accenture

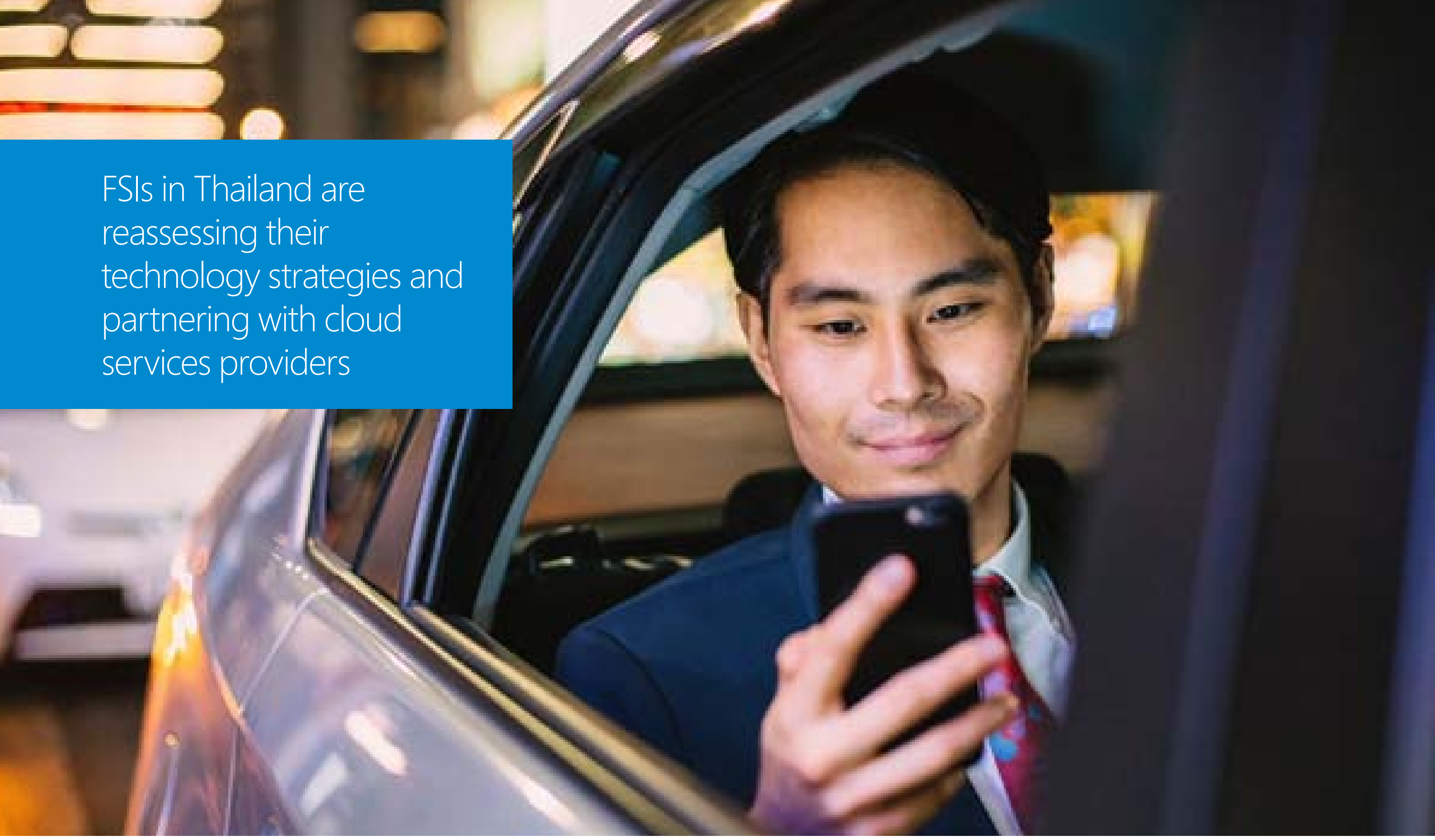
Microsoft

Navigating your way to the cloud

A practical guide for financial institutions in Thailand

Contents

Navigating your way to the cloud



FSIs in Thailand are reassessing their technology strategies and partnering with cloud services providers

Moving to the digital economy

Thailand has been subject to one of the most dramatic economic transformations in the Asia-Pacific region. This has been fuelled by the growth of the digital economy, a policy priority for the Thai government. The financial services industry is at the forefront of this transformation, supported by the Bank of Thailand (BOT), which has implemented policies and guidelines to bring clarity for Financial Services Institutions (FSIs) wishing to adopt technology.

