(Draft) Recommendations on Policies, Laws, Measures, and Standards Related to Suitable Cloud Service Provision and Usage for Government Agencies

(Draft) Recommendations on Policies, Laws, Measures, and Standards Related to Suitable Cloud Service Provision and Usage for Government Agencies

Project to Formulate Regulations for the Accommodation of the Central Government Cloud System Services and Draft an Operational Plan for Advancing Thailand's Data Strategy

Office of the National Digital Economy and Society Commission

June 2024

Table of Contents

Executive Summary

Nowadays cloud technology plays an increasingly critical role in every sector, including government agencies, the private sector, and the public sector. The National Digital Economy and Society Commission is therefore aware that there is an urgent need to use cloud technology as an important tool in response to the need to adapt work processes and provide public services to quickly transform into a digital government. This sustainably aligns with the goals of national development according to the National Strategy (2018–2037).

Cloud technology is offered by a variety of providers with different Cloud Deployment Models and Cloud Service Models to meet the needs of users, legal compliance, and system management capabilities, which are the key considerations for utilizing cloud technology. The different types of cloud services have the following advantages:

(1) Public Cloud: Users can pay for services based on actual usage, allowing them to quickly and diversely utilize new technologies and tools as they are developed and made accessible. Public clouds also has low investment, management, and maintenance costs due to economies of scale, where resources are shared with a wide range of users. Security measures are designed and implemented by the service provider.

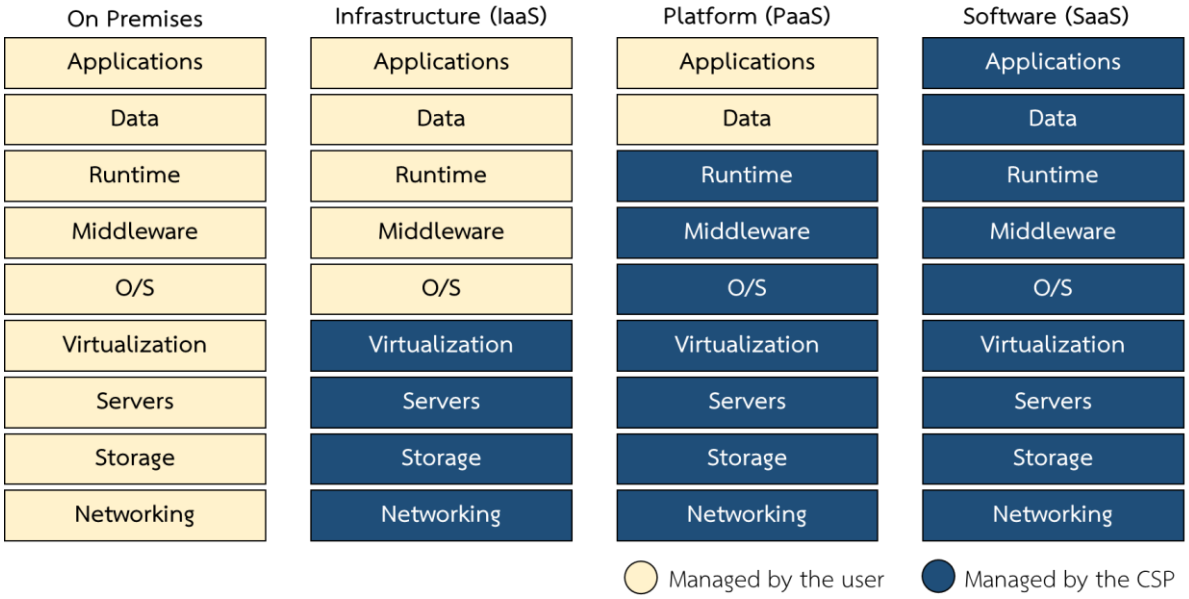
(2) Private Cloud: The service can be designed and managed to meet the specific needs of users, and users can design their own security measures to match the sensitivity of their data. However, private clouds have high investment, management, and maintenance costs, and may require extensive security measures to be defined and implemented themselves.

(3) Hybrid Cloud: The service provides a combination of public and private cloud services, allowing users to choose to store and process data in the type of cloud that aligns with data classification. Users of private clouds can also expand their processing resources for increased system flexibility. However, there are no economies of scale due to the inclusion of the private cloud component.

At the same time, each Cloud Service Model has a Shared Responsibility Model (Figure 1) that divides responsibilities between users and cloud providers. This can meet the needs, capabilities, and requirements of users, facilitate utilization and system expansion, and reduce

unnecessary expenses for users, such as developing systems themselves when the same service is already provided by the provider.

Figure 1: Shared Responsibility Model between Users and Cloud Providers for Different Service Models



Origin of the Cloud First Policy

On May 7, 2019, the Cabinet resolved to implement the Prime Minister's directive on utilizing Big Data.[1] It approved the Ministry of Digital Economy and Society (MDES) to establish a Government Data Center and Cloud Service (GDCC), with CAT Telecom Public Company Limited[2] as the operator. Government agencies were instructed to adopt the Infrastructure Architecture and Data Governance Framework standards and practices, with MDES and the Digital Government Development Agency (Public Organization) providing guidance, monitoring, and evaluation. Government agencies were also asked to collaborate with MDES and the National Statistical Office to create a Government Data Catalog and Directory Services.

Subsequently, the Ministry of Digital Economy and Society proposed a project to develop a government cloud system. Relevant agencies submitted their opinions for the Cabinet's consideration, and on May 5, 2020, the Cabinet approved the "Government Data Center and Cloud Service (GDCC) Development Project"[3] as proposed by the Ministry. The budget for the

[1] Office of the Secretary-General of the Cabinet, Urgent Letter No. Nor 0505/V187 dated May 13, 2019.

[2] Currently known as National Telecom Public Company Limited.

[3] Office of the Secretary-General of the Cabinet, Urgent Letter No. Nor 0505/V 216 dated May 8, 2020.

project for 2020-2022 was to be determined based on the recommendations of the National Digital Economy and Society Committee. The Ministry of Digital Economy and Society was instructed to prioritize cybersecurity in terms of prevention, response, and mitigation of cyber threats that could impact critical information infrastructure. The Ministry was also tasked with developing government personnel to have the knowledge and understanding to utilize Big Data in the future. The Ministry was to consider the opinions of relevant agencies for further action, and all government agencies and state enterprises requiring the use of the government cloud system were to urgently submit their requests to the Ministry to connect or transfer data to the system within the 2020 fiscal year.

Later, on December 22, 2023, the 1/2023 meeting of the National Digital Economy and Society Committee approved the Cloud First Policy with four approaches: (1) managing cloud demand, (2) ensuring sufficient cloud supply, (3) managing with Government Cloud Management, and (4) improving the cloud service ecosystem by linking the supply and demand sides. The committee also approved the establishment of a special committee to drive the Cloud First Policy and assigned the Ministry of Digital Economy and Society to coordinate the promotion and implementation of the policy.

On November 28, 2023, the Cabinet passed a resolution on "Promoting and Transitioning to a Digital Government"[4], stating that: "In accordance with the government's policy statement to Parliament that it will fully utilize technology and digital systems for the benefit of the country and its people, and that investment in digital infrastructure is necessary to become a fully digital government, the Ministry of Digital Economy and Society is requested to accelerate the 'Go Cloud First Policy,' which emphasizes the integration of cloud technology with government operations, to achieve practical results promptly. The Ministry is to present this matter to the National Digital Economy and Society Committee for consideration and then submit the results to the Cabinet for further action to promote all sectors to become a digital government through cooperation between the public and private sectors, in order to enhance the government's operational capabilities to be fast and keep up with the ever-changing technological advancements."

Then, at the 1/2023 meeting of the National Digital Economy and Society Committee on December 22, 2023, the committee approved the Cloud First Policy implementation guidelines

[4] Office of the Secretary-General of the Cabinet, Urgent Letter No. Nor 0505/25725 dated November 30, 2023.

to be proposed to the Cabinet for consideration. The key implementation guidelines consist of four components:

(1) Manage the demand of cloud usage by establishing a Cloud First Policy Committee to supervise, monitor, and provide recommendations to drive Government Cloud Management operations, including setting appropriate budgets.

(2) Manage the supply by setting measures to encourage the private sector to invest in cloud services. This is to be jointly handled by the Ministry of Digital Economy and Society with the Office of the Board of Investment (BOI).

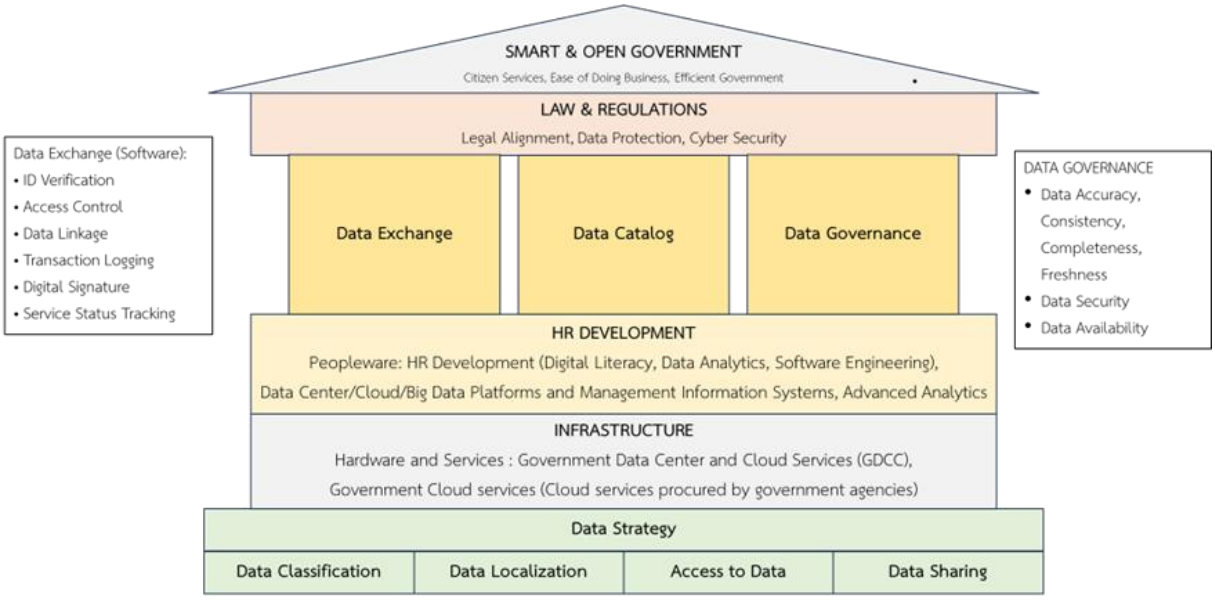
(3) Government Cloud Management is to be handled by the Ministry of Digital Economy and Society and other related agencies under the supervision of the Cloud First Policy Committee.

(4) Improve the cloud service ecosystem to create a linkage between the supply side and the demand side. This is necessary to drive the migration toward cloud service. There must be budgetary considerations and adjustments to the new budgeting model since payment would be in rental form, requiring a longer budget period. In this regard, the Budget Bureau needs to take the different payment format into consideration during budget allocation, from original lump sum payments to pay-per-use. Consequently, the Ministry of Finance and the Comptroller General's Department may have to revise the procurement regulations through the appointment of a task force within the Ministry of Digital Economy and Society. This approach should yield results within the first year.

In addition, the meeting also resolved to assign the Ministry of Digital Economy and Society to coordinate the promotion and implementation of the aforementioned policy.

Meanwhile, the Office of the National Digital Economy and Society Commission (ONDE) has developed a framework for driving data and digital infrastructure operations that are crucial for the integration, sharing, and utilization of data within the Thai government sector. This framework serves as a guideline for moving towards a digital government era and can be extended to a framework suitable for driving the Cloud First Policy (Figure 2). It consists of four key components:

Figure 2: Framework for data integration, sharing, and utilization



Source: Edited from the Office of the National Digital Economy and Society Commission.

(1) Data Strategy

Data Strategy is a crucial mechanism in driving organizations and agencies to have the capability to operate and achieve success. It must cover (1) Data Classification, (2) Data Localization (storing and processing data within the country), (3) Access to Data, and (4) Data Sharing.

Driving the Cloud First Policy for government agencies is therefore important in the implementation in conjunction with the Data Strategy because they are essential components of each other.

(2) Cloud Infrastructure for Government Agencies

Promoting the information technology infrastructure of government agencies in the form of cloud systems, which consists of the Government Data Center and Cloud Service (GDCC) under the supervision of the Office of the National Digital Economy and Society Commission and the Electronic Transactions Development Agency, as well as cloud systems of various agencies that procure and use services from various Cloud Service Providers (CSPs).

(3) Government Personnel Development

Developing government personnel to be users and administrators of cloud services, with knowledge and understanding of cloud computing skills, practices, laws, and regulations. Currently, there are training and development programs for government personnel

in cloud systems under the Government Cloud (GOCC) project to ensure they understand the process of using the GDCC. They also gain cloud computing skills to use the GDCC securely and efficiently, under the operation of the Digital Government Development Agency (Public Organization) and the Digital Economy Promotion Agency.

(4) Laws and Regulations to Support Processes and Services

Laws, regulations, and relevant practices are crucial for governance, building trust, and protecting critical and sensitive processes and data in government agencies. They also serve as enablers that must support processes and services in various areas, including:

(4.1) Data Exchange under the National Statistical Office and the Digital Government Development Agency (Public Organization), especially for software that can be classified as common services required by all sectors, such as ID Verification, Access Control, Data Linkage, Online Payment, Transaction Logging, Digital Signature, and Big Data.

(4.2) Data Catalog under the supervision of the National Statistical Office and the Digital Government Development Agency (Public Organization), and

(4.3) Data Governance under the supervision of the Digital Government Development Agency (Public Organization) and the Electronic Transactions Development Agency, particularly in areas such as Data Localization, Data Accuracy, Consistency, Completeness, Freshness, Data Security, and Data Availability.

The aforementioned operational approaches in Thailand reflect that the GDCC is currently piloting Infrastructure as a Service (IaaS) for government agencies by inviting agencies ready to migrate their systems to the GDCC. However, with the rapid changes in technology, the demand for diverse systems has increased to enhance processes and service delivery to the public. Therefore, it is advisable to increase the utilization of cloud systems from private providers, with appropriate standards and guidelines for service provision and usage, and facilitating procurement mechanisms. At the same time, it is necessary to strike a balance between meeting the current and future needs of government agencies, ensuring transparency, fairness, security, reliability, and effective management of the government budget, within the context of Thailand.

Overview of the Cloud First Policy

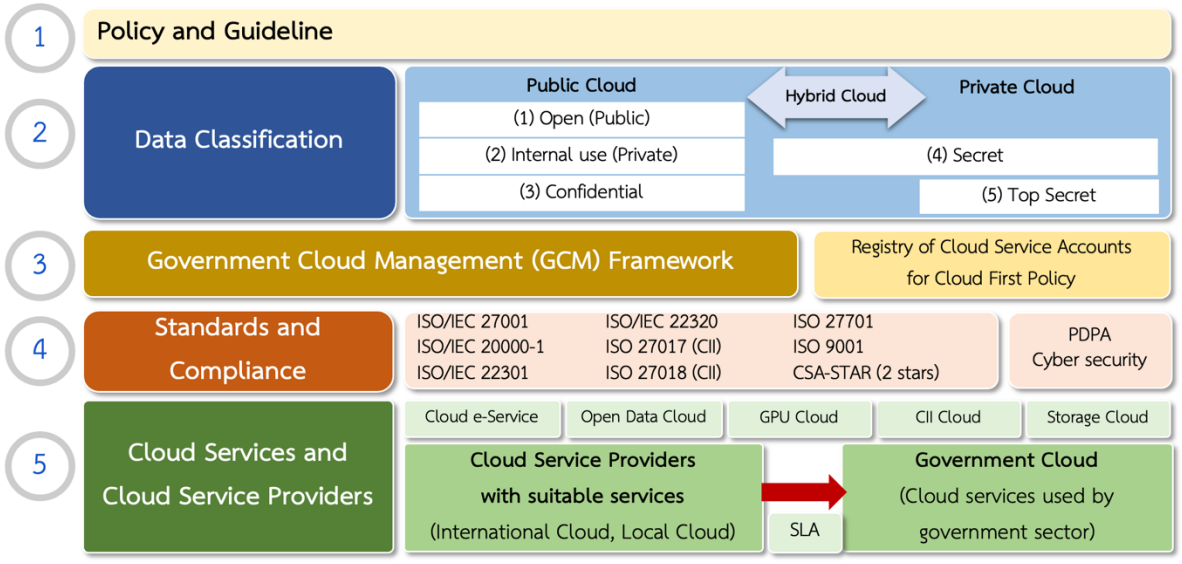
The objectives of the Cloud First Policy are based on utilizing secure cloud technology and accessing modern technology, as well as saving and maximizing government resources, reducing the burden and addressing the shortage of IT personnel in various agencies, increasing government productivity through system and data integration, and enhancing the government's bargaining power in using cloud services. This includes policy principles for determining the appropriate direction of cloud service usage, such as focusing on utilizing Software as a Service (SaaS) and Public Cloud.

For the goals of driving cloud service usage in government agencies, in the initial 1-2 years, the focus should be on three areas: (1) policy, (2) standards and practices, and (3) personnel support. After that, the focus should shift to two areas: (4) technical support and (5) procurement processes.

Components of the Cloud First Policy

To clarify the Cloud First Policy and its future implementation guidelines (draft), policy recommendations, regulations, measures, and standards related to the appropriate provision and use of cloud services for government agencies, this document consists of recommendations on various issues within the policy components, which are considered based on the ecosystem of cloud service usage by government agencies. This ecosystem comprises 5 components (Figure 3), with details as follows:

Figure 3: Components of the Cloud First Policy



(1) Policy and Guideline Framework

Relevant agencies will collaborate to establish policies and guidelines related to the use of cloud services by government agencies. The details of these policies and guidelines must take into account the Personal Data Protection Act, B.E. 2562 (2019), relevant announcements from the National Cybersecurity Committee, and announcements from the Electronic Transactions Committee, such as the Electronic Transactions Committee Announcement on Cloud Service Usage Guidelines, B.E. 2562 (2019).

(2) Selecting the Appropriate Service Type and Model Based on Data Classification

Government agencies must choose cloud services based on the appropriate cloud service type, namely Public Cloud, Private Cloud, and Hybrid Cloud, taking into account the data classification according to the Data Classification Framework and Data Governance principles. Currently, there are various data classification guidelines, such as personal data, security data, official secret data, and public data, as per the Digital Government Development Committee announcement on Public Sector Data Governance, and government information, personal information, and non-disclosable information according to the Official Information Act, B.E. 2540 (1997).

In addition to considering the appropriate type of cloud, when considering the nature of usage requirements, agency capabilities, and budget, it will be possible to truly select and utilize cloud services according to the appropriate type and model of cloud service.

(3) Government Cloud Management (GCM) Framework

The GCM framework aims to facilitate the procurement of cloud services in the budgeting and procurement processes, following the concept of a Digital Marketplace. This involves screening the qualifications of suitable service providers to register in the Cloud Service Catalog in accordance with the Cloud First Policy ("Cloud Service Catalog"), as well as facilitating procurement and budgeting processes.

(4) Standards and Compliance as Qualifications for Cloud Service Providers and Guidelines for Government Agencies Using Cloud Services

Public cloud service providers must be certified with appropriate standards and must be able to provide services with a high enough quality to meet government missions and provide government services in various areas, such as:

- International standards or equivalent standards in Thailand related to overall cloud service provision, which are the minimum qualifications for cloud service providers, and specific standards for cloud services in each sector that users should consider when procuring cloud services.
- Practices for maintaining and managing security risks of cloud services (Security)
- Compliance practices for government agencies using cloud services.

(5) Cloud Service Providers and Cloud Service Characteristics Based on Government Missions or Services

This policy considers various cloud service providers, both public (GDCC or equivalent) and private. In addition to the type and model of cloud services, the user agency must select the service provider themselves or from the list of providers in the Government Cloud Management (GCM) framework.

The use of cloud services must consider the characteristics of cloud services based on the government's mission or services, following the concept of Government as a Platform, which has various types of cloud services that are diverse and constantly evolving. Examples of widely used service groups that can benefit a wide range of government agencies are as follows:

- **Cloud e-Service** for electronic service systems (e-Service) is suitable for government service types such as One Stop Service and various e-Services that require security, as well as back-office systems of agencies with critical data.
- **Open Data Cloud** for general systems and creating open data/public sector information. Suitable for general government services that are public information, creating open data for data integration, and general government systems and public relations work.
- **GPU Cloud Computing** for advanced systems. Suitable for scientific data processing, high-performance simulation processing, and artificial intelligence technology.
- **Critical Information Infrastructure Cloud (CII Cloud)** for agencies using critical information infrastructure. Suitable for work in national security,

banking and finance, information and communication technology, transportation and logistics, energy and utilities, and public health.

- **Storage Cloud** for storing and backing up critical agency data. Suitable for tasks that require long-term data storage, data archiving, and data sharing systems.

Selecting the appropriate cloud service provider, as well as monitoring and evaluation, requires establishing criteria to assess operational capabilities, security, risk assessment and management, and thorough consideration of Service Level Agreements (SLAs), especially service availability.

All recommendations can be linked to the four approaches for driving the Cloud First Policy, as per the resolution of the 1/2023 meeting of the National Digital Economy and Society Committee.

