Unofficial Translation
This translation is for the convenience of those unfamiliar with the Thai language
Please refer to Thai text for the official version

Notification of the Bank of Thailand
No. FPG. 19/2559
Re: Regulations on IT Outsourcing for Business Operations of Financial Institutions

---

1. Rationale

The Bank of Thailand has permitted financial institutions to outsource IT activities to service providers, located in the country or abroad, to promote the efficiency of business operations and cost management of the financial institutions, and to facilitate the development of financial services under the circumstances where technologies have rapidly changed. However, financial institutions must still be liable for the continuity of services provided to their customers and must maintain the credibility of services as if they operate the outsourced activities themselves. In addition, financial institutions must take into consideration risks of outsourcing that may differ from those as they perform the outsourced activities themselves, such as operational risk from the operation of service providers, strategic risk from business planning, reputational risk and legal risk, especially protection of customer information. Therefore, financial institutions must appropriately manage risks of IT outsourcing, in accordance with the Triad of IT Management, namely security of IT system and information, integrity of IT system and information and availability of IT system, while the board of directors of financial institutions must be responsible for appropriate supervision of IT outsourcing (board oversight). On this, the Bank of Thailand has classified IT outsourcing into 2 types, which are critical IT outsourcing and other IT outsourcing, as well as prescribed supervisory regulations appropriate to each type of outsourcing.

Currently, financial institutions increasingly wish to utilize the IT services from service providers, especially the use of cloud computing, which involves the allocation of IT resources for storing, processing or arranging information of the financial institutions, however, formerly financial institutions were required to consult with the Bank of Thailand before using cloud computing, which might lead to certain practicality issues. Therefore, for supervision to be in line with risks of cloud computing, while allowing more flexibility for the compliance with supervisory regulations, the Bank of Thailand thereby amends the regulations on use of cloud computing by emphasizing on management of risks associated with the use of cloud computing,

while amending the regulations on request for the use of cloud computing to be appropriate to the type of cloud computing, as classified by their features, namely private cloud and public cloud. The essence of the amendments to the regulations is as follows:

(1) Notification or request for the permission to use cloud computing

The definition of "cloud computing" is specified, and the regulations on notification and request for the permission to use cloud computing are specified according to the type of cloud computing. If financial institutions wish to use (1) private cloud computing provided by companies outside the group; or (2) public cloud computing for critical IT activities, the financial institutions shall notify (1) to or seek approval for (2) from the Bank of Thailand 30 days in advance before using it or making any changes.

(2) Supervision of risks associated with the use of cloud computing

Financial institutions are emphasized to put more importance on management of risks associated with the use of cloud computing, for example, the assessment and management of associated risks must cover the control and protection of personal data (data privacy) and degree of reliance on service providers that may limit any further change or cancelation (vendor lock-in), as well as risks of offshore outsourcing, for example, risk of being unable to access data due to a disruption or blocking of cross-border communication network or system (information access risk) and legal risk associated with compliance with overseas regulations (cross-border compliance). In addition, financial institutions should use cloud computing service provided by those that have been certified according to relevant international standards.

(3) Examination of service providers

In case where financial institutions cannot conduct the examination of service providers, they may use the results of the examination conducted by independent external auditors with qualifications according to international standards on IT examination. And, the results of the examination must be endorsed by the board of directors or committee with delegated authority. The Bank of Thailand may also require financial institutions to arrange for external auditors to examine service providers according to the specified scope and report the results of the examination to the Bank of Thailand directly.

Furthermore, as the Bank of Thailand requires financial institutions to submit the Report on IT Outsourcing on a yearly basis, in this Notification, the Bank of Thailand has specified the reporting form to facilitate the preparation of the report by financial institutions. Still, the report shall be submitted no later than the time limit as formerly specified.

2. Statutory Power

By virtue of Section 47 and Section 71 of the Financial Institution Business Act B.E. 2551 (2008), the Bank of Thailand hereby issues the regulations on IT outsourcing for business operations of financial institutions to comply with.

3. Repealed/Amended Notification and Circulars

The following Notification and Circular shall be repealed:

(1) The Bank of Thailand Notification No. FPG. 6/2557 Re: Regulations on IT Outsourcing for Business Operations of Financial Institutions dated 14 July 2014

(2) The Circular No. RPD.(01) C.17/2557 Re: Dispatch of notification of the Bank of Thailand Re: Regulations on IT Outsourcing for Business Operations of Financial Institutions dated 4 August 2014

4. Scope of Application

This Notification shall apply to all financial institutions according to the law on financial institution business.

5. Content

5.1 Definition

"IT outsourcing" means the outsourcing of an IT activity from a financial institution to a service provider, where that activity must normally be performed by the financial institution itself.

"Service provider" means a domestic or overseas external party, including a company in the same group, that enters into a contract or agreement with a financial institution to perform an activity that must normally be performed by the financial institution itself.