Strong regulatory support for innovation

To further drive this digital transformation, the Thai government announced in 2016 that it would create a new Digital Economy and Society Ministry. This was accompanied by a fresh legislative strategy with personal data protection and cybersecurity at its core.

BOT is also supporting digital transformation in financial services through forward-looking policy moves such as the "regulatory sandbox" initiative, a policy approach that is also being pursued by progressive regulators in Singapore, Australia, the UK and France.

Increasing adoption of new technologies

As a result of these positive developments, FSIs in Thailand are increasingly partnering with cloud services providers (CSPs) such as Microsoft to empower their organisations to achieve more. But despite the strong interest in cloud technology, recent research reveals that the pace of public cloud adoption has been slowed due to common misconceptions about its permissability[1]. However, as set out in this paper, the use of cloud services by Thai FSIs is permitted. In fact, a number of Thai FSIs have already adopted Microsoft cloud services and many are taking active steps towards doing so.

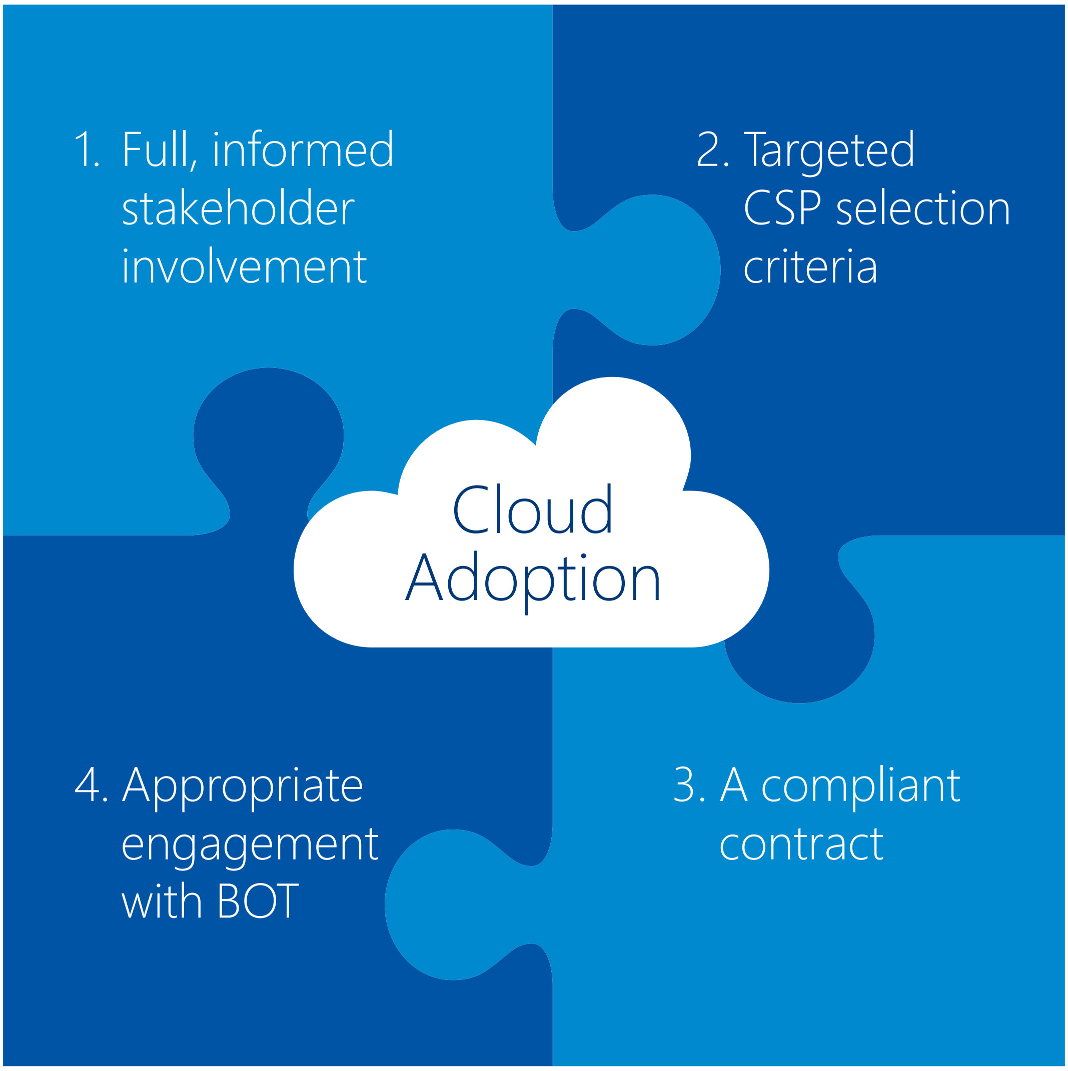
Microsoft's role in the digital transformation