Summary of Study Result on the Readiness and Needs of Thailand and Design Guidelines for the Cloud First Policy

The analysis of data on the policies, plans, regulations, measures, and standards related to the use of cloud services in Thailand and abroad covered the topic of readiness in five dimensions: (1) policy, (2) personnel, (3) technology, (4) procurement, and (5) standards and practices. It was found that in comparison to other countries and territories, Thailand achieved a certain level of progress in every dimension. These include the Republic of Singapore, Hong Kong Special Administrative Region (SAR) of the People's Republic of China, European Union, United States of America, Commonwealth of Australia, and United Kingdom of Great Britain and Northern Ireland. These countries and territories were chosen based on their clear cloud policies and evident support for government cloud usage.

(1) Policy

Thailand has specified the use of cloud services in accordance with the National Policy and Plan on Digital Development for Economy and Society (2018-2037). Additionally, there is a policy to promote the use of cloud technology in the public sector, which has established guidelines for cloud usage in the public sector, emphasizing security, data migration, and data processing in the digital economy, which has stimulated some interest in cloud services among government agencies.

Following the Cabinet resolutions on May 7, 2019, regarding the implementation of the Prime Minister's directive on utilizing Big Data[5] [5], which approved the Ministry of Digital Economy and Society (MDES) to establish the Government Data Center and Cloud Services (GDCC), and on May 5, 2020, approving the "Government Data Center and Cloud Service (GDCC) Development Project"[6] as proposed by MDES, it was found that after the GDCC began providing services to government agencies, there was a continuous increase in interest from government agencies in using the GDCC services. However, due to this high and continuous increase in interest, the GDCC Development Project received more attention from government agencies

[5] Office of the Secretary-General of the Cabinet, Urgent Letter No. Nor 0505/V187 dated May 13, 2019.

[6] Office of the Secretary-General of the Cabinet, Urgent Letter No. Nor 0505/V 216 dated May 8, 2020.

than its capacity could handle, leading to waiting lists for services and challenges in supporting large-scale systems.[7]

The results of driving the aforementioned policies in Thailand show that the relevant policies and the Government Data Center and Cloud Service (GDCC) development project have raised awareness and promoted the demand for cloud services. At the same time, the next phase of the policy to drive cloud service usage in government agencies will need to enhance their capability to utilize cloud service resources from cloud providers in the market, with clear, unified, and reliable principles, guidelines, and procurement processes.

Policy Lessons-learned from International Case Studies

In this aspect, it is possible to apply the direction of the Cloud First Policy or equivalent in leading countries in terms of driving cloud service usage in the public sector, such as:

- Federal Cloud Computing Strategy ("Cloud First") of the United States (2011): Accelerating the public sector's utilization of cloud technology by prioritizing secure and robust cloud service options when investing in systems.
- Federal Cloud Computing Strategy ("Cloud Smart") of the United States (2018): Encouraging the public sector to fully utilize cloud technology by providing practical principles and recommendations.
- Government Cloud First policy of the United Kingdom (2011 and revised in 2019): Prioritizing the use of public cloud and SaaS in the public sector, and managing services, not servers.
- The European Commission Cloud Strategy of the European Union (2019): Prioritizing the use of cloud services in the public sector, with mechanisms to support the procurement of secure Hybrid Multi-cloud services for the public sector.

(2) Standards and Practices

Currently, standards and practices regarding the use of cloud services have been established in various agencies, both those that can set policies and those with specific missions related to cloud service usage. However, the aforementioned practices and regulations are only guidelines for standards and the selection of cloud services, specific to

[7] Information from the opinions of various agencies from in-depth interviews, focus group discussions, and public hearings.

agencies or limited in scope according to the authority of agencies in each sector. They have not yet been enforced as policies at the national level. These practices allow agencies to choose cloud services, but there is no general enforcement at the user level.

Lessons-learned on Standards and Practices from International Case Studies

In terms of standards and practices, the strengths of several countries and regions can be applied. For example, the Republic of Singapore has established standards for work and joint operations of all parties involved. The Hong Kong SAR has created a list of qualified cloud service providers and SaaS providers that government agencies can use. The European Union has guidelines for replacing legacy information systems with cloud services. The United States has guidelines certifying systems and standards, especially those related to security. Various types of procurement contracts have been established.

(3) Human resources

The Digital Government Development Agency (Public Organization) (DGA) has training programs on Government Clouds with upskill courses such as digital workforce development, infrastructure support for digital workforce development, and new-generation leadership to support the digital economy. The GDCC project also offers training and certification courses and there has been collaboration through Memorandums of Understanding (MOUs) with the private sector to develop training courses on cloud usage. However, there is still no permanent agency with the authority to provide specific knowledge and understanding about cloud service usage and appropriate cloud procurement.

Lessons-learned on Personnel from International Case Studies

In terms of personnel, the Republic of Singapore has established a support unit for the use of the Government Cloud, which helps drive the increased use of cloud services by providing skills and knowledge to personnel in managing cloud services as users. Meanwhile, the Commonwealth of Australia has partnered with the private sector to support expert cloud consultants and develop cloud skills for personnel.

(4) Technology

Work process design is supported, along with the training in the use of cloud systems, by the GDCC to allow government agencies to begin the transfer of existing services and systems onto the Infrastructure as a Service (IaaS), which is on the central government

cloud. Improvements have been made in the design of working in the cloud, and advice is provided on the use of government central cloud systems.

Lessons-learned on Technology from International Case Studies

When considering international case studies, technological readiness is found to be a dimension that goes hand in hand with personnel readiness to use new technology in a timely and secure manner. For example, Singapore has developed personnel in government agencies to procure, use, and manage cloud services effectively.

(5) Procurement

There are guidelines for cloud service procurement in which the Ministry of Digital Economy and Society announced the 2023 median prices and basic specifications for the procurement of computer equipment and systems in relation to details on private cloud and public cloud systems in the specification document. However, these do not fully cover the actual usage requirements at present, and there are still problems and obstacles in terms of procurement methods, qualifications of cloud service providers, types of government cloud service contracts, and budget. These can be summarized as follows:

- The announcement of median price guidelines provides some clarity for cloud services, but these guidelines cannot cover the diversity of cloud services. Therefore, determining the median price for cloud service procurement requires price investigation, and the basic specifications presented do not align with current technology and the diversity of usage needs.
- Budget disbursement cannot be processed immediately upon receiving a payment notification.
- Contract templates for procurement do not include templates related to cloud services for government agencies.
- The development of procurement processes with the Digital Marketplace concept still lacks supporting components, such as methods and processes that facilitate quick procurement of cloud services, defining and screening the qualifications of cloud service providers, and guidelines for establishing budgets in the first year.

The Relationship between Cloud Service Pricing and Budgeting and Procurement Processes

For the budgeting process to support cloud service procurement, the current cloud pricing principles are diverse and divided into Fixed Pricing and Dynamic Pricing. Fixed Pricing is more suitable for government agencies than Dynamic Pricing, where prices change and are not fixed until the end of the service, even after signing a contract.

The fixed price in Fixed Pricing can be either for the entire system used or for each service within that system. It can be set as a fixed price per unit of usage, such as for using system resources for processing, setting a fixed price per usage in that manner. It can be further classified into 4 sub-types: (1) Subscription-based, (2) Pay-per-Reservation, (3) Pay-per-use, and (4) Hybrid Pricing. All 4 pricing models can be presented as a list of prices (List Pricing or Menu List). Therefore, the budgeting process in Thailand for cloud services, which currently still relies on the median price announcement, needs to be prepared to accommodate these cloud pricing models.

Lessons-learned on Procurement from International Case Studies

For the procurement process, guidelines can be referenced from case studies of leading countries and regions in cloud usage by government agencies that revealed the facilitation of procurement processes for government agencies in the form of Digital Marketplaces, which often cover the screening of provider qualifications, service screening, and consulting on system migration and cloud usage. For example:

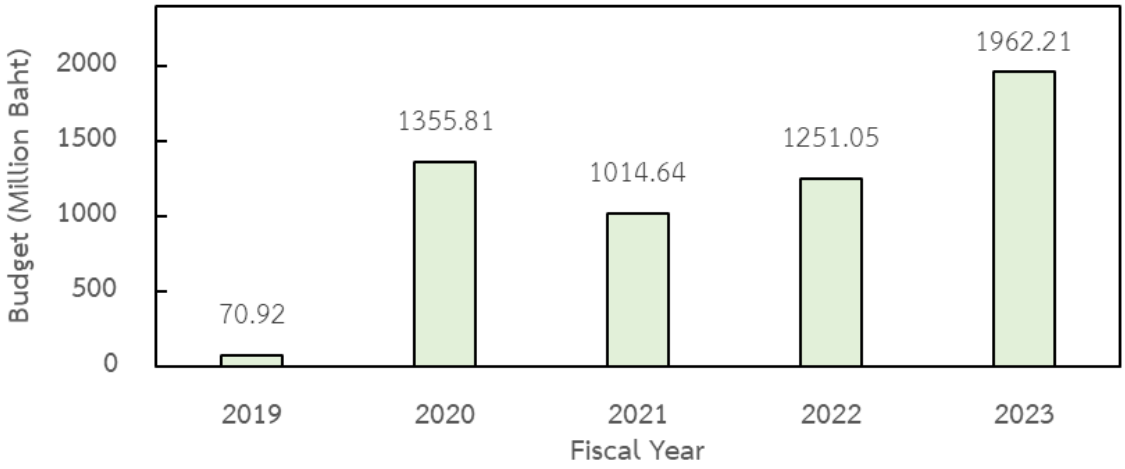
- United States: The Federal Risk and Authorization Management Program (FedRAMP) is an open database of cloud service providers offering certified Cloud Service Offers (CSOs) through FedRAMP's rigorous security standards screening, which government agencies can access when procuring cloud services.
- United Kingdom: The G-Cloud framework and the Commonwealth of Australia's BuyICT platform are lists of pre-screened service providers from which user agencies can directly request quotes and contract cloud services.
- European Union: The DIGIT agency has created the CLOUD III DPS platform, a platform with pre-screened service providers where user agencies can "post" their requirements for those providers to offer prices and services.

- Singapore: The SGTS agency has established the Government on Commercial Cloud (GCC) project to directly procure from service providers and is responsible for selecting cloud service providers to contract with in a Pay-per-use model.

Analysis of Thailand's Readiness and Demand Situation from Statistics and Surveys

As shown in Figure 4, the budget for procurement projects of government agencies nationwide (including the cost of migrating systems to GDCC) shows that government agencies are spending more and more on cloud services. This may reflect that they are increasingly using cloud services.

Figure 4: Budget for Cloud Service-Related Projects (million baht)



Source: Government Expenditure Information System (2024)

Furthermore, a survey on the current readiness and needs of government agencies in Thailand conducted in February 2024 revealed the following issues:

(1) In terms of overall national readiness, Thailand is at a moderate level. It is crucial to prioritize and urgently enhance capabilities in standards and practices, as well as procurement. At the same time, it is necessary to improve data readiness, which is currently at level 2, meaning that most data is stored in non-proprietary formats such as CSV, ODS, XML, JSON, KML, SHP, and KMZ instead of Excel formats.

(2) On the demand side, government agencies will increasingly use cloud systems according to their system resource and budget (data from surveyed subjects). In terms of demand, all cloud service models, IaaS, PaaS, and SaaS, must be considered even though IaaS is the most widely known and preferred. Despite government agencies often not being aware

of the Could First Policy, their demand for cloud services is still likely to increase, which highlights the importance of driving the Cloud First Policy.

This preliminary survey was conducted to investigate and analyze the readiness and demand of government agencies. In the future, a mechanism to evaluate readiness and demand may be implemented.

1. Objectives

1.1 To promote the use of cloud technology to maximize the benefits of government resources, reduce information technology costs, and build resilience to change.

1.2 To alleviate and solve issues regarding the lack of information technology personnel in various government agencies, especially in the areas of cybersecurity and data security.

1.3 To increase government sector productivity through systems and data integration, efficiently driving the sector towards a digital government and allowing the government to play a significant role in driving the digital economy per Thailand's Data Strategy.

1.4 To increase the bargaining power of the government sector in cloud service usage both in quality and price, allowing the sector to maximize cloud service utilization. At the same time, the capability and efficiency in operations and public servicing will also be enhanced.

2. Definition and Scope of the Cloud First Policy

The Cloud First Policy drives ideas and recommends actions for the parties involved. It stipulates that the government considers the cloud system a priority when procuring and developing information technology systems. This shall begin with transferring suitable agency data to a cloud system of the appropriate model and type.

The Cloud First Policy as mentioned in this (Draft) Recommendation on Policy, Laws, Measures, and Standards Related to Suitable Cloud Service Provision and Utilization for the Public Sector, will cover the relevant parties and services as follows:

2.1 Users shall mean government agencies, from central government, provincial government, local government, and state enterprises according to the law on public organization budget procedures, as well as independent organizations, organs under the constitution, or other government agencies according to the Administrative Procedure Act.

2.2 Cloud Service Providers (CSPs) shall include the Government Data Center and Cloud Service (GDCC) project, local CSPs, and international CSPs.

Cloud Service shall mean Cloud Computing services, which are processing on-demand services utilizing shared computer resources over a network according to demand.

2.3 Cloud Service Models shall include Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) with the following definitions:[8]

(1) Software as a Service (SaaS) provides users with ready-made computer programs supplied by, stored in, and running on the service provider's infrastructure. Users can use these programs via the Internet or the program page without having to manage the infrastructure, networks, operating systems, database management systems, and computer program configurations. Nevertheless, users can configure parts of the programs to work according to their needs.

(2) Platform as a Service (PaaS) provides platform services and tools for use in developing and installing software applications, such as computer programs, database systems, and management systems or services. Users can develop, install, and customize computer programs using the cloud infrastructure that the service provider manages without having to manage the infrastructure, networks, operating systems, and database management systems.

(3) Infrastructure as a Service (IaaS) provides the main infrastructure of cloud services, consisting of data processing systems, data storage systems, network systems, and other basic resources related to the computing system. Users can install and use computer programs as required within the infrastructure and resources given by the service provider without having to manage the necessary infrastructure themselves.

2.4 Cloud Deployment Models The types of cloud services considered in this policy consist of three categories: Public Cloud, Private Cloud, and Hybrid Cloud, with the following definitions:[9]

(1) A Public Cloud is a service system that provides cloud infrastructure that is open to the public and agencies for general use. Management and servicing may be provided by firms and educational institutions. Cloud system infrastructures are owned, managed, and operated by cloud providers, or in some cases, by multiple entities. In any case, the cloud system infrastructure resides within the cloud service provider's premises.

---

[8] Adapted from P M Mell and T Grance, "The NIST Definition of Cloud Computing," 0 ed. (Gaithersburg, MD: National Institute of Standards and Technology, 2011), https://doi.org/10.6028/NIST.SP.800-145.

[9] Adapted from P M Mell and T Grance, "The NIST Definition of Cloud Computing," 0 ed. (Gaithersburg, MD: National Institute of Standards and Technology, 2011), https://doi.org/10.6028/NIST.SP.800-145.

(2) A Private Cloud is a type of cloud with a service system that provides cloud infrastructure for use by a single agency or organization. The cloud infrastructure is owned, managed, and operated by the agency itself, an organization, or a third party such as a cloud operator or multiple entities, depending on the case. The cloud infrastructure may be on-premise or off-premise.

(3) A Hybrid Cloud is a type of cloud with a service system that provides both public and private cloud infrastructures. The infrastructures are separate, but allows for mixed usage through data integration and transfer, and application portability.

3. Importance and Benefits of Cloud Technology for Government Agencies

Cloud computing technology is beneficial for information system management, process development and facilitation, and data management. Specifically, for government agencies, the benefits include:

3.1 Reduction of IT System Costs: By reducing investment in expensive software and hardware and switching to internet-based services, government agencies can adopt a Pay-as-you-go or Pay-per-use model, effectively lowering Transaction Costs for exchanging, accessing, maintaining, and processing data. This approach also offers flexibility in adjusting resources based on actual usage patterns.

3.2 Flexibility and Scalability: Cloud computing allows for easy up-scaling or down-scaling of computing resources to match the agency's needs, accommodating fluctuations in usage, development, and ongoing improvements. It also enables flexible software upgrades and resource additions for enhanced efficiency and service stability.

3.3 Easy Access and Usage: Users can access data and applications in the cloud from any location and at any time with an internet connection. This facilitates real-time collaboration by enabling simultaneous access to resources.

3.4 Security: Data is protected from various risks, as users are partially relieved of the burden of designing and implementing security systems. Cloud providers play a role in monitoring and implementing security measures, and users can utilize reliable data backup systems.

3.5 Up-to-date Service: Cloud providers can keep software updated, enabling them to offer new features to meet user needs or address problems, including system security.

3.6 Promoting Innovation: Utilizing cloud technology with a focus on supporting and choosing SaaS fosters innovation and the development of new products. Additionally, Application Programming Interfaces (APIs) allow developers to create applications that integrate with the system.

3.7 Data Sharing: Primarily using cloud systems encourages data storage in machine-readable formats, enabling the linking of data from multiple databases. The system can support two-way data exchange, reducing barriers to interagency data access and ensuring real-time data updates.

3.8 Data Utilization: Cloud computing facilitates convenient data retrieval and utilization, supporting the creation of a data ecosystem and promoting maximum data utilization across government, private sector, and public domains. This enhances competitiveness and strengthens government policy planning.

4. Goals for Government Agency Cloud Service Usage

The adoption of cloud services by government agencies in Thailand in the initial 1-2 years focuses on three main areas: (1) Policy, (2) Standards and Practices, and (3) Personnel Support. From the third year onwards, the focus shifts to two areas: (4) Technical Support and (5) Procurement Processes.

Table 1: Goals of Cloud Service Adoption by Government Agencies

Focus Areas	Phase 1-2 Years	Phase 3-5 Years
Policy	• Central and regional government agencies migrate to cloud services where feasible or easily implemented, particularly for open data. • Establish policies for agencies to primarily utilize cloud technology in digital technology development. • Promote investment and development in cloud service providers.	• All central, regional, and local government agencies utilize cloud services wherever possible. • Sustainably drive the public sector towards digital government. • Save the government budget on cloud service utilization.
Standards and Practices	• Establish standards and practices related to cloud services, cloud security, and data.	• Cloud services provided to all government agencies can adhere to Service Level Agreements (SLAs),

	• Define guidelines for decision-making and collaboration among government agencies, cloud service providers, and all other relevant stakeholders. • Ensure that government agencies and CII entities using cloud services utilize cloud services that meet the minimum cybersecurity requirements as prescribed by law. • Develop domestic standards and certifications to support cloud services that meet specified criteria. • Government agencies select cloud services that are appropriate for their needs, primarily focusing on SaaS and public cloud options.	particularly in terms of Service Availability. • Cloud services provided to all government agencies are fully certified with relevant international or domestic standards.
Personnel Support	• Prepare personnel with the skills and knowledge to manage cloud systems effectively. • Develop government personnel to efficiently procure, utilize, and manage cloud services.	• Assign support agencies to provide knowledge and consultation, encouraging increased cloud adoption as agencies become more familiar with its use. • Provide personnel with the skills and knowledge necessary for managing cloud services.
Technology Support	• Achieve integration of government data under a unified standard. • Enable flexibility in management and resource sharing among government agencies.	• Achieve integration of government data under a unified standard. • Enable flexibility in management and resource sharing among government agencies. • Facilitate the utilization of integrated data and Big Data.
Procurement	• Establish a framework mechanism to facilitate the procurement process. • Register cloud service providers and cloud service accounts that meet specified qualifications.	• Fully streamline the budgeting and procurement processes to support cloud service acquisition. • Designate a specific agency responsible for procuring cloud services suitable for various agencies.

5. Cloud First Policy Principles

5.1 Government agencies must prioritize the use of cloud services as the first option when procuring or upgrading IT systems, whenever feasible and appropriate.

5.2 Government agencies should select cloud services from providers that meet the standards and requirements outlined in this policy.

5.3 Government agencies prioritize the use of SaaS and Public Cloud over on-premise solutions, with considerations on long-term cost-effectiveness.

5.4 Government agencies assess the confidentiality of processed data to select the appropriate type of cloud service.

5.5 Government cloud services shall be reliable, with resources continuously audited and maintained for optimal availability. Government agencies to prioritize security measures, privacy, and data backup for recovery.

5.6 Government agencies using cloud services establish and implement access control measures for various service components.

5.7 Government agencies using cloud services consider and evaluate usage-based pricing based on actual needs, taking into account fluctuations in usage throughout the contract period.

6. Recommendations in accordance with the components of the Cloud First Policy

6.1 Policy and Guideline Conceptual Framework

Recommendation 1.1: Conceptual framework to create guidelines, recommendations, and standards for government agency users

Type of recommendation: Standards and Guidelines

In the preparation of guidelines for government agency users, there should be a conceptual framework that aligns with the Personal Data Protection Act, B.E. 2562 (2019), the relevant announcements of the National Cyber Security Agency, and the announcements of the Electronic Transactions Committee, such as the Announcement of the Electronic Transactions Committee on Cloud Computing Guidelines, B.E. 2562 (2019), as well as alignment with the Principles of the Cloud First Policy.

Recommendation 1.2: Data security and privacy principles for reliable use of cloud services by government agencies

Type of recommendation: Standards and guidelines

To adopt the Cloud First Policy, government agencies need to prioritize data security and protection measures to encourage the use of government cloud systems. This would lead to the preparedness of the agency regarding Confidentiality, Data Accuracy and Integrity, and Data Availability.

