Cloud Compliance Center - Thailand

| Contents |
| --- |
| To generate table of contents, right-click here and select **Update Field.** |

Thailand

*This content was last reviewed around May 2023.*

**Cloud-neutral**

**1. Are financial institutions legally permitted to use cloud services?**

Yes, there is no prohibition on financial institutions using cloud services under applicable regulatory laws.

Please note that the term "financial institution" refers to a licensed securities company under the Securities and Exchange Act B.E. 2535 (1992)  that is regulated by, among others, the Office of Securities and Exchange Commission of Thailand ("**SEC**"). In the case of other financial institutions (e.g., commercial banks), each type of entity is generally subject to different laws and regulations.

**2. Are there any rules that apply to cloud use by financial institutions (e.g., rules regarding outsourcing or the use of cloud services)?**

The key regulation relating to outsourcing is the Notification of the Capital Market Supervisory Board No. TorThor. 60/2561 re: Rules, Conditions and Procedures for Outsourcing Functions related to Business Operations with Third Parties ("**Outsourcing Regulation**"). Financial institutions can outsource any of their functions provided that they will not as a result be considered to be a shell business with no operations.

In outsourcing any function other than a "central utility function," the cloud service provider must have the prescribed qualifications, such as being ready and able with respect to personnel and operating systems to ensure that the service provider's operational functions are in line with relevant regulations. Moreover, it must be solvent and a going concern financially. In addition, the cloud service provider must be monitored on a regular basis and prepare a due diligence report on the outsourced activity. The financial institution also needs to ensure that the Office of the Securities and Exchange Commission of Thailand ("**SEC**") can carry out on-site inspections of the cloud service provider upon request.

A "central utility function" is defined as a function related to a business operation that, in the event that a service provider ceases to provide services might affect the overall capital market because there are few service providers or a replacement of another service provider cannot be arranged immediately. Currently, the functions that are considered central utility functions by the SEC are e-payment for settlement of securities transactions and fund service platform functions.

**3. Are there any specific contractual requirements for cloud outsourcing?**

The Notification of the Capital Market Supervisory Board No. TorThor. 60/2561 re: Rules, Conditions and Procedures for Outsourcing Functions related to Business Operations with Third Parties requires that at least the following issues be addressed in the written contract with the cloud service provider:

The cloud service provider's duties and responsibilities, including details about liability, arrangements for business continuity, confidentiality and compliance with the relevant laws and regulations

The cloud service provider's consent for the Office of Securities and Exchange Commission of Thailand ("**SEC**") to inspect its operations and retrieve documentation for viewing or examination

Reasons, conditions and procedures for terminating the contract or suspending operation under the contract

Remuneration and charged expenses

In addition, the Notification of the Office of the Securities and Exchange Commission No. Nor Por. 7/2565 re: Guidelines for Establishment of Information Technology Systems, specifies that there must be a written contract on the use of services, connection or data access from a third party. This is to ensure that the third party is responsible for maintaining the appropriate security level for the IT system, with the details commensurate with the risk and importance of the third party as follows:

Scope of service, connection and access to data from the third party

Roles, duties and responsibilities of the third party and the financial institution

Minimum standards for the third party's operations, such as IT system security, confidentiality of data and use of data only for purposes specified in the service contract

Service level agreement for the use of services provided by the third party

Monitoring and reporting of the third party's performance, covering notification of any significant changes or problems and reporting of irregular events in a timely manner

The list of contact persons and channels in the case of IT system security-related problems and incidents

Disposal of data upon termination or cancellation of service, connection and access to data from the third party

Conditions or rights of the financial institution to change, terminate or cancel a contract with the third party, such as in the case that the third party breaches the contract

Provision of an IT contingency plan that conforms with the financial institution's IT contingency plan

Responsibility for damage caused by the third party, (e.g., the service provision is not as specified in the SLA)

The financial institution should assess the risk and consider adequate and appropriate measures for risk control.