Having helped a number of FSIs move to the cloud in close co-operation with BOT, Microsoft has deep experience in helping to deliver solutions that meet the compliance requirements of the financial services sector in Thailand. We recognise that a CSP needs to actively facilitate compliance through full, transparent, proactive engagement with the FSI community and, on request, with BOT. Through this collaboration over a number of years, Microsoft has developed experience and practical resources to help FSIs move to the cloud in a way that meets the highest compliance, risk and security standards. This paper shares our experience, addresses common misconceptions and steps you through the procurement stages of a cloud adoption, explaining when and how to engage with BOT and what to look out for in the cloud contract itself.

[1] Forrester Consulting, *Ensuring Agility and Trust in a Rapidly Changing Financial Services Market*, published April 2016.

Four essential steps to a successful cloud adoption and deployment

Microsoft's experience of working with FSIs in Thailand has shown that a successful cloud adoption requires four inter-related and inter-dependent steps.



1. Full, informed stakeholder involvement
2. Targeted CSP selection criteria
Cloud Adoption
4. Appropriate engagement with BOT
3. A compliant contract

Step 1: Full, informed stakeholder involvement

A smooth cloud adoption requires informed stakeholder involvement from the outset, with decisions being based on a full understanding of the proposed cloud solution. As a CSP, Microsoft takes responsibility for providing detailed product and service information to assist your key decision makers.

Key actions

1. Build the core stakeholder team and develop the business case

BOT expects the board and chief executive to use clear rules and standards in the decision-making and approval process when selecting a CSP. The FSI should also have evidence that it has taken into consideration the business requirements and the cost/benefit analysis of the solution.

Establish a multi-disciplinary team from day one.

Put your technology and procurement teams in charge of developing the business case, with a focus on the operational and commercial factors driving the decision to adopt cloud services.

Ensure your legal, risk and compliance teams are involved in these discussions from the outset. They'll need to map the proposed solutions against legal and regulatory requirements and build in the necessary time frames to engage with regulators. Many technology projects have been delayed due to involving legal and compliance functions too late.

The board and senior management will typically require early reassurance regarding the business case for cloud services and the oversight, review, reporting and response arrangements with the CSP.

The information and analysis captured in developing the business case will also form a critical part of the CSP selection criteria (see Step 2) and the FSI's engagement with BOT (see Step 4).

2. Obtain detailed product and service information

BOT expects the FSI to understand the CSP's specific service capabilities.

In addition to building the core stakeholder team and understanding the technical solution, the FSI is expected to understand the cloud product being considered and the implications of the use of such cloud product for its particular organisation. In Microsoft's experience, successfully demonstrating this level of knowledge is dependent on the CSP's willingness and ability to share specific product and service information.

3. Understand the technical solutions available

One of BOT's principal expectations is that FSIs must be able to demonstrate a deep understanding of any proposed technical solution. This requires a thorough understanding of the proposed cloud solution and its specific impact on the FSI's business.

Microsoft has prepared a summary of the different types of cloud delivery and deployment models to support your core team and assist with the early scoping of any cloud project.