The National Cyber Security Agency (NCSA) should be responsible for, and collaborate with relevant agencies in establishing policies, regulations, or practices regarding the protection of security and privacy of data for cloud services for government agencies. This should include mechanisms for overseeing government agency usage and guidelines for determining responsibility, with consideration of the Shared Responsibility between cloud providers and government agencies using cloud services. These measures should encompass the following principles of data security and privacy:

(1) A governance framework is needed to oversee security and safety, risk assessment and management, and the operating practices of cloud services. This includes the Deployment of systems and services in the cloud such as Data Governance and cloud-based artificial intelligence technology supervision systems.

(2) Data In Transit Protection demands that government agencies should use encryption technology such as HTTPS or SSL/TLS in data transmission to prevent data interception, or use Virtual Private Network (VPN) technology to create a secure network for sending data between organizations. Additionally, standards and procedures for data transmission should be set up, including regular data transmission audits and monitoring, particularly for information that is significant and has legal implications regarding liability and accountability, such as security information and personal data etc.

(3) Operational Security The provision and use of cloud services should adhere to comprehensive security standards and practices tailored to the specific use case. This includes guidelines for access control, data backup, and data recovery.

(4) Secure Use of the Service Government agencies should establish criteria for selecting service providers that align with their usage needs. This includes employing

security measures appropriate for the workflows and confidentiality of processed data and ensuring adequate Service Availability.

6.2 Selecting the Suitable Service Type and Model Based On Data Classification

Recommendation 2.1: Classification of data and related data practices

Type of recommendation: Guidelines and Law Amendment

Implementing the storage, processing, and sharing of government data via cloud systems necessitates the establishment of data classification guidelines and relevant data practices. This is crucial to ensure security, data accessibility, data management, and consistent operations. These measures will enable seamless data integration and sharing, maximizing benefits of government cloud.

Related agencies should formulate or amend relevant regulations and guidelines, taking into account storage, processing, and linking of data on cloud. Relevant topics include:

(1) Data classification: relevant agencies shall expedite their data classification requirements, taking into account the types of cloud services. Initially, they may refer to the standards set by the Digital Government Development Agency (Public Organization) regarding the criteria for classifying and sharing government information (DGAS, 8-2565), as shown in Table 2.

Currently, there are many challenges related to storing data in digital format and in the cloud. Laws and guidelines regarding data classification only cover data storage in information systems and as hard copies. Top secret data is to be stored in hard copy only and is prohibited from being moved into an information system. Thus, the relevant agencies may consider amending the related laws and guidelines to allow Top Secret Data to be stored in a highly secure information system.

Requirements for data classification should be formulated for easy understanding and implementation. The levels of data classes should be reduced to avoid overlapping definitions and obscurity concerns which could lead to data overclassification. The trends in classification amendment in other countries can be referred to as follows: The United Kingdom has revamped its information classification to open data and three levels of classified data: Official, Secret, and Top Secret. Thus, all related laws had to be amended for consistency, including the Official Information Act, Regulation on Maintenance of Official

Secrets, Regulation of the Prime Minister's Office on Correspondence Work, and Regulation of the Prime Minister's Office on National Security, as a minimum.

Table 2: Classification of Government Information (DGAS 8-2565)

Classification	Details	Data samples
Open to the public	Government information that state agencies must disclose to the public for their knowledge, awareness, or audit without the need for a request.	Rules, the Cabinet's resolutions, regulations, academic reports, and open government data
Private to an organization, to be disclosed with permission	Information that an organization does not freely publish, typically involving private data, whether personal or organizational. Even though the loss or disclosure of such information may not result in significant impact, it is undesirable for the information to be disclosed without authorization.	Registration records, personnel data, operation documents, and the agency's work procedures.
Confidential/Sensitive, to be disclosed with permission	Information that would create loss if disclosed to unauthorized individuals/organizations and result in significant embarrassment to the person/organization, and could lead to legal consequences or incur damage to national interests.	Litigation information and unresolved opinions within the organization.
Secret, to be disclosed with permission	Reserved information that, if lost or improperly disclosed, would cause significant loss/severe impact, potentially leading to reputational damage and financial/asset losses and significantly impacting national security and interests.	Medical reports, information on international relations, and key policies implemented toward foreign states
Top-Secret, classified information that cannot be disclosed/is a confidential document.	Restricted/Non-Disclosure Information: Information that, if lost or improperly disclosed, would cause the most severe loss/impact, resulting in significant damage to reputation and financial/asset losses, and could have a vital impact on national security and interests.	Military strength information, strategic intelligence information, and security policy information.

Source: Digital Government Development Agency (Public Organization), Government Data Classification and Data Sharing Framework (2565).

(2) Establishing dataset evaluation criteria for confidentiality classification in relation to the cloud system level of standards and security measures Relevant agencies should establish the criteria for evaluating datasets to classify information, taking into account the different types of cloud services, by designing an assessment form and specifying the roles of the assessors. Such criteria must clearly state the evaluation guidelines and score metrics, to reduce dependency on the evaluator's discretion. The criteria shall be fully enforced and concise and prevent unassessed data classification or overclassification. Utmost consideration to risks of cyber threats and potential consequences if the data is leaked, lost, or improperly disclosed shall be addressed in compliance with the Data Protection Impact Assessment (DPIA) and in alignment with cloud security standards and measures. This implementation shall follow the guidelines in the announcement of the National Cyber Security Agency on Standards for Specifying Cyber Security Characteristics for Data or Information Systems, B.E. 2566 (2023).

(3) Establishing guidelines for data handling based on Classification Labels to augment access rights in accordance with security principles. Manuals or guidelines shall be prepared for government agencies in possession of classified data, enabling them to select a secure cloud system to enhance cybersecurity and facilitate cloud service selection.

(4) Developing comprehensive data handling procedures for each classification label, in consideration of digital data and cloud services to augment the definition of access rights based on data security principles. This includes guidelines for recording data creation, access, and modification history, data destruction procedures, and data set inventories reporting guidelines, while promoting data transparency and outlining procedures for declassification over time.

This should be urgently implemented as a collaborative effort between relevant agencies, including updating relevant laws in conjunction with the actions mentioned in point (1). Additionally, manuals or guidelines should be created for government agencies holding classified information on how to choose secure cloud services, to appropriately enhance cybersecurity for government agencies. This will facilitate the selection and use of cloud services by the government, maximizing benefits for the public and government operations.

(5) Data Residency and Data Sovereignty Relevant agencies should establish clear guidelines regarding Data Residency and Data Sovereignty for data used in government missions and operations. When formulating these guidelines, consideration should be given to ensuring compliance with relevant international cooperation frameworks, agreements, or laws.

- **Data residency** Clear guidelines should be established covering personal data and each level of classified data of various government agencies. These guidelines should stipulate that classified data, ranging from public to secret levels, can be transferred across borders and processed offshore, provided that the destination country has security standards at least equivalent to those of Thailand. A copy of the data must be kept within the country for audit purposes and to prevent data leakage to other countries. This approach is comparable and consistent with the case of personal data as per the Personal Data Protection Act, B.E. 2562 (2019). However, for Secret and Top-Secret data, it should be mandated that processing and storage of data be done exclusively within the country (Data Localization).

- **Data sovereignty** Provisions should be made to ensure that laws pertaining to government data and information systems apply to cases where data controllers or processors located outside the kingdom collect, use, or disclose government data. The data-owning agency should have the authority to designate data access and easily transfer data to other systems if needed.

Recommendation 2.2: Criteria for selecting cloud services for government agencies by specifying the type and model of services offered by cloud service providers

Type of recommendation: Process and Methods of Implementation

The selection of cloud types (Public Cloud, Private Cloud, and Hybrid Cloud) and cloud service models (SaaS, PaaS, and IaaS) for government agencies demands consideration of various factors, particularly Data Classification. If a Government Cloud Management (GCM) Framework is available to assist with procurement, it must be determined whether the needed service is present in the Registry of Cloud Service Accounts. This recommendation proposes eight factors in cloud service selection, as follows:

- Data Classification
- Data Residency
- The number of users, the volume of data, and the amount of processing in the system
- Availability of On-Demand services in the Registry
- Agency capability in maintaining the system, based on the division of responsibility with the operator, when using the desired service
- Agency capability in system development, or in the ability to hire a system developer, when using the desired service.
- Support for application development according to usage needs (in the case of PaaS)
- Certified standards and legal compliance by the cloud service operator (in case that the operator is not registered in the Registry)

To select a suitable cloud service that covers the above factors, three steps need to be considered, details for consideration in each step are as follows:

(1) Selecting cloud service type based on data classification

To obtain the most benefit from cloud services such as technology, resource savings by utilizing the resources of a large-scale cloud service provider and the high level of security provided by cloud service providers, **a Public Cloud should be considered as the first option**. Agencies choosing cloud services other than a Public Cloud must have appropriate and justifiable reasons. However, when using a public cloud, caution should be exercised in planning and designing the use of services for maximum efficiency (Optimization) to prevent costs from exceeding what is necessary.

The criteria for considering the cloud deployment model (Table 3) should comply with data handling at each level of classification as well as resource requirements. There are two factors to consider as follows:

- Data classification
- Data residency

Open data, defined as data that can be shared openly according to the Government Data Sharing Framework, and Private, Confidential, and Secret data, defined as

data that can be shared if authorized, can be kept in the public cloud. Top Secret data can be kept in a private cloud administered by the service provider, in an agency-managed private cloud, or on-premise. Data access rights must be appropriately controlled for all types. Currently, Top Secret data is strictly forbidden from being uploaded into an information system.

Data residency should comply with the requirements related to data localization for storage and processing, whether offshore or onshore. This recommendation focuses on the technical suitability that can ensure operational credibility.

Another factor to be considered is:

- Number of users, volume of data, and amount of internal processing

In the event that a data handling system on a Public Cloud is connected to a data handling system on a Private Cloud that is managed by a service provider or is an agency-managed private cloud (Agency-managed Private Cloud), or is an on-premise system (On-premise), or is a Private Cloud or an On-premise system (On-premise), with a high volume of users, data, and internal processing (Usage Demand) in the system, especially systems that are expected to have usage demand peaks at certain times, then a Hybrid Cloud should be considered.

(2) Selecting the suitable cloud service model

Choosing a cloud service model should comply with the Principles of this policy, which **prioritizes the SaaS** model (Figure 5) with five factors for consideration:

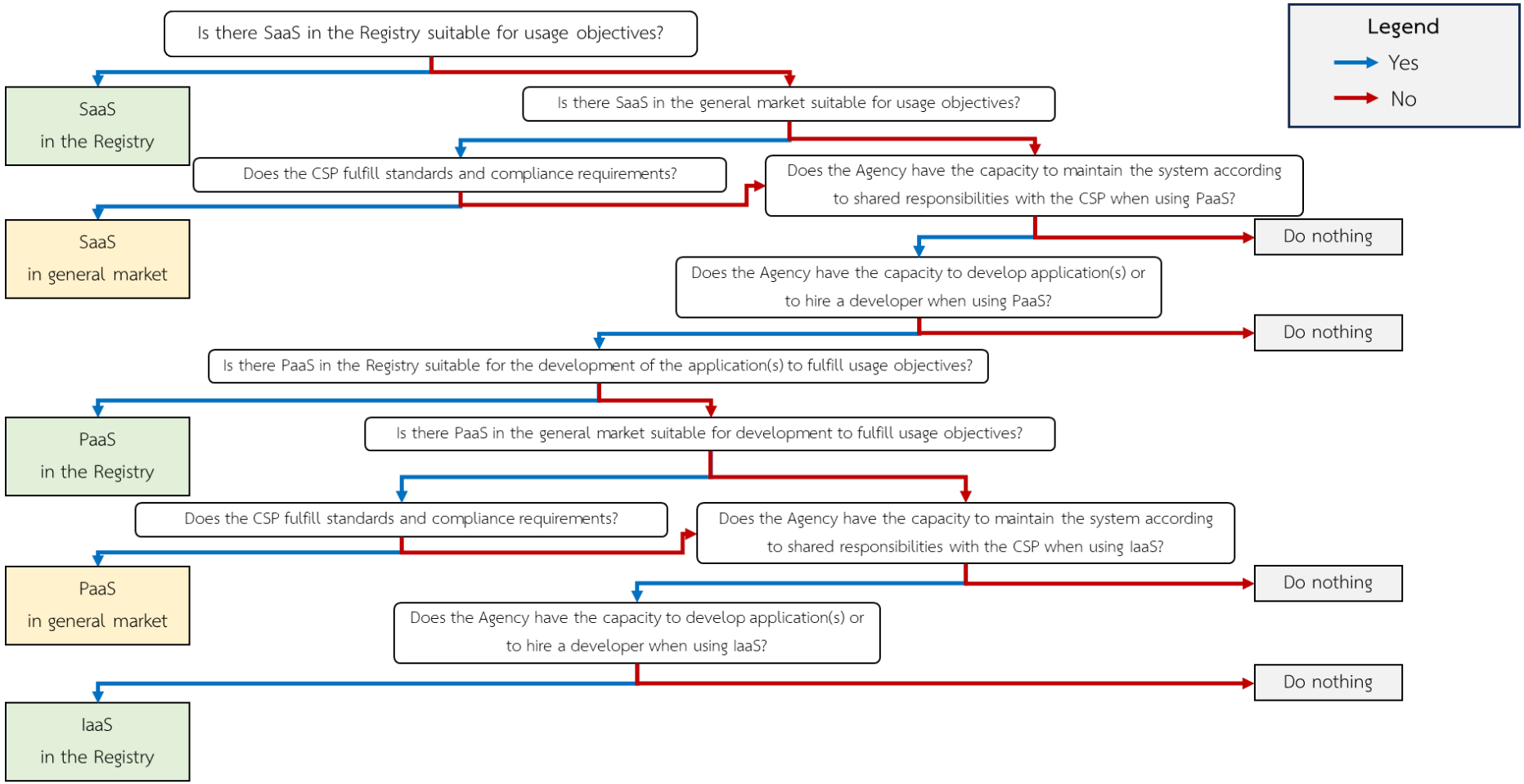
- Availability of on-demand services in the Registry
- Agency capability in maintaining the system, based on the division of responsibility with the provider, when using the desired service
- Agency capability in system development or in the ability to hire a system developer when using the desired service.
- Support for application development according to usage needs (in the case of PaaS
- Certified standards and legal compliance of cloud service providers (in the case that the provider is not registered in the Registry)

Agencies opting for cloud service systems other than SaaS must have appropriate and justifiable reasons.

Table 3: Criteria for selecting the suitable cloud service type according to the level of data classification

	Public Cloud		Private Cloud		Hybrid Cloud		On-premise	
Data Classification	Offshore	Onshore	Offshore	Onshore	Offshore	Onshore	Offshore	Onshore
Open	✓	✓			✓	✓		
Private								
Confidential								
Secret		✓		✓		✓		✓
Top Secret				✓				✓

Figure 5: Evaluating the appropriate type of Cloud Service



(3) Considering the feasibility of cloud service models based on cloud service types.

After determining the appropriate type of cloud service and cloud service model, it is necessary to consider the feasibility of the cloud service model according to the type of cloud service. This is because various service models are often designed and provided on the Public Cloud, especially in the case of SaaS and PaaS, which may not be fully available on the Private Cloud and Hybrid Cloud in all cases. In addition, it may be necessary to consider the support for different data classification levels again. For example, organizing meetings or preparing documents at a top-secret level using SaaS requires a Public Cloud or Private Cloud that processes data within the country, which may not have comprehensive services available. Therefore, it is necessary to consult with experts before proceeding with the procurement of cloud services.

For Private Clouds managed by the organization or on-premise server systems, SaaS, PaaS, and IaaS are not applicable. In such scenarios, the organization must independently develop and maintain all system components.

Table 4: Evaluating Feasibility of Using Cloud Service Models with Cloud Type

		Cloud Service Models			
		SaaS	PaaS	IaaS	On-premise
Cloud Deployment Models	Public Cloud	✓	✓	✓	✗
	Private Cloud	Consult an expert	Consult an expert	✓	✗
	Hybrid Cloud	Consult an expert	Consult an expert	✓	✗
	On-premise				✓

(4) Additional considerations

When selecting cloud services, government agencies should take into account the following additional factors alongside the previously outlined guidelines:

(4.1) Budgetary factors in choosing cloud services: Even if the service meets the requirements according to the criteria for selecting the type and model of cloud service above, there may be additional budgetary factors to consider.

- The use of Private Clouds or On-premise servers should be limited to essential data only, due to the significant costs associated with system implementation, maintenance, and the recruitment of specialized personnel with expertise in digital infrastructure, computer networks, and high-level security. Other data and operations can be managed through Public Cloud services that can be in the form of a Hybrid Cloud model. This approach helps reduce the costs associated with Private Cloud or On-premise servers.

- The use of IaaS should be considered only for components that PaaS cannot support. This is due to the Shared Responsibilities with service providers. Utilizing IaaS incurs additional costs for system implementation, maintenance, and the recruitment of personnel for system development.

- The volume of data transfer typically depends on the amount of data exchanged within a system, often measured by the number of Transactions. Providers usually establish minimum usage and offer pricing tiers, such as 1-10,000 transactions at a certain rate, and anything exceeding this range incurs a different pricing.

(4.2) Data Center location has a significant impact on service charges across different regions of the World. These charges are influenced by the local operational costs incurred by the service providers. Additionally, the effect on service speed should be taken into consideration as well.

(4.3) Local hosts are crucial for systems that require data localization. The service provider's data center must be certified by relevant authorities, meeting either international or domestic standards. It must also be capable of providing services during maintenance or equipment changes (concurrently maintainable) or an equivalent level of availability.

To facilitate government agencies in procuring cloud services that support local hosting, the qualifications of cloud service providers can be specified in the Registry of Cloud Service Accounts. Providers should either own or have long-term usage rights to at least one data center within the country. The definition of a data center is based on the announcement by the National Electronics and Computer Technology Center, which outlines specific certification requirements. This includes “a building or part of a building designated

for housing computer rooms or computer systems, including the areas and various support systems intended for receiving, transmitting, storing, and processing data."

(4.4) Vendor lock-in or technical lock-in must be taken into account when using cloud services. Government agencies utilizing cloud services should recognize that some degree of technical lock-in is often necessary to maximize the benefits of cloud services. It is important to balance the acceptable level of technical lock-in with the associated risks and opportunities. Such balance involves considering the value offered from the services and portability.

For example, cloud providers often develop technologies or tools that are modern, convenient, and meet user needs, but may only be usable within that specific provider's cloud environment. Whether these technologies or tools are developed as open-source can impact price bargaining power, the ability to change providers, and future cloud system portability. Rejecting technical lock-in may enhance system flexibility and ease of migration, but the opportunity to benefit from the cloud service will also be lost. Such a decision will necessitate the development of systems entirely in-house using IaaS as well as the purchase of tool licenses. This leads to impacts on license costs and personnel or consultant fees for system development. This approach may not align well with the principles of the Policy.

6.3 Framework for Government Cloud Management

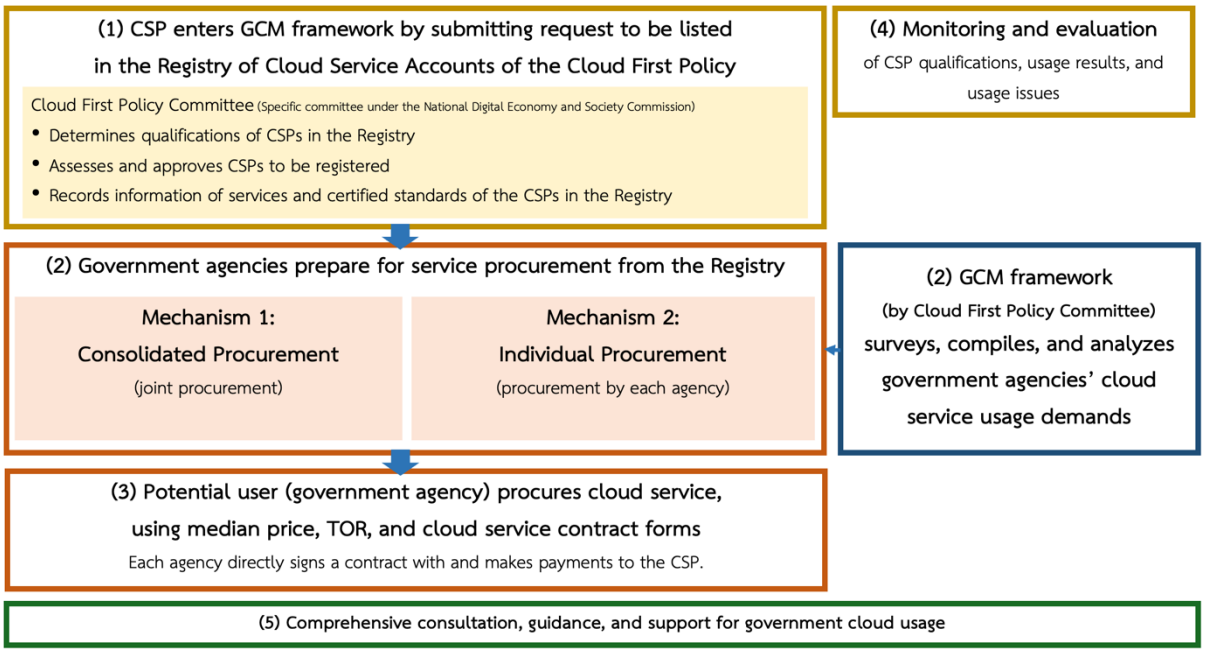
The recommendations related to the GCM framework call for the establishment of this framework. The Cloud First Policy Committee should lead this effort in collaboration with relevant agencies. The goal is to facilitate the procurement and budgeting processes, provide consultation, and offer information on services and the qualifications of operators listed in the Registry per the Cloud First Policy (Recommendations 3.1 to 3.7). At the same time, to ensure efficient procurement of cloud services, other preparations are also necessary (Recommendations 3.7 to 3.13).