The financial institution should specify the rights of the financial institution, the SEC and external auditors appointed by the financial institution or the SEC as part of the contract, to audit IT operation and internal control of the significant third party providing IT services. Otherwise, the financial institution should choose a third party whose IT operation has been audited by independent auditors that meet international standards.

**4. When does cloud outsourcing fall within the scope of the rules?**

To determine when outsourcing falls within the scope of Thai law, with respect to a licensed securities company under the Securities and Exchange Act B.E. 2535 (1992), all of the following elements must be met:

It is an operational function for the undertaking of a securities business or a function having a direct connection to the undertaking of a securities business of the financial institution.

The financial institution has an obligation to perform the function, but the function has been outsourced to another entity.

The cloud service provider has the power to control, manage or decide how to perform the outsourced function. If the financial institution must still take key decisions on the operation of the function, this will not be considered outsourcing (e.g., it might be considered to be using services from a vendor).

**5. Does the outsourcing need to be notified to the regulator?**

The details of the outsourcing of the functions related to a business operation to a client service provider must be notified to the Office of Securities and Exchange Commission of Thailand ("**SEC**") within 15 days . In the case of a material change, the financial institution must notify the SEC within 15 days using the form on the SEC's website. Additionally, it is necessary to provide a summary report of the outsourcing to the SEC at least once a year.

**6. What are the potential consequences for breaching financial services rules on cloud outsourcing?**

The Office of Securities and Exchange Commission of Thailand ("**SEC**") has the power to order the financial institution to amend, act or refrain from acting in any way to ensure compliance with the Notification of the Capital Market Supervisory Board No. TorThor. 60/2561 re: Rules, Conditions and Procedures for Outsourcing Functions related to Business Operations with Third Parties ("**Outsourcing Regulation**"), or to order a suspension of the outsourcing to a cloud service provider.

In addition, noncompliance with the Outsourcing Regulation may be subject to a fine not exceeding THB 300,000 (approximately USD 9,000) and a further fine not exceeding THB 10,000 (approximately USD 300) for every day the violation continues.

**7. Are there any data privacy and/or data security laws that would apply?**

Yes, the Personal Data Protection Act B.E. 2562 (2019) ("**PDPA**") governs data privacy in general in Thailand. Under the PDPA, a financial institution would be deemed a data controller where it has the authority and duty to make decisions regarding the collection, use or disclosure of the personal data. The cloud service provider would be deemed a data processor under the PDPA where it processes and hosts personal data on behalf of and/or under the instructions of the data controller, and does not have the power and duty to makes its own decisions regarding the collection, use or disclosure of such personal data.

According to Section 40 para. 3 of the PDPA, the data controller is required to put in place a contract with the data processor to control the activities carried out by the data processor in accordance with the latter’s duties under the PDPA.

**8. Are there any restrictions under local data protection laws that would impact the overseas hosting of data?**

Yes, the Personal Data Protection Act B.E. 2562 (2019) ("**PDPA**") prescribes rules and requirements that must be met for the cross-border transfer of personal data outside Thailand. According to Section 28 and 29 of the PDPA, cross-border transfer of personal data is restricted unless one of the following grounds can be relied on:

Adequacy of the destination country's data protection standard, where the transfer of data is carried out in accordance with the criteria for personal data protection to be prescribed by the Personal Data Protection Committee

Legal exceptions for cross-border transfer apply in the following circumstances:

- It is for legal compliance.

- Consent has been obtained from the data subject, where the data subject has been informed of the inadequate personal data protection standards of the destination country.

- It is necessary for the performance of a contract to which the data subject is a party or to take steps at the request of the data subject prior to entering into such contract.

- It is for compliance with a contract between the data controller and other persons or legal entities for the interests of the data subject.

- It is to prevent danger to the life, body or health of the data subject or another person, when the data subject is incapable of giving the consent at such time.

- It is necessary for carrying out activities of substantial public interest.