"Company in the same group"

(1) For a locally incorporated commercial bank – means a company in the financial business group according to the Bank of Thailand Notification Re: Consolidated Supervision

(2) For a locally incorporated commercial bank that is a subsidiary of a foreign financial institution (subsidiary bank) – means a company in the financial business group according to the Bank of Thailand Notification Re: Consolidated Supervision, including a related company of that subsidiary bank

(3) For a branch of foreign bank (foreign bank branch) – means a head office, overseas branch, regional office of a foreign bank branch, as well as a related company of that foreign bank

"Related company" means a parent company, subsidiary and associated company according to the definition as prescribed in Section 4 of the Financial Institution Business Act B.E. 2551 (2008).

"Information technology (IT) activity" means an activity related to information technology, including IT application, information and infrastructure, as well as people and process involved in the IT management.

"The use of cloud computing" means the outsourcing of an IT activity of a financial institution related to IT infrastructure or IT system by the application of cloud computing through the internet for storing, processing or arranging data or operating systems. This service is adjustable according to user needs.

"Board of directors" means the board of directors of a locally incorporated bank or executive committee with delegated authority of a foreign bank branch.

5.2 Permission for financial institutions to engage in IT outsourcing

The Bank of Thailand allows financial institutions to engage in IT outsourcing for their business operations according to the guidelines and conditions as prescribed in this Notification. However, financial institutions, especially Thai financial institutions, must consider if the outsourcing of IT activities is corresponding to their business strategies and should also put the importance on the investment in IT systems as it helps promote the competitiveness.

On this, the essential principles of the permission for financial institutions to engage in IT outsourcing are as follows:

(1) Financial institutions must be liable for the continuity of services provided to customers and maintain credibility of services as if they perform those IT activities themselves. In addition, financial institutions must be aware of possible risks, which may be different from the circumstances where the financial institutions perform those activities themselves.

In case where the service providers subcontract the IT activities outsourced by financial institutions to other service providers, financial institutions must ensure that the service providers are liable for those activities as if they perform those activities themselves.

(2) Financial institutions must set out guidelines on management of risks of IT outsourcing, which should cover all possible risks, according to the Triad of IT Management, namely security of IT system and information, integrity of IT system and information and availability of IT system.

(3) Financial institutions must have appropriate supervision of risks of IT outsourcing by the application of self-assessment, internal control and effective risk management under the supervision of the board of directors (board oversight).

5.3 Classification of IT outsourcing

Financial institutions shall classify their IT outsourcing arrangements as follows:

5.3.1 Critical IT outsourcing

Critical IT outsourcing means the outsourcing of IT activities that may incur:

(1) Risk and impact on financial institutions on a wide scale (bank wide impact), such as a disruption of services provided to customers and the public; or

(2) Risk and impact on the financial institution system or other businesses on a wide scale (banking system wide impact), such as a disruption of the operating system connected with the payment system

The outsourcing of the following activities are considered the critical IT outsourcing: core banking system, data center, and network system

5.3.2 Other IT outsourcing

Other IT outsourcing means the outsourcing of IT activities that is not within the scope of the critical IT outsourcing as specified in Clause 5.3.1.

If financial institutions have any inquiries about the classification of IT outsourcing, they may consult with **the Information System Examination Department, Payment Systems Policy and Financial Technology Group**, Bank of Thailand, before proceeding with further operations.

5.4 Supervisory regulations on IT outsourcing

The Bank of Thailand prescribes the supervisory regulations on IT outsourcing according to the type of IT outsourcing as specified in Clause 5.3 as follows:

5.4.1 Financial institutions engaging in critical IT outsourcing must comply with the general and specific control requirements, appropriately to the size and volume of transactions, complexity of the outsourced IT activities and associated risks.

5.4.2 Financial institutions engaging in other IT outsourcing must comply with the general control requirements, appropriately to the size and volume of transactions, complexity of the outsourced IT activities and associated risks.

5.5 Supervisory requirements on IT outsourcing

Financial institutions must comply with laws, regulations or international standards related to the outsourced IT activities as well as the supervisory requirements on IT outsourcing as follow:

5.5.1 General control requirements

Financial institutions engaging in IT outsourcing for both types as prescribed in Clause 5.3 must put importance on the formulation of outsourcing policy, outsourcing risk management, service provider management, security of IT system and information, integrity of IT system and information, availability of IT system, and consumer protection, appropriately to the size and volume of transactions, complexity of the outsourced IT activities and associated risks as follows:

(1) Policy on IT outsourcing

When engaging in IT outsourcing including the use of cloud computing, financial institutions must set out strategies and policy on IT outsourcing as follows:

(1.1) Financial institutions must set out clear strategies for determination to engage in IT outsourcing, such as on grounds of business necessity as well as cost and benefit. Financial institutions must ensure that their IT outsourcing does not violate laws and regulations as prescribed by Thai supervisory authorities and those as prescribed by supervisory authorities of the country where the service providers are located, and does not give rise to any loopholes for serious frauds or cyber attacks, both internally and externally, which could severely affect business operations of the financial institutions. Moreover, such IT outsourcing should not severely affect the stability of Thai financial system.