Recommendation 3.1: Government Cloud Management Framework concept and related recommendations

Type of Recommendation: Process

The GCM framework outlined in this recommendation has five key functions in the procurement process and related operations, as shown in Figure 6.

Figure 6: Overview of the Procurement Process under the Government Cloud Management Framework



(1) Registration in the Registry of Cloud Service Accounts of the Cloud First Policy: the GCM framework establishes appropriate standards and qualifications for cloud service operators, accepts applications from operators, and screens their qualifications before registering them as service providers in the Registry of Cloud Service Accounts of the Cloud First Policy.

(2) Facilitating service users (government agencies) in procuring cloud services from the Registry: the GCM framework collects the needs of government agencies in order to identify common services. It then prepares for cloud service procurement by providing information to and coordinating with relevant parties. The procurement process under the GCM framework is divided into two mechanisms. A brief overview of these mechanisms is as follows.

Mechanism 1 : Consolidated procurement of high-demand cloud services (GCM Lot)

- The GCM framework surveys, compiles, and analyzes cloud service usage demands from government agencies nationwide.
- The GCM framework identifies common services with high demand across the government sector to enhance bargaining power with operators.
- Agencies requiring these common services jointly procure cloud services from the Registry, draft a memorandum of understanding, and negotiate prices with the operators through a consolidated procurement process.

Mechanism 2: Individual procurement by each agency

- The agencies procure the service through the Registry. The procurement is handled using the specific method.

(3) Facilitating cloud service procurement and procurement processes when the user (government agency) procures using the median price, Terms of Reference (TOR), and cloud service contract template for government agencies.

(4) Monitoring and evaluation: By monitoring and evaluating the qualifications of cloud service providers in the "Cloud Service Account" and monitoring, evaluating, and supporting the use of cloud services and problems in the use of cloud services by government agencies.

(5) Comprehensive consultation, guidance, and support for cloud service usage: Comprehensive consultation services include cost estimation for budget planning and analysis. Develop or compile relevant practices for users and providers. Provide training for government personnel to make informed decisions about cloud service procurement, usage, and system maintenance based on the type and model of cloud services.

Based on the aforementioned principles, the primary roles of the relevant parties, namely the GCM framework, government agencies (users), and cloud service operators (vendors) in the procurement process are summarized in Table 5.

Table 5: Roles of Relevant Parties Within the Government Cloud Management (GCM) Framework for Managing Cloud Usage in Government Agencies

Component	Roles of GCM Framework	Roles of Government Agencies (Users)	Roles of Cloud Service Operators (Providers)
Registry of Cloud Service Accounts of the Cloud-First Policy	• Establishing standards and appropriate qualifications for cloud service operators, as well as the registration process for cloud service operators. • Screening the qualifications of cloud service operators to qualify them as cloud service providers in the Registry. • Compiling the certified services and standards of the operators into the Registry.	-	• Cloud service operators enter the GCM framework by registering as cloud service providers in the Registry.
Mechanism 1: Consolidated procurement of common services with high demand (GCM Lot)	• Surveying, compiling, and analyzing cloud service requirements from government agencies nationwide. • Identifying and defining common services. • Inviting government agencies whose needs align with common services to participate in consolidated procurement. • Coordinating and facilitating the signing of memorandums of understanding (MOUs) between agencies involved in consolidated procurement and overseeing the procurement process.	• Notify the agency's cloud service usage characteristics and quantity to the Framework. • Agencies requiring common cloud services jointly procure cloud services by documenting mutual agreements and proceeding with the procurement process. • Enter into contracts with the winning cloud service provider(s) and pay service fees.	• Submit proposal when agencies requiring common services jointly procure cloud services. • Upon winning the proposal, enter into contracts with the government agencies that will utilize the services and invoice each government agency for service fees.

Component	Roles of GCM Framework	Roles of Government Agencies (Users)	Roles of Cloud Service Operators (Providers)
	• Facilitating the development of the TOR and contracts for common services, referencing standardized TOR and cloud service contracts for government agencies.		
Mechanism 2: Individual procurement by each government agency	• Providing consultation for the development of TOR and contracts for the agencies intending to utilize the services. • Approving the principles and budgetary allocations for the services required by the agencies. • Facilitating the procurement process by supplying a list of service providers and services available in the Registry and offering advice on qualifications and median prices.	• Acquire the list of service providers from the Registry to prepare invitations to businesses and initiate procurement, employing either selection or specific methods. • Develop TOR and contracts, referencing standardized TOR and cloud service contracts for government agencies within the framework. • Enter into contracts with the winning cloud service providers and pay service fees.	• Submit proposal when the agencies needing cloud services have sent invitations and initiated the procurement process through selection or specific methods. • Upon winning the proposal, enter into contracts with government agencies that will utilize the services, and invoice each government agency for service fees.

To ensure completeness of the procurement processes, budgeting procedures, and support for cloud service utilization by government agencies, a comprehensive framework called Government Cloud Management (GCM) is established. This framework aims to link cloud service ecosystems for government agencies according to the aforementioned principles. Therefore, it is imperative to implement various recommendations as follows:

(1) Recommendations for establishing and defining the processes of the GCM framework:

- Establishment of the GCM framework (Recommendation 3.2)
- Implementation of the GCM framework by the Cloud First Policy Committee (Recommendation 3.3)
- Specifying and screening cloud service operator qualifications suitable for registration as cloud service providers for government agencies in the Registry of Cloud Service Accounts of the Cloud First Policy (Recommendation 3.4)
- Facilitating government agencies in the preparation to procure cloud services from the Registry (Recommendation 3.5)
- Facilitating government agencies in procuring cloud services and procurement processes (Recommendation 3.6)
- Monitoring and evaluation, providing consultation, guideline setting, and support for government agency cloud service utilization (Recommendation 3.7)

(2) Recommendations regarding budgeting processes to accommodate government agencies' cloud service usage:

- Guidelines for establishing and disbursing budgets related to government cloud services to align with pay-per-use billing (Recommendation 3.8)
- Consideration of long-term budgeting process improvements (Recommendation 3.9)

(3) Recommendations for transitioning to cloud service procurement under the GCM framework:

- Clarify guidelines for selecting government agencies' cloud service procurement approaches (Recommendation 3.10)

- Preparation for government agencies to utilize cloud services (Recommendation 3.11)
- Initial budgeting guidelines (Recommendation 3.12)

Recommendation 3.2: Establishment of the GCM Framework

Type of Recommendation: Legislative Amendment

The establishment of the GCM framework can be facilitated by assigning tasks related to government cloud service usage to the Cloud First Policy Committee, with the Office of the National Digital Economy and Society Commission (ONDE) acting as the administrative unit pursuant to the Digital Economy and Society Development Act, B.E. 2560 (2017).

This can be achieved by creating the (draft) Ministerial Regulation: Prescribing of Supplies that the State Needs to Promote or Support (No. 5), B.E. .... By virtue of Section 5, paragraph one; Section 56, paragraph one (2) (h) and paragraph two; Section 65, paragraph two; Section 70(2) (d) and (3)(g); and Article 75, paragraph two of the Public Procurement and Supplies Administration Act, granting the Minister of Finance the authority to issue ministerial regulations on cloud service procurement for government agencies as promoted supplies. As such, a new category of cloud service supplies should be added in Chapter 7/4, and should include the following key points:

- Define “cloud-promoting supplies” as cloud services, which include various service models such as SaaS, PaaS, and IaaS. These services are deployed as one of the following cloud types: Public Cloud, Private Cloud, and Hybrid Cloud. It is imperative that they receive digital certification as stipulated by the Ministry of Digital Economy and Society.
- Define “cloud-promoting supplies” as supplies registered in Registry of Cloud Service Accounts according to the Cloud First Policy, intended to be promoted or supported by the government.
- Specify that the criteria, methods, and conditions for registering in the Cloud Service Accounts according to the Cloud First Policy should comply with the announcements issued by the National Digital Economy and Society Commission.
- Specify that government agencies are authorized to procure cloud-promoting supplies through either the selection method or the specific method. If there is only one vendor providing such supplies, the procurement should be done through the

specific method or direct contracts. If there are three or more vendors, procurement should follow the selection method.

The criteria, methods, and conditions for registering in the Registry of Cloud Service Accounts, as specified by the National Digital Economy and Society Commission, are such that it is the responsibility of the Commission to oversee cloud service procurement. The Commission may delegate the task to the Cloud First Policy Committee. Further details are provided in Recommendation 3.4.

Recommendation 3.3: Taking Action on the GCM Framework by Subcommittees under the Cloud First Policy Committee

Type of Recommendation: Operational Method

To ensure the efficient operation of the GCM framework, the Cloud First Policy Committee should appoint subcommittees to assess and drive operations in various areas based on expertise. There should be four subcommittees to undertake specific tasks as follows:

(1) Procurement Specifications Subcommittee

- Survey, compile, analyze, and categorize the service requirements of government agencies seeking to procure cloud systems.
- Develop joint agreements between agencies with similar service needs to facilitate joint procurement. Streamline signing or operational procedures.
- Draft terms of reference (TOR) outlining minimum requirements for procuring cloud services.

(2) Selection Criteria Subcommittee

- Define the operational procedures for registration, verification, and eligibility that align with the Ministry of Digital Economy and Society's announcement regarding the criteria for creating the Registry of Cloud Service Accounts under the Cloud First Policy.
- Evaluate and screen cloud service providers eligible for registration based on the criteria set by the relevant agencies.
- Report on the screening results for approval by the Cloud First Policy Committee.
- Screen cloud service providers according to the Cloud First Policy and create a long list for government agencies wishing to individually procure cloud services.

- Evaluate the budgets of the government agencies intending to procure cloud services, establish the median price for cloud services in cases of consolidated procurement, and provide consultation on the appropriate median price in cases of individual procurement.
- Designate task forces to carry out the above activities, consisting of experts in the relevant fields, including:
  - A registration task force to screen the qualifications of operators eligible for the GCM framework.
  - A screening task force to screen and compile the list of service providers for selection by agencies.
  - A pricing task force to evaluate budget allocation and establish median prices.

(3) Monitoring and Evaluation Subcommittee

- After registration, monitor, inspect, and evaluate the qualifications and services of cloud service providers listed in the Registry of Cloud Service Accounts.
- Establish the criteria, conditions, and procedures for filing complaints regarding cloud services, including coordinating with relevant parties for corrective actions.

(4) Advisory Subcommittee

- Advise and provide consultations to government agencies on cloud procurement-related activities, including service selection, budgeting, or other related matters.
- Publicize and foster understanding of the procurement mechanism for cloud systems among public sector agencies.

Recommendation 3.4: Specification and Assessment of Cloud Service Operator Qualifications for Registration in the Registry of Cloud Service Accounts

Type of Recommendation: Legal and Procedural Improvement

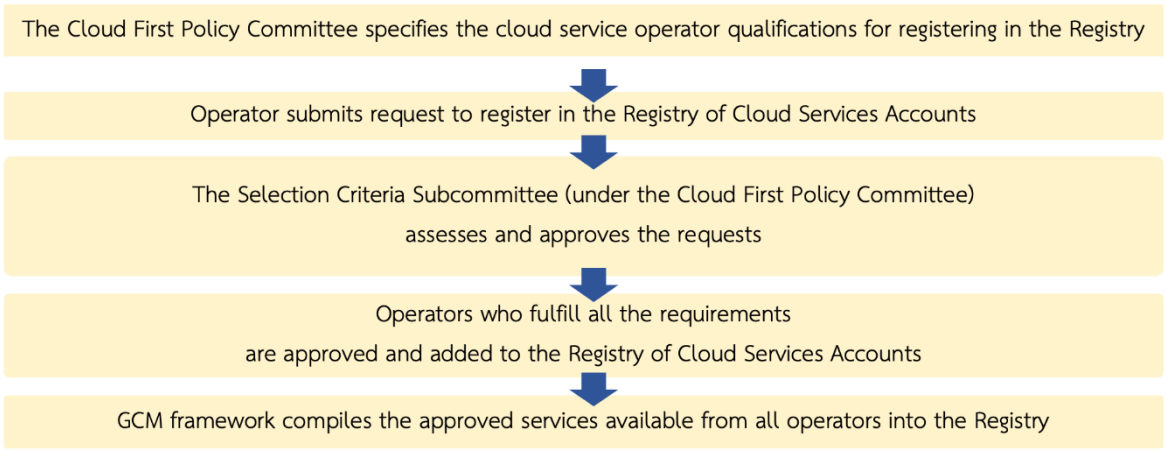
The Cloud First Policy Committee, under the GCM framework, establishes the standard qualifications and characteristics of cloud service operators (service providers) for screening future candidates (Figure 6).

This initiative will align with the (draft) Ministerial Regulation: Prescribing of Supplies that the State Needs to Promote or Support (No. 5) B.E.... according to

Recommendation 3.2, by drafting a (draft) announcement from the National Digital Economy and Society Commission regarding the principles for creating the Registry of Cloud Service Accounts. At minimum, the content should contain the following:

- Criteria and considerations for registration. This includes the capabilities and needs of government agencies, as well we applicant qualifications such as business registrations, certified standards, and service records. Reference should be made to Recommendation 2 and Recommendation 4 for further consideration.
- The authority of the committee to establish the selection criteria for evaluating cloud service operator applications under the Cloud First Policy. The criteria shall adhere to established principles.

Figure 8: Process of Defining and Evaluating the Qualifications of Cloud Service Operators for Registering in the Registry of Cloud Service Accounts



In cases where an operator does not pass the qualification screening, the Office of the National Digital Economy and Society Commission (ONDE) shall act as the administrative unit of the Cloud First Policy Committee to issue a notification explaining the reasons for the dismissal to the operator. Should the operator wish to reapply, they may revise their qualifications according to the Committee's guidelines and resubmit them for re-evaluation by the Committee.

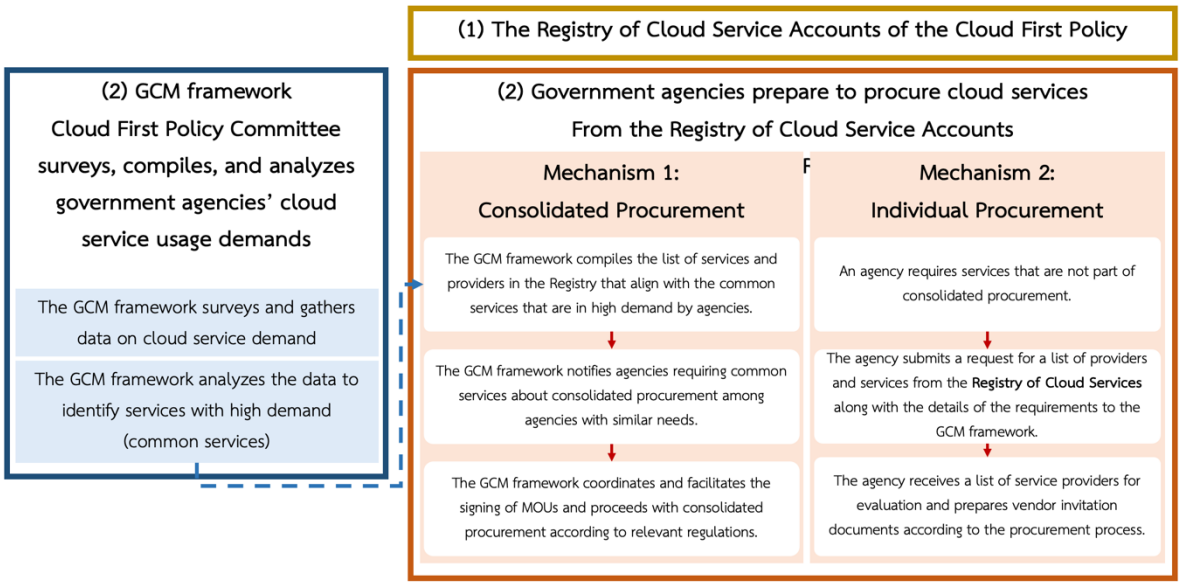
Recommendation 3.5: Facilitating Procurement from the Registry of Cloud Service Accounts

Type of Recommendation: Operational Procedure

To facilitate government agencies in preparing to procure cloud services from the Registry of Cloud Service Accounts based on the Cloud First Policy, two mechanisms are

available. Mechanism 1 involves the consolidated procurement of cloud services with high usage demand among government agencies (GCM Lot), while Mechanism 2 entails the separate procurement of cloud services by each individual agency (Figure 9).

Figure 9: Process for Facilitating Procurement of Cloud Services by Government Agencies



Before any government agency proceeds with procurement using any mechanism, Cloud First Policy Committee, under the GCM framework, would survey, compile, and analyze the cloud service needs of those agencies. This is to identify any common cloud services that are required, and shall entail the following actions:

- Establish the criteria and screening procedures for government cloud service providers to ensure adherence to the Government Cloud Management Framework. The Cloud First Policy Committee shall have the leading authority to survey and assess the readiness and requirements for cloud systems across government agencies. If there is a need for a digital readiness survey, the Office of the National Digital Economy and Society Commission (ONDE), acting as the administrative unit, shall be empowered to coordinate with ministries and other relevant agencies[10] to conduct comprehensive readiness assessments.
- Distribute a circular letter to agencies outside the ministry to engage them in the survey regarding anticipated cloud service needs, and the expected usage timeframe, such as in the next fiscal year.

[10] Development of Digitality for Economy and Society Act, B.E. 2560 (2017), Section 17.

- Establish survey timelines, taking into account the timeframe of the budgetary processes.

Mechanism 1: Consolidated Procurement for high-demand services (GCM Lot)

If agencies share some common service demands, meaning that these services are in high demand, they are eligible for consolidated procurement with other agencies, thus increasing bargaining power. The process should include:

(1.1) The GCM framework invites the agencies that had expressed their need for the common services outlined in the GCM framework to jointly procure cloud services through consolidated procurement. The procurement criteria, conditions, and methods should adhere to those announced by the Government Procurement and Inventory Management Committee regarding the criteria, methods, and operational details for consolidated procurement, as stipulated in the Government Procurement and Inventory Management Act, B.E. 2560 (2017).

(1.2) The GCM framework coordinates and facilitates collaboration among agencies involved in joint cloud service procurement. The roles related to consolidated procurement shall be defined as follows:

- Pre-Procurement Budgeting: The GCM framework's Advisory Subcommittee provides budgeting guidance to agencies according to the GCM framework.
- MOU for Consolidated Procurement: The GCM framework's Procurement Specifications Subcommittee surveys the needs of the agencies, creates a grouping for the needs, develops the specifications for the items to be procured, and drafts a Memorandum of Understanding (MOU) among the agencies with similar needs.
- Consolidated Procurement Authorization: authority is given to the Cloud First Policy Committee to act as the representative body to conduct procurement, and empowers it to authorize subcommittees to carry out the consolidated procurement.
- Consolidated Procurement Committee: (a) The GCM framework's Procurement Specifications Subcommittee develops the specifications of the items to be procured. (b) GCM framework's Selection Criteria Subcommittee determines the selection criteria and median price. (c) Procurement Acceptance Committees: Each department can establish its own committee according to the procurement mechanism.

Mechanism 2: Individual Cloud Service Procurement

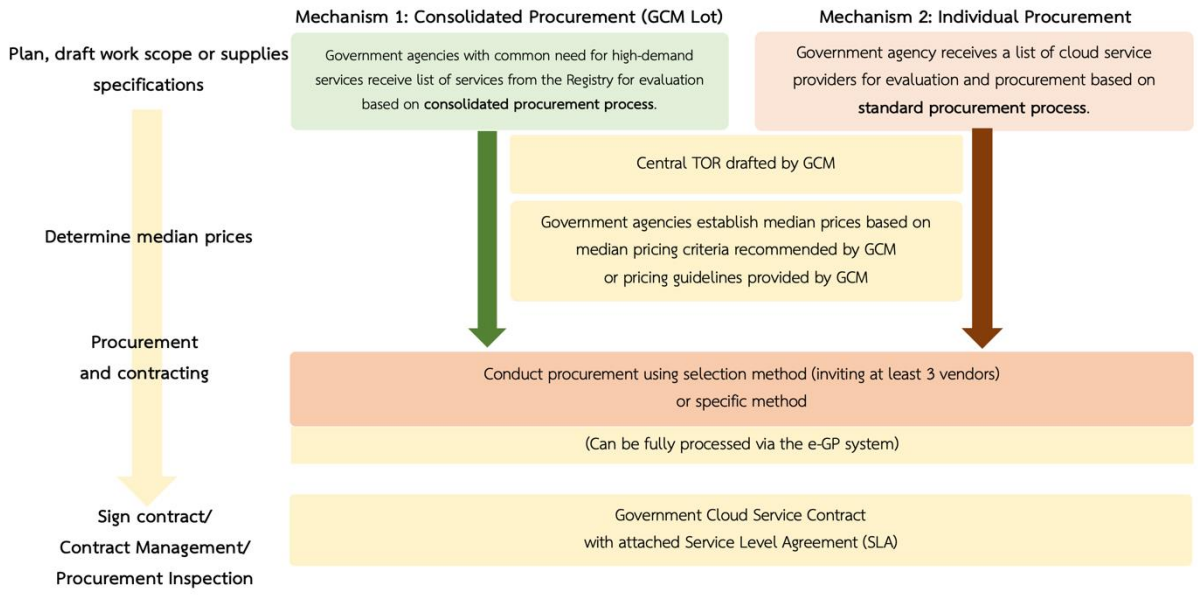
If an agency requires a service that is not commonly used among other agencies, it is eligible to receive a list of suitable service providers without having to conduct its own qualification screening. The list is then evaluated and actioned using the selection method or specific method.

