the planner needs to incorporates only the necessary details of the requirements into the procurement specification.	Detailed Example of Measures	Examples of Supporting Information Note: Consider whether to request provision of the supporting information from the service provider as necessary.	(Reference) Correspondence with the "Various Templates" in the "DS-120 Digital Government Promotion Standard Guideline Implementation Guidebook"
Requirements on Organizational Matters	1	Compliance with the Common Guiding Principles of the AI Guidelines for Business	Basic Requirements	1	To be able to declare the capability of understanding, comprehending and complying the Common Guiding Principles of the AI Guidelines for Business.	To be able to submit and explain the status of compliance with the checklist of the "Common Guiding Principles" in the AI Guidelines for Business.	-	Checklist from Appendix 7A of the AI Guidelines for Business, etc.	"Standard Template of Procurement Specification" 8.Matters Regarding Bid Participation 8.1.Acquisition of Official Licenses or Certifications
	2	Establishment of AI Governance	Basic Requirements	2	AI governnance* is applied in developments and operations of generative AI systems. *A control mechanism/operation mechanism to maximize the positive impact of AI, while managing AI-related risks at an acceptable level.	Considering the goals of AI governance on the process of development and operation of generative AI systems	-	・Documentation explaining the organization's approach and initiatives regarding AI governance. ・Rules for development and operation of generative AI systems, etc.	"Standard Template of Procurement Specification" 8.Matters Regarding Bid Participation 8.1.Acquisition of Official Licenses or Certifications
						In the development and operation of generative AI systems, deviations from AI governance goals are checked and risk assessments are conducted, followed by corrective actions.	In the development and operation of generative AI systems, deviations from AI governance goals are identified.	・Documentation explaining the organization's approach and initiatives regarding AI governance. ・Rules for development and operation of generative AI systems, etc.	
							In the development and operation of generative AI systems, deviations from related rules are checked, and risks are evaluated.	・Documentation explaining the organization's approach and initiatives regarding AI governance. ・Rules for development and operation of generative AI systems, etc.	
							When identifying deviations from AI governance goals and conducting risk assessments, external stakeholders are participated as necessary.	・Documentation explaining the organization's approach and initiatives regarding AI governance. ・Rules for development and operation of generative AI systems, etc.	
						Explainability is ensured in the management of generative AI system development and operation.	The management status of the development and operation of generative AI systems is possible in a manner that allows for explanation to relevant stakeholders, to an appropriate and reasonable extent.	・Documentation expaining the organization's approach and initiatives regarding AI governance. ・Rules for development and operation of generative AI systems, etc.	
							To enhance explainability in the development and operation of generative AI systems, the following initiatives are undertaken: ・Recording the implementation status of the processes for evaluating deviations from AI governance goals. ・Maintaining records of internal and external meetings related to the development, provision, and use of generative AI systems and services. (Ensure that these records are accessible to stakeholders beyond just those directly involved.) ・Conducting internal training sessions on AI.	・Documentation expaining the organization's approach and initiatives regarding AI governance. ・Rules for development and operation of generative AI systems, etc.	
							The following matters related to the generative AI system are determined, and information is provided to users in a timely and appropriate manner: ・Proper/improper usage methods, etc. ・Information regarding safety, including the technical features of the generative AI system to be provided, mechanisms for ensuring safety, foreseeable risks that may arise from the results of use, and the relevant mitigation measures, etc. ・The potential for changes in outputs or programming, due to training, etc. of the generative AI system. ・Information regarding the operational status of the generative AI system, causes of malfunctions and their resolution status, example cases of information security incidents and risk cases particular to generative AI systems, etc. ・Information on updates made to the generative AI system, including the details and reasons for these updates. ・Policies regarding the collection of data for training, training methods, and training implementation framework, etc. ・Terms of services and privacy policies. ・Setting the intended scope of use as designed by AI developers to prevent harm from unintended provisions/uses not anticipated during development. ・Information regarding the operational status of the generative AI system, causes of malfunctions, and their resolution status.	・Documentation provided to users, such as manuals and contracts, etc. as well as materials available on the service provider's website or product brochures, which include the items mentioned in the left . ・Documentation expalining the organization's approach and initiatives regarding AI governance. ・Rules for development and operation of generative AI systems, etc.	
							A unique checklist for deviation evaluation (deviation from governance rules) is created and used as the basis for checking and recording the implementation status of the deviation evaluation process.	・Documentation explaining the organization's approach and initiatives regarding AI governance. ・Rules for development and operation of generative AI systems, etc.	
						Verification is conducted to ensure that the management methods and functionalities in the development and operation of generative AI systems are appropriate.	Monitoring is conducted to determine whether management in the development and operation of generative AI systems is functioning appropriately.	・Documentation explaing the organization's approach and initiatives regarding AI governance. ・Rules for development and operation of generative AI systems, etc.	
							Continuous improvements are made based on the results of monitoring.	・Documentation expaining the organization's approach and initiatives regarding AI governance. ・Rules for development and operation of generative AI systems, etc.	
	3	Understanding of Trends in the AI Industry and Latest Technologies	Basic Requirements	3	Grasping trends in the AI industry and latest technologies to improve quality and explainability in the development and operation of generative AI systems.	Industry guidelines, laws, and the latest technologies related to the development and operation of generative AI systems are grasped.	References are made to initiatives like the "Machine Learning Quality Management Guideline" by the National Institute of Advanced Industrial Science and Technology for standardization efforts.	Industry guidelines and list of technologies referenced.	"Standard Template of Procurement Specification" 8.Matters Regarding Bid Participation 8.1.Acquisition of Official Licenses or Certifications
							Initiatives such as participation in AI-related study groups and industry associations, understanding latest technologies, and exchanging opinions with experts are conducted.	List AI-related study groups and industry associations in which membership is held.	
	4	Response to Information Security Incidents and Risk Cases Risk Cases Particular to Generative AI Systems	Basic Requirements	4	Having response frameworks and procedures for information security incidents and risk cases particular to generative AI systems (limited to those within the service provider's scope of responsibility), including cooperation responding to users' reports about the insidents in services that your business have developed and is operating.	Schemes and procedures for responding to information security incidents and risk cases particular to generative AI systems are established.	Response schemes, policies, and plans are formulated for handling information security incidents and risk cases particular to generative AI systems during their development and operation.	・Documentation explaining AI governance rules, etc. (including materials that demonstrate the establishment of schemes and procedures for responding to information security incidents and risk cases particular to generative AI systems).	"Standard Template of Procurement Specification" 6.Compliance Matters in the Execution of Tasks 6.1.Confidentiality and Handling of Materials "Standard Template of Requirement Definition Document" 3.Non-functional Requirements Definition 3.10.Regarding Information Security Matters
							In preparation for information security incidents and risk cases particular to generative AI systems, the following schemes are established in advance: ・Setting up a contact reception desk ・Assigning responsible officials to projects ・Allocating roles among individual personnel ・Defining response approaches and processes ・Establishing processes for notifying affected stakeholders, etc.	・Documentation explaining AI governance rules, etc. (including materials that demonstrate the establishment of schemes and procedures for responding to information security incidents and risk cases particular to generative AI systems).	
						Education and training on the response to information security incidents and risk cases particular to generative AI systems are implemented.	Practical rehearsals are conducted as necessary regarding the response policies and plans for information security incidents and risk cases particular to generative AI systems, which may arise during the development and operation of generative AI systems.	・Documentation explaining AI governance rules, etc. (including materials about education and training related to responses to information security incidents and risk cases particular to generative AI systems have been conducted).	
	5	Enhancement of Education/Literacy Regarding Generative AI for Stakeholders	Basic Requirements	5	Taking necessary actions to enhance literacy about generative AI for staff or sections involved in the development and operation of generative AI systems.	Education and training tailored to specific roles are conducted to ensure that individuals involved in the development and operation of generative AI possess appropriate literacy, including technical knowledge, risk awareness, and ethics related to generative AI.	-	・Documentation explaining AI governance rules, etc. (including materials about initiatives undertaken to enhance AI literacy through education, training, etc.).	"Standard Template of Procurement Specification" 5.Matters Regarding the Work Execution Structure and Methods 5.2.Requirements for Licenses of Personnel
Requirements on Development/ Implementation Processes	6	Handling of Data	Basic Requirements	6	Properly suprevise the handlings of inputs, outputs, or processed data within generative AI systems.	In alignment with the project's objectives, the purposes and conditions for using inputs (such as prompts and raw data for training) are defined within the necessary scope.	-	Documentation that clarifies the purposes for which the inputs (such as prompts, raw data for training) are used by the service provider, etc.	"Standard Template of Requirement Definition Document" 3.Non-functional Requirements Definition 3.2.Matters Regarding System Architecture 3.3.Matters Regarding System Scale 3.10.Matters Regarding Information Security
						In alignment with the project's objectives, management and security frameworks for inputs (such as prompts and raw data for training) are established within the necessary scope, with measures taken to prevent issues.	-	Documentation that clarifies the policies for the management and security framework of inputs (such as prompts, raw data for training), etc.	
						In alignment with the project's objectives, the retention period and deletion of inputs (such as prompts and raw data for training) are managed within the necessary scope, with measures taken to prevent issues.	-	Documentation that clarifies the management policy for the retention period and deletion of inputs (such as prompts, raw data for training), etc.	
						In alignment with the project's objectives, management of external provision of inputs (such as prompts and raw data for training) is well conducted within the necessary scope, including stipulating obligations for providing the inputs to users of the generative AI system.	-	Documentation that clarifies the obligation to provide inputs (such as prompts, raw data for training) to users, etc.	
						In alignment with the project's objectives, management related to third-party provision of inputs (such as prompts and raw data for training) is secured within the necessary scope.	-	Documentation that clarifies the management policy regarding the provision of inputs (such as prompts, raw data for training) to third parties, etc.	