(1.2) Financial institutions must set out a clear and written policy on IT outsourcing, which must be in line with the outsourcing policy and corresponding to business strategies and competitiveness of the financial institutions. The policy must be approved by the board of directors and cover the classification of IT outsourcing, management of outsourcing risks, management of service providers, security of IT system and information, integrity of IT system and information, availability of the outsourced IT activities, customer protection, additional guidelines for critical IT outsourcing, reporting and examination etc.

(1.3) Financial institutions must review the IT outsourcing policy at least once a year to ensure that it is still corresponding to business strategies of the financial institutions that may have changed.

(2) Risk management

When engaging in IT outsourcing including the use of cloud computing, financial institutions must set out a framework for management of IT outsourcing risks as follows:

(2.1) Financial institutions must set out a clear and written policy on management of IT outsourcing risks. The policy must be in line with the overall risk management framework of the financial institutions and commensurate with the size and volume of transaction, and complexity of the outsourced IT activities, as well as associated risks. **The policy on management of IT outsourcing risks** must be approved by the board of directors or committee with delegated authority. **Furthermore, financial institutions** must set out clear and written guidelines, practices, and assign responsible staff for management of IT outsourcing risks. The implementation of those guidelines and practices must be assessed regularly and the results must be reported to the board or senior management with delegated authority in a timely manner.

BOT Notification No 19-2559 (1 September 2017)-check

(2.2) Financial institutions must have sufficient knowledge and understanding of the outsourced IT activities as they must assess the severity of possible risks of IT outsourcing, and must have in place a system to assess, control, and manage key related IT outsourcing risks (such as strategic risk, operational risk, legal risk, and IT risk). The system should be commensurate with the size and volume of transaction, and complexity of the outsourced IT activities, as well as associated risks.

On this, the assessment of risks of IT outsourcing, including the use of cloud computing, should cover risks associated with the control and protection of personal data (data privacy) and degree of reliance on service providers that may limit any further change or cancelation (vendor lock-in), and impact on critical systems of the financial institutions. Furthermore, for financial institutions that outsource IT activities to overseas service providers, especially activities related to data storage/processing or any arrangements with respect to data, they must also assess risks of outsourcing those activities to the overseas service providers, such as risk of being unable to access the data due to a disruption or blocking of cross-border communication network or system (information access risk) and legal risk associated with compliance with overseas regulations (cross-border compliance).

(2.3) Financial institutions must set out a framework for monitoring the effectiveness of service providers on a regular basis, a framework for monitoring any alteration made by service providers, as well as a framework for monitoring day-to-day incidents occurred with service providers. On this, financial institutions must take part in the resolution of an incident, if they consider that it may significantly affect their business operations. In addition, financial institutions must review and assess the effectiveness of service providers on a regular basis, and the results of the assessment must be reported to the committee or senior management with delegated authority in a timely manner.

(2.4) Financial institutions must set out the business continuity plan, which covers IT outsourcing. The plan should be commensurate with the size and volume of transactions, complexity of the outsourced IT activities, as well as associated risks, and the assessment of impact of outsourcing on business operations. In addition, there must be the IT disaster recovery plan to accommodate problems or incidents from IT outsourcing and to mitigate severity of the impact. Financial institutions must ensure that they have information available within the country to maintain the continuity of business operations and services provided to customers. The BCP and IT disaster recovery plan must be regularly reviewed and tested to ensure their effectiveness.

There must also be a process for resolving problems or incidents from IT outsourcing, and those problems or incident as well as the resolutions of those problems or incidents must be reported to the committee or senior management with delegated authority in a timely manner.

(3) Service provider management

When engaging in IT outsourcing including the use of cloud computing, financial institutions must have a framework for service provider management as follows:

(3.1) Financial institutions must set out a clear process and guidelines for selection of service providers, and must evaluate the readiness and appropriateness of the service providers to ensure that they can maintain the continuity of services and serve the needs of the financial institutions. The factors that should considered for the evaluation are, such as IT knowledge, experience, internal management system, potential and capability to provide services both under usual and unusual circumstances, especially in case where the service providers have a number of clients (concentration risk).