Recommendation 3.6: Facilitating Government Cloud Service Procurement and Procurement Processes

Type of Recommendation: Legal, Procedural, and Operational Improvement

After preparations for procurement under Mechanism 1 or Mechanism 2, government agencies can proceed with procurement using either consolidated or individual procurement, respectively. Throughout, the GCM framework facilitates every step, including planning, defining the scope or supplies specifications, determining median prices, procurement, and contracting (Figure 9).

Figure 10: Procedures for facilitating government agencies in procuring cloud services and the procurement process



(1) Planning, Defining Scope of Work or Supplies Specifications

The process of planning and defining the scope of work or supplies specification is a follow-on operation after the preparation of cloud service procurement as suggested in Recommendation 3.5. Under Mechanism 1, the group of agencies intending to

procure cloud services with high common usage (common services) will receive a service listing from the Registry of Cloud Service Accounts for consideration in the procurement process. Similarly, agencies wishing to procure cloud services individually under Mechanism 2 are eligible to receive a list of suitable service providers and services for evaluation.

In terms of drafting the Terms of Reference (TOR), the GCM framework facilitates this by empowering the Procurement Specifications Subcommittee to draft a preliminary scope of work. This establishes the minimum requirements for procuring cloud services that are most suitable for the broadest general usage.

For the procurement of high common usage services (common services), under Mechanism 1, the Procurement Specifications Subcommittee can further facilitate the drafting of the scope of work. This is because the usage requirements are clearly defined and can be shared with other agencies intending to conduct consolidated procurement. Therefore, it is advisable to have a draft of the scope of work for common services.

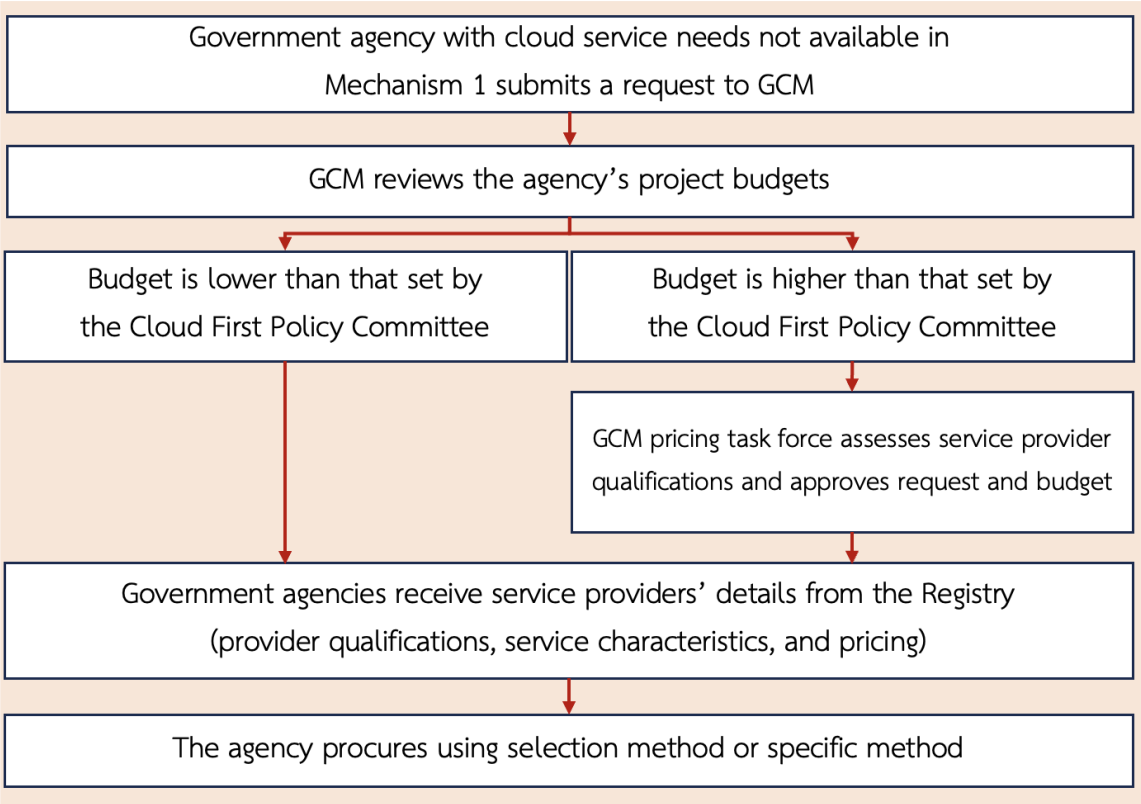
Upon commencing the procurement process, government agencies can issue invitations to qualified operators based on the registration criteria. This is done for both the selection and specific methods. At minimum, the qualifications must match those submitted to the GCM framework, and must be relevant to the specific service requirements. For instance, when procuring cloud-based health data processing systems, there must be standards for managing health data security (ISO/IEC 27799).

(2) Determining the Median price

For the procurement of services with high common usage (common services), under Mechanism 1, the GCM framework facilitates the determining of the median price. The Procurement Specifications Subcommittee is tasked with detailing the specific characteristics of the supplies to be procured, and is made up of experts who are qualified to establish the median price.

Regarding agencies wishing to procure cloud services under Mechanism 2, agencies express their interest and submit a project proposal to the GCM framework. The Selection Criteria Subcommittee then evaluates the agency's budgets. This is illustrated in Figure 11.

Figure 11: Procedures for Budget Consideration and Median Price Determination for Cloud Service Procurement under Mechanism 2



- If a project uses a lower budget than that set by the Cloud First Policy Committee, the agency can obtain details of service providers from the Registry of Cloud Service Accounts. This information can then be used for procurement through the selection method or specific method.
- For projects that use a larger budget, exceeding the amount set by the Cloud First Policy Committee, the GCM pricing task force evaluates the service provider's qualifications and approves a go-ahead and the budget. The details of service providers from the Registry of Cloud Service Accounts are then forwarded to the agency to proceed with procurement.
- The GCM pricing task force provides guidance on establishing median prices in order for agencies to independently determine them. The task force utilizes service provider details such as qualifications, service characteristics, and service costs collected in the Registry of Cloud Service Accounts.

(3) Procurement of Supplies

Procurement activities under both Mechanisms 1 and 2 can be carried out using the selection method or specific method as stipulated in the (draft) Ministerial Regulation: Prescribing of Supplies that the State Needs to Promote or Support (No. 5), B.E. ... (Recommendation 3.2). Procurement can be conducted through e-GP in accordance with Section 9 of the Government Procurement and Inventory Management Act, B.E. 2560 (2017).

(4) Contracting

To ensure that cloud service contracts for government agencies are comprehensive and suitable for engaging cloud service providers in the procurement process, it is advisable to prepare a (draft) Government Cloud Service Contract along with an attached Service Level Agreement (SLA). The draft contract should be submitted to the Office of the Attorney General for approval to serve as a standard template for future procurement contracts. A preliminary draft contract can be found in the Appendix.

Recommendation 3.7: Monitoring and Evaluation, Providing Consultation, Guideline Setting, and Support for Government Agency Cloud Service Utilization

Type of Recommendation: Operational Procedure

(1) Monitoring and Evaluation: To ensure smooth utilization of cloud services within government agencies and consistent service quality from cloud service providers, the GCM framework stipulates that the Monitoring and Evaluation Subcommittee conducts the following activities:

- Monitor and evaluate the characteristics and services of the cloud service providers in the Registry of Cloud Service Accounts after registration
- Monitor and evaluate service usage in terms of satisfaction levels, user experience, and usage issues, including in the area of system migration. Criteria, conditions, and complaint procedures for cloud service usage should be established, and relevant committees or agencies should be contacted to address any issues.
- Compile case studies regarding the usage and best practices of various agencies to serve as examples or cautions for government agencies using cloud services. These case studies become knowledge resources and contribute to future policy improvements in cloud service utilization for government agencies.

(2) Consultation: The Advisory Subcommittee should support the utilization of cloud services and the benefits of cloud technology for government agencies through public relations efforts, knowledge management, and training. Additionally, it should gather the laws and practices related to cloud service usage from relevant agencies and may propose regulations and practices to promote reliable cloud service usage within the government. This includes, but is not limited to:

- Technical knowledge: Highlighting cloud technologies and the potential applications of cloud services for agency missions and public services (use cases).
- Operational guidelines and procurement and contracting procedures.
- Procurement-related activities, including service selection and budgeting, among others.
- Technical operation guidelines, prevention and resolution of issues, adherence to regulations and practices, such as in secure system migration.
- Government staff training at various levels to facilitate cloud service selection, usage, and maintenance according to the type and model of cloud service.

Recommendation 3.8: Budgeting and Expenditure Guidelines for Cloud Services in the Public Sector in Alignment with Usage-Based Billing (pay-per-use).

Type of Recommendation: Legal and Procedural Improvement

According to the Budgetary Procedures Act, B.E. 2561 (2018), agencies can provide rationale regarding proposed expenditure budgets, including the anticipated performance outcomes and benefits, that are in line with national strategies. Operational budgets for public utilities can proceed as usual under the Budgetary Procedures Act, B.E. 2561 (2018) by providing a budgetary rationale to Parliament.

To ensure that budget allocation does not hinder cloud utilization, the following actions should be taken:

(1) Classify cloud service costs as public utility expenses, as they facilitate communication and telecommunications services. Amend the Regulations of the Ministry of Finance on the Disbursement of Administrative Expenses for Government Agencies, B.E. 2553 (2010) by adding cloud service costs to Section 4: Public Utility Expenses. This adjustment enables government agencies to utilize operational budgets to cover these service costs.

(2) The Ministry of Finance issued a memorandum (MOF 0502/W 178) dated November 12, 1992, revising the expenses deemed payable upon receipt of debt notification. This revision is to include cloud service charges.

(3) Budget proposals should specify the details of public utility expenses, such as system migration fees, service charges, maintenance costs, etc., in the annual expenditure budget proposal. System migration fees apply only to the initial budget year and are disbursed under the public utility operational budget category because these expenses facilitate communication and telecommunications services.

In cases where government agencies encounter issues in paying public utility fees, action should be taken in accordance with the measures from the Budget Bureau[11] that were approved by the Cabinet on June 7, 2017. The following steps can be taken:

- Transfer of other budgets to cover public utility fees.
- Use off-budget funds, such as revenue or subsidies, to pay for public utility fees.
- If unable to pay within the fiscal year of the expense, agencies can request payment for outstanding expenses in the form of carry-over expenses.

In cases of overestimation or underestimation of accrued public utility fees at the end of the fiscal year, agencies can rectify and adjust the accounts for accrued public utility fees. If the amounts of subsequent invoices do not align with the adjusted estimates for accrued public utility fees, agencies can amend the relevant accounting data in the following fiscal year.[12]

---

[11] The Cabinet passed a resolution on June 7, 2017, approving the guidelines outlined in Budget Bureau document OPM 0728/13043 dated May 26, 2017, regarding measures to address outstanding utility debts. In cases where the allocated budget for utility payments is insufficient, the following actions should be taken:
(1) If there are any remaining funds in a budget or any part of a budget that can be reallocated, these funds should first be transferred to pay for utility expenses before reallocation for other purposes.
(2) Agencies with off-budget funds must use at least 25% of these funds to pay for utilities for that year, except in cases where the off-budget funds are insufficient.
(3) In cases where an agency is unable to pay utility debts within the fiscal year in which the expenses were incurred, the agency may carry over the expenses to the following fiscal year as outstanding expenses (per the Ministry of Finance's urgent letter MOF/0409.3/C14 dated January 27, 2005).

[12] Comparable to the guidelines outlined in Most Urgent Correspondence DLF/0010.32/2083

Recommendation 3.9: Considerations for the Long-Term Improvement of the Budgeting Process

Type of Recommendation: Legislative and Procedural Adjustment

The establishment and disbursement of cloud service-related budgets for government agencies, as per the Recommendation 3.8, could expedite the implementation of pay-per-use service fees. However, state agencies often struggle to fully settle public utility fees, even when utilizing budgets from other sources. Moreover, cloud service fees may inflate the overall public utility budget. In the long term, alternative approaches should be considered. It's worth noting that such practices abroad remain unclear, warranting further comprehensive study.

(1) Agile Procurement involves a flexible approach that prioritizes the type and format of cloud services and the needs of cloud service users over the procurement process itself. For example, the United States of America developed agile procurement by introducing modular contracting to support the needs of the procurement, development, and implementation steps for a required technology. This methodology is based on the Agile Software Development principles that support modern system development, and can be incorporated into existing procurement process frameworks. Additionally, this procurement approach reduces proposal evaluation redundancy as cloud service providers can concurrently outline the scope of service and the accompanying services to be offered.[13]

(2) Annual expense budget improvements to allow for budget adjustments during the fiscal year (supplementary estimates). An example exists in the case of the United Kingdom government, where the executive branch and relevant agencies could hold a policy discussion with HM Treasury and adjust the details of the annual expenditure budgets during the fiscal year. This practice adheres to the principle of distinguishing between foreseeable and unforeseeable budget allocations, which can be adjusted if agencies demonstrate necessity in alignment with the actual usage-based service costs. However, such process adjustments impact the overall budgeting process, necessitating further study and consideration. For Thailand, at present, there are mechanisms for additional expenditures according to the Additional Annual Budget Expenditure Act for each fiscal year.

[13] GOV.uk, “Agile Delivery Management for cloud services”, Accessed March 20,2024. <https://www.applytosupply.digitalmarketplace.service.gov.uk/g-cloud/services/990582757118321>

As a result, it is necessary to clarify that cloud service fees can be considered as justifiable expenses and receivable funds for additional expenditures as requested in the proposal for the additional expenditure budget under the Budgetary Procedures Act, B.E. 2561 (2018).

(3) Disbursement based on annual budget using a new expense category. The current budgeting process involves multiple steps, which may not adequately meet the evolving needs of cloud service users who must adapt to the pace of technological change. Consequently, if state agencies wish to utilize cloud services, they must adhere to the regulations set forth in the Government Procurement and Inventory Management Act, B.E. 2560 (2017). When considering the annual expenditure budget, as stipulated in the Budgetary Procedures Act, B.E. 2561 (2018), and the regulations on budget management for 2019, the budget review process can take up to one year. This prolonged review period may result in cloud system budgets that do not align with rapidly changing technologies.

Therefore, there should be a reform of the procurement and payment processes, in addition to amending the regulations of the Regulations of the Ministry of Finance on the Disbursement of Administrative Expenses for Government Agencies, B.E. 2553 (2010), specifically Section 4 on public utilities, in the initial phases. The impact on the budgeting process is such that budgets are established for the upcoming fiscal year, while cloud expense budgets are disbursed in the current fiscal year.

In this reform, cloud service expenses can be categorized as a new expenditure type. Two preliminary options are available: adding cloud service costs as a separate operational budget from public utility costs, or designating them as a new budget category called “Digital Budget”. As such, how it works, preliminary action guideline, benefits, and limitations, in comparison to the case of adding cloud service costs to public utility expenses as proposed in Recommendation 3.8, are shown in Table 6.

Table 6: Options for Cloud Service Budget Implementation

Implementation Option	How it Works	Preliminary Action Guideline	Benefits	Limitations
Include cloud service fees in public utility charges.	Designate cloud service fees as a type of operational budget for public utility charges to accommodate budget expenditures for services paid based on actual usage (Pay-per-use).	1. Amend the Ministry of Finance on the Disbursement of Administrative Expenses for Government Agencies, B.E. 2553 (2010), under Section 4: Public Utilities Fees to include cloud service charges. 2. Issue a memorandum to revise the Ministry of Finance's memorandum MOF 0502/W 178, dated November 12, 1992, regarding expenses deemed payable upon receipt of notification for payment, to include cases of cloud service charges.	1. Supports usage of pay-per-use service payments. 2. In cases where the allocated public utility budget is insufficient for payment, funds can be transferred from other categories or sourced externally. Adjustments to outstanding public utility account balances can be made in the subsequent fiscal year for budgets set too high or too low.	1. Proper budget planning is essential to avoid encroaching upon budgets allocated to other areas (such as water and electricity costs). 2. In cases where allocated budgets are insufficient for payment, transferring or reallocating funds from other departments to cover public utility costs may not meet the timely operational needs of each department.
Include cloud service fees in operational budgets, separate from public utility charges.	Assign cloud system service fees as a new budget category termed “Digital Service Fees”, a distinct category within operational budgets, separate from public utility charges.	1. Amend the Ministry of Finance regulations regarding government operational expenditure, fiscal year 2010, by adding a new category, Category 5: “Digital Services Fees”, as a separate category from public utilities. 2. Further amendments to relevant subordinate laws, such as the	1. Separating the budget from public utility costs allows for more flexible expenditure. 2. Prevents digital service costs from encroaching upon other budgets.	1. Operational constraints may arise if budget allocations are insufficient for payment or are set lower than actual expenses. 2. Some portions of the digital service expenditure category may overlap with existing

Implementation Option	How it Works	Preliminary Action Guideline	Benefits	Limitations
		Ministry of Interior's regulations on budgeting methods for local administrative organizations, 2020, are necessary to add category definitions related to digital service charges.		allocations in the public utility expenditure category. 3. Multiple amendments to legislation, as well as consultations with various departments, are necessary to assess the feasibility of adding a new budget category.
Designate a new budget type: “Digital Budget”	Revise the budget structure by introducing a new budget type, “Digital Budget,” in addition to the five existing types: (1) Personnel Budget (2) Operational Budget (3) Investment Budget (4) Subsidy Budget (5) Other Expenditure Budget	Revise, amend and supplement laws and regulations related to budget type classification, which may encompass the following: ● Laws governing expenditure budgets, budgeting methods, budget transfers, treasury regulations, or fiscal discipline laws. ● Relevant regulations (e.g., Ministry of Interior regulations on budgeting methods for local administrative organizations, 2020) ● Relevant Budget Bureau documents (e.g., Budget Bureau document OPM 0704/C 33 and Urgent Correspondence OPM 0704/C 68)	Addresses challenges in budget structure and expenditure methods to support future digital operations	1. Budgets in a new type may overlap existing ones. 2. Challenges persist in addressing inadequacies in budget allocation or setting budgets below actual expenditures. 3. Several revisions of laws are required, along with consultations with multiple agencies, to assess the feasibility of establishing new budget types, a process that may take a considerable amount of time.

Recommendation 3.10: Build Clarity in Cloud Service Procurement Strategies for Government Agencies

Type of Recommendation 3.10: Operational Procedure

The Announcement of Median Price and Basic Specifications for the Procurement of Computer Equipment and Systems, March 2023, issued by the Ministry of Digital Economy and Society, provides guidelines whereby when considering the use of cloud server systems, it is recommended to request services from the Government Data Center and Cloud (GDCC) . As a result, government agencies have begun the process of requesting cloud services. Initially, these agencies apply for permission to use the GDCC. If the request is denied or delayed, the agencies are allowed to procure cloud systems independently.

Therefore, the Ministry of Digital Economy and Society should ensure clarity in the selection of Cloud service procurement strategies for government agencies without the need for regulatory amendments. It should be clarified that the recommendations are non-binding and not mandatory. Procurement processes under the Government Contracting Mechanism (GCM) are voluntary. If agencies opt out of GCM procurement, they have the option to proceed with independent procurement. However, this must be done in accordance with the general procurement process, which may be time-consuming. Additionally, agencies may have limited negotiation power with suppliers, and must develop the terms of reference and contracts for cloud service procurement independently, which may not cover all the aspects necessary for cloud service utilization.

Recommendation 3.11: Preparedness of Public Sector Agencies for Cloud Service Adoption

Type of Recommendation: Operational Procedure

Transitioning from the current procurement practice to the Government Cloud Management Framework requires government agencies to adequately prepare for cloud service utilization, both in the initial adoption of cloud services and the transition to new cloud service models. The following actions should be taken:

(1) **The Office of the National Digital Economy and Society Commission (ONDE) should develop guidelines for data transfer** to facilitate seamless migration from legacy cloud systems to new cloud service models. This may involve informing users 30 days in advance, specifying data retention periods, and sourcing new service providers.

(2) Ministerial resolutions should be formulated to endorse data transfer guidelines, ensuring that measures and methodologies regarding data transfer are standardized and mandatory across all agencies.

(3) GCM Training & Certification Services develop training courses to help government agencies understand the processes and methodologies at every stage of the GCM framework, including system maintenance, design, development, and operation, in compliance with relevant regulations and practices with an emphasis on the security of data in transit.

Recommendation 3.12: Establishing Guidelines for Initial Budget Allocation

Type of Recommendation: Operational Procedure

(1) Initial Budget Allocation in the First Year

It is not possible to precisely determine the actual expenses from the beginning of the first year of budget planning, particularly in cases where agencies have increasing needs for usage or data storage over time, leading to higher service costs. It is advisable to use estimated expenditure from Virtual Machines (VM) services.[14]

The Cloud First Policy Committee, led by the Office of the National Digital Economy and Society Commission (ONDE), should formulate operational guidelines for budget allocation for cloud service usage by government agencies. Leveraging historical data from the GDCC usage records of agencies previously using the service can provide preliminary insights into the requirements and help forecast service costs, serving as a reference for estimating initial budgetary allocations.

