Cloud Compliance Center - Singapore

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

Singapore

*This content was last reviewed around October 2022.*

**Cloud-neutral**

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

Yes, provided that the institution meets all applicable legal requirements for the use of cloud services.

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

Yes, a financial institution's use of a cloud service provider's services is likely to be directly subject to the following rules and guidelines specifically relating to outsourcing:

The Monetary Authority of Singapore ("**MAS**") Guidelines on Outsourcing if the cloud use relates to outsourced services — financial institutions that are regulated by MAS are subject to these guidelines.

The Association of Banks in Singapore Cloud Computing Implementation Guide 2.0 — this guide is a set of industry codes and best practices applicable to banks.

The MAS Guidelines on Technology Risk Management — financial institutions that are regulated by MAS are subject to these guidelines.

There are also various other related rules/best practices on the use of technology or third parties more generally, such as the MAS Notice on Technology Risk Management, the MAS Notice on Cyber Hygiene, the Business Continuity Management Guidelines and the MAS Public Cloud Advisory. Financial institutions should be mindful of the obligations/best practices in these regulatory instruments and advisory notices, and ensure they can still be met even if operations/services are outsourced. MAS' August 2022 Information Paper on "Operational Risk Management — Management Of Outsourcing And Third-Party Arrangements" also provides further relevant guidance.

Changes were made to the Banking Act in 2020 that contemplate MAS would issue revised outsourcing notices that would mandate banks' compliance with a range of requirements, including certain matters currently covered by the MAS Guidelines on Outsourcing, and more. At the time of writing, those notices have not yet been issued, so the contemplated changes are not in effect.

In December 2020, MAS issued a consultation paper on a proposed notice to banks on managing outsourced relevant services, which expressly includes public cloud services as relevant services. The proposals are still at the consultation stage.

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

The Monetary Authority of Singapore ("**MAS**") Guidelines on Outsourcing set out MAS' expectations about the provisions that should, minimally, be included in outsourcing agreements. These terms include the following:

The scope of the outsourcing arrangement and service description

Terms and standards on performance, operational, internal control and risk management matters

The parties' rights and responsibilities relating to confidentiality and security (This includes allocation of liability in the event of a breach, and rights of access to and disclosure of customer information by the service provider.)

Business continuity management, including as to recovery time objectives, recovery point objectives and resumption of operating capacities (See also MAS' Business Continuity Management Guidelines for the latest guidance on business continuity management generally.)

Terms to ensure there is effective monitoring and control by the institution on a continuing basis

Rights for the financial institution or MAS to audit the service provider and its subcontractors (whether by the financial institution's internal or external auditors, or their agents), and to obtain copies of any audit report on the service provider and its subcontractors

An obligation for the service provider to comply with any request from the financial institution or MAS to submit any reports on the security and control environment of the service provider and its subcontractors to MAS

The types of events and circumstances under which the service provider should report to the financial institution for the institution to take prompt risk mitigation measures and notify MAS of any adverse developments

A dispute resolution process, events of default, and the indemnities, remedies and recourse of the parties

The financial institution's rights to terminate for default and early exit (This includes the institution's right to terminate the agreement where the service provider undergoes a change in ownership or insolvency, a breach of security or confidentiality occurs, or where there is a demonstrable deterioration in its ability to perform.)

The minimum period to execute a termination and other provisions to ensure a smooth transition when the agreement is terminated or being amended

Rules and limitations on subcontracting, including the service provider's obligation to obtain the financial institution's prior consent for subcontracting any part of material outsourcing

Governing law and jurisdiction

The MAS Public Cloud Advisory also advises that contractual agreements should clearly delineate all parties' cybersecurity responsibilities and that contract terms should not impede financial institutions' ability to manage risk and meet regulatory requirements/expectations. Additionally, cloud agreements should provide rights for financial institutions to request that the cloud service provider remedy issues identified during audits and/or assessments in a timely manner.