Privacy policy for cross-border transfer to recipients in the same group of undertakings or group of businesses (binding corporate rules)

Where there are appropriate safeguards (e.g., standard contractual clauses)

**9. Does a cloud service provider need a financial services authorization or license to provide cloud services?**

Yes, if the outsourced function is considered a "central utility function" (as described in Question 2). Under Clause 12 of the Notification of the Capital Market Supervisory Board No. TorThor. 60/2561 re: Rules, Conditions and Procedures for Outsourcing Functions related to Business Operations to Third Parties, a financial institution can only outsource the central utility function to a service provider that has been approved by the Office of Securities and Exchange Commission of Thailand ("**SEC**").

A "central utility function" is defined as a function related to a business operation that, in the event that a service provider ceases to provide services, fails to continue operations or is unable to provide services appropriately, may affect the wider overall capital market because there are few service providers or a replacement of another service provider cannot be arranged immediately. Currently the functions that are considered central utility functions by the SEC are e-payment for settlement of securities transactions and fund service platform functions.

According to the Notification of the Office of the SEC No. SorThor. 40/2560 re: Approval for Service Provider of E-Payment for a Settlement of Securities Transactions, an applicant's key requirements and qualifications for approval from the SEC include strong prudential criteria, conducting business fairly having adequate and efficient systems and controls (covering risk management, internal controls, information security, information technology and crisis management), having monitoring and compliance systems, having sufficient personnel, and allowing the SEC to conduct on-site audits.

**10. Is express consent from customers or other data subjects required before moving data to the cloud?**

This depends on what legal basis the data controller (e.g., financial institution) relies on for the cross-border transfer of data. In the absence of any regulation on cross-border transfer of data, the following approaches can be considered:

Not obtaining consent from customers (risk-based approach)

Obtaining consent from customers (consent-based approach)

The Personal Data Protection Act B.E. 2562 (2019) ("**PDPA**") prescribes rules and requirements concerning requests for consent. The consent request should be in line with the consent requirements under Section 19 of the PDPA, where it prescribes, among others, that a request for consent should be made in a written statement or via electronic means, unless it is not practical to do so.

On 7 September 2022, the Office of the Personal Data Protection Committee published the Guideline on Seeking Consent from Data Subjects under the Personal Data Protection Act B.E. 2562 (2019) ("**Consent Guideline**"). The Consent Guideline provides an overview of consent requirements , which are generally in line with the provisions of the PDPA.

**11. Are there any local laws that require a cloud service provider to be able to access the data it hosts?**

No.

**12. Are there any local laws that would require a cloud service provider to disclose the data it hosts to any third parties in any circumstances (including regulatory or law enforcement authorities)?**

Generally, there is no local law that would require a cloud service provider to disclose the client's data it hosts to a third party. However, if the cloud service provider is the service provider for a "central utility function" and has received approval from the Office of Securities and Exchange Commission of Thailand ("**SEC**"), the SEC has the power to request documents and information from the cloud service provider for inspection. In addition, for the purpose of making inquiries and investigations in the event that of reasonable grounds to believe that an offense prescribed under the Computer-Related Crime Act B.E. 2550 2007) ("**CCA**")[1] has occurred (or there is a request in relation to criminal offenses), the competent official may request data from cloud service providers. Please note, however, that the permanent secretary of the Ministry of Digital Economy and Society stated in August 2021 that if an organization engages an outsourced data storage provider (such as a cloud service provider) to help store its data, it would be responsible for complying with requests made under the CCA, since the cloud service provider is not the data owner.

[1] For instance, entering false computer data into a computer system in a manner likely to cause damage to the protection of national security, public safety, economic safety, infrastructures for public benefit, or cause panic to the general public; entering into a computer system any computer data that is an offense related to national security or terrorism.

# Permissibility of cloud

## 1. Are financial institutions legally permitted to use cloud services?

Yes, there is no prohibition on financial institutions using cloud services under applicable regulatory laws.

Please note that the term "financial institution" refers to a licensed securities company under the Securities and Exchange Act B.E. 2535 (1992)  that is regulated by, among others, the Office of Securities and Exchange Commission of Thailand ("**SEC**"). In the case of other financial institutions (e.g., commercial banks), each type of entity is generally subject to different laws and regulations.