Procurement Check Sheet									
Classification	Evaluation Viewpoints No.	Evaluation Viewpoints	Classification of Items for Evaluation and Selection	Req. No.	Note: Items in this coulmn are requirements that the service provider must comply with as specified in the procurement specifications Requirements	Note: Examples of methodologies for complying with the "Requirements" are provided. It is not necessary to strictly adhere to the example of measures. Based on selection, the planner needs to incorporates only the necessary details of the requirements into the procurement specification. Example of Measures	Detailed Example of Measures	Note: Consider whether to request provision of the supporting information from the service provider as necessary. Examples of Supporting Information	(Reference) Correspondence with the "Various Templates" in the "DS-120 Digital Government Promotion Standard Guideline Implementation Guidebook"
						In alignment with the project's objectives, the use and utilization of input processing results (such as training data, intermediate outputs, and derivative intellectual property) are well managed within the necessary scope.	-	Documentation that clarifies management policies for the use and utilization of input processing results (such as training data, intermediate outputs, derivative intellectual property), etc.	
						In alignment with the project's objectives, the external provision of input processing results (such as training data, intermediate outputs, and derivative intellectual property) is well managed within the necessary scope.	-	Documentation that clarifies the management policy for the external provision of input processing results (such as training data, intermediate outputs, derivative intellectual property), etc.	
						In alignment with the project's objectives, appropriate protective measures can be implemented, such as considering the implementation of data management and restriction functions to manage data access throughout the pre-training and the overall training process, within the necessary scope.	-	Documentation that clarifies policies for protective measures for data throughout the pre-training and the entire training process, etc.	
	7	Assurance of Outputs Quality	Basic Requirements	7	Taking proper actions to meet the expected quality standards of generative AI systems.	When using generative AI for chats, the expected quality standards of chat uses are defined, and measurements and evaluations are conducted to determine if these standards are met.	-	Documentation that clarifies the evaluation criteria and thier contents using benchmarks, etc.* such as JMMLU, JHumanEval, JBBQ. (*)This does not preclude independent evaluations based on certain reliable evaluation standards.	"Standard Template of Requirement Definition Document" 3.Non-functional Requirements Definition 3.12.Matters Regarding Testing 3.17.Matters Regarding Maintenance
						Evaluate whether the expected quality standards of generative AI are met using test cases. In doing so, propose multiple test cases (such as batch processing, information retrieval, program creation from natural language).	-	Documentation that clarifies test case examples and testing policies when using generative AI for batch processing.	
	8	Avoidance of Vendor Lock-In	Basic Requirements	8	To be able to explicitly describe information on LLMs being used, including version information.	Organize and publish a list of available LLMs and their information about versions, etc.	-	Documentation that clarifies the methods for disclosing version information of the LLMs in use, etc.	"Standard Template of Requirement Definition Document" 3.Non-functional Requirements Definition 3.8.Matters Regarding Neutrality 3.11.Matters Regarding Information System Operating Environment
			Optional Additional Requirements (Optional Criteria)	9	To be able to provide disclosure or share information to the planner to a reasonable extent, in order to make sure that parts of the prompts or parameters entered into generative AI systems are not concealed.	Declare and ensure that it is technically possible to disclose and provide information, such as system prompts, to planners during development and operation to a reasonable extent.	-	Documentation declaring that certain prompts and parameters input to the LLM are not concealed.	"Standard Template of Requirement Definition Document" 3.Non-functional Requirements Definition 3.8.Matters Regarding Neutrality 3.10.Matters Regarding Information Security
			Optional Additional Requirements (Optional Criteria)	10	Having technology to offer features such as saving past chat histories, registering prompts as templates, and exporting such data.	Declare and ensure the capability to develop functions for saving past chat histories, templating prompts, and exporting these features.	-	Documentation that clarifies the methods for implementing functions to save past chat histories, register prompts as templates, and export such data, etc.	"Standard Template of Requirement Definition Document" 3.Non-functional Requirements Definition 3.8.Matters Regarding Neutrality 3.1.Matters Regarding Usability and Accessibility 3.13.Matters Regarding Migration
			Optional Additional Requirements (Optional Criteria)	11	Having technology to select or combine the optimal LLM from multiple options, considering that each LLM has characteristics that lead to different functions and behavior, when the primary purpose is not to use of a specific model.	Declare and ensure the capability (1) to utilize multiple LLMs and (2) to select LLMs, including the possibility to use them in combination.	-	Documentation that clarifies the track record of having the technology to select or combine the most suitable LLM from multiple options, etc.	"Standard Template of Requirement Definition Document" 3.Non-functional Requirements Definition 3.8.Matters Regarding Neutrality 3.11.Matters Regarding Information System Operating Environment
	9	Consideration of Proper Updates to Generative AI Systems	Basic Requirements	12	Mitigate risks from viewpoints particular to generative AI with regard to major system updates or migrations.	Before major updates or transitions of LLM models, ensure that it is possible to verify whether the performance of the candidate LLM for transition meets the standards for output quality and safety, among other factors.	-	Documentation that clarifies the methods that enable to verify whether the candidate LLM for transition meets the standards for output quality and safety, among other factors, before updating the LLM, etc.	"Standard Template of Requirement Definition Document" 3.Non-functional Requirements Definition 3.16.Matters Regarding Operations 3.17.Matters Regarding Maintenance
	10	Cultural/Linguistic Considerations	Optional Additional Requirements (Optional Criteria)	13	Making outputs from generative AI systems align with the Japanese linguistic and cultural environment.	Providing a generative AI system capable of producing outputs that consider the Japanese linguistic and cultural environment.	-	Documentation that clarifies the verification policies for ensuring outputs are in accordance with the Japanese linguistic and cultural environment; documentation that clarifies initiatives are undertaken during development with training data, etc., to align with the Japanese linguistic and cultural environment; documentation that clarifies the evaluation results using benchmarks for measuring Japanese language proficiency (for example, as benchmarks for measuring Japanese language proficiency, there are JGLUE (Japanese General Language Understanding Evaluation), JMMLU (Japanese Massive Multitask Language Understanding Benchmark), etc.), etc. *This does not preclude the use of widely recognized and reliably established evaluation criteria.	"Standard Template of Requirement Definition Document" 3.Non-functional Requirements Definition 3.1.Matters Regarding Usability and Accessibility
	11	Environmental Considerations	Optional Additional Requirements (Optional Criteria)	14	Developing and providing environmentally conscious generative AI systems.	Providing or using a generative AI system that considers environmental impact; for example, by using models trained on hardware featuring energy-efficient semiconductors.	-	Documentation that clarifies superior environmental performance in terms of power consumption, etc.	"Standard Template of Procurement Specification" 4.Matters Regarding the Content of Task Execution 4.17.Other
Basic Functional Requirements of the Generative AI System	12	Control of Harmful Output	Basic Requirements	15	Controlling outputs of harmful information by generative AI systems, such as information related to terrorism, crime, or offensive expressions.	Having technology that provides a mechanism to ensure that when test data containing harmful information is input or expected to be output, the generative AI system either excludes such information from its outputs or has the ability to refuse generating the output.	Having technology that provides a mechanism to ensure that when test data containing information that could be used in cyberattacks, crimes such as terrorism, or CBRN (Chemical, Biological, Radiological, Nuclear) is input or expected to be output, the generative AI system excludes such harmful information from its outputs or has the ability to refuse generating the output.	Documentation that clarifies the implementation methods of a mechanism ensuring that the generative AI system excludes harmful information from its outputs or has the ability to refuse generating harmful output, etc., when test data containing information that could be used in cyberattacks, crimes such as terrorism, or CBRN is input or expected to be output.	"Standard Template of Requirement Definition Document" 3.Non-functional Requirements Definition 3.1.Matters Regarding Usability and Accessibility
							Having technology that provides a mechanism to ensure that when test data containing discriminatory expressions or information that could cause emotional distress to end users is input or expected to be output, the generative AI system excludes such harmful information from its outputs or has the ability to refuse generating the output.	Documentation that clarifies the implementation methods of a mechanism ensuring that the generative AI system excludes harmful information from its outputs or has the ability to refuse generating hurmful output, etc., when test data containing discriminatory expressions or information that could cause emotional distress to end users is input or expected to be output, .	
						Measuring and evaluating the harmfulness score of generative AI system outputs, which quantifies aspects like offensiveness.	-	Documentation that clarifies the harmfulness scores of generative AI system outputs, along with the methods for measuring these scores, etc.	
	13	Prevention of Misinformation, Disinformation and Manipulation	Basic Requirements	16	Implementing measures to prevent the output of misinformation/disinformation by generative AI systems.	Measures are in place to ensure that when the same factual test data is input into different LLMs, the outputs are semantically identical and factually correct.	-	Documentation that outlines the results when the same factual test data is input into different LLMs, etc.	"Standard Template of Requirement Definition Document" 3.Non-functional Requirements Definition 3.1.Matters Regarding Usability and Accessibility
						The evaluation scores concerning the prevention of misinformation, disinformation outputs have been measured, and it has been confirmed that there are no issues with the scores.	The scores, related to the relevance between prompts and output data in generative AI systems, are measured and evaluated.	Documentation that clarifies the scores related to the relevance between prompts and output data in generative AI systems, along with the methods for measuring these scores, etc.	