A summary of cloud delivery and deployment models

Definition

Cloud Computing, Cloud Services or **Cloud** means on-demand network access to a shared pool of configurable computing resources. In other words, cloud services provide FSIs with on-demand access, using a network connection, to information technology or software services, all of which a CSP configures to the needs of the FSI.

Cloud delivery models

1. **Software as a Service (SaaS)**
   Where the CSP makes software applications available to customers.
2. **Platform as a Service (PaaS)**
   Where the CSP provides a computing platform for customers to develop and run their own applications.
3. **Infrastructure as a Service (IaaS)**
   Where the CSP delivers IT infrastructure; e.g., storage space or computing power and may include delivery of the operating system.

Cloud deployment models

1. **Public Cloud**
   Infrastructure is owned and managed by the CSP and not located on the customer's premises. Although each customer's data and services are protected from unauthorised access, the infrastructure is accessible by multiple customers. Given the operational and commercial benefits to customers, public cloud is increasingly seen as the de facto deployment model.
2. **Private Cloud**
   Infrastructure is usually managed by the CSP (but sometimes by the customer). The infrastructure is located either on customer premises or, more typically, on the CSP's premises. The data and services are able to be accessed only by the particular customer.
3. **Community Cloud**
   Serves members of a community of customers with similar computing needs or requirements. The infrastructure may be owned and managed by members of the community or by a CSP. The infrastructure is located either on customer premises or the CSP's premises. The data and services are accessible only by the community of customers.
4. **Hybrid Cloud**
   A combination of two or more of Private Cloud, Public Cloud or Community Cloud.

How Microsoft helps

Microsoft's expert team is on hand to support you throughout your cloud project, from initial stakeholder engagement through to assisting with the BOT engagement process. Our cloud services span all of the above delivery and deployment models. Each of these services is supported with a range of materials, including product fact sheets, online trust centres and checklists, to help FSIs make an informed decision. In addition, we have subject-matter experts available to meet with you and your core stakeholders. They'll provide specific and detailed information on the technical, contractual and practical aspects of your proposed cloud project.

Step 2: Targeted CSP selection criteria

You'll need to develop selection criteria to verify that your proposed CSP can meet the applicable compliance, risk and security requirements. To comply with FSI regulation in Thailand, FSIs should ensure that these criteria include the five listed below.

Recommended selection criteria

1. Technical capability, expertise and experience	**BOT expects the FSI to assess the CSP's technical capability, expertise and experience.** • When it comes to assessing technical capability, industry standards are a useful objective tool for the FSI to use. Although not specifically required by BOT, ISO/IEC 27001[2] and ISO/IEC 27018[3] have become an expected minimum within the industry around the world. • A core aspect of technical capability is the security of the proposed cloud solution. There is now a growing acceptance that cloud services can meet or even exceed the highest on-premises security practices. In addition to measuring compliance with international industry standards as described above, FSIs can measure and evaluate CSPs against the "FSI Safe Cloud Principles", a set of ten principles developed by the Asia Cloud Computing Association[4]. • Expertise and experience in financial services are also important from BOT's perspective. A CSP that has a deep understanding of the FSI regulatory landscape in Thailand and extensive experience of working with FSIs and BOT will be well-placed to proactively support the FSI as part of a successful cloud adoption.
2. Financial stability	**BOT expects the FSI to assess the financial stability of the CSP.** In any technology procurement, the financial strength of the supplier provides comfort as to its ability to provide continuity of operations and to compensate the FSI for any service failures or breaches of contract. Contractual promises carry little weight if the CSP cannot stand behind them financially. Accordingly, the FSI will want to carefully consider the financial position of the CSP. It is common for FSIs to request audited financial statements for at least each of the last three years and CSPs should be in a position to provide these.
3. Business reputation, complaints and litigation record	**BOT expects the FSI to consider the CSP's business reputation and history of complaints and litigation.** • To lay the foundations for a successful long-term relationship you'll need to carefully consider the CSP's longevity and track record in Thailand and around the world • As part of due diligence, ask CSPs to demonstrate their track record through case studies of successful cloud projects they've undertaken with FSIs in Thailand and around the world. A competent CSP will have all of the required information readily available.
4. Culture and expertise with FSIs	**BOT expects the FSI to work with CSPs who have FSI-specific expertise and an understanding of their culture and requirements.** • Ask the CSP whether they have a specific cloud compliance program for FSIs, designed to support collaboration and compliance with regulatory requirements. • Confirm to what extent the CSP has previously engaged with BOT on cloud adoption in Thailand.