# Rules for cloud outsourcing

## 2. Are there any rules that apply to cloud use by financial institutions (e.g., rules regarding outsourcing or the use of cloud services)?

The key regulation relating to outsourcing is the Notification of the Capital Market Supervisory Board No. TorThor. 60/2561 re: Rules, Conditions and Procedures for Outsourcing Functions related to Business Operations with Third Parties ("**Outsourcing Regulation**"). Financial institutions can outsource any of their functions provided that they will not as a result be considered to be a shell business with no operations.

In outsourcing any function other than a "central utility function," the cloud service provider must have the prescribed qualifications, such as being ready and able with respect to personnel and operating systems to ensure that the service provider's operational functions are in line with relevant regulations. Moreover, it must be solvent and a going concern financially. In addition, the cloud service provider must be monitored on a regular basis and prepare a due diligence report on the outsourced activity. The financial institution also needs to ensure that the Office of the Securities and Exchange Commission of Thailand ("**SEC**") can carry out on-site inspections of the cloud service provider upon request.

A "central utility function" is defined as a function related to a business operation that, in the event that a service provider ceases to provide services might affect the overall capital market because there are few service providers or a replacement of another service provider cannot be arranged immediately. Currently, the functions that are considered central utility functions by the SEC are e-payment for settlement of securities transactions and fund service platform functions.

# Contract requirements

## 3. Are there any specific contractual requirements for cloud outsourcing?

The Notification of the Capital Market Supervisory Board No. TorThor. 60/2561 re: Rules, Conditions and Procedures for Outsourcing Functions related to Business Operations with Third Parties requires that at least the following issues be addressed in the written contract with the cloud service provider:

The cloud service provider's duties and responsibilities, including details about liability, arrangements for business continuity, confidentiality and compliance with the relevant laws and regulations

The cloud service provider's consent for the Office of Securities and Exchange Commission of Thailand ("**SEC**") to inspect its operations and retrieve documentation for viewing or examination

Reasons, conditions and procedures for terminating the contract or suspending operation under the contract

Remuneration and charged expenses

In addition, the Notification of the Office of the Securities and Exchange Commission No. Nor Por. 7/2565 re: Guidelines for Establishment of Information Technology Systems, specifies that there must be a written contract on the use of services, connection or data access from a third party. This is to ensure that the third party is responsible for maintaining the appropriate security level for the IT system, with the details commensurate with the risk and importance of the third party as follows:

Scope of service, connection and access to data from the third party

Roles, duties and responsibilities of the third party and the financial institution

Minimum standards for the third party's operations, such as IT system security, confidentiality of data and use of data only for purposes specified in the service contract

Service level agreement for the use of services provided by the third party

Monitoring and reporting of the third party's performance, covering notification of any significant changes or problems and reporting of irregular events in a timely manner

The list of contact persons and channels in the case of IT system security-related problems and incidents

Disposal of data upon termination or cancellation of service, connection and access to data from the third party

Conditions or rights of the financial institution to change, terminate or cancel a contract with the third party, such as in the case that the third party breaches the contract

Provision of an IT contingency plan that conforms with the financial institution's IT contingency plan

Responsibility for damage caused by the third party, (e.g., the service provision is not as specified in the SLA)

The financial institution should assess the risk and consider adequate and appropriate measures for risk control.

The financial institution should specify the rights of the financial institution, the SEC and external auditors appointed by the financial institution or the SEC as part of the contract, to audit IT operation and internal control of the significant third party providing IT services. Otherwise, the financial institution should choose a third party whose IT operation has been audited by independent auditors that meet international standards.

# Regulated cloud outsourcing

## 4. When does cloud outsourcing fall within the scope of the rules?

To determine when outsourcing falls within the scope of Thai law, with respect to a licensed securities company under the Securities and Exchange Act B.E. 2535 (1992), all of the following elements must be met:

It is an operational function for the undertaking of a securities business or a function having a direct connection to the undertaking of a securities business of the financial institution.

The financial institution has an obligation to perform the function, but the function has been outsourced to another entity.