Procurement Check Sheet									
Classification	Evaluation Viewpoints No.	Evaluation Viewpoints	Classification of Items for Evaluation and Selection	Req. No.	Note: Items in this coulmn are requirements that the service provider must comply with as specified in the procurement specifications Requirements	Note: Examples of methodologies for complying with the "Requirements" are provided. It is not necessary to strictly adhere to the example of measures. Based on selection, the planner needs to incorporates only the necessary details of the requirements into the procurement specification. Example of Measures	Detailed Example of Measures	Note: Consider whether to request provision of the supporting information from the service provider as necessary. Examples of Supporting Information	(Reference) Correspondence with the "Various Templates" in the "DS-120 Digital Government Promotion Standard Guideline Implementation Guidebook"
							The scores, related to the relevance between output data from generative AI systems and search results produced by RAG, are measured and evaluated. *This measure applies only to generative AI systems using RAG.	Documentation that clarifies the scores related to the relevance between output data from generative AI systems and search results produced by RAG, along with the methods for measuring these scores, etc.	
							The scores, related to the consistency between output data from generative AI systems and search results produced by RAG, are measured and evaluated. *This measure applies only to generative AI systems using RAG.	Documentation that clarifies the scores related to the the consistency between output data from generative AI systems and search results produced by RAG, along with the methods for measuring these scores, etc.	
							The scores, related to the semantic consistency between correct data and search results produced by RAG, are measured and evaluated. *This measure applies only to generative AI systems using RAG.	Documentation that clarifies the scores related to the semantic consistency between correct data and search results produced by RAG, along with the methods for measuring these scores, etc.	
							Having the technology that provides mechanisms for ensuring appropriate content authentication in generative AI systems with output content verification, even when various prompts are input.	Documentation that clarifies the implementation methods for mechanisms ensuring appropriate content authentication for various prompts input into generative AI systems, etc.	
							To be able to check that (i)documents targeted for search in generative AI systems using RAG or (ii) the correct data prepared for evaluation by evaluators are fact-based data. *This measure applies only to generative AI systems using RAG.	Records confirming that documents targeted for search in generative AI systems using RAG or the correct data prepared by evaluators for evaluation are fact-based data, etc.	
			Applicable as Basic Requirements when used outside of ministries or agencies (For example, used by citizens, etc.)	17	Ensuring that end users can distinguish the output of generative AI systems from information output by humans.	Having technology that provides mechanisms for end users to distinguish outputs by generative AI systems from information output by humans.	-	Documentation that clarifies the implementation mechanisms for end users to distinguish outputs by generative AI systems from information output by humans, etc.	"Standard Template of Requirement Definition Document" 3.Non-functional Requirements Definition 3.1.Matters Regarding Usability and Accessibility
				18	Preventing the undue inducement of generative AI systems on the decision-making of end users.	Having technology that provides mechanisms for end users to identify content generated by generative AI systems in news articles, social media, etc.	-	Documentation that clarifies the implementation methods for mechanisms for end users to identify content generated by generative AI systems in news articles, social media, etc.	"Standard Template of Requirement Definition Document" 3.Non-functional Requirements Definition 3.1.Matters Regarding Usability and Accessibility
						Measures are in place to prevent end users from being induced into actions that may lead to subjective or objective disadvantages, based on recommendations or instructions from the generative AI system.	-	Documentation that clarifies the methods for verifying that outputs from generative AI systems do not induce end users into actions that may lead to subjective or objective disadvantages due to the systems' recommendations or instructions, etc.	
						Having technology to provide mechanisms for including opt-in or opt-out options regarding the inducement by the generative AI (for example, message generation including URL links, etc.) in the outputs of generative AI systems.	-	Documentation that clarifies the implementation methods for mechanisms to include opt-in or opt-out options regarding inducement by generative AI systems in their outputs, etc.	
14	Fairness and Inclusion	Applicable as Basic Requirements when used outside of ministries or agencies (For example, used by citizens, etc.)	19	Ensuring that the output of generative AI systems does not contain harmful biases and discrimination.	Having technology that provides mechanisms for the generative AI system to refuse to respond when test data containing harmful biases regarding specific groups (such as race, gender, nationality, age, political beliefs, religion, etc.) is input or included in expected outputs.	-	Documentation that clarifies the implementation methods for mechanisms that enable the generative AI system to refuse to respond when test data containing harmful biases against specific groups (related to diverse backgrounds such as race, gender, nationality, age, political beliefs, religion, etc.) is input or included in expected outputs, etc.	"Standard Template of Requirement Definition Document" 3.Non-functional Requirements Definition 3.1.Matters Regarding Usability and Accessibility
						Measures are in place to ensure that output results are not influenced by attributes when test data, which is presumed to be unaffected by human attributes, is input into the system.	-	Documentation that clarifies the testing policies used to verify that output results are not influenced by attributes when test data, presumed to be unaffected by human attributes, is input into the system, etc.	
						Having technology to use multiple LLMs, considering that different LLMs may have varying ideologies or biases, especially when the primary purpose is not the use of a specific model.	-	Documentation that clarifies the adoption of system design using multiple LLMs, etc.	
						Having methods for verifying that there is no unfair bias in the generative AI system during the training process of training data and models.	-	Documentation that clarifies the validation processes and methods for generative AI systems, etc.	
						Output results are regularly monitored to ensure that harmful biases are not included.	-	Documentation that clarifies the verification viewpoints used for regular monitoring to ensure that harmful biases are not included, etc.	
			Basic Requirements	20	Ensuring that the output of generative AI systems is sufficiently readable to all end users.	The fluency scores of generative AI system outputs, which quantifies grammatical appropriateness, are measured and evaluated.	-	Documentation that clarifies the fluency score of generative AI system outputs and the measurement policies for the score, etc.	"Standard Template of Requirement Definition Document" 3.Non-functional Requirements Definition 3.1.Matters Regarding Usability and Accessibility
						Readability scores of generative AI outputs are measured and evaluated.	-	Documentation that clarifies the readability score of generative AI system outputs and the measurement policies for the score, etc.	
						Measures are in place to ensure that, even when grammatically incorrect test data is input into the generative AI system, the output remains grammatically correct and easily understandable by humans.	-	Documentation that clarifies the methods for verifying that the output remains grammatically correct and easily understandable by humans, even when grammatically incorrect test data is input into the generative AI system, etc.	
						Having technology that provides mechanisms to ensure that even when test data anticipating outputs other than expected use cases is input into the generative AI system, outputs that may harm the life, body, property, etc. of the end user are prevented, or the system can refuse to output such results.	-	Documentation that clarifies the implementation methods for mechanisms to ensure that even when test data anticipating outputs other than expected use cases is input into the generative AI system, outputs that may harm the life, body, property, etc. of the end user are prevented, or the system can refuse to output such results, etc.	
						Having technology that provides mechanisms to ensure that within the intended purpose of use cases for the generative AI system, outputs that may harm the life, body, property, etc. of the end user are prevented, or the system can refuse to output such results.	-	Documentation that clarifies the implementation methods for mechanisms to ensure that within the intended purpose of use cases for the generative AI system, outputs that may harm the life, body, property, etc. of the end user are prevented, or the system can refuse to output such results, etc.	
						To ensure that end users can use the generative AI system safely and appropriately, the generative AI system's usage methods, points of consideration for use, expected usage environment, and relevant guidelines are established and regularly updated.	-	Documentation that outlines the generative AI system's usage methods, points of consideration for use, expected usage environment, etc.	
15	Addressing Uses for Purpose Other than the Original Intent	Basic Requirements	21	Preventing uses for the purpose other than the original intent and ensuring that even if misuse occurs, no significant harm or disadvantage arises.					
16	Personal Information, Privacy, Intellectual Property	Applicable as Basic Requirements when handling personal information, privacy, and intellectual property	22	Ensuring appropriate handling of personal information collected, processed, and stored by generative AI systems, as well as protecting intellectual property and privacy.	Having technology that provides mechanisms to control the inappropriate output of personal information, when using a generative AI system with RAG and the search target includes information related to individuals. *This measure applies only to generative AI systems using RAG.	-	Documentation that clarifies the implementation methods for mechanisms to properly control the inappropriate output of personal information when using a generative AI system with RAG and the search target includes information related to individuals, etc.	"Standard Template of Procurement Specification" 6.Compliance Matters in the Execution of Tasks 6.3.Handling of Personal Information, etc. "Standard Template of Requirement Definition Document" 3.Non-functional Requirements Definition 3.1.Matters Regarding Usability and Accessibility
					Procedures are established for addressing situations where privacy infringements are recognized.	-	Documentation that clarifies the procedures for addressing situations where privacy infringements are recognized, etc.	
					Data is collected from users in compliance with the Act on Protection of Personal Information (refer to notices from the Personal Information Protection Commission: https://www.ppc.go.jp/files/pdf/230602_alert_AI_utilize.pdf).	-	Documentation that shows compliance with the Act on Protection of Personal Information (including rules, regulations, and records of their implementation status).	