[2] http://www.microsoft.com/en-us/TrustCenter/Compliance/iso-iec-27001

[3] https://www.microsoft.com/en-us/TrustCenter/Compliance/iso-iec-27018

[4] https://www.asiacloudcomputing.org/images/research/2014_-_Safe_Cloud_Principles_for_FSI.pdf

Culture and expertise with FSIs continued	• Ensure the CSP can demonstrate an understanding of and solution compatibilty with FSI culture and requirements. • In Microsoft's experience, being able to demonstrate all of the above factors will help facilitate a smoother process with BOT and a more successful cloud adoption.
5. Capacity to adjust to change and developments	**The FSI landscape in Thailand is changing quickly and BOT expects FSIs to consider the capacity of the CSP's solution to adjust to rapid change and developments.** • First, it makes practical sense that the cloud solution is readily scalable to meet the FSI's requirements, as they scale up or scale down. Scalability is of course a core benefit of cloud technology. • Second, CSPs need to be able to demonstrate an ability to keep up with an ever-changing risk and regulatory environment. A CSP should be assessed against its ability to be current with international standards. ISO will soon release its 19086 standard for cloud service level agreements and a CSP's ability to meet this standard will no doubt be viewed favourably. Similarly, the FIDO Alliance is working with many of the world's leading banks, payment providers and government regulators to develop new device-to-cloud authentication standards based on public key encryption and flexible biometrics. FSIs should ensure that their CSPs have active, well-funded programs to implement such new standards in a timely and effective manner.

How Microsoft helps

Based on our close working relationship with FSIs and BOT, Microsoft confirms its ability to meet all of the criteria specified above. BOT is already very familiar with Microsoft's offerings, which should make for a much smoother engagement process. We're also confident that our understanding of the FSI environment is market-leading in Thailand and around the world, with a proven track record of successful cloud deployments that comply with financial services regulatory requirements and global security and risk standards. Microsoft has large dedicated teams consisting of hundreds of lawyers, software engineers and policy experts whose sole mission is to identify and implement new cloud security and privacy standards across Microsoft's portfolio of cloud services. We also have a long track record of being one of the first CSPs to implement major new cloud standards, including recent or forthcoming examples such as ISO/IEC 27018 and ISO/IEC 19086.

Microsoft's financial services compliance program extends the compliance features of Microsoft Azure, Office 365, Microsoft Dynamics and Intune to provide FSIs with deeper, ongoing engagement with Microsoft, including:

- Customer access to additional information from Microsoft subject matter experts (SMEs).
- Access to additional compliance-related information developed by Microsoft over time.
- The opportunity for one-to-one discussions with Microsoft's third-party auditors.
- Participation in webcast walk-throughs of ISO and SSAE audit reports with Microsoft SMEs.
- The ability to view the Microsoft control framework for the cloud services.
- The opportunity to recommend future additions to the audit scope of the cloud service.
- Access to detailed reports of external audit penetration tests conducted on the cloud service.

Step 3:
A compliant contract

BOT regulation and guidance stipulate mandatory terms to include in a binding cloud contract with your CSP. These are listed below with explanations to assist you.

Terms to address in your contract

1. Service description	The contract should clearly set out the type of service, availability and reference to the location of facilities.
2. Responsibilities of the parties	The contract should clearly set out the respective responsibilities of both parties in relation to data protection, service delivery, payment and liability.
3. Internal control and monitoring	The contract should refer to cloud control systems, including performance and incident-reporting obligations. It should also include a requirement on the CSP to notify the FSI of any significant change that may affect the CSP's compliance with the contract.
4. Risk management	The contract should include details of applicable risk management processes and procedures.
5. Availability	The contract should include a service level agreement (SLA) specifying the service standards (such as service availability percentages).
6. Business continuity planning	The contract should include plans for business continuity and dealing with emergencies.
7. Inspection and performance monitoring	The contract should address ways in which the CSP may be inspected and its performance monitored.
8. Fees	The contract should include details of the fees payable for the services.
9. Duration	The contract should include details of the duration, termination provisions, rights of renewal and amendment of the contract.
10. Service transition	The contract should anticipate end of service.
11. Service disruption and dispute resolution	The contract should set out the responsibilities of the parties if there is a service disruption and include a process for resolving disputes, with terms addressing liability and compensation.