On this, when selecting cloud computing service providers, financial institutions should consider readiness and service standards of the service providers as they should be certified according to relevant international standards, such as international standards on system and information security

(3.2) Financial institutions must prepare a written IT outsourcing contract, or a written service level agreement in case where service providers are companies in the same group. The contract/agreement should clearly detail roles, duties, responsibilities of service providers, and service conditions, as well as responsibilities for any damage in case where the service providers fail to comply with the service conditions as specified in the contract/agreement. The contents of the contract/agreement should cover the following key information:

- Scope of the outsourced IT activity and conditions of the service provided by the service provider

- Minimum operating standards as required from the service provider (such as standard on information security and confidentiality, **prohibition on use of information apart from that as specified in the contract/agreement**, integrity of IT system and information, and availability of the outsourced activity)

- Internal control system of the service provider

- Contingency plan of the service provider, which should be consistent with the contingency plan of the financial institution

- Reporting of operations performed by the service provider, which should cover problems or incidents from providing the service

- Responsibilities and obligation between the financial institution and service provider in case of problems, conditions or guidelines on change or cancellation of the contract/agreement, **such as when the service provided by the service provider has ended or is canceled, the information of customers of the financial institution and that of the financial institution must be destroyed**

- Rights of the financial institution, internal auditors, external auditors and the Bank of Thailand to request relevant information and to examine the operation and internal control of the service provider, for both domestic and overseas service provider

Furthermore, financial institutions must keep the contract/agreements at their offices available for the examination by the Bank of Thailand or for submission as requested by the Bank of Thailand.

In case where overseas service providers and supervisory authorities in any particular country impose constraints on the examination of such service providers, or where the laws or supervisory regulations differ from those as prescribed by the Bank of Thailand, which makes financial institutions to further comply with the laws, regulations and guidelines as prescribed by those supervisory authorities, the Bank of Thailand reserves rights to impose any other supervisory regulations and/or conditions as deemed appropriate.

(4) System and information security

When engaging in IT outsourcing including the use of cloud computing, financial institutions must have system and information security measures as follows:

(4.1) Financial institutions must ensure that service providers have a framework or standards on system and information security, for both information of customers and that of the financial institutions, which should be commensurate with the size and volume of transactions, complexity of the outsourced IT activities, as well as associated risks. On this, financial institutions may require service providers to apply the

best practices on IT security that are in accordance with international standards and generally accepted, as deemed appropriate.

On this, for financial institutions engaging in cloud computing, they must ensure that cloud computing service providers have a framework on security of critical or sensitive information of customers and that of the financial institutions in accordance with international standards, such as data encryption and key management

(4.2) Financial institutions must have in place a process, procedures or systems for monitoring, evaluating and examining service providers to ensure that the service providers are able to comply with the framework or standards on security of system and information as agreed upon with the financial institutions.

(4.3) Financial institutions must have in place a process, procedures or systems for retrieving all information of customers and that of the financial institutions from service providers. In addition, financial institutions must ensure that service providers have a process, procedures and systems for destroying information of customers and that of the financial institutions when the outsourcing agreements have ended or are canceled.

(4.4) Financial institutions must ensure that service providers have a framework or standards for taking care of and safeguarding important information of customers **and that of the financial institutions**, which should be in accordance with the relevant laws, supervisory regulations and international standards.

(5) System and information integrity

When engaging in IT outsourcing including the use of cloud computing, financial institutions must have system and information integrity measures as follows:

(5.1) Financial institutions must **arrange to** ensure that service providers have a framework or standards on system and information integrity, **covering a process of system development or replacement, input validation, processing control and output control**, as well as must arrange to ensure that the outsourced IT activities are effective, accurate and reliable. This should be commensurate with the size and volume of transactions, complexity of the outsourced IT activities, as well as associated risks. On this, financial institutions may require service providers to apply the best practices on IT security

that are in accordance with international standards and generally accepted, as deemed appropriate.

(5.2) Financial institutions must have in place a process, procedures or systems for monitoring, evaluating, and examining service providers to ensure that the service providers are able to comply with the framework or standards on system and information integrity as agreed upon with the financial institutions.

(6) Availability of outsourced IT activities

When engaging in IT outsourcing including the use of cloud computing, financial institutions must manage to ensure the availability of the outsourced IT activities as follows:

(6.1) Financial institutions must ensure that service providers have a framework and standards to ensure the availability of the outsourced IT activities under usual and unusual circumstances. This should be commensurate with the size and volume of transactions, complexity of the outsourced IT activities, as well as associated risks. On this, financial institutions may require service providers to apply the best practices on IT security that are in accordance with international standards and generally accepted, as deemed appropriate.

(6.2) Financial institutions must have in place a process, procedures or systems for monitoring, evaluating, and examining service providers to ensure that the service providers are able to comply with a framework or standards on availability of the outsourced IT activities as agreed upon with the financial institutions.

(7) Consumer protection

When engaging in IT outsourcing including the use of cloud computing, financial institutions must make the arrangements with respect to customer protection as follows:

(7.1) Financial institutions must ensure that service providers will not disclose information of customers and that of the financial institutions to other parties without consent of the financial institutions.

(7.2) Financial institutions must have in place a process, procedures or systems for monitoring, evaluating, and examining service providers to ensure that the service providers are able to comply with a framework or standards on customer protection as agreed upon with the financial institutions.