Procurement Check Sheet									
Classification	Evaluation Viewpoints No.	Evaluation Viewpoints	Classification of Items for Evaluation and Selection	Req. No.	Note: Items in this coulmn are requirements that the service provider must comply with as specified in the procurement specifications Requirements	Note: Examples of methodologies for complying with the "Requirements" are provided. It is not necessary to strictly adhere to the example of measures. Based on selection, the planner needs to incorporates only the necessary details of the requirements into the procurement specification. Example of Measures	Detailed Example of Measures	Note: Consider whether to request provision of the supporting information from the service provider as necessary. Examples of Supporting Information	(Reference) Correspondence with the "Various Templates" in the "DS-120 Digital Government Promotion Standard Guideline Implementation Guidebook"
	17	Ensuring Security	Basic Requirements	23	Addressing vulnerabilities across the entire generative AI system and preventing impacts from unauthorized operations.	Measures are in place to ensure that even when multiple test data, which are costly and challenging to process, are repeatedly input into the generative AI system, unacceptable performance degradation or system shutdown does not occur.	-	Documentation that clarifies the methods for verifying that even when multiple test data, which are costly and challenging to process, are repeatedly input into the generative AI system, unacceptable performance degradation or system shutdown does not occur, etc.	"Standard Template of Requirement Definition Document" 3.Non-functional Requirements Definition 3.10.Matters Regarding Information Security 3.4.Matters Regarding Performance 3.5.Matters Regarding Reliability
						Measures are in place (i) to prevent the possibility of circumventing the generative AI system's defenses through prompt injection, etc., as well as (ii) to ensure that unintended operations are not performed on the backend system of the generative AI system.	-	Documentation that clarifies the methods for (i) verifying that the defense measures of generative AI systems cannot be circumvented by attacks such as prompt injection, and (ii) ensuring that unintended operations are not performed on the backend system through such attacks, etc.	
						As attack methods targeting generative AI systems evolve constantly, mechanisms are under review and development to address these risks. Such mechanisms can be implemented necessary.	-	Documentation related to measures against the latest attack methods, etc.	
						Measures are in place to ensure there are no deficiencies in the configuration of access permissions to RAG search targets, etc., preventing the output of confidential information in generative AI systems using RAG. *This measure applies only to generative AI systems using RAG.	-	Documentation that clarifies the procedures for verifying that there are no deficiencies in the configuration of access permissions to the data sources retrieved by RAG, in order to ensure that confidential information is not output by a generative AI system using RAG, etc.	
						Having technology that provides defense mechanisms at the input phase of the generative AI system, such as prompt detection by utilizing a prohibition list.	-	Documentation that clarifies the implementation methods of defense mechanisms at the input phase of a generative AI system, such as prompt detection by utilizing a prohibition list, etc.	
			Basic Requirements	24	Appropriately implementing security measures throughout the development process of generative AI systems.	Having appropriate security measures and technologies throughout the development process of the generative AI system, in alignment with the characteristics of the technologies being adopted.	-	Documentation related to security measures, etc.	"Standard Template of Requirement Definition Document" 3.Non-functional Requirements Definition 3.10.Matters Regarding Information Security 3.4.Matters Regarding Performance 3.5.Matters Regarding Reliability
	18	Explainability	Basic Requirements	25	Ensuring that the rationale for outputs can be confirmed to a technically reasonable extent.	Having technology that provides mechanisms for displaying the rationale of outputs (such as internal operations, their states, and sources) when various test data are input into generative AI systems equipped with functionalities for visualizing output rationale.	-	Documentation that clarifies the implementation methods for technology providing mechanisms to display the rationale of outputs (such as internal operations, their states, and sources) when various test data are input into a generative AI system equipped with functionalities for visualizing output rationale, etc.	"Standard Template of Requirement Definition Document" 3.Non-functional Requirements Definition 3.1.Matters Regarding Usability and Accessibility
						Ensuring that in a generative AI system performing step-by-step reasoning, it is possible to confirm that the reasoning process leading to the output can be presented to the end user.	-	Documentation that clarifies the methods for confirming that in a generative AI system performing step-by-step reasoning, the reasoning process leading to the output can be presented to the end user, etc.	
						Documentation is made regarding various aspects such as the generative AI system's development process, data collection and labeling that influence decision-making, the algorithms used, the system architecture of the generative AI system, and the data processing processes.	-	Documentation that clarifies the development process of generative AI systems, the data collection and labeling that influence decision-making, the algorithms used, the system architecture, and the data processing processes are managed in documented form, etc. *This does not indicate a request for the submission of detailed documented content.	
	19	Robustness	Basic Requirements	26	Ensuring that generative AI systems provide stable outputs in response to inputs.	Measures are in place to ensure consistency in the outputs when the same test data is input multiple times into the generative AI system.	-	Documentation that clarifies the measures in place to ensure the consistency of outputs when the same test data is input multiple times into generative AI systems, etc.	"Standard Template of Requirement Definition Document" 3.Non-functional Requirements Definition 3.4.Matters Regarding Performance 3.5.Matters Regarding Reliability 3.9.Matters Regarding Continuity
						Measures are in place to ensure consistency in the outputs when multiple semantically similar test data are input into the generative AI system.	-	Documentation that clarifies the methods for verifying the consistency of outputs when multiple semantically similar test data are input into generative AI systems, etc.	
						Measures are in place to ensure stable operation of the generative AI system even when perturbed data (including erroneous inputs, adversarial prompts, garbled text data, and data with inconsistent notation) is input into the system.	-	Documentation that clarifies the methods for verifying whether generative AI systems operate stably even when perturbed data (including erroneous inputs, adversarial prompts, garbled text data, and data with inconsistent notation) are input, etc.	
	20	Data Quality	Basic Requirements	27	Maintaining the data accessed by generative AI systems in an appropriate state.	Measures are in place to ensure that quality issues do not arise in data (including pre-training data, training data and test data for purposes such as fine-tuning and In-Context Learning, etc.) that could negatively affect the generative AI system, taking into account the possibility of biases (including latent biases not evident in training data) being included during the learning process of both data and models.	As part of quality management for data that could negatively affect the generative AI system, including pre-training data, training data and test data for purposes such as fine-tuning and In-Context Learning, etc., measures are implemented to manage the data accuracy and to ensure that no issues arise with the data.	Documentation that clarifies the methods for managing the accuracy, confidentiality, and integrity of pre-training data, training data and test data for purposes such as fine-tuning and In-Context Learning, etc., as part of quality management for data that could affect generative AI systems, etc.	"Standard Template of Procurement Specification" 4.Matters Regarding the Content of Task Execution 4.13.Data Management Method "Standard Template of Requirement Definition Document" 2.Functional Requirements Definition 2.4.Matters Regarding Data
							As part of quality management for data that could negatively affect the generative AI system, including pre-training data, training data and test data for purposes such as fine-tuning and In-Context Learning, etc., management systems are in place to prevent data corruption, and measures are implemented to ensure that no issues arise with the data.	Documentation that clarifies the methods for managing the accuracy, confidentiality, and integrity of pre-training data, training data and test data for purposes such as fine-tuning and In-Context Learning, etc., as part of quality management for data that could affect generative AI systems, etc.	
							Regarding data that could negatively affect the generative AI system, including pre-training data, training data and test data for purposes such as fine-tuning and In-Context Learning, etc., measures are implemented to ensure that the data is grammatically correct and easily understandable by humans.	Documentation that clarifies the methods for verifying that pre-training data, training data and test data for purposes such as fine-tuning and In-Context Learning, etc., which could affect generative AI systems, are grammatically appropriate and easily understandable by humans, etc.	
							Regarding data that could negatively affect the generative AI system, including pre-training data, training data and test data for purposes such as fine-tuning and In-Context Learning, etc., measures are implemented to ensure that there is no bias in data distribution based on factors such as race, gender, nationality, age, political beliefs, or religion.	Documentation that clarifies the methods for verifying that pre-training data, training data and test data for purposes such as fine-tuning and In-Context Learning, etc., which could affect generative AI systems, are free from biases in their distribution related to race, gender, nationality, age, political beliefs, religion, etc.	
							Regarding data that could negatively affect the generative AI system, including pre-training data, training data and test data for purposes such as fine-tuning and In-Context Learning, etc., measures are implemented to ensure that inappropriate content, such as offensive language towards users, is not included in the data.	Documentation that clarifies the methods for verifying that pre-training data, training data and test data for purposes such as fine-tuning and In-Context Learning, etc., which could affect generative AI systems, do not contain inappropriate content, such as offensive language towards users, etc.	
							Regarding data that could negatively affect the generative AI system, including pre-training data, training data and test data for purposes such as fine-tuning and In-Context Learning, etc., measures are implemented to prevent information that could be used for cyber attacks or terrorism, etc. from being included in the data.	Documentation that clarifies the methods for verifying that pre-training data, training data and test data for purposes such as fine-tuning and In-Context Learning, etc., which could affect generative AI systems, do not contain information that could be used for cyber attacks or terrorism, etc.	
							Regarding data that could negatively affect the generative AI system, including pre-training data, training data and test data for purposes such as fine-tuning and In-Context Learning, etc., measures such as Privacy-Enhancing Technologies (PETs) are implemented to ensure that the data is in a condition suitable for use as training data, and the system is able to verify this status.	Documentation that clarifies the methods for verifying that pre-training data, training data and test data for purposes such as fine-tuning and In-Context Learning, etc., which could affect generative AI systems, are appropriately processed with measures like Privacy-Enhancing Technologies (PETs) etc., to ensure they are suitable for use as training data, etc.	