12. Data security and ownership	The contract should include provisions on security, confidentiality, data access and ownership. This includes setting out the procedures for data protection, receipt, transmission and storage as well as the consequences if data is disclosed to third parties. The CSP should be required to separate both the FSI's and its customers' data from that of its other customers. Logical separation is acceptable.
13. Subcontractors	The contract should include provisions to ensure that any CSP subcontractor is bound by the key contractual commitments. Ultimate responsibility for performance should rest with the CSP. Although not a contractual requirement, BOT states in its guidance that the FSI may choose to provide in the contract that the CSP must inform the FSI or obtain its permission before undertaking subcontracting or changing subcontractors.
14. Overseas facilities	The use of facilities and data centres outside of Thailand is permitted. The contract should include any additional provisions that are necessary due to the solution being provided from outside of Thailand. Although BOT guidance does not expand upon what these additional provisions should include, Microsoft's experience is that robust contractual protections on matters such as data security and confidentiality should be sufficient to address this requirement.
15. Restrictions to CSP's other customers	A contract between an FSI and CSP must not limit the CSP's ability to provide the same services to any other FSIs, including competitors.
16. Compliance with laws	The contract should require the CSP to comply with all relevant laws and regulations.
17. Audit	The contract should include provisions enabling BOT to inspect the CSP performance.

How Microsoft helps

Microsoft understands the value and importance of binding contractual commitments. To make the contract review process easier for you, Microsoft provides a checklist of the contractual terms that BOT expects, and explains where they are addressed in the Microsoft contract. This is available from your Microsoft contact upon request. This checklist gives you the confidence that your contract with Microsoft meets the applicable regulatory requirements.

Step 4: Appropriate engagement with BOT

In Microsoft's experience, a successful cloud adoption requires open engagement with BOT, not just by the FSI but also by the CSP. To assist you in streamlining this process, this section provides further detail on the BOT regulatory environment with practical suggestions.

Overview of the FSI Regulatory Environment in Thailand

Who is the regulator?	Bank of Thailand (BOT) is the primary regulator, although the Ministry of Finance also plays an important role.
Are cloud services permitted?	• Yes. BOT has specific guidelines that anticipate and permit the use by regulated entities of outsourced IT services such as cloud computing. • Microsoft has partnered with a number of FSI customers who have satisfied BOT's requirements and successfully deployed Microsoft cloud services in Thailand.
What regulations and guidance are relevant?	• BOT Notification Sor Nor Sor 8/2557 (Outsourcing Policy) • BOT Notification Sor Nor Sor 6/2557 (IT Outsourcing Policy)
How would the use of Microsoft cloud services be classified?	Our experience is that the use of Microsoft cloud services will in most cases fall into "material, non-strategic" or "non-material" activities (under the Outsourcing Policy) and/or "critical" activities (under the IT Outsourcing Policy). These classifications are also shown in the summary set out in the Appendix to this paper. Although not a requirement, FSIs are advised to consult with the BOT prior to making a decision as to materiality of the activities. **Outsourcing Policy** **Material** activities are activities that if disrupted would greatly affect the FSI. Within material activities are two separate groups: 1. **Strategic** functions are the decision-making functions of the FSI's business and which may directly affect the capital, income or profit of the business. These functions cannot be outsourced other than in very limited circumstances and even then only with approval from the BOT on a case-by-case basis. 2. **Non-strategic** functions are the functions unrelated to the strategy of the FSI but which support the strategy, such as finance and accounting. An approval is required if the services are provided from outside of Thailand. **Non-material** activities are activities that support the operation of the FSI, including activities such as document storage. If activities are "non-material" under the Outsourcing Policy, FSIs do not need to notify the BOT unless the activities are also "critical" under the IT Outsourcing Policy. **Low-risk** activities are activities such as cleaning services and are therefore not relevant for the purposes of Microsoft cloud services. **IT Outsourcing Policy** **Critical** IT outsourcing means IT outsourcing that may cause risk and widespread effect on the FSIs, or other damage or incidents. Examples of critical IT outsourcing are core banking, data centre, and network. It is very likely that the use of Microsoft cloud services would be considered "Critical". No approval is required but the FSI must give at least 30 days' notice to BOT prior to the commencement of, or change to, the outsourcing. **Other** IT outsourcing means IT outsourcing other than "Critical".

