Navigating your way to the cloud

Microsoft's response to the MAS Outsourcing Guidelines and the ABS Cloud Implementation Guide

Microsoft

Contents

Foreword: Navigating your way to the cloud

On 27 July 2016, the Monetary Authority of Singapore (MAS) issued an updated version of the MAS Guidelines on Outsourcing (Guidelines), setting out MAS's expectations for outsourcing by financial institutions in Singapore.

The Guidelines have been rightly hailed as a major step forwards for the financial services industry in Singapore. They acknowledge that, to adapt and compete, financial institutions need to adopt new technologies. Importantly, the Guidelines are unequivocal in emphasising that financial institutions can use cloud services, including public cloud, and that they stand to benefit from doing so.

Shortly after the release of the Guidelines, the Association of Banks in Singapore (ABS) introduced the ABS Cloud Implementation Guide (ABS Guide), a non-binding practical guide designed to assist banks in Singapore as they implement cloud services.

Microsoft welcomes both of these developments. As a leading provider of cloud services to financial institutions in Singapore, we have witnessed the digital transformation that is empowering financial institutions to achieve more.

We have, however, noticed that despite widespread recognition of the benefits of cloud, the pace of cloud adoption in Singapore has been slowed by some misconceptions about the permissibility of cloud.

By issuing a clear "green light" for cloud and suggesting practical steps for cloud adoption, the Guidelines and ABS Guide clarify those misconceptions and open the door for financial institutions to benefit from cloud services in a way that addresses all applicable risk management and compliance requirements.

We are pleased to have participated in the conversations with MAS and ABS that led to these positive developments. This paper is a further contribution to those conversations. In it, we summarise the key provisions of the Guidelines and ABS Guide, provide a detailed response to the key issues raised and comment on how Microsoft can assist financial institutions to ensure that their adoption of cloud services meets the new recommendations and guidelines.

We hope you find our response useful and we look forward to continuing the cloud conversation with you.

Alberto Granados
Vice President
Sales, Marketing &
Services Group,
Microsoft Asia Pacific

Andrew Cooke
Regional Director – Corporate,
External & Legal Affairs
Microsoft Asia Pacific & Japan

About this Paper

Overview

This paper is designed to:

- help financial institutions understand the key issues raised by the Guidelines and the ABS Guide as they apply to cloud services;
- set out Microsoft's interpretation of (and response to) each of these key issues, based on its experience of working with financial institutions in Singapore and around the world; and
- provide financial institutions with information about how Microsoft helps facilitate compliance with the new guidelines.

This paper is not designed to be an exhaustive list of the compliance features of Microsoft's cloud services. For this purpose, Microsoft has developed checklists that directly map its cloud services and contractual offerings against the applicable guidelines. These are available from your Microsoft contact upon request. More detailed product and service information is available via the Microsoft Trust Center, the Service Trust Portal.

How to use this paper

This paper is divided into two parts:

Part 1

Microsoft's response to the Guidelines

Part 2

Microsoft's response to the ABS Guide

Part 1: Microsoft's Response to the MAS Guidelines on Outsourcing

About the Guidelines

How the Guidelines apply

The new Guidelines took effect immediately from publication on 27 July 2016 and apply to all regulated financial institutions in Singapore, including banks, insurance companies and trust companies. These financial institutions are expected to conduct a self-assessment of all outsourcing arrangements against the Guidelines by 27 October 2016 and rectify deficiencies identified by 27 July 2017.

As at the date of publication of this paper, the updated MAS Notice on Outsourcing (Notice) has not been issued. Whilst the Guidelines provide a set of best practices, the Notice will specify a set of minimum requirements. MAS has confirmed that it will issue the Notice at a later date.

How the Guidelines are structured

Sections 1 and 2 of the Guidelines set out various preliminary matters, including an introduction to the Guidelines and explanation of how they apply to financial institutions. We will not comment on these preliminary sections since they simply set the tone for the more detailed guidelines that follow.