The cloud service provider has the power to control, manage or decide how to perform the outsourced function. If the financial institution must still take key decisions on the operation of the function, this will not be considered outsourcing (e.g., it might be considered to be using services from a vendor).

# Regulatory notifications

## 5. Does the outsourcing need to be notified to the regulator?

The details of the outsourcing of the functions related to a business operation to a client service provider must be notified to the Office of Securities and Exchange Commission of Thailand ("**SEC**") within 15 days . In the case of a material change, the financial institution must notify the SEC within 15 days using the form on the SEC's website. Additionally, it is necessary to provide a summary report of the outsourcing to the SEC at least once a year.

# Consequences of regulatory breach

## 6. What are the potential consequences for breaching financial services rules on cloud outsourcing?

The Office of Securities and Exchange Commission of Thailand ("**SEC**") has the power to order the financial institution to amend, act or refrain from acting in any way to ensure compliance with the Notification of the Capital Market Supervisory Board No. TorThor. 60/2561 re: Rules, Conditions and Procedures for Outsourcing Functions related to Business Operations with Third Parties ("**Outsourcing Regulation**"), or to order a suspension of the outsourcing to a cloud service provider.

In addition, noncompliance with the Outsourcing Regulation may be subject to a fine not exceeding THB 300,000 (approximately USD 9,000) and a further fine not exceeding THB 10,000 (approximately USD 300) for every day the violation continues.

# Data privacy and security

## 7. Are there any data privacy and/or data security laws that would apply?

Yes, the Personal Data Protection Act B.E. 2562 (2019) ("**PDPA**") governs data privacy in general in Thailand. Under the PDPA, a financial institution would be deemed a data controller where it has the authority and duty to make decisions regarding the collection, use or disclosure of the personal data. The cloud service provider would be deemed a data processor under the PDPA where it processes and hosts personal data on behalf of and/or under the instructions of the data controller, and does not have the power and duty to makes its own decisions regarding the collection, use or disclosure of such personal data.

According to Section 40 para. 3 of the PDPA, the data controller is required to put in place a contract with the data processor to control the activities carried out by the data processor in accordance with the latter’s duties under the PDPA.

# Overseas hosting

## 8. Are there any restrictions under local data protection laws that would impact the overseas hosting of data?

Yes, the Personal Data Protection Act B.E. 2562 (2019) ("**PDPA**") prescribes rules and requirements that must be met for the cross-border transfer of personal data outside Thailand. According to Section 28 and 29 of the PDPA, cross-border transfer of personal data is restricted unless one of the following grounds can be relied on:

Adequacy of the destination country's data protection standard, where the transfer of data is carried out in accordance with the criteria for personal data protection to be prescribed by the Personal Data Protection Committee

Legal exceptions for cross-border transfer apply in the following circumstances:

- It is for legal compliance.

- Consent has been obtained from the data subject, where the data subject has been informed of the inadequate personal data protection standards of the destination country.

- It is necessary for the performance of a contract to which the data subject is a party or to take steps at the request of the data subject prior to entering into such contract.

- It is for compliance with a contract between the data controller and other persons or legal entities for the interests of the data subject.

- It is to prevent danger to the life, body or health of the data subject or another person, when the data subject is incapable of giving the consent at such time.

- It is necessary for carrying out activities of substantial public interest.

Privacy policy for cross-border transfer to recipients in the same group of undertakings or group of businesses (binding corporate rules)

Where there are appropriate safeguards (e.g., standard contractual clauses)

# Financial services authorizations licenses

## 9. Does a cloud service provider need a financial services authorization or license to provide cloud services?

Yes, if the outsourced function is considered a "central utility function" (as described in Question 2). Under Clause 12 of the Notification of the Capital Market Supervisory Board No. TorThor. 60/2561 re: Rules, Conditions and Procedures for Outsourcing Functions related to Business Operations to Third Parties, a financial institution can only outsource the central utility function to a service provider that has been approved by the Office of Securities and Exchange Commission of Thailand ("**SEC**").