In addition, the Association of Banks in Singapore Cloud Computing Implementation Guide 2.0, which contains best practice recommendations and guidance for the safe adoption of cloud, further adds that outsourcing agreements should include terms relating to the following:

Data confidentiality and control ownership, including change management processes and the circumstances under which each party has the right to change security requirements

Data transfers and location of data, including the financial institution's right to be notified of any changes to the location of the data and of any local requirements compelling the service provider to disclose the data to a third party

Data retention, such as the management of data in online or offline backups

Exit planning, including procedures and tools for the deletion of data, transferability of outsourced services and recovery of data for the purposes of continuity of services

Finally, having made changes to the Banking Act, the Singapore government has proposed that MAS issue revised outsourcing notices, which will codify and build on certain aspects of the MAS Outsourcing Guidelines, and formally make compliance mandatory for banks. If the proposed revised outsourcing notices were issued, banks would (among other things) be required to comply with written notices issued by MAS when contracting with an outsourced service provider, stipulating requirements for the outsourcing contract. Such requirements might require the inclusion of a provision allowing the bank to terminate the contract in certain circumstances. It is also contemplated that MAS would be able to require the bank to exercise its right to terminate the outsourcing contract in those circumstances.

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

A financial institution's use of cloud services provided by a third-party cloud service provider may be considered outsourcing, although this will ultimately depend on what the cloud services are used for. Where the arrangement constitutes outsourcing, the arrangement will fall within the local rules mentioned in question 2.

The extent and degree to which certain aspects of the Monetary Authority of Singapore ("**MAS**") Guidelines on Outsourcing will apply depend on whether the arrangement is a "material outsourcing arrangement." "Material outsourcing" means the following:

An outsourcing arrangement that, in the event of a service failure or security breach, has the potential to materially impact either of the following:

An institution's business operations, reputation or profitability

An institution's ability to manage risk and comply with applicable laws and regulations

An outsourcing arrangement that involves customer information and, in the event of any unauthorized access or disclosure, loss, or theft of customer information, may have a material impact on an institution's customers

The MAS Public Cloud Advisory relates to financial institutions' use of public cloud services generally.

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

There is no requirement to notify or obtain approval from the Monetary Authority of Singapore ("**MAS**") prior to entering into a cloud services outsourcing arrangement, although certain ex post notification requirements may apply, i.e., the following:

A financial institution is required to maintain a register, setting out details of all outsourcing arrangements. The outsourcing register needs to be submitted to MAS, at least annually or upon request.

A financial institution is required to notify MAS if the following occurs:

Any overseas authority seeks access to its customer information or if the institution's and MAS' rights of access have been restricted or denied.

There are any adverse developments arising from its outsourcing arrangements that could impact the institution or members of its group, including any event that could potentially lead to prolonged service failure or disruption in the outsourcing arrangement, or breach of security or confidentiality.

A financial institution is also required to confirm in writing to MAS that it has provided, in its outsourcing agreements, for MAS to have the right to inspect the service provider, as well as the rights of access to the financial institution's and service provider's information, reports and findings related to the outsourcing arrangement.

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

Guidelines issued by the Monetary Authority of Singapore ("**MAS**"), such as the MAS Guidelines on Outsourcing, the MAS Guidelines on Technology Risk Management and the Business Continuity Management Guidelines, do not have statutory force in that the contravention of guidelines is not a criminal offense and does not result in civil penalties. They are intended to be a set of principles or best practice standards that govern the conduct of specified institutions or persons. However, how well an institution observes the guidelines may have an impact on MAS' overall risk assessment of that institution.

Particularly where MAS is not satisfied with an institution's observance of the relevant guidelines, it may require the institution to take additional measures to address the deficiencies noted. MAS may also take noncompliance into account in its assessment of the institution, depending on various factors and the circumstances of the case. MAS may also directly communicate with the home or host regulators of the institution and the institution's service provider about their ability and willingness to cooperate with MAS in supervising the risks that outsourcing poses to the institution. In addition, MAS may require an institution to modify its outsourcing arrangements, make alternative arrangements or reintegrate an outsourced service into the institution.

Unlike guidelines, notices issued by MAS (such as the MAS Notice on Technology Risk Management) are legally binding, i.e., contravening a notice would be a criminal offense and would result in penalties/sanctions.

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

Yes, the Personal Data Protection Act 2012.

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

Yes. Although there are no data localization requirements, financial institutions are required to ensure compliance with the transfer limitation obligation in the Personal Data Protection Act 2012 (i.e., ensuring that personal data may only be transferred to overseas locations with comparable data protection laws, or that the recipients, e.g., data centers or sub-processors in these locations, are legally bound by similar contractual standards).