Section 3 of the Guidelines is a list of defined terms, including an important new definition of "customer information".

Section 4 of the Guidelines explains how financial institutions should engage with MAS in relation to their outsourcing arrangements, including how to demonstrate observance of the Guidelines and when to notify MAS.

Section 5 of the Guidelines emphasises the responsibility of the board and senior management to implement a sound risk management framework. It also sets out the issues a financial institution should consider when it is evaluating risk.

Section 6 of the Guidelines is important because it sets out MAS's position on cloud computing. This section describes the benefits that loud computing brings to financial institutions and gives a green light for the use of cloud services (be they public, private or hybrid cloud) by financial institutions.

Annexes 1 and 2 provide helpful clarification as to the definitions of "outsourcing arrangements" and "material outsourcing arrangements" and Annex 3 sets out the template form of the outsourcing register that financial institutions should maintain. We will not comment on these Annexes, other than in our responses to the definitions and guidelines to which these Annexes relate.

Updated Definitions

Section 3: Annex 1 and Annex 2 of the Guidelines

The Guidelines bring welcome clarity to various important definitions and concepts in outsourcing. In this section, we comment on the key changes to the definitions that are introduced by the Guidelines.

"Institutions"

Section 3 of the Guidelines

The revised Guidelines include a new definition of "institutions", which covers all financial institutions defined under section 27A of the Monetary Authority of Singapore Act. This includes licensed financial advisers, stored value facilities holders, registered insurance brokers, licensed trust companies, registered fund management companies, exempt corporate finance advisers and moneychangers.

We welcome this clarification, which will help to set a level playing field for all categories of financial institutions in Singapore.

"Customer information"

Section 3 of the Guidelines

MAS has clarified that "customer information" does not include information that is "public, anonymised, or encrypted in a secure manner such that the identities of the customers cannot be readily inferred".

This is an important clarification from MAS, since it reflects the view that anonymising or encrypting information can reduce risks associated with its storage and processing. In practical terms, it means that any of the provisions of the Guidelines that apply to "customer information" do not apply to information that is public, anonymised or securely encrypted. This is particularly important when assessing whether an outsourcing is "material", as described below. As a company that has long implemented strong encryption controls to protect information in the cloud, we welcome this refined definition, which reduces the burden on financial institutions and reflects the lower risks that are attached to securely encrypted information. More information about the encryption controls enabled by Microsoft cloud services can be found in the Microsoft Trust Center.

"Material outsourcing arrangement"

Section 3 of the Guidelines

The Guidelines expand the definition of "material outsourcing arrangement". This definition is important, since certain provisions of the Guidelines apply only to material outsourcing arrangements (namely, obligations to perform annual reviews, mandatory contractual clauses addressing audit rights and an obligation to ensure that outsourcing outside of Singapore does not affect MAS's supervisory efforts).

The first change is that an outsourcing arrangement will be "material" if a service failure or breach has the potential to materially affect the institution's ability to manage risk and comply with applicable laws and regulations. This further emphasises that sound risk management and compliance with laws are core principles of the Guidelines. The second change is that an outsourcing will be "material" if it involves customer information and, in the event of any unauthorised access or disclosure, loss, or theft of customer information, may have a material impact on an institution's customers. As noted above, the definition of "customer information" expressly excludes securely encrypted information.

These changes will assist financial institutions to help ensure that their outsourcing arrangements are correctly categorised and that the correct controls are put in place. The reference to customer information, read alongside the new definition (described above), is particularly important. In our view, if a cloud solution applies secure encryption then the use of that cloud solution is unlikely to constitute a "material outsourcing arrangement". This is because secure encryption reduces risks associated with the storage and processing of that information. However, financial institutions should be mindful that an outsourcing arrangement can potentially constitute a "material outsourcing arrangement" (even if encryption is used) if a service failure or breach has the potential to materially affect the institution's ability to manage risk and/or comply with applicable law and regulations.