A "central utility function" is defined as a function related to a business operation that, in the event that a service provider ceases to provide services, fails to continue operations or is unable to provide services appropriately, may affect the wider overall capital market because there are few service providers or a replacement of another service provider cannot be arranged immediately. Currently the functions that are considered central utility functions by the SEC are e-payment for settlement of securities transactions and fund service platform functions.

According to the Notification of the Office of the SEC No. SorThor. 40/2560 re: Approval for Service Provider of E-Payment for a Settlement of Securities Transactions, an applicant's key requirements and qualifications for approval from the SEC include strong prudential criteria, conducting business fairly having adequate and efficient systems and controls (covering risk management, internal controls, information security, information technology and crisis management), having monitoring and compliance systems, having sufficient personnel, and allowing the SEC to conduct on-site audits.

# Customer data subject consent

## 10. Is express consent from customers or other data subjects required before moving data to the cloud?

This depends on what legal basis the data controller (e.g., financial institution) relies on for the cross-border transfer of data. In the absence of any regulation on cross-border transfer of data, the following approaches can be considered:

Not obtaining consent from customers (risk-based approach)

Obtaining consent from customers (consent-based approach)

The Personal Data Protection Act B.E. 2562 (2019) ("**PDPA**") prescribes rules and requirements concerning requests for consent. The consent request should be in line with the consent requirements under Section 19 of the PDPA, where it prescribes, among others, that a request for consent should be made in a written statement or via electronic means, unless it is not practical to do so.

On 7 September 2022, the Office of the Personal Data Protection Committee published the Guideline on Seeking Consent from Data Subjects under the Personal Data Protection Act B.E. 2562 (2019) ("**Consent Guideline**"). The Consent Guideline provides an overview of consent requirements , which are generally in line with the provisions of the PDPA.

# Data access requirements

## 11. Are there any local laws that require a cloud service provider to be able to access the data it hosts?

No.

# Data disclosure requirements

## 12. Are there any local laws that would require a cloud service provider to disclose the data it hosts to any third parties in any circumstances (including regulatory or law enforcement authorities)?

Generally, there is no local law that would require a cloud service provider to disclose the client's data it hosts to a third party. However, if the cloud service provider is the service provider for a "central utility function" and has received approval from the Office of Securities and Exchange Commission of Thailand ("**SEC**"), the SEC has the power to request documents and information from the cloud service provider for inspection. In addition, for the purpose of making inquiries and investigations in the event that of reasonable grounds to believe that an offense prescribed under the Computer-Related Crime Act B.E. 2550 2007) ("**CCA**")[1] has occurred (or there is a request in relation to criminal offenses), the competent official may request data from cloud service providers. Please note, however, that the permanent secretary of the Ministry of Digital Economy and Society stated in August 2021 that if an organization engages an outsourced data storage provider (such as a cloud service provider) to help store its data, it would be responsible for complying with requests made under the CCA, since the cloud service provider is not the data owner.

[1] For instance, entering false computer data into a computer system in a manner likely to cause damage to the protection of national security, public safety, economic safety, infrastructures for public benefit, or cause panic to the general public; entering into a computer system any computer data that is an offense related to national security or terrorism.

©Copyright © 2025 Baker & McKenzie. All rights reserved. **Ownership**: This documentation and content (Content) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms). The Content is protected under international copyright conventions. Use of this Content does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion**: All Content is for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulations and practice are subject to change. The Content is not offered as legal or professional advice for any specific matter. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any Content. Baker McKenzie and the editors and the contributing authors do not guarantee the accuracy of the Content and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the Content. The Content may contain links to external websites and external websites may link to the Content. Baker McKenzie is not responsible for the content or operation of any such external sites and disclaims all liability, howsoever occurring, in respect of the content or operation of any such external websites. **Attorney Advertising**: This Content may qualify as “Attorney Advertising” requiring notice in some jurisdictions. To the extent that this Content may qualify as Attorney Advertising, PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME. **Reproduction**: Reproduction or copying of the Content on this Site without express written authorization is strictly prohibited.