BOT Notification No 19-2559 (1 September 2017)-check

(7.3) Financial institution must have in place sufficient and appropriate systems for taking care of and managing customer complaints. The resolutions of those complaints must be reported to the committee or senior management with delegated authority in a timely manner. **On this, in case where customers encounter losses from the outsourcing of financial institutions, the financial institutions must make compensation to those customers as deemed appropriate.**

5.5.2 Specific control requirements

Where financial institutions engaging in critical IT outsourcing, such as outsourcing of core banking function, data center and network system, **including the use of cloud computing for critical activities**, the financial institutions must comply with the general control requirements as prescribed in Clause 5.5.1 and must also have additional controls, which are in line with the best practices on IT security, in accordance with international standards, and generally accepted. This should be commensurate with the size and volume of transactions, complexity of the outsourced IT activities, as well as associated risks, under the appropriate supervision of the board of directors, as follows:

(1) Specific risk controls

(1.1) Financial institutions must ensure that service providers have a process, procedures, controls on risk management, which should, at least, cover the Triad of IT Management, namely security of IT system and information, integrity of IT system and information and availability of IT system, and should be commensurate with the size and volume of transactions, complexity of the outsourced IT activities, as well as associated risks. In addition, service providers should be certified in accordance with international standards, such as the standards of the International Organization for Standardization (ISO) and the Telecommunication Industry Association (TIA).

(1.2) Financial institutions must have in place a process, procedures or systems for monitoring, evaluating, and examining service providers to ensure that the service providers are able to comply with the framework or relevant international standards as agreed upon with the financial institutions. Moreover, financial institutions must conduct a test to ensure that their engaging in critical IT outsourcing will not incur any risks, according to the Triad of IT Management, namely security of IT system and information, integrity of IT system and information and availability of IT system, or lead to loopholes for frauds and/or cyber attacks, both internally and externally, which may severely affect the business operations or key financial services of the financial institutions on a wide scale, such as conducting a penetration test for internet banking system services.

(1.3) Financial institutions engaging in critical IT outsourcing, including the use of cloud computing for critical activities, must require service providers to provide details of locations where data of the financial institutions is stored, processed or arranged (data location) in order that the financial institutions can appropriately manage outsourcing risks associated with data. In addition, financial institutions must have in place a contingency plan in case where cloud computing service is not available, and must conduct a test for that plan before using that service to ensure that the financial institutions can maintain the continuity of financial services according to the specified policy and business continuity plan.

(2) Board oversight

(2.1) Financial institutions must present details of critical IT outsourcing as well as results of risk assessment to the board of directors or committee with delegated authority for approval before entering into critical IT outsourcing arrangements, or when there are significant revisions to those arrangements according to the internal guidelines, or when those arrangements are renewed.

(2.2) Financial institutions must report the following to the board of directors or committee with delegated authority in a timely manner: the results of evaluation, monitoring and examination of service providers, according to the Triad of IT Management, namely security of IT system and information, integrity of IT system and information and availability of IT system, as well as problems or incidents or complaints from outsourcing.

5.6 Guidelines on notification and request for approval of IT outsourcing arrangements

Financial institutions must comply with the guidelines on IT outsourcing according to the type and **feature** of IT outsourcing **(Attachment 1)** as follows:

5.6.1 Critical IT outsourcing

(1) Non-cloud computing arrangements

(1.1) In case where service providers are companies in the same group, financial institutions are not required to notify or **seek approval** from the Bank of Thailand before entering into the arrangements or before making any changes to the arrangements.

(1.2) In case where service providers are companies outside the group, financial institutions are required to notify the Bank of Thailand 30 days in advance before entering into the arrangements or before making any changes to the arrangements.

(2) Cloud computing arrangements

(2.1) The use of cloud computing in case of sole user or where the service is provided only to companies in the same group (private cloud):

(2.1.1) In case of using private cloud from service providers that are companies in the same group, financial institutions are not required to notify or seek approval from the Bank of Thailand before entering into the arrangements or before making any changes to the arrangements.

(2.1.2) In case of using private cloud from service providers that are companies outside the group, financial institutions shall notify the Bank of Thailand 30 days in advance before entering into the arrangements or before making any changes to the arrangements.

(2.2) The use of cloud computing in case where there are several users using the service (public cloud), or where the service is provided to limited customers but there are companies outside the group sharing the service, or where the service is the combination of private cloud and public cloud provided by either service providers that are companies in the same groups or those outside the group, financial institutions shall seek approval from the Bank of Thailand 30 days before entering into the arrangements or before making any changes to the arrangements.

If financial institutions have any inquiries about the classification of cloud computing, they may consult with the Information System Examination Department, Payment Systems Policy and Financial Technology Group, Bank of Thailand, before proceeding with further operations.