For agencies that have not previously utilized GDCC, with no usage history in the system, this practice can be adopted for their own operations as well. They may initially assess their cloud usage requirements and compare them to the usage volumes of similar agencies. GCM can provide consultation or recommendations regarding the initial budget allocation process. Initially, GCM should engage in discussions or evaluate the usage needs of each agency before commencing the annual budget allocation process.

[14] Referenced from the Ministry of Digital Economy and Society. Urgent Correspondence (MU 0100.4/579) on Government Data Center and Cloud Services: GDCC

(2) Budget Allocation for the Following Year

For the subsequent fiscal year, agencies should assess their usage needs, possibly comparing them with past fiscal year usage statistics, to accurately estimate expenses for the new fiscal year.

(3) Development of Budget Analysis Guidelines

The costs of cloud services differ from other utility expenses, such as electricity and water charges. To maximize the benefits of cloud services, it is essential to ensure continuous, multi-year usage without any budgetary constraints that could hinder future utilization. Continuous growth in cloud usage can be expected, and there is a tendency towards the continuous expansion of storage space.

The Cloud First Policy Committee should develop budget analysis guidelines that align with this trend. For instance, a guideline for estimating the budget needed for ever-expanding cloud usage is can be presented to the Budget Bureau, and serve as a guidance for future budget analysts.

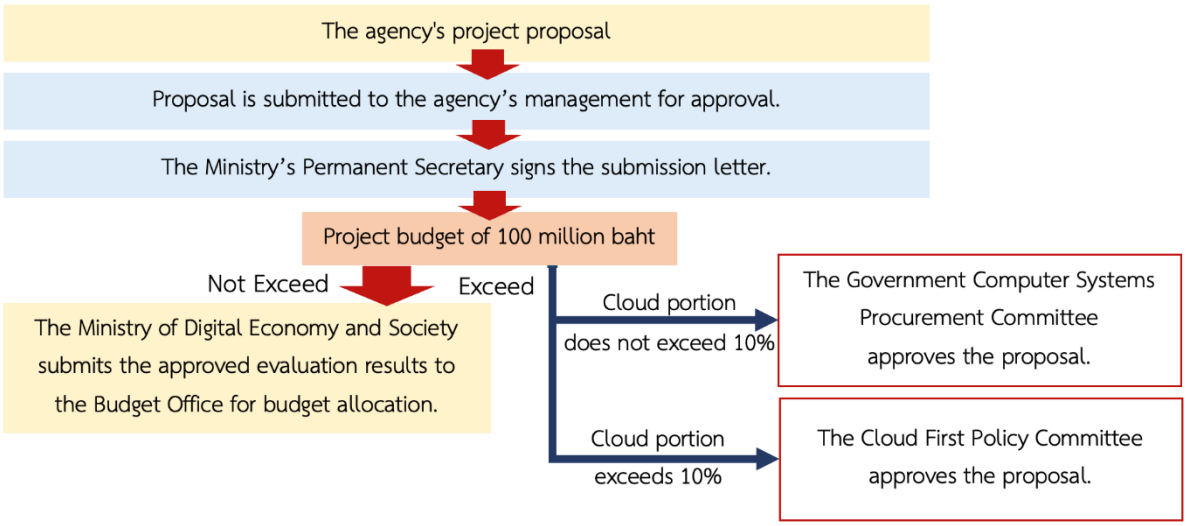
Recommendation 3.13: Guidance for Procuring Cloud Services Exceeding 100 Million Baht.

Type of Recommendation: Legal and Procedural Enhancement

To ensure a non-overlap between the jurisdictions of the Government Computer Systems Procurement Committee and the Cloud First Policy Committee in cases where state computer systems are procured with budgets exceeding 100 million Baht, the following principle is followed.

The Cabinet should adopt a resolution, referring to the previous resolutions (the Cabinet resolution dated March 23, 2004, on the criteria and guidelines for procuring government computer systems, and the Cabinet resolution dated October 14, 2015, approving the additional duties of the Government Computer Systems Procurement Committee to amend its authority). This is to modify the authority of the Government Computer Systems Procurement Committee such that, for projects exceeding 100 million Baht and the portion related to cloud services exceeds 10% of the total budget, the Cloud First Policy Committee should be the reviewing authority for such projects. The process can be summarized as illustrated in Figure 12.

Figure 12: Proposed Guidelines for Government Computer Systems Procurement



6.4 Standards for Cloud Service Providers and Best Practices for Government Agencies Utilizing Cloud Services

Recommendation 4.1: Overall Standards and Sector-Specific Standards for Cloud Service Providers

Type of Recommendation: Standards and Best Practices

In establishing and evaluating the qualifications of cloud service providers, it is essential to incorporate overall- as well as sector-specific standards for cloud service provision. Promoting national certification efforts should also be considered in tandem.

(1) Overall Cloud Service Standards

The overall cloud service standards should be established as minimum requirements for cloud service providers catering to government agencies. Within the framework of the GCM, these standards can serve as criteria for registering providers in the Registry of Cloud Service Accounts. Consideration should be given to standards in the areas of cloud systems and information technology (organisational policies and practices, physical asset security, cybersecurity, data management, and personal data protection), service-related standards, and government policies such as greenhouse gas management (Table 7).

Consideration should be given to the feasibility and implications of setting these overall cloud service standards as minimum requirements for the GCM framework moving forward.

Table 7: Overall Cloud Service Standards

Item	Standard Name (or Equivalent)	Details
1	ISO/IEC 27001 (or TCAS 27001)	Information Security Management System
2	ISO/IEC 27701 (or TCAS 27701)	Security Techniques - Extensions to ISO/IEC 27001 and ISO/IEC 27002 for Personal Information Management - Requirements and Guidelines
3	ISO/IEC 20000-1	Information Technology Service Management
4	CSA-STAR Level 2	Cloud Information Security
5	ISO/IEC 22301 (TCAS 22301)	Business Continuity Management System
6	ISO/IEC 22320 (TCAS 22320)	Guidelines for Managing Incidents
7	ISO/IEC 27017	International Practices for Information Security Management Systems in Cloud Computing * For Critical Information Infrastructure (CII)
8	ISO/IEC 27018	Personally Identifiable Information (PII) Standards in public clouds * For Critical Information Infrastructure (CII) ** For public cloud services
9	Uptime Institute Tier III (Concurrently Maintainable) (or TIA-942 or BICSI-002 or ISO/IEC 22237 or EN 50600 or the Thailand Data Center Standard EIT 022012)	Data Center Standards
10	ISO 9001	Quality Management System (QMS)
11	ISO 14064 (or TCAS 14064 or Greenhouse Gas Protocol (GHG) Certification for Thailand Greenhouse Gas Management Organization (Public Organization)	Management of Greenhouse Gases

(2) Sector-Specific Cloud Service Standards

Sector-specific cloud service standards are a group of standards tailored to each sector (Table 8). They are not a part of requirements for registering in the Registry of Cloud Service Accounts under the GCM framework. Nevertheless, they are recommended for agencies for screening services that are suitable for their operational needs.

Table 8: Sector-Specific Cloud Service Standards

Sector	International Standards
Public Health Sector	• HIPAA: Health Insurance Portability and Accountability Act – Security Standards for Healthcare Data • ISO 27799: Standard for Health Information Security Management
Financial and Banking Sector	• PCI DSS: Payment Card Industry Data Security Standard

(3) Promotion of Domestic Certification

The use of all international standards may pose high costs for domestic service providers, especially for developers who are just getting started with systems development. The Ministry of Digital Economy and Society should collaborate with the Thai Industrial Standards Institute, the National Cyber Security Agency, and other related agencies to create relevant domestic standards that align with, and are comparable to, international standards by using the mechanisms of the National Standardization Act, B.E. 2551 (2008). This would enable Thailand to have comprehensive standards of its own, starting with overall cloud service standards. This would also help to support and drive local service providers to obtain domestic standards that are equivalent to international ones due to the lower costs for testing and obtaining various certifications.

At the same time, the Ministry of Digital Economy and Society should collaborate with the Thai Industrial Standards Institute and relevant agencies to promote the establishment of the Certification Body (CB) and Conformity Assessment Body (CAB) in the country in areas related to cloud services, in accordance with the mechanisms of the National Standardization Act, B.E. 2551 (2008).

Recommendation 4.2: Best Practices for Maintaining and Managing Security Risks in Cloud Services.

Type of Recommendation: Standards and Best Practices

The National Cyber Security Agency (NCSA), in collaboration with relevant agencies, establishes suitable practices for government agencies regarding cloud service security. These practices include mechanisms for overseeing cloud services and the necessary actions that government agencies, in the role of users, need to perform. Various topics include:

(1) Encryption Standards

Service providers must establish encryption guidelines when transmitting data, such as AES, RSA, ECC, TLS, IPSec, or other suitable algorithms based on the environment and usage of government agencies. For instance, key sizes should be defined to maintain high-level security, and should be at least 128 bits. Standards in this area can referenced from the National Institute of Standards and Technology (NIST).

(2) Access Control

Service providers must establish standards for managing and controlling access to data and information resources within the system to maintain data security and integrity. This can be referenced from the NIST Special Publication 800-53, published by the National Institute of Standards and Technology (NIST).

(3) Cyber Threat Incident Response Plan

Service providers must establish incident response plans for various information security incidents to maintain the security of data and information systems used by service users. This aims to reduce service disruptions caused by potential information security incidents. Reference to NIST SP 800-61 by the National Institute of Standards and Technology (NIST) may be made in this regard.

- Identifying and categorizing incidents based on severity and type.
- Incident reporting procedures and alerts to relevant parties.
- Situational control to prevent escalation and respond to the issue.
- Incident investigation and analysis to understand causes and severity.
- Risk mitigation and elimination of issues according to defined procedures, with regular review of the action plan.

The Office of the National Digital Economy and Society Commission, in collaboration with the National Cyber Security Agency, should develop a handbook for selecting cloud services for government agencies based on cybersecurity integrity and safety. It should include essential security standards suitable for various government agencies. At minimum, the content should contain the standards related to cloud security governance and cloud infrastructure security and operation.

Recommendation 4.3: Compliant Practices for Cloud Users in Government Agencies

Type of Recommendation: Standards and Practices

To ensure confidence in utilizing cloud services, government agencies must comply with the relevant laws and regulations. This may encompass secondary legislation, guidelines, and other practices issued by various agencies. The Ministry of Digital Economy and Society and related entities should develop guidelines for compliant practices tailored to government agencies utilizing cloud services. This ensures comprehensive adherence to laws and regulations during system usage and maintenance, maximizing the benefits of technology. Key aspects to include are:

(1) Data Disclosure

The disclosure of government information promotes good governance and drives the integration of data utilization, creating transparency in national administration. This is a crucial factor in driving the data strategy. In Thailand, the approach to information disclosure is reflected in the Official Information Act, B.E. 2540 (1997), which upholds the right of the public to access information extensively, including the right to access official information, even for individuals with no involvement or vested interests. This reflects the transparency of information and the work of government agencies, enabling the public to identify problems in government operations more easily and encouraging them to utilize the information for maximum benefit.

(2) Data Integration and Exchange

The approach to data linkage and exchange in Thailand is reflected in the Digitalization of Public Administration and Services Delivery Act, B.E. 2562 (2019). This act serves as the legal basis for establishing standards and guidelines for the creation of digital processes and operations within the government, or for transforming existing processes into digital formats (Digitisation). This enables government administration and public service delivery to be convenient, fast, efficient, and responsive to the needs of the people, leading to the management and integration of government data that is consistent, interconnected, secure, and adheres to technological governance principles. It also promotes the use of electronic transactions in accordance with established standards, which is a crucial factor in driving the data strategy and the utilization of cloud systems.

(3) Legal Requirements and Regulations for Personal Data Protection

In promoting the use of cloud systems, the government must take into consideration the principles of personal data protection in accordance with the Personal Data Protection Act, B.E. 2562 (2019), which recognizes individuals' rights to their own data, such as the right to access and verify the accuracy of the data as well as to amend it. Additionally, it mandates the government to implement suitable security measures, including Technical, Physical, and Administrative Safeguards, to prevent loss and unauthorized access, use, alteration, or disclosure of personal data. These measures enhance data security and effectively support the National Data Strategy while safeguarding individuals' privacy rights.

(4) Legal Requirements and Regulations for Cybersecurity

In promoting the use of cloud systems by the government, it is essential to implement cybersecurity measures to ensure data integrity and to prevent, manage, and mitigate the risks of cyber threats occurring domestically and arising from abroad. Thailand's cybersecurity efforts are outlined in the Cyber Security Act, B.E. 2562 (2019).

6.5 Cloud Service Providers and Characteristics for Government Missions or Services

In addition to government agency users and cloud service users being able to consider the appropriate models and types of cloud service systems, carry out procurement and budget expenditure, evaluate qualifications based on standards, and prepare their agencies in terms of cloud practices, there is also the provider selection process. The cloud service providers must be capable of providing services according to requirements, such as Storage Cloud, GPU Cloud, CII Cloud, and must be dependable and trusted to deliver services in accordance with established standards and agreements.

Recommendation 5.1: Guidelines for Establishing Criteria for Selecting, Monitoring, and Evaluating Cloud Service Providers

Type of Recommendation: Best Practices and Processes

When government agencies procure cloud services or when the GCM framework, as established by the Cloud First Policy Committee, screen service providers, adherence to the selection, monitoring, and evaluation criteria is essential. Therefore, comprehensive guidelines should be developed to ensure that both small and large-scale agencies can confidently select suitable service providers and receive consistently high-quality services throughout the service period. The following are proposed for the preparation of such guidelines.

(1) Cloud Service Provider Selection

(1.1) Cloud service users should establish clear processes and criteria for selecting cloud service providers and assess their readiness and suitability to ensure continuous service delivery. Key aspects include the provider's knowledge, expertise, experience and financial capability that ensures ability to provide constant and reliable services.

(1.2) Certification and compliance with IT security standards and other relevant standards as proposed in Recommendation 4.1.

(1.3) Service providers must undergo independent audits of their information technology security standards, where the audit scope, timeframe, results, and key findings must be evaluated. The competence and reliability of auditors should also be considered. Cloud service users should look for the following in audit reports:

- The audit scope aligns with the security measures within the provider's responsibility.
- The audit scope aligns with relevant standards and requirements.

(1.4) An assessment of the alignment between the cloud service provider's service continuity guidelines and the Impact Analysis results on the level of work process employed on the Cloud Services. This comprises the Maximum Tolerable Downtime (MTD), the Recovery Time Objective (RTO), and the Recovery Point Objective (RPO). Assessment of the consistency of cloud service providers' business continuity guidelines and the results of the Impact Analysis at the process level where cloud systems will be used, including the acceptable downtime (Maximum Tolerable Downtime: MTD), the acceptable recovery time for systems and data (Recovery Time Objective: RTO), and the latest data set that can be recovered (Recovery Point Objective: RPO).

(1.5) Risk assessment and risk management guidelines on cybersecurity and service continuity in the event that the assessment results of the service provider do not meet the specified security standards or requirements.

(1.6) A Service Level Agreement (SLA) appropriate for the needs and usage patterns.

At the same time, the criteria for selecting cloud service providers must be consistent with the laws related to information systems, cloud services, and the

characteristics of cloud services, such as Critical Information Infrastructure (CII), and must comply with guidelines or criteria established by the National Cyber Security Agency.

(2) Tracking and Evaluating Service Providers

(2.1) Service users should clearly define the roles and responsibilities of personnel tasked with monitoring, evaluating, and reviewing service delivery to ensure compliance with service agreements and service quality, as well as to address potential risks associated with service usage.

(2.2) Service users should establish processes for tracking, evaluating, and reviewing service delivery by service providers in accordance with the terms of the service agreements between providers and users. This includes monitoring the effectiveness of service delivery and ensuring that security measures align with the contractual requirements or service level agreements. Details include:

- Service performance reports prepared by the service provider, such as the percentage of continuous service delivery, response and resolution times, upgrade and installation of bug-fixing software, and backup data reports, etc..
- Independent audit reports covering the following components: (1) Report types, such as SOC1, SOC2, SOC3; (2) Scope of audit covering security measures as per service agreements or relevant standards; (3) System scope under audit covering service-providing systems; (4) Audit methodology and findings; (5) Audit timeframe; (6) Auditor's competence and reliability, etc.
- In cases where independent audit reports have limitations, such as incomplete coverage of security measures or the lack of details regarding the controls and audit procedures, there should be risk assessment and risk management approaches in the event of control or security failures.

(2.3) Regular capacity planning assessments of cloud service providers' resources, categorized as follows:

- In instances where fees are based on actual usage, the users should assess the accuracy of usage reports, including capacity guarantees.
- In instances where usage is based on predefined conditions and resources (Fixed Capacity), service providers should evaluate resource usage and estimate usage patterns to effectively plan for procurement and utilization.

(2.4) Review the terms of service in the event of changes to ensure that the service remains consistent with the usage and information security policies of government agencies and public services, as well as relevant regulations (Compliance). This includes Cross-Border Data Transfers, information security maintenance, and other relevant regulations.

(2.5) Regularly review the qualifications of cloud service providers to assess financial security, work processes, operations, and operational efficiency, etc..

Recommendation 5.2: Establishing Governance Mechanisms for Monitoring and Evaluation

Type of Recommendation: Best Practices and Processes

The monitoring and evaluation of the quality of cloud service providers, as well as the monitoring and assessment of situations, outcomes, issues, and obstacles in the use of these services by government agencies, should be studied and clearly designed by considering the following points:

- The monitoring and evaluation process must consider all stakeholders, including (1) Government agencies using cloud services, (2) the GCM framework led by the Cloud First Policy Committee, and (3) Regulatory agencies involved in setting standards and ensuring service quality.
- The monitoring and evaluation process must be linked to the governance of standards and service quality to ensure enforceability. This includes contract compliance and enforcement actions such as warnings, contract termination, or removal from the Registry of Cloud Service Accounts. Since cloud services often involve diverse standards and quality measures as well as multiple regulatory bodies, appropriate governance strategies should be considered, taking into account the authority and capacity of the governing bodies.
- The monitoring and evaluation of cloud service provision and usage should be in real time and capable of reflecting the situation and issues in detail, in an accurate and timely manner, to enable immediate resolution when problems arise. This also helps prevent inaccurate reporting.
- The monitoring and evaluation of cloud service provision and usage must be comprehensive, supporting various types of cloud deployment models, service models, and the nature of cloud services.

Recommendation 5.3: Appropriate Service Level Agreements for Cloud Services

Type of Recommendation: Best Practices and Processes

When government agencies procure cloud services and select suitable service providers through the procurement process, it is essential to consider Service Level Agreements (SLA) that align with their needs and usage characteristics. For government agencies, as suggested in Recommendation 3.6 regarding government cloud service contracts, it is recommended to include SLAs as an appendix to the contract. When reviewing SLAs, the following should be evaluated:

- Oversight and Responsibility: Cloud service providers oversight and responsibility entail checking data backup and restore periods, service availability, and security.
- Troubleshooting and Support: Swift troubleshooting, quick issue response, and technical support when problems arise.
- Communication: Clear and prompt communication with service users, including providing information on system updates and issue resolution, is vital for user satisfaction.

When evaluating cloud service providers according to Service Level Agreements (SLAs), the following guidelines should be followed:

- When reviewing SLAs, it is essential to study and understand the requirements and usage characteristics of the organization, including the service availability requirements.
- The cloud service provider's SLA should be thoroughly examined to understand the scope and specifics of the available services, including all relevant conditions and terms of use.
- Effectiveness assessment should include verifying whether the cloud service provider effectively adheres to the declared SLA. This involves examining operational histories related to SLAs, such as response times and system uptime, among others.
- Data collection involves gathering the performance data of the cloud service provider according to SLA for future analysis and evaluation. Data could be obtained from monitoring systems, user surveys (regarding satisfaction with provider oversight and

adherence to SLA), or service provider performance monitoring based on the SLA. The findings are then reported to the relevant parties.

The preliminary service availability as per the SLA for each type of service is provided in Table 9. However, it is essential to examine and determine the service availability level appropriate for each government agency. This is because governmental and public services often require varying levels of high service readiness. Therefore, assessing the risk of operational issues and potential impacts arising from service availability is crucial. Different types of cloud provide different levels of service readiness. For example, public clouds may offer the highest level due to the utilization of data centers in multiple locations. This, however, depends on the service offerings of each cloud provider.

Table 9: Preliminary Service Availability for Each Service Type

No.	Type of Service	Service Availability According to SLA
1	Cloud e-Service	Not less than 99.99%
2	Critical Information Infrastructure Cloud (CII Cloud)	Not less than 99.99%
3	GPU Cloud	Not less than 99.95%
4	Open Data Cloud	Not less than 99.90%
5	Storage Cloud	Not less than 99.90%

7. Suggestions on the Implementation of the Cloud First Policy

The Cloud First Policy has four important operational guidelines, according to the adopted resolution of the National Digital Economy and Society Commission meeting No. 1/2023, where the meeting approved the guidelines for implementation of the Cloud First Policy with recommendations for implementation as follows:

7.1 Managing Cloud Usage Demand

Manage the demand for cloud usage by government agencies by appointing the Cloud First Policy Committee, under the Ministry of Digital Economy and Society, to determine the direction for usage demand management. This includes supervising, following up, and providing recommendations to drive operations.