Procurement Check Sheet									
Classification	Evaluation Viewpoints No.	Evaluation Viewpoints	Classification of Items for Evaluation and Selection	Req. No.	Note: Items in this coulmn are requirements that the service provider must comply with as specified in the procurement specifications Requirements	Note: Examples of methodologies for complying with the "Requirements" are provided. It is not necessary to strictly adhere to the example of measures. Based on selection, the planner needs to incorporates only the necessary details of the requirements into the procurement specification. Example of Measures	Detailed Example of Measures	Note: Consider whether to request provision of the supporting information from the service provider as necessary. Examples of Supporting Information	(Reference) Correspondence with the "Various Templates" in the "DS-120 Digital Government Promotion Standard Guideline Implementation Guidebook"
							As part of quality management for data that could negatively affect the generative AI system, including pre-training data, training data and test data for purposes such as fine-tuning and In-Context Learning, etc., measures are implemented for data configuration management and for ensuring that no issues arise with the data.	Documentation that clarifies the configuration management policies as part of the quality management for pre-training data, training data and test data for purposes such as fine-tuning and In-Context Learning, etc., that could affect generative AI systems, etc.	
							As part of quality management for data that could negatively affect the generative AI system, including pre-training data, training data and test data for purposes such as fine-tuning and In-Context Learning, etc., measures are implemented to ensure that annotation is conducted appropriately when automated.	Documentation that clarifies the methods for verifying that automated annotation is being conducted appropriately, as part of the quality management for pre-training data, training data and test data for purposes such as fine-tuning and In-Context Learning, etc., that could affect generative AI systems, etc.	
							As part of quality management for data that could negatively affect the generative AI system, including pre-training data, training data and test data for purposes such as fine-tuning and In-Context Learning, etc., measures are implemented to prevent malicious or malfunction-inducing texts/programs from being included in the data.	Documentation that clarifies the methods for verifying that malicious or malfunction-inducing programs are not included in the data, etc., as part of the quality management for pre-training data, training data and test data for purposes such as fine-tuning and In-Context Learning, etc., that could affect generative AI systems, etc.	
							As part of quality management for data that could negatively affect the generative AI system, including pre-training data, training data and test data for purposes such as fine-tuning and In-Context Learning, etc., measures are implemented to manage data provenance and ensure that no issues arise with the data through utilization of tools and other resources.	Documentation that clarifies the methods for managing the provenance, as part of the quality management for pre-training data, training data and test data for purposes such as fine-tuning and In-Context Learning, etc., that could affect generative AI systems, etc.	
			Optional Additional Requirements (Optional Criteria)	28	Structuring input data appropriately to enhance the outputs of generative AI systems.	The structuring of input data can be considered and implemented as necessary, to improve the accuracy of outputs.	-	Documentation explaining the methods and related materials for achieving the structuring of input data aimed at improving the accuracy of output, etc.	"Standard Template of Requirement Definition Document" 2.Functional Requirements Definition 2.4.Matters Regarding Data
	21	Verifiability	Basic Requirements	29	Making the development and provision processes of generative AI systems verifiable.	Management are in place to ensure that the overview, origins, and operations of the system, model, and data can be verified from logs and technical specifications, etc., along with measures to be implemented to prevent related issues.	System cards, model cards, and data cards are created and managed to ensure the verifiability of the overview, origins, and operations of the system, model, and data, with measures implemented to prevent related issues.	Documentation explaining the technical specifications, management policies, and other related materials to clarify the overview, origin, and operation of systems, models, and data, for ensuring their verifiability, etc.	"Standard Template of Requirement Definition Document" 3.Non-functional Requirements Definition 3.16.Matters Regarding Operations 3.17.Matters Regarding Maintenance
							Measures are implemented to ensure that data logs are accurately recorded when various test data are input into the generative AI system, thus securing the verifiability of the overview, origins, and operations related to the system, model, and data.	Documentation explaining the verification methods and related approaches to ensure data logs are recorded correctly when various test data are input into generative AI systems, etc.	