For the notification and request for approval to enter into outsourcing arrangements as prescribed in Clause 5.6.1, financial institutions shall submit a notification or request for approval to the Financial Institution Applications Department, Financial Institutions Policy Group, Bank of Thailand, by specifying reasons, details of outsourcing arrangements, and risk assessment for those arrangements, which have been approved by the board of directors or committee with delegated authority. **On this, for the approval request, the Bank of Thailand will finish its consideration of the**

request within 30 days from the day the request and related documents have been completely received.

5.6.2 Other IT outsourcing

For other IT outsourcing, **in case of cloud computing and non-cloud computing arrangements**, financial institutions shall enter into the arrangements without notifying **or seeking approval** from the Bank of Thailand before entering into the arrangements or before making any changes to the arrangements.

5.7 Reporting and examination

As IT outsourcing arrangements of financial institutions, **including the use of cloud computing**, may have certain effect on customers, the financial institutions themselves, financial systems and other businesses, therefore, the financial institutions must closely monitor service providers and arrange for the Bank of Thailand, external auditors and other supervisory agencies to be informed of those outsourcing arrangements and to be able to examine the service providers.

5.7.1 Reporting to the Bank of Thailand

(1) Financial institutions must prepare all reports on IT outsourcing **using the forms as specified in Attachment 2**. The reports must be accurate and up-to-date, and must be submitted to **the Financial Institution Applications Department, Financial Institutions Policy Group**, Bank of Thailand on a yearly basis within 30 days from 31st December or as requested by the Bank of Thailand.

(2) When there occurs any problems or incidents from outsourcing that makes financial institutions unable to provide basic financial services to customers on a wide scale, **the financial institutions must comply with the Bank of Thailand Notification Re: Significant events That are Required to Report to the Bank of Thailand.**

5.7.2 Examination of service providers

(1) Financial institutions must conduct the examination of service providers by internal auditors or external auditors. **The frequency of the examination should be appropriately specified according to the significance of the outsourced IT activities**. The results of the examination must be prepared and kept at financial institutions for the examination by the Bank of Thailand.

In case where financial institutions cannot conduct the examination of service providers since, for example, the service providers are located abroad and there are many data centers involved, the financial institutions may use the results of the examination conducted by independent external auditors that are certified according to international standards on IT risk examination. And, those results must be endorsed by the board of directors or committee with delegated authority of the financial insitution. On this, the Bank of Thailand may require financial institutions to arrange for external auditors to examine their service providers according to the specified scope and report the results of the examination to the Bank of Thailand directly.

(2) In case where financial institutions enter into IT outsourcing arrangements with overseas service providers that are companies in the same group, the financial institutions may use the results of the examination conducted by their parent companies that have been certified by internal auditors or independent external auditors. And, those results must be endorsed by the board of directors or committee with delegated authority.

5.7.3 Examination by the Bank of Thailand, external auditors or other supervisory authorities

Financial institutions must arrange for the Bank of Thailand, external auditors, or other supervisory authorities to examine service providers or acquire information from service providers, **as well as to examine subcontractors or acquire information from subcontractors**.

5.8 Power to consider, command, revoke or allow relaxation

5.8.1 The Bank of Thailand may consider imposing any other regulations according to significant risks that may arise, as deemed appropriate and as discussed with financial institutions on a case-by-case basis.

5.8.2 The Bank of Thailand may consider issuing commands and/or impose any other conditions as deemed appropriate on a case-by-case basis or revoke the IT outsourcing arrangements of financial institutions, both before and after entering into those arrangements, if found that they are not in accordance with the regulations or conditions as prescribed by the Bank of Thailand.

5.8.3 The Bank of Thailand may consider allowing relaxation, on a case-by-case basis, in case where financial institutions are unable comply with the specified

guidelines or conditions. In such case, the financial institutions shall submit a request, by specifying reasons and details of necessity, to **the Financial Institution Applications Department, Financial Institutions Policy Group, Bank of Thailand**.

5.9 Transitional provision

5.9.1 Financial institutions that have already notified their critical IT outsourcing arrangements with service providers that are companies outside the group to the Bank of Thailand before the effective of this Notification, they are not required to notify **those arrangements** to the Bank of Thailand once again, unless those arrangements are revised or renewed or financial institutions enter into new arrangements.

5.9.2 Financial institutions must comply with the regulations as specified in this Notification and any additional conditions as prescribed by the Bank of Thailand in case where the financial institutions have already notified their outsourcing arrangements to the Bank of Thailand, if those regulations/conditions are not contradict to this Notification. On this:

(1) For the arrangements that are in effect before the effective date of this Notification, financial institutions must arrange for those arrangements to be in accordance with the regulations as specified in this Notification within 1 year from the effective date of this Notification.

(2) In case where the arrangements are renewed, automatically renewed, or revised or financial institutions enter into new arrangements, the financial institutions shall comply with the regulations as specified in this Notification from the effective date of this Notification.