In addition, financial institutions need to identify risks associated with any outsourcing outside Singapore (e.g., government policies, political, social and economic conditions, and legal and regulatory developments) and ensure such risks can be adequately addressed. Financial institutions also need to ensure that outsourcing outside Singapore does not impede the financial institution and the Monetary Authority of Singapore's ability to inspect the service provider and access data and records maintained by the service provider under the outsourced arrangement, and that the service provider is operating in jurisdictions that uphold a duty of confidentiality.

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

Generally, the provision of cloud services per se is not an activity or service that is regulated by the Monetary Authority of Singapore. That said, what these services are and how they are used and delivered should be examined to ensure that the service provider does not inadvertently trigger any financial services authorization or licensing requirements.

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

Yes, unless a statutory or legal exception applies.

While there is no requirement to obtain express consent from customers to move data to the cloud per se, financial institutions are subject to a common law duty of confidence and, in the case of banks, merchant banks and trust companies, a statutory duty of confidence. Additionally, under the Singapore Personal Data Protection Act, disclosing any personal data (e.g., to a third-party cloud service provider) also requires the data subject's consent, unless a statutory or legal exception applies.

Disclosing or transferring customer information to a cloud service provider will therefore require a customer's consent. In the case of banks, merchant banks and trust companies that are subject to a statutory duty of confidence, such consent needs to be in writing (unless other statutory exemptions apply). Financial institutions should also ensure that any disclosures to their service providers are made in accordance with the terms of the customer contracts.

**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)?**

Yes, there are regulatory requirements that, while not necessarily applicable to the cloud service provider, would apply to the financial institutions. These requirements are likely to affect the cloud service provider's contractual duties where the services are considered outsourced services by the financial institutions.

For example, financial institutions are required to secure rights for the financial institution or the Monetary Authority of Singapore to audit the service provider and its subcontractors, whether by the financial institutions' internal or external auditors, or their agents.

# Permissibility of cloud

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

Yes, provided that the institution meets all applicable legal requirements for the use of cloud services.

# 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)?

Yes, a financial institution's use of a cloud service provider's services is likely to be directly subject to the following rules and guidelines specifically relating to outsourcing:

The Monetary Authority of Singapore ("**MAS**") Guidelines on Outsourcing if the cloud use relates to outsourced services — financial institutions that are regulated by MAS are subject to these guidelines.

The Association of Banks in Singapore Cloud Computing Implementation Guide 2.0 — this guide is a set of industry codes and best practices applicable to banks.

The MAS Guidelines on Technology Risk Management — financial institutions that are regulated by MAS are subject to these guidelines.

There are also various other related rules/best practices on the use of technology or third parties more generally, such as the MAS Notice on Technology Risk Management, the MAS Notice on Cyber Hygiene, the Business Continuity Management Guidelines and the MAS Public Cloud Advisory. Financial institutions should be mindful of the obligations/best practices in these regulatory instruments and advisory notices, and ensure they can still be met even if operations/services are outsourced. MAS' August 2022 Information Paper on "Operational Risk Management — Management Of Outsourcing And Third-Party Arrangements" also provides further relevant guidance.

Changes were made to the Banking Act in 2020 that contemplate MAS would issue revised outsourcing notices that would mandate banks' compliance with a range of requirements, including certain matters currently covered by the MAS Guidelines on Outsourcing, and more. At the time of writing, those notices have not yet been issued, so the contemplated changes are not in effect.

In December 2020, MAS issued a consultation paper on a proposed notice to banks on managing outsourced relevant services, which expressly includes public cloud services as relevant services. The proposals are still at the consultation stage.

# Contract requirements

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

The Monetary Authority of Singapore ("**MAS**") Guidelines on Outsourcing set out MAS' expectations about the provisions that should, minimally, be included in outsourcing agreements. These terms include the following:

The scope of the outsourcing arrangement and service description

Terms and standards on performance, operational, internal control and risk management matters

The parties' rights and responsibilities relating to confidentiality and security (This includes allocation of liability in the event of a breach, and rights of access to and disclosure of customer information by the service provider.)