Appendix7 A

Checklist
[For all AI business actor]

2024.4.19

This checklist summarizes “Part 2 C. Common Guiding Principles” from AI Guidelines for business.
Use this checklist to review the key initiatives required of business operators.
※AI Business actors involved in advanced AI systems should also implement “Checklist Appendix7 B. For AI Business actors involved in advanced AI systems”

Checklist Items

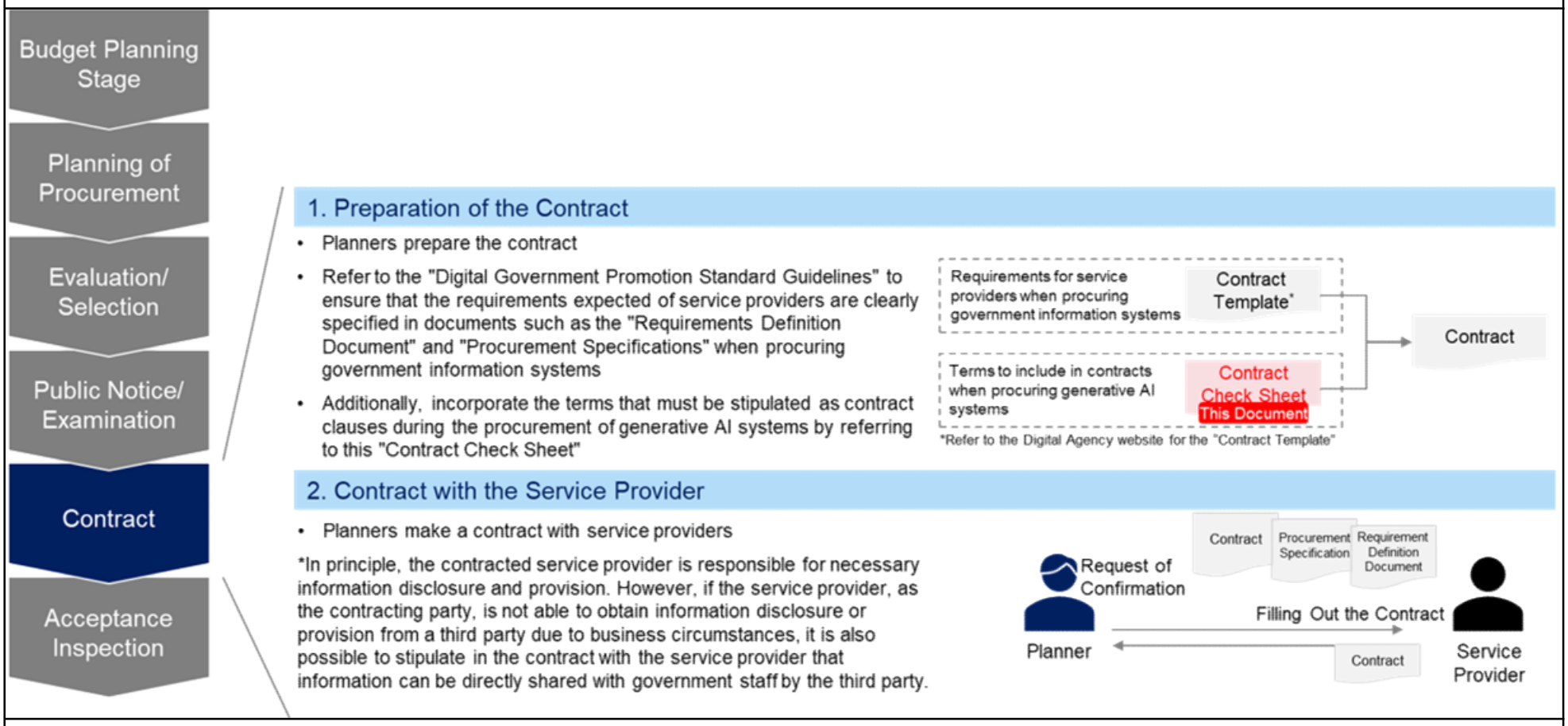
- ☐ Based on **Human-Centric approach**, act in a way that does not violate the human rights guaranteed by the Constitution of Japan or granted internationally.
- ☐ Ensure **safety** to avoid damage to the lives, bodies, minds, properties of all persons engaged in AI, and the environment.
- ☐ Take care to eliminate potential biases, recognize that there are some unavoidable biases even if such attention is paid, and determine whether the unavoidable biases are allowable from the **fairness** viewpoints of respect for human rights and diverse cultures.
- ☐ Respect and protect **privacy**, and obey relevant laws.
- ☐ Ensure **security** to prevent the behaviors of AI from being unintentionally altered or stopped by unauthorized manipulations.
- ☐ To ensure **transparency**, provide stakeholders with information of AI itself and AI system or service to the extent reasonable and technically possible.
- ☐ Execute **accountability** regarding the traceability of data sources and AI decision-making as well as the status of risk response, to concerned stakeholders.
- ☐ Establish **the policies relevant to privacy and AI governance**.
- ☐ **Consider specific approaches** tailored to the circumstances of each business to achieve the above checklist items.