Engagement with MAS

Section 4 of the Guidelines

MAS does not require prior approval or notification in relation to outsourcing arrangements. However, it does expect financial institutions to be ready to demonstrate to MAS how they are compliant. MAS also expects financial institutions to notify MAS of adverse developments. In this section, we comment on the new engagement process and how Microsoft works with financial institutions and MAS to help ensure a successful engagement.

Observance of the Guidelines

An institution should be ready to demonstrate to MAS its observance of the Guidelines

Section 4.1 of the Guidelines

Under the previous Guidelines, financial institutions were expected to notify MAS prior to entering into any material outsourcing arrangements. They were also expected to complete a detailed technology questionnaire. These provisions have been removed. Instead, financial institutions should complete a simple outsourcing register in the form set out in Annex 3 of the Guidelines.

This will streamline the process and therefore make new technology adoption significantly easier. However, whilst the requirement to complete a questionnaire and pre-notify no longer applies, Microsoft believes it is incumbent on service providers and financial institutions to work together to help ensure compliance. With that in mind, Microsoft has developed a range of resources to help financial institutions assess and communicate relevant information about Microsoft cloud services, including a checklist that can be used to measure your institution's compliance with the Guidelines. This is available from your Microsoft contact upon request.

Notification of Adverse Developments

An institution should notify MAS as soon as possible of any adverse development

Section 4.2 of the Guidelines

Although there is no requirement for pre-notification of each outsourcing arrangement, financial institutions are still expected to notify MAS as soon as possible of any adverse development. An "adverse development" includes an event that could potentially lead to prolonged service failure or disruption, or any breach of security or confidentiality of the financial institution's customer information.

This will be an important part of ensuring that MAS is able to exercise its powers of regulatory oversight and we believe that service providers will have a key role to play. First, we believe that service providers should have robust incident management processes. To support this, the Microsoft Security Incident Management (SIM) team, which is responsible for assessing and mitigating computer security incidents, will promptly respond to potential security issues when they occur. Second, we believe that service providers should make binding commitments to notify customers if they become aware of any unlawful access, loss, disclosure, or alteration of customer data, and we confirm that Microsoft's contractual terms provide for this. Finally, we believe that service providers should offer tools that enable ongoing examination, verification, access and control of the cloud services, so that institutions can track performance. Microsoft's tools include the Office 365 Management Activity API and the Microsoft Azure Active Directory.

Risk Management Practices

Section 5 of the Guidelines

Although the Guidelines streamline the process for adopting cloud, they do not represent a lowering of expected standards when it comes to managing risk. It is now more important than ever that financial institutions work with providers who have the right policies and processes in place to help them manage risk. In this section, Microsoft comments on the risk management requirements imposed by the Guidelines and explains how its services can support a sound risk management framework.

Overview

MAS will review the institution's implementation of the Guidelines

Section 5.1 of the Guidelines

MAS is clear that its streamlined approach does not represent a lowering of expected standards and that it will continue to review the institution's implementation of the Guidelines, the quality of its board and senior management oversight and its governance, internal controls and risk management processes.

We discuss each of these themes further below.

Responsibility of Board and Senior Management

The board and senior management should be fully aware of and understand the risks arising from outsourcing

Section 5.2 of the Guidelines

MAS expects the board and senior management of the institution to play pivotal roles in ensuring that the institution has a sound risk management culture and environment. They also expect the board and senior management to be fully aware of and to understand the risks arising from outsourcing. The responsibilities of the board, senior management and the personnel to whom responsibilities are delegated are all set out in detail in section 5.2 of the Guidelines.

Our experience is that the most successful adoptions of new technology depend on the involvement of stakeholders from across the institution. The best way to achieve this is to put in place a broad, multidisciplinary team from the outset. We have also learned that decisions must be based on all of the key stakeholders, including the board and senior management, having a full understanding of the proposed cloud solution. In our view, the service provider should play its part by providing the information needed to ensure that all stakeholders have a clear understanding of the technology solution. To help institutions reach the required knowledge threshold in relation to Microsoft cloud services, we provide various information tools. One of these is the SAFE Handbook, which follows a five-step, vendor-neutral process to help institutions evaluate the risks of all potential options.