Implementation Guideline 1.1: Government agencies recognize their demand for cloud services, and can specify the model and type of cloud service required.

- Government agencies that use or will use cloud services must look into their demand for cloud usage services, conduct a self-assessment survey, and analyze the results to determine the readiness, needs, and suitability of the choice of cloud services.
- The Cloud First Policy Committee creates and oversees the criteria for selecting cloud services for government agencies as per Recommendation 2.2, specifying the models and types of cloud services to be provided. The three models are namely SaaS, PaaS, and IaaS, while the three types include public cloud, private cloud, and hybrid cloud.

Implementation Guideline 1.2: Government agencies classify data and implement relevant data guidelines to determine the appropriate model and type of cloud service.

- Government agencies prepare by classifying data and implementing the relevant data guidelines according to Recommendation 2.1 in order to identify their demand based on the selection criteria in the Cloud First policy.
- The Ministry of Digital Economy and Society creates a government data management policy that aligns with the Cloud First policy and emphasizes the importance of data security and protective measures in promoting government cloud adoption. This shall drive the agencies' readiness to maintain confidentiality, integrity, and availability, to be able

to store, process, and use data in government missions as well as to integrate important data and high-value datasets and disseminate open data using public clouds.

Implementation Guideline 1.3: Establish standards and guidelines related to security and legal compliance.

- The National Cyber Security Agency (NCSA) works with the relevant agencies to establish the policies, regulations, or guidelines for protecting data security and privacy for government cloud services, with a mechanism for overseeing usage by those agencies. Accountability guidelines are to be created, taking into account the division of responsibilities between cloud service providers and government agencies (shared responsibility) according to Recommendation 1.2.
- The Cloud First Policy Committee establishes the qualifications and guidelines for selecting appropriate cloud service providers for government agencies according to Recommendations 3.4, 4.1, 5.1 and 5.2, and creates operational guidelines for government agencies that use cloud services according to Recommendations 1.1, 4.3, 5.1 and 5.2.
- The National Cyber Security Agency (NCSA), in collaboration with relevant agencies, establish the appropriate security guidelines and mechanisms for regulating cloud services and for government agencies to follow as per Recommendation 4.2.

7 .2 Managing Cloud Service Supply

Management of cloud services to ensure adequate supply is essential for responding to the nationwide demand in a timely manner, and is necessary to preserve the government's procurement interests by allowing competition among service providers. The Ministry of Digital Economy and Society and the Office of the Board of Investment, in collaboration with cloud service providers, create policies and measures to promote investment in domestic cloud services in order to ensure that the number of standardized services is sufficient to satisfy the demand. They will also collaborate with the Thai Industrial Standards Institute (TISI) to establish the relevant standards for Thailand.

Implementation Guideline 2.1: Create measures to promote domestic cloud investment

- The Ministry of Digital Economy and Society collaborates with the Office of the Board of Investment (BOI) to create policies and measures to promote domestic cloud investments to establish data centres in the country. This is done by granting rights or considerations to service providers who established domestic data centers, taking into account

the security, safety, and service quality as well as international cooperations or tax laws and measures for cross-border cloud services.

Implementation Guideline 2.2: Ensuring adequate services according to standards

- The Ministry of Digital Economy and Society creates a strategic roadmap to encourage cloud service providers, both in the public and private sectors, to plan their cloud services and have backup plans to support the continuous use of cloud resources.
- The Ministry of Digital Economy and Society empowers the Cloud First Policy Committee, in collaboration with the relevant departments, to create the criteria for selecting cloud service providers, determining monitoring and evaluation mechanisms, and ensuring comprehensive governance according to Recommendations 5.1, 5.2, and 5.3.

Implementation Guideline 2.3: Determine standards for Thailand

- From Implementation Guideline 1.3, in which relevant agencies set standards and qualifications for cloud service providers, the Ministry of Digital Economy and Society collaborates with the Thai Industrial Standards Institute (TISI), National Cyber Security Agency (NCSA), and other related agencies to prepare relevant domestic standards in Thailand that align with, and are comparable to, international ones. This is done using the mechanisms in the National Standardization Act, B.E. 2551 (2008) according to Recommendation 4.1. The highest priority is given to the group of standards related to the security of the cloud systems as a whole within a period of 1-2 years.
- The Ministry of Digital Economy and Society should collaborate with the Thai Industrial Standards Institute (TISI) and relevant agencies to promote the establishment of a cloud-related Certification Body (CB) and Conformity Assessment Body (CAB) within the country according to the mechanism of the National Standardization Act, B.E. 2551 (2008) pursuant to Recommendation 4.1.

7.3 Government Cloud Management Framework

The Government Cloud Management Framework is an important management mechanism that connects demand with the provision of cloud services to ensure compliance with the SLA, cybersecurity, and other relevant standards. This is the responsibility of the Cloud First Policy Committee in collaboration with relevant agencies. The goal is to become a mechanism or center for driving the use of clouds by government agencies, and to supervise, control, screen, monitor, and

evaluate service quality standards and cybersecurity. Other goals are to provide advice to government users to encourage them to comply with operational, legal, pricing, and service selection guidelines.

Implementation Guideline 3.1: Create the Government Cloud Management Framework

- The Cloud First Policy Committee creates the Government Cloud Management Framework to act as a mechanism or center for driving cloud usage by government agencies.
- The Cloud First Policy Committee collaborates with the Comptroller General's Department, the Budget Bureau, and the Office of the Attorney General to improve relevant laws and prepare contract forms to allow government agencies that will use cloud services to proceed with procurement by taking advantage of the Government Cloud Management Framework according to Recommendation 3.

Implementation Guideline 3.2: Determine guidelines for using the Government Cloud Management Framework in accordance with the digital ecosystem

- The Cloud First Policy Committee supports the government's Paperless policy to reduce paper usage. It encourages aligning operations with the digital ecosystem, potentially through platforms for coordination and various actions. For example, a Government Cloud Management Platform could manage cloud services, facilitating the transition from paper to electronic documents, and enhancing convenience and speed.

7.4 Improve Cloud Service Ecosystem to Connect Users (Demand) to Service Providers (Supply)

Improving the cloud service ecosystem involves improving the procurement processes and budgeting formats to support cloud service rental. This effort is primarily driven by the Ministry of Digital Economy and Society, Comptroller General's Department, and the Budget Bureau.

Implementation Guideline 4.1: Promote the public sector's knowledge and understanding of cloud service usage

- The Ministry of Digital Economy and Society supports the Cloud Fist Policy Committee by organizing training and public relations campaigns through various media. This aims to enhance personnel's knowledge, understanding, and awareness of the importance

of principles and practices related to Data Classification, Data Security, and Data Sharing, as per recommendations 2.1, 4.2, and 4.3. This will lead to safe and correct practices in selecting and utilizing different types and forms of cloud services, following recommendations 2.2, 4.1, 5.1, and 5.2. Additionally, the ministry provides knowledge, facts, and practices to address concerns of government agencies regarding cloud usage, such as data privacy, Vendor Lock-in situations, and security vulnerabilities when using cloud services, which are often caused by human factors.

- The Ministry of Digital Economy and Society supports the Cloud First Policy Committee by encouraging cloud service providers for government agencies to register their services under the GCM framework. The Ministry will disseminate information and provide guidance on the account registration process on the platform to facilitate and build confidence in the procurement of cloud services for government agencies.

Implementation Guideline 4.2: Periodically set goals, monitor and evaluate the results of the Cloud First Policy.

- The Ministry of Digital Economy and Society proposes clear goals for governmental usage of the cloud to the Cabinet.
- The Ministry of Digital Economy and Society monitors and evaluates the amount of cloud service usage by government agencies in comparison to the use of other forms of information technology systems, especially for on-premise systems. Problems, obstacles, benefits, and impacts on the economy and government processes are evaluated.

Implementation Guideline 4.3: Improve laws related to procurement mechanisms, budgeting, and disbursement to accommodate cloud usage

- The Ministry of Digital Economy and Society supports the Cloud First Policy Committee, in collaboration with the Comptroller General's Department and the Budget Bureau, to improve related laws based on the Recommendations, such as Recommendations 3.1 – 3.13.
- The Cloud First Policy Committee drafts the contract forms for government cloud services and sends them to the Office of the Attorney General for approval. The agencies will then use these standardized forms, pursuant to procurement contracting principles.

Appendix

(Draft) Government Agency Cloud Contracts and Annexes

Appendix 1 (Draft) Government Cloud Service Contract

(Draft) Contract Form

Government Sector Cloud Service Contract

Contract No.....

This Contract is executed at ..... Sub-district ..... District..... Province..... on Date: ..... Month: ..... Year: ..... between..... hereafter referred to as the "Employer" of the one part, and ..... a registered juristic person at ..... whose registered office is located at address No. ..... Road ..... Sub-district..... District ..... Province ..... Represented by ..... as the authorized representative to sign this Contract as evidenced by the certificate of the Office of the Company and Partnership Registration of the ..... dated: ..... (and the Power of Attorney dated: .....) as attached hereto *(In case that the contractor is a natural person, the following clause shall be applied)*, and ..... Residing at address No. ..... Road ..... Sub-district ..... District ..... Province ..... Holding the National ID Card No. ..... as appears in the copy of the National ID card attached hereto) hereafter referred to as the "Contractor" of the other part,

Now therefore, in consideration of mutual covenants herein contained, the Parties hereby agree on the following terms and conditions:

Article 1 Definition

"Cloud Computing" shall mean the process of providing services to access a network of resources used in a shared data processing system that is customizable.

"Software as a Service: SaaS" shall mean software service model via the internet that is similar to rental, accept that the buyer only pays for the software usage as required (pay-as-you-go).

"Platform as a Service: PaaS" shall mean cloud-based software that acts as an intermediary integration tools and database, including memory analysis, mobile devices, big data, document processing and management, etc.

"Infrastructure as a Service: IaaS" shall mean network processor system and storage space utilized to support the use of software and applications.

Article 2 Scope of Work and Terms of Payment

2.1 The Employer agrees to hire and the Contractor agrees to provide cloud system services in accordance with the terms and conditions in this Contract and attachments. The cloud system services are detailed in the attached Appendix I.

2.2 The duration of the cloud system services in this Contract shall commence from the date on which the Employer is able to fully utilize the cloud system, and shall end on the date of ....., totaling ..... (.....) years, ... (.....) months, and .....(.....) days.

Article 3 Contractor Warranty

3.1 The Contractor warrants and affirms that the Contractor is the owner of the intellectual properties, including relevant rights thereof, and has complete and exclusive rights without any obligations that may impair rights to the cloud system or user manuals or any other matters related to the cloud system and/or the Contractor warrants and affirms that the Contractor has the legal right and authorization to provide cloud services or any other related services to the cloud system to the Employer in accordance with this Contract.

In case the Contractor is not the owner of the copyrights of the cloud system and is the party with the rights and authority to provide cloud services to the Employer according to this Contract, the Contractor must provide evidence of rights and authority to provide cloud services issued by the copyright owners and submit them to the Employer upon signing of this Contract.

In this regard, evidential documents certifying the Contractor's rights and authority to provide cloud services that shall be submitted to the Employer must contain clauses

confirming that in the event that the contractor terminates its business or is revoked of the rights to provide cloud services under this Contract from the copyright owner, the copyright owner shall agree to be bound by this Contract on behalf of the Contractor or arrange for another party with rights and authority to provide cloud services to enter into contract on behalf of the Contractor, and to provide cloud services to the Employer at no additional costs to the Employer.

3.2 The Contractor will not transfer any copyrights in the cloud system nor the rights to be the authorized cloud service provider in its cloud system to any other party, neither in whole nor in part.

Article 4 Documents forming an integral part of the contract

The following documents attached to the Contract shall be considered integral parts of this Contract:

4.1 Appendix 1.....(Service Level Agreement)..... totaling ..... (.....) pages

4.2 Appendix 2.....(List of specific attributes and cloud usage requirements)..... totaling ..... (.....) pages

4.3 Appendix 3.....(Cloud usage training).totaling ..... (.....) pages

4.4 Appendix 4.....(Cloud system development details)..... totaling ..... (.....) pages

.....etc.....

Should any content in the documents attached to the Contract contradict the contents of this Contract, the contents in this Contract shall take precedence, and in the event that the documents attached to the Contract are in contradiction, the Contractor will comply with the decision of the Employer. The decision of the Employer is final, and the Contractor shall not be entitled to demand any additional wages, damages, or expenses from the Employer.

Article 5 Service provision

The Contractor shall ensure that the cloud system under this Contract has correct and complete attributes as specified in Appendix 1 and Appendix 2 of this Contract, with the cloud system being available for use by the Employer within (.....xx.....) days following the signatory date of the Contract.

In the event that the Contractor wishes to provide cloud services with differing details from those specified in the Contract attachments Appendix 1 and Appendix 2, the Contractor must obtain prior written consent from the Employer, and the cloud system's attributes shall not be lower than those specified in the documents attached to the Contract Appendix 1 and Appendix 2.

Article 6 Method of Payment

6.1 Payment Method

The Employer agrees to pay the Service Provider for cloud services using one of the following methods:

6.1.1 Payment in Installments

The Employer agrees to pay the Contractor for cloud services in the total amount of ..... (.....) baht, divided into installments totaling ..... (.....) installments as follows:

The first installment is ..... (.....) baht and will be paid when the Contractor has provided cloud services for ..... (.....) months.

The second installment is ..... (.....) baht and will be paid when the Contractor has provided cloud services for ..... (.....) months.

.....etc.....

The last installment is ..... (.....) baht and will be paid at the end of the cloud service period as specified in Article 2.2.

6.1.2 Payment made in a Single Installment prior to commencement of Cloud Services

The Employer agrees to pay the Contractor a total of ..... Baht (.....) for cloud services. This payment will be made in a single installment before the commencement of cloud services.

6.1.3 One-time payment after cloud service usage (Pay-per-use)

The Employer agrees to pay the Contractor for cloud services based on actual usage, calculated at the rate of ..... Baht (..... .....) per

(billing unit, e.g., hour/day/month). The Employer will make a one-time payment for these services after the end of the cloud service provision period as per clause 2.2.

6.2 Payment Terms

In the case of 6.1.1, if the Contractor ceases operations or has their right and authority to provide cloud services under this agreement revoked during any given period, the Employer will pay the cloud service fees due on, or after the date the Employer becomes aware of such event to the new copyright holder or another authorized cloud service provider appointed by the copyright holder to be bound by this agreement, as the case may be.

For payments under the terms of this agreement, the Employer will transfer the funds to the Service Provider's bank account: Bank Name ..... Branch ..... Account Name ..... Account Number .....

The Contractor agrees to bear all transfer fees, service charges, or other expenses (if any) charged by the bank and consents to the deduction of such fees from the transferred amount in each installment. (This paragraph applies to cases where the government agency will pay directly to the Contractor (Direct Payment system) by transferring funds to the Contractor's bank account according to the guidelines set by the Ministry of Finance or the budget-owning government agency, as the case may be.)

Article 7 Service Warranty

7.1 Within the cloud service period specified in Article 2.2, the Contractor guarantees that as of the time the cloud system is available to the Employer, the cloud system will be fully functional in all attributes as specified in this Contract.

7.2 The Contractor agrees to be responsible for any defects or damages to computers, electronic devices, peripherals, and any other defects or damages resulting from any anomaly of the cloud system that is providing services, regardless of the cause, within the cloud service period specified in Article 2.2.

Article 8 Contract Performance Securities

Upon entering into this Contract, the Contractor has submitted as security a ..... in the amount of ..... baht (.....), which is equal to ..... (.....) percent of the Contract price to the Employer as a guarantee of compliance to this Contract.

In case the Contractor submits a letter of guarantee as security for the performance of the Contract, the letter of guarantee must be issued by a bank operating in Thailand, or by a finance company or a securities finance company that is licensed to conduct commercial financing and guarantees business in accordance with the announcements of the Bank of Thailand and according to the list of financial companies that the Bank of Thailand has circulated according to the form specified by the Policy Committee on Public Procurement and Management of Supplies, or may be an electronic letter of guarantee according to the methods specified by the Comptroller General's Department, and the guarantee must be valid up to and until the Contractor is released from his obligations under this Contract.

The security to be provided by the Contractor, as per paragraph one above, must be valid and cover all liabilities of the Contractor throughout the Contract's lifetime. Should the security provided by the Contractor decrease or depreciate in value or does not cover the Contractor's liability throughout the Contract's lifetime, regardless of the reason, the Contractor must find a new security or additional security to fulfill the amount specified in paragraph one above and submit the security to the Employer within ..... (.....) days following the date of receipt of written notification from the Employer.

The security provided by the Contractor under this Article will be returned by the Employer to the Contractor without interest when the Contractor is released from all obligations and liabilities under this Contract.

Article 9 Training

The Contractor must provide effective computer program usage training in accordance with this Contract to the staff of the Employer to create a good understanding and proficiency in the use of the cloud system. The training schedule and training location must be submitted to the Employer or the administrator appointed by the Employer for approval in writing before the training proceeds. The training must be completed within ..... (.....) days after the effective date of this Contract, without additional training charges from the Employer. Details of the training are as per the document attached to the Contract, Appendix 3.

Article 10 Cloud System User Guide and Advice

The Contractor must submit originals of the cloud system user manual and all due rights in the amount of ..... (.....) sets to the Employer as detailed in the document attached to the Contract, Appendix 2. The Contractor shall update the said manual at every instance the cloud system is improved and must provide additional advice on using the cloud system with the corresponding manual for using the cloud system whenever it is improved or whenever requested by the Employer throughout the service period under the Contract without any additional costs being incurred to the Employer.

Article 11 Improved Cloud System

The Contractor shall offer updates and improvements to the foundation cloud system under this Contract or from another foundation cloud system related to this cloud system in accordance with this Contract to the Employer and the Employer shall be entitled to the rights to use the updated and improved cloud services without any additional costs and/or have to reimburse the Contractor for any additional compensation costs as agreed in the document attached to the Contract, Appendix ...

The Employer's choice to use the updated and improved cloud system, as per the paragraph above, does not affect other contractual terms.

Article 12 Confidentiality

12.1 The Employer shall not disclose the cloud system's proprietary information nor technical data, that the Contractor wishes to keep as trade secrets and that may incur damages to the Contractor, details of which the Contractor has already informed the Employer in writing.

12.2 The contractor, staff, agent, or employee of the Contractor shall not take, disclose, or use the information and/or data of the employer, or cause any other person in any way to take, disclose, or use the information and/or data of the employer, or access without authorization the information and/or data of the employer through the cloud, or inappropriately learn of the measures to prevent access to the information and/or data of the employer through the cloud, or do any act by unlawful electronic means to intercept the information and/or data of the employer and the person related to the employer during

transmission through the cloud without legal authorization or without the written consent of the employer.

12.3 The Contractor shall thoroughly delete or destroy all data within 30 (thirty) days after the Contract's ending date or the date of Contract Cancellation.

Article 13 Copyright Protection

Should any third party claim or make any claim that there is an infringement of copyright or patent or any rights regarding the cloud system according to this Contract, the Contractor shall indemnify and hold harmless the Employer and take all reasonable steps to ensure that any such claims or demands are expeditiously terminated and the Employer can continue to use the cloud system. In this regard, the period during which the Employer is unable to use the cloud system shall not be included in the service period under the Contract. If the Contractor is unable to take due action thus rendering the Employer liable for damages to third parties due to the violation of such rights, the Contractor shall be liable for damages, fines, and other expenses, including court fees and attorney's fees, on behalf of the Employer. The Employer shall notify the Contractor in writing of such claims or exercise of rights without delay.

Article 14 Termination of Contract

At the commencement date of the cloud service, as specified in Article 5, should the Contractor be unable to commence the cloud service or provide cloud services that do not meet the detailed specifications of the cloud system - as per the documents attached to the Contract, Annex 1 and Annex 2, and the terms and conditions of this Contract - or the cloud system is not operational, or the Contractor breaches any Article of this Contract, the employer has the right to terminate the entire Contract or any part thereof. The exercise of the right to terminate the Contract shall not affect the right of the employer to claim damages from the contractor.

In the event that the Employer exercises the right to terminate the Contract, the Employer has the right to confiscate or enforce the performance guarantee under clause 8, in whole or in part, as the Employer deems appropriate, as well as the right to claim any damages arising from the Contractor's failure to comply with this Contract. If the Employer procures cloud services under this Contract from another party in whole or in part

within ..... (.....) months from the date of termination of the Contract, the Contractor shall be liable for the price increase from the price specified in this Contract.

Article 15 Fine

In the event that the Employer has not yet exercised the right to terminate the contract according to Article 14, the Contractor must pay a fine to the Employer on a daily basis at the rate of ..... (.....) of cloud service fees that are not yet available, starting from the due date according to the contract until the day the Contractor makes the said cloud system fully available to the Employer.

While the Employer has not exercised the right to terminate the Contract, if the Employer sees that the Contractor cannot continue to comply with the Contract, the Employer is entitled to exercise its right to terminate the contract and forfeit or enforce the security for performance of the contract according to Article 8 and demand compensation for the increased price as specified in Article 14, paragraph two, and if the Employer has sent the notification to demand for payment of fines to the Contractor when the service is due to commence, the Employer is entitled to fine the Contractor until the contract termination date as well.