If any financial institution cannot comply with the regulations as specified in this Notification or additional conditions as prescribed by the Bank of Thailand, the financial institutions shall consult, by specifying reasons and details of necessity, with **the Financial Institution Applications Department, Financial Institutions Policy Group, Bank of Thailand**, on a case-by-case basis.

5.9.3 In the period during which the Bank of Thailand Notification Re: Significant Events That Are Required to Report to the Bank of Thailand, as specified Clause 5.7.1 (2), are not in effect, financial institutions shall immediately report problems or incidents, as well as the resolutions of those problems or incidents, to the Information System Examination Department, Financial Technology Department, Bank of Thailand, by no later than 24 hours from when the problems or incidents occur or are detected.

BOT Notification No 19-2559 (1 September 2017)-check

6. Effective Date

This Notification shall come into force as from the day following the dates of its publication in the Government Gazette.

Announced on 28th December 2016

(Mr. Veerathai Santipraphob)
Governor
Bank of Thailand

Regulatory Policy Department
Tel. 0 2283 6938, 0 2283 5839
Fax. 0 2283 5938

Attachment 1

Summary of the Guidelines on Notification and Request for Approval of IT Outsourcing Arrangements

---

1. Critical IT outsourcing

(1) Non-cloud computing arrangements

(1.1) In case of entering into outsourcing arrangements with service providers that are companies in the same group, financial institutions are not required to notify or seek approval from the Bank of Thailand before entering into those arrangements or before making any changes to those arrangements

(1.2) In case of entering into outsourcing arrangements with service providers that are companies outside the group, financial institutions must notify the Bank of Thailand 30 days in advance before entering into those arrangements or before making any changes to those arrangements

(2) Cloud computing arrangements (refer to Clause 5.6.1 (2) of the Notification)

(2.1) In case of entering into "private cloud" arrangements with service providers that are companies in the same group, financial institutions are not required to notify or seek approval from the Bank of Thailand before entering into those arrangements or before making any changes to those arrangements

(2.2) In case of entering into "private cloud" arrangements with service providers that are companies outside the group, financial institutions must notify the Bank of Thailand 30 days in advance before entering into those arrangements or before making any changes to those arrangements

(2.3) In case of entering into "public cloud" with service providers that are either companies in the same group or companies outside the group, financial institutions must seek approval from the Bank of Thailand 30 days in advance before entering into those arrangements or before making any changes to those arrangements

<table>
<tr><th rowspan="3">Service providers</th><th colspan="3">Critical IT outsourcing</th></tr>
<tr><th rowspan="2">Non-cloud computing</th><th colspan="2">Cloud computing</th></tr>
<tr><th>Private</th><th>Public</th></tr>
<tr><td>1. Companies <u>in</u> the same group</td><td colspan="2">No notification / approval required</td><td rowspan="2">Seek approval from the BOT 30 days in advance before entering into the arrangements / making any changes to the arrangements</td></tr>
<tr><td>2. Companies <u>outside</u> the group</td><td colspan="2">Notify the BOT 30 days in advance before entering into the arrangements / making any changes to the arrangements</td></tr>
</table>

2. Other IT outsourcing

When entering into “other IT outsourcing” arrangements, in case of either “non-cloud computing” or “cloud computing” arrangements, financial institutions are not required to notify or seek approval from the Bank of Thailand before entering into those arrangements or before making any changes to those arrangements

Attachment 2.1

Name of financial institution .....

Report on Critical IT Outsourcing

As of 31 December 20XX

IT activity (refer to IT activities as specified in Attachment 2.3)	Details and scope of outsourcing arrangement [1/]	Details of cloud computing [2/] (if any)	Name of service provider [3/]	Details of service provider							IT certificate [5/]	Start date and end date of outsourcing contract / agreement [6/]	Service fee [7/] (if any)	e-Application number (if any)	No. of notification letter / no. of request letter – date/month/ year of notification/ approval (if any)	Problems/ obstacles from outsourcing / additional details (if any)
				Type of service provider				Location (of registration)	Location of computer center [4/]							
				Company in the same group		Company outside the group										
				Domestic	Overseas	Domestic	Overseas		Main center	Backup site						
1. IT infrastructure 1.1 Main data processing center 1.2																
2. Service channel 2.1 Branch operating system 2.2																
3. Processing system 3.1 Lending system 3.1.1 Commercial loan system 3.1.2																
4. Middle and back office support system 4.1 Financial accounting system 4.2																
For example, *3.1.2 Consumer loan system*	*Processing of consumer loan data*	-	*ABC (Thailand)*	-	-	✓	-	*Thailand*	*Bangkok*	*Rayong*	*ISO 27001*	*5 March 20XX – 31 December 20XX*	*1,000,000 Baht per year*	*A25XXXXXXXX XX*	*FIAD. (02) XX/25XX dated 15 January 20XX*	*Late submission of report*

Remarks:

[1/] specify summarized details and scope of the outsourced IT activity, and report only critical IT outsourcing arrangements that are in effect on the reporting date

[2/] specify the type of cloud computing: private or public cloud (if any)

[3/] specify only the name of main service provider, excluding subcontractors

[4/] specify a location of computer center related to the outsourced IT activity, such as data location

[5/] specify the international certification related to the outsourced IT activity

[6/] If the end date is not specified or is conditionally specified - specify only the start date of the outsourcing contract/agreement, and specify further details in the “Problems/obstacles from outsourcing / additional details” column, such as the contract/agreement is open-ended

[7/] specify a service fee according to the outsourcing contract/agreement, such as a fixed fee per year/month, per transaction fee (if any)

BOT Notification No 19-2559 (1 September 2017)-check

Attachment 2.2

Name of financial institution .....

Report on Other IT Outsourcing

As of 31 December 20XX

IT activity (refer to IT activities as specified in Attachment 2.3)	**Details and scope of outsourcing arrangement** [1/]	**Details of cloud computing** [2/] (if any)	**Name of service provider** [3/]	**Details of service provider**								**Start date and end date of outsourcing contract / agreement** [6/]	**Service fee** [7/] (if any)	**e-Application number (if any)**	**No. of notification letter / no. of request letter – date/month/ year of notification/ approval** (if any)	**Problems/ obstacles from outsourcing / additional details** (if any)
				Type of service provider				**Location (of registration)**	**Location of computer center** [4/]		**IT certificate** [5/]					
				Company in the same group		**Company outside the group**										
				Domestic	**Overseas**	**Domestic**	**Overseas**		**Main center**	**Backup site**						
1. IT infrastructure 1.1 Main data processing center 1.2																
2. Service channel 2.1 Branch operating system 2.2																
3. Processing system 3.1 Lending system 3.1.1 Commercial loan system 3.1.2																
4. Middle and back office support system 4.1 Financial accounting system 4.2																
For example, *3.4 Sales support system*	*Data processing for sales of financial products*	*Public cloud*	*XYZ*	-	-	-	✓	*Singapore*	*Singapore*	*Hong Kong*	*ISO 27018*	*1 May 20XX – 31 December 20XX*	*200,000 Baht per year*	-	-	-

Remarks:

[1/] specify summarized details and scope of the outsourced IT activity, and report only critical IT outsourcing arrangements that are in effect on the reporting date

[2/] specify the type of cloud computing: private or public cloud (if any)

[3/] specify only the name of main service provider, excluding subcontractors

[4/] specify a location of computer center related to the outsourced IT activity, such as data location

[5/] specify the international certification related to the outsourced IT activity

[6/] If the end date is not specified or is conditionally specified - specify only the start date of the outsourcing contract/agreement, and specify further details in the “Problems/obstacles from outsourcing / additional details” column, such as the contract/agreement is open-ended

[7/] specify a service fee according to the outsourcing contract/agreement, such as a fixed fee per year/month, per transaction fee (if any)

BOT Notification No 19-2559 (1 September 2017)-check

Attachment 2.3

Examples of IT activities

1. IT infrastructure
1.1 Main data processing center
1.2 Backup data processing center
1.3 Network system
1.4 Core banking system
1.5 Customer information filing system (CIF)
1.6 System connected to centralized payment and settlement system, such as cross-border money transfer system, BAHTNET system, ORFT, SWIFT, ICAS, Payment Gateway
1.7 IT security system
1.8 Storage system
1.9 Others (please specify)
2. Service channel
2.1 Branch operating system
2.2 ATM system
2.3 CDM system
2.4 Call center system (IVR)
2.5 Internet banking system
2.6 Mobile banking system
2.7 e-Money system
2.8 Others (please specify)
3. Processing system
3.1 Lending system
3.1.1 Commercial loan system
3.1.2 Consumer loan system
3.1.3 Hire purchase system
3.1.4 Housing loan system
3.1.5 Credit card system
3.1.6 Credit rating / scoring system
3.1.7 Collateral / appraisal system
3.1.8 Loan approval system
3.1.9 Collection and debt management system
3.1.10 Others (please specify)
3.2 Deposit system (account opening / deposit / withdrawal / transfer / payment)
3.2.1 ..... (please specify)
3.3 Treasury and money market system
3.3.1 Treasury management system
3.3.2 Trade finance system
3.3.3 FX system
3.3.4 Cash management system
3.3.5 Others (please specify)
3.4 Customer relationship management system
3.4.1 ..... (please specify)
4. Middle and back office support system
4.1 Financial accounting system
4.2 Risk management system
4.3 AML/CFT system

4.4 Office and document management system (Document management, office, email)
4.5 Data management, data analysis and reporting system, such as Enterprise Data Warehouse, MIS, DMS-BOT
4.6 Fraud Monitoring System
4.7 Others (please specify)

Remark: please refer to the ordering and names of IT activities as specified by the Bank of Thailand