Business continuity management, including as to recovery time objectives, recovery point objectives and resumption of operating capacities (See also MAS' Business Continuity Management Guidelines for the latest guidance on business continuity management generally.)

Terms to ensure there is effective monitoring and control by the institution on a continuing basis

Rights for the financial institution or MAS to audit the service provider and its subcontractors (whether by the financial institution's internal or external auditors, or their agents), and to obtain copies of any audit report on the service provider and its subcontractors

An obligation for the service provider to comply with any request from the financial institution or MAS to submit any reports on the security and control environment of the service provider and its subcontractors to MAS

The types of events and circumstances under which the service provider should report to the financial institution for the institution to take prompt risk mitigation measures and notify MAS of any adverse developments

A dispute resolution process, events of default, and the indemnities, remedies and recourse of the parties

The financial institution's rights to terminate for default and early exit (This includes the institution's right to terminate the agreement where the service provider undergoes a change in ownership or insolvency, a breach of security or confidentiality occurs, or where there is a demonstrable deterioration in its ability to perform.)

The minimum period to execute a termination and other provisions to ensure a smooth transition when the agreement is terminated or being amended

Rules and limitations on subcontracting, including the service provider's obligation to obtain the financial institution's prior consent for subcontracting any part of material outsourcing

Governing law and jurisdiction

The MAS Public Cloud Advisory also advises that contractual agreements should clearly delineate all parties' cybersecurity responsibilities and that contract terms should not impede financial institutions' ability to manage risk and meet regulatory requirements/expectations. Additionally, cloud agreements should provide rights for financial institutions to request that the cloud service provider remedy issues identified during audits and/or assessments in a timely manner.

In addition, the Association of Banks in Singapore Cloud Computing Implementation Guide 2.0, which contains best practice recommendations and guidance for the safe adoption of cloud, further adds that outsourcing agreements should include terms relating to the following:

Data confidentiality and control ownership, including change management processes and the circumstances under which each party has the right to change security requirements

Data transfers and location of data, including the financial institution's right to be notified of any changes to the location of the data and of any local requirements compelling the service provider to disclose the data to a third party

Data retention, such as the management of data in online or offline backups

Exit planning, including procedures and tools for the deletion of data, transferability of outsourced services and recovery of data for the purposes of continuity of services

Finally, having made changes to the Banking Act, the Singapore government has proposed that MAS issue revised outsourcing notices, which will codify and build on certain aspects of the MAS Outsourcing Guidelines, and formally make compliance mandatory for banks. If the proposed revised outsourcing notices were issued, banks would (among other things) be required to comply with written notices issued by MAS when contracting with an outsourced service provider, stipulating requirements for the outsourcing contract. Such requirements might require the inclusion of a provision allowing the bank to terminate the contract in certain circumstances. It is also contemplated that MAS would be able to require the bank to exercise its right to terminate the outsourcing contract in those circumstances.

# Regulated cloud outsourcing

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

A financial institution's use of cloud services provided by a third-party cloud service provider may be considered outsourcing, although this will ultimately depend on what the cloud services are used for. Where the arrangement constitutes outsourcing, the arrangement will fall within the local rules mentioned in question 2.

The extent and degree to which certain aspects of the Monetary Authority of Singapore ("**MAS**") Guidelines on Outsourcing will apply depend on whether the arrangement is a "material outsourcing arrangement." "Material outsourcing" means the following:

An outsourcing arrangement that, in the event of a service failure or security breach, has the potential to materially impact either of the following:

An institution's business operations, reputation or profitability

An institution's ability to manage risk and comply with applicable laws and regulations

An outsourcing arrangement that involves customer information and, in the event of any unauthorized access or disclosure, loss, or theft of customer information, may have a material impact on an institution's customers

The MAS Public Cloud Advisory relates to financial institutions' use of public cloud services generally.

# Regulatory notifications

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

There is no requirement to notify or obtain approval from the Monetary Authority of Singapore ("**MAS**") prior to entering into a cloud services outsourcing arrangement, although certain ex post notification requirements may apply, i.e., the following:

A financial institution is required to maintain a register, setting out details of all outsourcing arrangements. The outsourcing register needs to be submitted to MAS, at least annually or upon request.