Article 16 Enforcement of fines, damages, and expenses

In the event that the Contractor fails to comply with any of the terms of the Contract for any reason, incurring fines, damages, or expenses to the Employer, the Contractor must compensate such fines, damages, or expenses in its entirety to the Employer within ..... (.....) days starting from the day following the receipt of the notification in writing from the Employer. If the Contractor does not fully compensate the Employer within the said period, the Employer is entitled to deduct the full sum from the amount of wages that must be paid or enforced from the security for the performance of the Contract according to Article 8 immediately.

If fines, damages, or expenses that are enforced from wages that must be paid or the guarantee of performance of the Contract is not sufficient, the Contractor agrees to pay the remaining amount in full according to the amount of fines, damages, or expenses within the specified period of ..... (.....) days after the date of receipt of the written notification from the Employer.

If there is any remaining amount of the Contract price after deducting any fines, damages, or expenses, the Employer shall return such remaining amount to the contractor in full.

Article 17 Waiving or reducing fines or extending the work time according to the Contract

In the event of an incident caused by the fault or negligence of the Employer, force majeure, or any other event that the Contractor is not liable for under the law, or otherwise as specified in the Ministerial Regulations issued under the Government Procurement and Supplies Administration Act, which prevents the Contractor from providing cloud services under the terms and conditions of this Contract, the Contractor shall notify the Employer of such event or circumstance, along with documentary evidence, in writing, to request a waiver or reduction of the penalty or an extension of the work period within 15 (fifteen) days from the date of the cessation of such event, or as specified in the said Ministerial Regulations, as the case may be.

If the Contractor does not comply with paragraph one, it shall be deemed that the Contractor has waived the right to demand the waiver or reduction of the fine or the extension of working period according to the Contract, without any conditions at all, except in the case of the cause being a fault or defect on the Employer's side which has explicit evidence or the Employer is well aware of from the beginning.

If the contractor fails to comply with paragraph one, the Contractor shall be deemed to have waived the right to claim a waiver or reduction of the penalty or an extension of the Contract period without any conditions whatsoever, except in the case of an incident caused by the fault or negligence of the Employer, which is clearly evident or already known to the Employer from the beginning.

The waiver or reduction of the penalty or extension of the Contract period as per paragraph one is at the discretion of the Employer to consider as deemed appropriate.

This Contract is made in duplicate and is identical in content. The parties to the Contract have read and understood the contents in detail. Therefore, they have signed their names and affixed their seals (if any) as proof in the presence of witnesses with each party holding one copy.

(Signed)..... Employer

(.....)

(Signed)..... Contractor

(.....)

(Signed)..... Witness

(.....)

(Signed)..... Witness

(.....)

Appendix 2 (Draft) Service Level Agreement

(Draft) Service Level Agreement

In this Service Level Agreement,

"Service provider" shall mean.....(Contractor)

"Service user" shall mean.....(Employer)

Article 1 Definition

"Service" shall mean Cloud service

"Service Level Agreement" shall mean the established criteria for IT service work to ensure work efficiency, which can be compared to the actual service provided against the defined service standards.

" Service Availability" shall mean the ability to provide services to Service users according to the specified goals.

" Downtime" shall mean the period during which the Service is not available to the Service user.

"Incidents" shall mean any event or condition that disrupts or degrades the Services, prevents users from accessing the Services, or causes the Services to fail to meet the agreed-upon Service levels, including damage to user assets under the Service provider's care or control.

" Service Requests" shall mean requests for services or alteration of the scope of Service or requirements of the Service users that are unrelated to usage problems or may be in the form of requests for advice about Service usage.

" Service Complaints" shall mean reporting of problems regarding service quality or non-compliance with service level agreements, through the complaint channel specified by the Service provider.

" Disaster" and "Force Majeure" shall mean any event that occurs and affects the organization's business, disrupting business continuation due to disasters, including demonstrations, riots, rebellion, sabotage, terrorism, civil war, coup d'état, national emergencies, fire disasters, geological disasters, storms, floods, adverse weather conditions, and epidemics, etc.

"Target Response Time" shall mean the timeframe within which the Service provider responds to the Service users, whether by phone or email, to provide corrective measures to service the goal.

" Target Resolution Time" shall mean the duration period in correcting incidents or processing service requests so the Service users can use the service as usual. The duration period commences from the time the service provider logs receipt of incidents or logs service request in the system.

" Every day" shall mean Monday to Sunday, including public holidays, holidays according to the Cabinet resolution, and holidays of the Service provider.

" Working day" shall mean Monday to Friday, excluding public holidays, holidays according to the Cabinet resolution, and holidays of the Service provider.

Article 2 Details and Scope of the Service

(specify details and scope of each type of cloud service as specified in each contract)

Article 3 Service time

3.1 cloud service hours

Service	Date	Time
(specify cloud service)	Every day	24 hours
(specify cloud service)	Every day	24 hours

3.2 Reception times for complaints, service requests and incidents

Service	Date	Time
Receiving service requests and incidents from the Service user	Every day	24 hours
Taking corrective action to service requests and incident resolution	[only working days]	[08.30 hrs. to 17.00 hrs.]

Article 4 Service and Support Services

The Service Provider shall provide staff to advise on usage and answer service questions, receive notification of incidents, service requests, and complaints and provide technical advice throughout the contract period. The Service provider contact is as follows:

E-mail.....

Phone.....

Fax.....

4.1 Incidents

Incidents will be processed according to priority and timeframe as follows:

Priority	Target Response Time	Target Resolution Time
Critical	By phone: Immediately By E-mail: [within 30 mins]	[3 hrs 36 mins]
High		[8 hrs]
Medium		[12 hrs (only on working days)]
Low		[24 hrs (only on working days)]

Definition of priority:

Critical: The service cannot be used, causing the Service user's work to be interrupted and affecting and/or damaging businesses and Service users on a large scale.

High: The service cannot be used, causing the Service user's work to be interrupted. However, it does not affect or cause damage to businesses and the Service users on a large scale.

Medium: The service is unstable. However, Service users can still use it, or there is a redundancy system.

Low: The service encountered a problem, but it is not significant. It does not have any impact on the work of Service users.

In resolving incidents, the Service provider will take steps to resolve service usage incidents from the detected causes. The timeframe for correcting incidents will start from the time the Service provider records the information on the incident(s) in the system until

the process is completed. The Service users can follow up on the status of incident resolution from the incident resolution number that the Service provider has given.

4.2 Service Requests

Service requests will be processed according to their priority within the following timeframe:

Priority	Target Response Time	Target Resolution Time
High	By phone: Immediately E-mail: [within 30 mins]	[8 hrs]
Medium		[12 hrs (only working days)]
Low		[24 hrs (only working days)]

Definition and Priority

High: The request and modification of Service details related to critical customer systems are in urgent need.

Medium: The request and modification of Service details.

Low: Request for details of service.

Upon implementing the service request, the Service user can track its progress by the service request processing number that the Service provider has given.

Article 5 Service guarantee

5.1 Service Availability

Service Availability means providing services to enable the Service users to be able to access and use the Service, but excludes failures caused by the Service user's equipment or network as follows:

Detail	Target
Percentage of service availability	[99.95%]
Aggregate downtime of the Service per month	[216 mins]

The percentage of service availability (Availability (%)) can be calculated as follows

$$\text{Availability (\%)} = \frac{\text{(Total number of minutes in a month – Total downtime (Minutes) x 100)}}{\text{Total number of minutes in a month}}$$

However, the aggregate downtime of service per month does not include the time allocated for network maintenance or system performance improvement.

5.2 Receiving of Service Requests and Complaints of Incidents

Detail	Target
Ability to achieve target response	[99.00]
Ability to achieve target resolution	[99.00]

5.3 Workload limit

The Service Target specified in this Service Level Agreement is based on specified service volumes. If the service volume increases significantly, it may affect the ability to provide services according to the specified goals.

(Specify limitations by cloud model and service)

Article 6 Duties of the Service User

6.1 The Service user must strictly comply with the Computer Crime Act, B.E. 2550 (2007) and its amendments, including other laws related to the use of the Service, and must refrain from acts that may cause damage to the Service provider.

6.2 If the Service user discovers any abnormalities with any equipment in service, the Service user must notify the Service provider without delay to prevent or mitigate damage that may occur to the Service user's or the Service provider's property.

(Consideration should be given to specifying additional duties of the Service user in accordance with each model of cloud service (if any).

Article 7 Terms and limitations of services

7.1 The Service provider shall take all due care in maintaining the Service user’s data and information, strictly adhere to all related laws on personal data protection, and shall not disclose information to any person unless such information is required to be disclosed by law or by court order.

The Service provider shall arrange for a Data Protection Officer (DPO) as required by the Personal Data Protection Act, B.E.2562 (2019).

(Additional service conditions and limitations should be considered in accordance with each model of cloud service (if any)).

Article 8 Reporting Service Results

The Service provider will deliver a report on Service results, in accordance with the scope of service, upon request from the Service user.

Appendix 3 (Draft) Details and Terms of Cloud Service Usage

(Draft) Details and Terms of Cloud Services Usage

1. Principle and Rationale

Cloud usage is an important mechanism in driving the strengthening and development of the efficiency of government agencies' public services in digital format. The fundamentals of cloud-based services have clear advantages over traditional information technology investments, but require a massive investment in infrastructure in terms of equipment, systems, and storage space.

The government sector's goal in using cloud systems is to develop government agencies' ability to provide more efficient public services while lowering costs, investments, and the use of redundant information systems. Moreover, it shall also promote collaboration between organizations in using and exchanging information more efficiently and securely to develop innovation and support public benefits.

2. Objective

2.1. To promote the use of cloud services and lead to a more flexible utilization and conservation of national resources.

2.2. To enhance information security, especially classified information and personal information, stored in cloud services.

2.3. To reduce the burden on agency personnel and enable them to carry out their key responsibilities more efficiently, reduce the burden of information technology of small agencies or agencies that do not directly work in information technology.

2.4. To achieve cost-effectiveness in Information Technology investment while providing system maintenance at a lower cost than before while maintaining the same level of service.

3. Scope of Work

3.1. The Contractor must be a provider of a data center and cloud computing services and must be certified with the following standards:

1) Cloud Security Alliance (CSA)–Security, ISO/IEC 27017 or Trust & Assurance Registry (STAR): CSA STAR and ISO/IEC 27018 or CSA STAR on Security for the Cloud Services

2) ISO/IEC 27001 Information Security Management System: ISMS

3) ISO/IEC 20000-1 Information Technology Service Management System (ITSMS) and is ready to provide the customer with a Service Level Agreement (SLA). The service provider must set service standards to ensure user confidence of: (1) not less than 99.99% for Cloud e-Service, (2) 99.90% for Open Data Cloud, (3) 99.95% for GPU Cloud, (4) 99.99% for CII Cloud, and (5) 99.90% for Storage Cloud.

4) ISO/IEC 27701 Data Privacy

This standard shall be referred to and is subject to change by the Cloud Security Alliance (CSA), which sets the CSA-STAR standard, and the International Organization for Standardization (ISO), which sets the ISO/IEC 27001 and ISO/IEC 20000-1 standards.

3.2 The Contractor shall configure the cloud system to be ready for use and achieve the availability levels specified herein.

3.3 The Contractor must install the operating system software files from the virtual host computer (VM) received from the Employer into the cloud system and configure it to ensure readiness for use.

3.4 The Contractor shall maintain the Infrastructure as a Service (IaaS) so that it is available for use 24 hours a day. In the event of an emergency that renders the system unavailable, the Contractor shall notify the Employer as soon as possible.

3.5 The Contractor shall configure the Firewall according to standard practices and configure settings that are related to API Web Service usage or Rules as specified.

3.6 The Contractor shall perform a data backup (Snapshot) at the main service site (DC Site) and at the backup service site (DR Site) at least once every day and keep the information for a period of not less than 7 days.

3.7 The Contractor shall prepare a Disaster Recovery Site to support Business Continuity Planning (BCP) with a recovery period (RPO) not exceeding 24 hours.

3.8 In the event of a force majeure event, the Contractor must restore the virtual machine (VM) to accessibility (RTO) within 24 hours.

3.9 In the event that the Contract ends and the Employer does not renew the Contract with the Contractor in the following year, the Contractor must deliver all VM files in the .vmdk file format or other formats that can be used to restore the entire system through a single file and allow the Employer to continue using the entire cloud system without any efficiency loss for a period of 7-15 days as agreed with the Employer without additional charge.

3.10 The Contractor must provide remediation or assistance in the event of usage problems reported by the Employer and must complete the resolution within 1-5 business days, depending on the case, as agreed upon.

3.11 The Contractor must establish appropriate cloud service billing guidelines for government agencies, utilizing a Pay-Per-Use model based on actual usage.

3.12 The Service Provider must establish a primary data center in Thailand (Data Localization).

3.13 The Service Provider must agree to connect the cloud system with the central Cloud Management Platforms of the Ministry of Digital Economy and Society through API channels to link data, at least as a minimum as follows:

(1) Cloud resource management data

(2) Pay-per-use cost calculation data

(3) Cloud system resource usage data

4. Budget

xxx

5. Period of Delivery of Work

xxx

6. Responsible Agency

xxx

Appendix 4 Personal Data Sharing Agreement

(Draft) Personal Data Sharing Agreement

between

...(Name of the contract party who is the Service user).... And

...(Name of the contract party who is the Service provider)....

This Personal Data Sharing Agreement ("Agreement") is made on ....(specify the signatory date in the Agreement)..... at .....(specify the place where the contract was made).....

Now therefore, in this Agreement, as agreed in ...(specify the name of the memorandum of understanding/main contract)... Date .....(specify the signatory date of the memorandum of understanding or main contract)..... hereafter referred to in this Agreement as the **"Main Contract"** and .....(specify the name of the other contract party)..... hereafter referred to in this Agreement as ".....(specify the referred name of the other contract party)....." other party. Hereafter collectively referred to as the **"Parties"**.

To achieve the objectives under the agreement of the Main Contract, it is necessary for the Parties to share, transfer, exchange, or disclose (hereafter collectively referred to as "Share") the personal information it maintains with the other party. For the personal data that each party collects, uses, or discloses (hereafter collectively referred to as "Process"), each party shall be the controller of the personal data according to laws related to personal data protection. Each party will have the authority to make decisions, determine the format, and determine the objectives in the processing of personal data that they must share under this Agreement.

For the aforementioned reason, the Parties have agreed to enter into this Agreement - to be treated as a part of the Main Contract - in order to serve as evidence of the sharing of personal information between the Parties and to carry out operations in accordance with the Personal Data Protection Act, B.E. 2562 (2019) and other laws issued in accordance with the Personal Data Protection Act, B.E. 2562 (2019), hereinafter referred to as the **"Personal Data Protection Laws"**, that is already in force on the date of entering into this Agreement, and that will be later put into force and/or amended in the future. The details are as follows:

(1) The Parties acknowledge that Personal Data refers to information relating to a natural person, which enables the identification of that person, whether directly or indirectly. Each party shall comply with the provisions of the Personal Data Protection Act to ensure that the processing of Personal Data is appropriate and lawful.

(2) For the Personal information to be shared by the Parties, each party agrees to share the following personal information with the other party:

a. Name and Surname

b. Facial photograph with national ID Card

c. Date, Month, and Year of Birth

d. National identification number and copy of national ID card

e. Current address/Tax invoice address

f. Phone number and E-mail

g. Credit card number

h. Bank account number and copy of bank book

i. Electronic data and electronic signature

(3) The Legal basis for sharing personal data under the purposes stated in Article 2 shall be the contractual basis (Contract), which each party has according to the Personal Data Protection Act for sharing personal data with the other party.

(4) The Parties acknowledge and agree that each party is a Personal Data controller for the personal data it processes and that each party is separately subjected to compliance with the Personal Data Protection Act in the provisions related to Personal Data.

(5) The Parties certify and confirm that prior to sharing personal information with the other party, they have informed the other party of the required information regarding data sharing as well as asking for consent from the owner of Personal Data and/or has a legal basis or rightful legal authority to disclose Personal Data to the other party, and for the other party to process the received Personal Data in accordance with the rightfully agreed upon purposes in accordance with the Personal Data Protection Law.

(6) The Parties certify that the party sharing personal data shall not be deprived of rights nor be barred nor prohibited from taking the following actions:

6.1 Processing of Personal Data that they themselves have shared under the objectives specified in this Agreement.

6.2 Sharing of Personal Data with the other party for the performance of duties in accordance with this Agreement.

(7) The Parties will process Personal Data received from the other party only to the extent necessary to achieve the purposes set out in Article 2 of this Agreement, and each party will not process the data for any other purpose unless they are granted consent from the owner of Personal Data or is legally required only.

(8) The Parties warrant that they will supervise and ensure that their officers and/or employees, representatives, or any person who processes Personal Data received from the other party under this agreement shall maintain confidentiality and strictly comply with the Personal Data Protection Act and process personal data for the purposes of this agreement only and shall not reproduce, copy, duplicate, nor record any images of personal data, whether in whole or in part, except as provided in the terms of the main contract or other relevant laws.

(9) The Parties warrant that access to Personal Data under this agreement shall be limited to officers and/or employees, representatives, or any person who is authorized, has relevant duty, or needs to access Personal Data under this agreement only.

(10) The receiving party shall not disclose Personal Data received from the transferring party to any individual of the receiving party who does not have relevant duties in the processing, or to any external party, except when it is necessary to perform its duties under the main contract, this agreement, or to comply with applicable law, or with prior written consent from the transferring party.

(11) The Parties shall provide and maintain security measures for data processing that are appropriate both organizationally and technically as announced by the Personal Data Protection Commission and/or in accordance with international standards. The Parties shall take into account the nature, scope, and purpose of data processing to protect Personal Data from risks associated with processing personal data, such as damage resulting

from breach, accident, deletion, destruction, loss, alteration, modification, access, use, disclosure, or transfer of personal data that are unlawful.

(12) In the event that one of the Parties discovers any behavior that affects the security of Personal Data shared under this Agreement that may cause damage from a breach, accident, deletion, destruction, loss, alteration, modification, access, use, disclosure or transfer of personal information that is unlawful, the party that discovers such incident will notify the other contracting party within 48 hours.

(13) In notifying of a Personal Data breach occurring under this Agreement, each party will take measures as it deems appropriate to address the cause of the breach and prevent such problems from reoccurring and will provide information to the other party within the scope specified by the Personal Data Protection Laws as follows:

13.1) A description of the nature and potential consequences of the breach.

13.2) Measures taken to reduce the impact of the breach.

13.3) The type of personal data and the owner of the Personal Data that has been breached, if any.

13.4) Other information related to the breach.

(14) The Parties agree to provide reasonable assistance to the other party to comply with applicable data protection laws in order to respond to any reasonable claims arising from the exercise of various rights under the Personal Data Protection Laws by the data owner, by considering the nature of processing, obligations under applicable Personal Data Protection Laws, and Personal Data processed by each party.

In the event that the owner of Personal Data submits a request to exercise such rights to any Parties to exercise rights over Personal data that is under their responsibility or received from another party, the party receiving the request must promptly notify and forward the request to the transferring party. The party receiving the request must inform the owner of the Personal Data of the handling of the request or complaint of the owner of the Personal Data.

(15) If either party needs to disclose Personal Data received from the other party to a foreign country, the export of such Personal Data must be protected in accordance with international data transfer standards as prescribed by the Personal Data Protection laws of

the foreign country to which the data is sent. In this regard, both Parties agree to enter into any agreements necessary to comply with applicable laws governing data transfers.

(16) Each party may employ a Personal Data processor to process transferred and received personal data. The party must enter a written contract with the data processor. Such contract must have conditions for protecting Personal Data transferred and received that are no less than the conditions specified in this Agreement, and all conditions must be in accordance with the Personal Data Protection Laws. In case of doubt, if either party employs or designates a personal data processor, that party remains liable to the other party for any acts or omissions of the said processor of that Personal Data.

(17) Unless the relevant law provides otherwise, the Parties will delete or destroy the Personal Data it receives from the other party under this Agreement within ....(specify the number of days for the data to be deleted)..... days from the date of processing for the purposes under this Agreement is completed or the date the Parties agree in writing to terminate the Main Contract, whichever comes first.

In the event that it appears that either party no longer has the need to retain Personal Data received from the other party under this Agreement before the end of the period under paragraph one, that party will immediately delete or destroy the Personal Data it receives in accordance with this Agreement.

(18) Each contracting party shall indemnify the other party for any fines, losses, or damages incurred by the non-breaching party arising from a breach of this agreement, even if there are limitations of liability under the main contract.

(19) The duties and liabilities of the Parties to comply with this agreement shall terminate as of the date on which the main contract is completed or the date on which the parties agree in writing to terminate the main contract, whichever shall occur first. However, the termination of this agreement does not affect the obligation of each party to delete or destroy personal data as specified in Clause 17 of this agreement.

In the event that any Agreement, testimonial, negotiation, or commitment that the Parties have made to each other, whether in oral or written form, contradicts or is contrary to the Agreement specified in this Agreement, the content of this Agreement shall take precedence.

Both parties have read and understood the content of this Agreement in its entirety. As evidence, the Parties hereto have executed their signatures as evidence in the presence of witnesses on the date, month, and year specified above.

Signed.....

(.....)

.....

Signed.....

(.....

.....

Signed.....Witness

(.....)

.....

Signed.....Witness

(.....

.....

Office of the National Digital Economy and Society Commission

120 Moo 3, 9 floor The Government Complex
Commemorating His Majesty, Chaeng Watthana Road,
Thung Song Hong,Khet Laksi Bangkok 10210

TEL: 02-142-1202

FAX: 02-143-7962

WEBSITE: www.onde.go.th