Use the 'Worksheet for Considering Specific Approaches’ for your review.

Overview of this Check Sheet

Provisional Translation | **Appendix 4**

This check sheet organizes the terms that should be considered for inclusion in contracts when procuring generative AI systems.
(As appropriate, these terms should be incorporated into procurement specifications.)
Planners should refer to this check sheet when creating contracts for the procurement of generative AI systems.
However, this check sheet only includes terms particular to the "procurement of generative AI systems" that require particular attention.
Therefore, it is necessary to also refer to the contract templates of each ministry or agency when creating the contract.
In this check sheet, "[Appendix 4] Contract Check Sheet (for Generative AI Systems)" is referred to as the "Contract Check Sheet."



Structure of this Check Sheet

No. of Agreed Term	Classification of Items for Contracts	Agreed Terms	Example Clauses to be Included in the Contract	Supplementary Explanations
1	Basic Terms	Agreements for Inputs Related to Generative AI Systems	Clauses stipulating the definition of inputs, purposes of input uses, conditions for input uses, ownership of rights related to inputs.	The following considerations are advisable when stipulating the clauses. Define the scope of inputs subject to contractual rules as service providers might freely use inputs without restrictions. Stipulate obligations prohibiting service providers from using or retaining inputs, in principle, for purposes other than those related to the provision of the generative AI system (*). When granting permission for service providers to use inputs, set clear conditions for such usage (i.e. whether training is involved, what the methods of data storage are). Stipulate the conditions for the acquisition of rights under which service providers may acquire certain rights, such as intellectual property rights relating to inputs. The conditions should include matters such as the scope of rights transfer of the inputs, compensation for the inputs, and the existence and terms of licensing the inputs, and any other relevant matters. (*) Note that while it is permissible to block unauthorized uses of inputs through an opt-out mechanism, it should be clearly stipulated in the contract that measures should be addressed to block unauthorized uses by opting out.
2	Basic Terms	Agreements for Processing Results of Input Related to Generative AI Systems	Clauses regarding results of inputs (other than outputs), which stipulate the scope of of the results covered by contructual rules, purposes of using the results, conditions for using the results, and owership of rights of the results.	The following considerations are advisable when stipulating the clauses. Define the scope of processing results of inputs subject to contractual rules as service providers might freely use them without restrictions. Stipulate obligations prohibiting service providers from using or retaining processing results of inputs, in principle, for purposes other than those related to the provision of the generative AI system. When granting permission for service providers to use processing results of inputs, set clear conditions for such usage (i.e. whether training is involved, what the methods of data storage are). Stipulate the conditions of the acquisition of rights under which service providers may acquire certain rights, such as intellectual property rights, relating to processing results of inputs, which should address matters such as the scope of rights transfer, presence or absence of compensation for the rights, existence and terms of licensing the rights, and any other relevant conditions.
3	Basic Terms	Agreements for Output Related to Generative AI Systems	Clauses stipulating the definition of outputs, whether the service provider has the obligation to supply outputs to users and the details of the obligation, requirements for guarantees from the service provider related to outputs, conditions under which users may provide outputs to third parties, and the ownership of rights regarding outputs that the service provider supplies to users.	The following considerations are advisable when stipulating the clauses. As for outputs subject to contractual regulation, define the scope of outputs in a way that fully covers the user's purposes for service use. If the service provider is obligated to provide outputs, define the conditions for the provisions, including timing, frequency, state, and other conditions, as well as the details of the outputs provided, such as their nature, quantity, and granularity, in light of the user's purposes for service use. In cases where the service provider is responsible for warranties or information provision regarding outputs, set the terms and conditions for such warranties and information provision. Define third-party provision conditions, including the recipients, scope of provision, and other related conditions. Stipulate the conditions for the acquisition of rights under which users may acquire certain rights, such as intellectual property rights, relating to the outputs. The conditions should address the scope of rights transfer, presence or absence of compensation for the rights, existence and terms of licensing the rights, and any other relevant matters.
4	Basic Terms	Agreements for Processing Results of Output Related to Generative AI Systems	Clauses regarding processing results of outputs, which stipulate the scope of the results covered by contractual rules, external provision of the results by users, and ownership of rights of the results.	The following considerations are advisable when stipulating the clauses. For the processing results of outputs subject to contractual regulation, define the scope of these results in a way that fully covers the user's purposes for service uses. Define external provision conditions, including the recipients of the results, scope of the provision of the results, and other relevant conditions, in light of the user's purposes for service uses. When acquiring certain rights, such as intellectual property rights, stipulate the conditions of the acquisition of the rights, including the scope of rights transfer, presence or absence of compensation for the rights, and the existence and terms of licensing the rights, and any other relevant conditions.
5	Basic Terms	Contractual Agreements Related to Generative AI Systems	Clauses stipulating the obligation for the service provider to finilize the generative AI system construction.	The following considerations are advisable when stipulating the clauses. In cases where the service provider is obligated to finilize the generative AI system construction under a contract for work, consider and incorporate into specific completion conditions of the contract, such as the timeframe for completion, acceptance criteria, and other relevant factors, aligned with the user's purposes for service uses.

Column B: Classification of Items for Contracts
Column C: Agreed Terms
Column D: Example Clauses to be Included in the Contract
Column E: Supplementary Explanations

【Column B: Classification of Items for Contracts】
As part of the agreed terms, the terms to be considered when contracting with service providers are labeled as "Basic Terms." The selection or expansion of agreed terms are to be considered, taking into account the project type, the project stage, the project's risk level, etc., as stated in "6.1.2 Measures to be Addressed Based on this Guideline."

【Column C: Agreed Terms】
As part of the agreed terms, these items are to be considered to be included in the contract with service providers.

【Column D: Example Clauses to be Included in the Contract】
These are examples of clauses that fulfill the terms listed in "Column C: Agreed Terms". It is not necessary to strictly adopt these example clauses as they are.

【Column E: Supplementary Explanations】
Supplementary explanations are provided for "Column C: Agreed Terms" and "Column D: Example Clauses to be Included in the Contract."

How to Use this Check Sheet

・Planners should incorporate necessary items from "Column C: Agreed Terms" into the contract or procurement specifications.
　*In principle, terms listed in "Column C: Agreed Terms" are mandatory items to be fulfiled for inclusion in the contract or procurement specifications.
　*"Column D: Example Clauses to be Included in the Contract" are literally examples and do not necessarily need to be fully satisfied. Adherence to requirements by using the methods other than these examples is also acceptable.
　*Additionally, include necessary items in this check sheet to documents such as the "Requirements Definition Document" or "Procurement Specifications" created in relation to the procurement for procuring government information systems."

Scope of this Check Sheet

This check sheet applies to systems that incorporate generative AI, as described in "2.2.2 Generative AI Targeted by this Guideline," within the government information systems mentioned in "2.2.1 Information Systems Targeted by this Guideline."