Are data transfers outside of Thailand permitted?	Yes.
Is regulatory approval required?	• No, unless the services constitute a "material, non-strategic" activity under the Outsourcing Policy, in which case BOT approval is required for the use of offshore data centres. • Where the services constitute a "Critical" IT outsourcing under the IT Outsourcing Policy, 30 days' advance notice to BOT is required. • Where the services constitute a "material, strategic" activity under the Outsourcing Policy, outsourcing is not permitted, except on a case-by-case basis as approved by BOT.
When should the FSI engage with BOT?	Aside from the approval and notice requirements above, the FSI should consult with BOT on the "materiality" of the proposed activities to be outsourced as soon as possible.
Are there particular forms or questionnaires the FSI needs to complete?	• Yes. The Outsourcing Policy contains a very short questionnaire for FSIs undertaking outsourcing to complete. • The form does not need to be submitted where the outsourcing falls into the category of "low-risk" or "non-material" activities, but FSIs are advised to consult with BOT to ensure that it is not of the view that the activities fall into the category of "material" activities. • The form needs to be submitted by FSIs together with a letter explaining the intention to outsource certain services. • BOT states that FSIs are able to submit additional information and adjust the method of presentation of the information (for example, using diagrams) if they wish. • All forms submitted to BOT must be kept on file at the FSI as BOT has authority to conduct on-site inspections of all activities of the FSI and its files.

How Microsoft helps

Microsoft has worked in close co-operation with BOT and has a detailed understanding of the regulatory framework and process. Issuing this paper is part of Microsoft's commitment to its FSI customers to help them navigate and comply with the regulatory framework as it applies to cloud services.

To streamline the process, Microsoft has developed a set of checklists that build on the mandatory BOT questionnaire by mapping to the regulatory requirements in Thailand. These checklists are used regularly by FSIs as part of their discussions with BOT and are available from your Microsoft contact upon request.

Appendix: Outsourcing classification summary

FSIs in Thailand are permitted to adopt cloud. The specific rules that apply depend on how the use of cloud services is classified. In the summary below, shading indicates how the definitions are likely to apply to Microsoft cloud services. More detail on each of the relevant classifications is contained in Step 4 of this paper.

How are different outsourced activities classified?	Outsourcing Policy				IT Outsourcing Policy	
	Material Activities		Non-Material Activities	Low-risk Activities	Critical IT Outsourcing	Other IT Outsourcing
	Strategic Functions	Non-Strategic Functions				
Outsourcing allowed?	No	Yes	Yes	Yes	Yes	Yes
Notification required?	N/A	No	No	No	Yes At least 30 days notice	No
Is approval required?	N/A	Yes If data being moved offshore	No	No	No	No

Microsoft

Find out more

Trust Center
microsoft.com/trustcenter

Service Trust Portal
aka.ms/trustportal

Financial Services Amendment
Contact your Account Manager

Online Services Terms
microsoft.com/contracts

Compliance program for regulated financial services customers
Contact your Account Manager

Service Level Agreements
microsoft.com/contracts

SAFE Handbook
aka.ms/safehandbook

This document is provided "as is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes. This paper is not intended to be a comprehensive analysis of all regulations and their requirements, nor is it legal advice; rather it is intended to be a summary and to provide guidance to FSIs in Thailand on the types of issues they should consider. Microsoft, the Microsoft logo, Azure, Dynamics and Office 365 are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.