A financial institution is required to notify MAS if the following occurs:

Any overseas authority seeks access to its customer information or if the institution's and MAS' rights of access have been restricted or denied.

There are any adverse developments arising from its outsourcing arrangements that could impact the institution or members of its group, including any event that could potentially lead to prolonged service failure or disruption in the outsourcing arrangement, or breach of security or confidentiality.

A financial institution is also required to confirm in writing to MAS that it has provided, in its outsourcing agreements, for MAS to have the right to inspect the service provider, as well as the rights of access to the financial institution's and service provider's information, reports and findings related to the outsourcing arrangement.

# Consequences of regulatory breach

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

Guidelines issued by the Monetary Authority of Singapore ("**MAS**"), such as the MAS Guidelines on Outsourcing, the MAS Guidelines on Technology Risk Management and the Business Continuity Management Guidelines, do not have statutory force in that the contravention of guidelines is not a criminal offense and does not result in civil penalties. They are intended to be a set of principles or best practice standards that govern the conduct of specified institutions or persons. However, how well an institution observes the guidelines may have an impact on MAS' overall risk assessment of that institution.

Particularly where MAS is not satisfied with an institution's observance of the relevant guidelines, it may require the institution to take additional measures to address the deficiencies noted. MAS may also take noncompliance into account in its assessment of the institution, depending on various factors and the circumstances of the case. MAS may also directly communicate with the home or host regulators of the institution and the institution's service provider about their ability and willingness to cooperate with MAS in supervising the risks that outsourcing poses to the institution. In addition, MAS may require an institution to modify its outsourcing arrangements, make alternative arrangements or reintegrate an outsourced service into the institution.

Unlike guidelines, notices issued by MAS (such as the MAS Notice on Technology Risk Management) are legally binding, i.e., contravening a notice would be a criminal offense and would result in penalties/sanctions.

# Data privacy and security

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

Yes, the Personal Data Protection Act 2012.

# Overseas hosting

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

Yes. Although there are no data localization requirements, financial institutions are required to ensure compliance with the transfer limitation obligation in the Personal Data Protection Act 2012 (i.e., ensuring that personal data may only be transferred to overseas locations with comparable data protection laws, or that the recipients, e.g., data centers or sub-processors in these locations, are legally bound by similar contractual standards).

In addition, financial institutions need to identify risks associated with any outsourcing outside Singapore (e.g., government policies, political, social and economic conditions, and legal and regulatory developments) and ensure such risks can be adequately addressed. Financial institutions also need to ensure that outsourcing outside Singapore does not impede the financial institution and the Monetary Authority of Singapore's ability to inspect the service provider and access data and records maintained by the service provider under the outsourced arrangement, and that the service provider is operating in jurisdictions that uphold a duty of confidentiality.

# Financial services authorizations licenses

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

Generally, the provision of cloud services per se is not an activity or service that is regulated by the Monetary Authority of Singapore. That said, what these services are and how they are used and delivered should be examined to ensure that the service provider does not inadvertently trigger any financial services authorization or licensing requirements.

# Customer data subject consent

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

Yes, unless a statutory or legal exception applies.

While there is no requirement to obtain express consent from customers to move data to the cloud per se, financial institutions are subject to a common law duty of confidence and, in the case of banks, merchant banks and trust companies, a statutory duty of confidence. Additionally, under the Singapore Personal Data Protection Act, disclosing any personal data (e.g., to a third-party cloud service provider) also requires the data subject's consent, unless a statutory or legal exception applies.

Disclosing or transferring customer information to a cloud service provider will therefore require a customer's consent. In the case of banks, merchant banks and trust companies that are subject to a statutory duty of confidence, such consent needs to be in writing (unless other statutory exemptions apply). Financial institutions should also ensure that any disclosures to their service providers are made in accordance with the terms of the customer contracts.

# 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)?

Yes, there are regulatory requirements that, while not necessarily applicable to the cloud service provider, would apply to the financial institutions. These requirements are likely to affect the cloud service provider's contractual duties where the services are considered outsourced services by the financial institutions.

For example, financial institutions are required to secure rights for the financial institution or the Monetary Authority of Singapore to audit the service provider and its subcontractors, whether by the financial institutions' internal or external auditors, or their agents.

©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.