Supplementary Explanation of Terms

・Large Language Model (LLM): A language model that treats the probability of occurrence of sentences and words as a deep learning model, built using a very large amount of training data. (Source: Guidelines for Quality Assurance of AI-based Products and Services by Consortium of Quality Assurance for Artificial-Intelligence-based Products and Services, 10-1)
・Generative AI: A general term representing AI developed from an AI model that can generate texts, images, programs, etc. (Source: AI Guidelines for Business, P.10)
・Generative AI System: Government Information Systems that comprise generative AI (only the types of generative AI which is targeted by this guideline) as a component. (In accordance with Guide to Evaluation Perspectives on AI Safety (Version 1.01) by Japan AI Safety Institute, P.9)
・Raw Data for Training: Data provided by the user to the provider for input into the generative AI system during training.
・Training Data: Data created by the service provider for training purposes through processing and modification of the raw data (for training) provided by the user.
・Input: Prompts, raw data for training, etc. (Note: Does not include processing results of inputs.)
・Processing Results of Inputs: Training data, intermediate products, and derivative intellectual property, etc. (Note: This refers to intangibles that have undergone some processing (modification, etc.) from inputs and may be referred to as "derivatives," "derivative intellectual property," "derivative data," "improvement results," etc. Intermediate products, such as learning datasets derived from raw data, are typically assumed.)
・Output: Products of AI systems, etc., AI-generated content such as analysis results and other content. (Note: Does not include processing results of outputs.)
・Processing Results of Outputs: Content modified by the user from outputs generated by AI-related services, etc. (Note: This refers to intangibles that have undergone some processing (modification, etc.) from outputs and may be referred to as "derivatives," "derivative intellectual property," "derivative data," "improvement results," etc.)
・Know-how: Expertise, technology, information, etc. held by the service provider or user during the research, development, and utilization processes of AI technology. (Note: Assumed examples of know-how include the following; obtaining raw data, modifying raw data suitable for training, training using training programs, tuning trained models, training history, and prompt history, etc.)
・Information Security Incidents: Refers to information security incidents as defined in JIS Q 27000:2019.
・Risk Cases Particular to Generative AI Systems: A condition where risks inherent to a generative AI system have materialized, or where signs or events indicating the possible materialization of such risks are observed, which may have significant impacts.

Contract Check Sheet		Note: The selection or expansion of agreed terms are to be considered, taking into account the project type, the project stage, the project's risk level, etc., as stated in "6.1.2 Measures to be Addressed Based on this Guideline."		
No. of Agreed Terms	**Classification of Items for Contracts**	**Agreed Terms**	**Example Clauses to be Included in the Contract**	**Supplementary Explanations**
1	Basic Terms	Agreements for Inputs Related to Generative AI Systems	Clauses stipulating the definition of inputs, purposes of input uses, conditions for input uses, ownership of rights related to inputs.	The following considerations are advisable when stipulating the clauses. Define the scope of inputs subject to contractual rules as service providers might freely use inputs without restrictions. Stipulate obligations prohibiting service providers from using or retaining inputs, in principle, for purposes other than those related to the provision of the generative AI system (*). When granting permission for service providers to use inputs, set clear conditions for such usage (i.e. whether training is involved, what the methods of data storage are). Stipulate the conditions for the acquisition of rights under which service providers may acquire certain rights, such as intellectual property rights relating to inputs. The conditions should include matters such as the scope of rights transfer of the inputs, compensation for the inputs, and the existence and terms of licensing the inputs, and any other relevant matters. (*) Note that while it is permissible to block unauthorized uses of inputs through an opt-out mechanism, it should be clearly stipulated in the contract that measures should be addressed to block unauthorized uses by opting out.
2	Basic Terms	Agreements for Processing Results of Inputs Related to Generative AI Systems	Clauses regarding results of inputs (other than outputs), which stipulate the scope of of the results covered by contructual rules, purposes of using the results, conditions for using the results, and owership of rights of the results.	The following considerations are advisable when stipulating the clauses. Define the scope of processing results of inputs subject to contractual rules as service providers might freely use them without restrictions. Stipulate obligations prohibiting service providers from using or retaining processing results of inputs, in principle, for purposes other than those related to the provision of the generative AI system. When granting permission for service providers to use processing results of inputs, set clear conditions for such usage (i.e. whether training is involved, what the methods of data storage are). Stipulate the conditions of the acquisition of rights under which service providers may acquire certain rights, such as intellectual property rights, relating to processing results of inputs, which should address matters such as the scope of rights transfer, presence or absence of compensation for the rights, existence and terms of licensing the rights, and any other relevant conditions.
3	Basic Terms	Agreements for Output Related to Generative AI Systems	Clauses stipulating the definition of outputs, whether the service provider has the obligation to supply outputs to users and the details of the obligation, requirements for guarantees from the service provider related to outputs, conditions under which users may provide outputs to third parties, and the ownership of rights regarding outputs that the service provider supplies to users.	The following considerations are advisable when stipulating the clauses. As for outputs subject to contractual regulation, define the scope of outputs in a way that fully covers the user's purposes for service use. If the service provider is obligated to provide outputs, define the conditions for the provisions, including timing, frequency, state, and other conditions, as well as the details of the outputs provided, such as their nature, quantity, and granularity, in light of the user's purposes for service use. In cases where the service provider is responsible for warranties or information provision regarding outputs, set the terms and conditions for such warranties and information provision. Define third-party provision conditions, including the recipients, scope of provision, and other related conditions. Stipulate the conditions for the acquisition of rights under which users may acquire certain rights, such as intellectual property rights, relating to the outputs. The conditions should address the scope of rights transfer, presence or absence of compensation for the rights, existence and terms of licensing the rights, and any other relevant matters.
4	Basic Terms	Agreements for Processing Results of Outputs Related to Generative AI Systems	Clauses regarding processing results of outputs, which stipulate the scope of the results covered by contractual rules, external provision of the results by users, and ownership of rights of the results.	The following considerations are advisable when stipulating the clauses. For the processing results of outputs subject to contractual regulation, define the scope of these results in a way that fully covers the user's purposes for service uses. Define external provision conditions, including the recipients of the results, scope of the provision of the results, and other relevant conditions, in light of the user's purposes for service uses. When acquiring certain rights, such as intellectual property rights, stipulate the conditions of the acquisition of the rights, including the scope of rights transfer, presence or absence of compensation for the rights, and the existence and terms of licensing the rights, and any other relevant conditions.
5	Basic Terms	Contractual Agreements Related to Generative AI Systems	Clauses stipulating the obligation for the service provider to finilize the generative AI system construction.	The following considerations are advisable when stipulating the clauses. In cases where the service provider is obligated to finilize the generative AI system construction under a contract for work, consider and incorporate into specific completion conditions of the contract, such as the timeframe for completion, acceptance criteria, and other relevant factors, aligned with the user's purposes for service uses.
6	Basic Terms	Agreements for Know-how Related to Generative AI Systems	Clauses regarding the know-how of service providers or users, specifically related to the definition of know-how, conditions for the user's usage of the service provider's know-how, conditions for the service provider's usage of the user's know-how, and ownership of rights of the know-how.	Since information that does not fit the definition of know-how may potentially be freely used by the service provider, unless restricted by applicable laws, it is advisable to stipulate, through this clause, the scope of know-how subject to contractual rules, the conditions of usage by both the user and the service provider(*), and the owenership of rights of the know-how. *Especially, consideration of whether to allow usage beyond the service provision purposes, such as the service provider's technological development or learning purposes, should be reviewed and incorporated into the contract.
7	Basic Terms	Agreements on the Service Provider's Obligations of Responses, Cooperation, and the Scope of these Responses, in cases of Information Security Incidents or Risk Cases Particular to Generative AI Systems	Clauses obligating the service provider to respond, cooperate, and provide the related data by in response to information security incidents or risk cases particular to generative AI systems.	It is necessary to reach an agreement with the service provider in advance on minimizing damages from information security incidents or risk cases particular to generative AI systems, providing information and data to a reasonable extent (including as necessary the generative AI system's training data or algorithms) to the government upon requests, identifying causes of service outage, information security incidents, or said risk cases , implementing improvement measures, and conducting inspections as necessary.
8	Basic Terms	Agreements to Minimize Damages Originating From Situations Where Expected Quality Level is Not Fullfiled, and to Identify Causes and Implement Measures for Improvement	Clauses requiring to minimize damages originating from situations where expected quality level is not fulfilled, and to identify causes and implement improvement measures.	Assuming those cases where the expected quality level of the generative AI system is not fullfiled, agreements should be reached beforehand on minimizing resulting damages, identifying causes, and implementing improvement measures by the service provider.