Evaluation of Risks

The board and senior management should be fully aware of, and understand, the risks arising from the outsourcing

Section 5.3 of the Guidelines

MAS expects the board and senior management to be aware of and assess all risks arising from the outsourcing. There are various aspects to this, as described in this section.

Under section 5.3.1(a), the institution should identify the role of the outsourcing in the overall business strategy and objectives of the institution.

In our experience, the best way to achieve this is to appoint a skilled team that is able to collaborate and provide an institution-wide view, as described in section 5.2 above. We also believe that helping to identify the role of the cloud project in the overall strategy of the institution's IT objectives is something that the service provider can assist with.

Evaluation of Risks continued

Under section 5.3.1(b), the institution should perform comprehensive due diligence on the nature, scope and complexity of the outsourcing arrangement.

This is the foundation of any new technology adoption. It is important that the service provider proactively facilitates the due diligence. Microsoft provides a range of tools designed to facilitate due diligence, including product fact sheets, the Microsoft Trust Center and checklists, all designed to ensure that financial institutions are able to make an informed decision.

Under section 5.3.1(c), the institution should assess the service provider's ability to provide a high standard of care in performing the outsourced service.

Section 5.4 of the Guidelines goes on to provide much more detail about service provider assessment and Microsoft's response to section 5.4 is set out below.

Under sections 5.3.1(d) and (e), the institution should analyse the impact of the outsourcing arrangement on the overall risk profile and analyse the institution's group aggregate exposure.

In our experience, informed consideration by a multidisciplinary team, drawing on information and tools provided by the service provider, is essential to understanding the impact and overall risk profile and exposure. Please also note our response to section 5.2 above.

Under section 5.3.1(f), the institution should analyse the benefits of outsourcing against the risks that may arise.

We agree that any new technology adoption should include a risk and benefit analysis. It is an increasingly accepted view that a failure by institutions to embrace new technologies may in itself actually increase risks and jeopardise competitive advantage. With this in mind, Microsoft believes that when the board and senior management are considering any risks associated with adopting new technology, it is appropriate that they should also factor the risk of maintaining the status quo, which could mean relying on legacy on-premises infrastructure that may not have kept pace with security and compliance requirements.

Under section 5.3.2, the institution should carry out risk evaluations when entering into a new outsourcing arrangement and periodically in relation to existing outsourcing arrangements.

This is important, since compliance does not end with signature of the contract. For this reason, we continue to make available Microsoft information tools and a team of subject matter experts throughout the term of the cloud contract.

Risk Management Practices

Assessment of Service Providers

The financial institution should assess all relevant aspects of the service provider

Section 5.4 of the Guidelines

MAS expects the institution to assess all relevant aspects of the service provider in considering, renegotiating or renewing the outsourcing arrangement. This should include an assessment of the service provider's:

- business reputation and financial strength and resources, including its ethical and professional standards;
- ability to meet obligations under the contract;
- experience and capability;
- corporate governance, business reputation and culture, compliance, and pending or potential litigation;
- security and internal controls, audit coverage, reporting and monitoring environment;
- risk management framework and capabilities, including technology risk management and business continuity risk management;
- disaster recovery arrangements and track record;
- reliance on and success in dealing with subcontractors;
- insurance coverage;
- external environment (such as the political, economic, social and legal environment of the service provider's jurisdiction); and
- ability to comply with applicable laws and regulations and associated track record.

The Guidelines also suggest that employees of the service provider should be assessed to meet the institution's hiring policies for the role they are performing. Finally, the Guidelines suggest that all due diligence is documented and re-performed.

We support the inclusion of all of these factors in the Guidelines. We believe that, ultimately, it is incumbent on the service provider to assist you with compliance by demonstrating its ability to address each of these factors. To assist with this, Microsoft has developed checklists for its core cloud products that you can use to measure Microsoft and our services against each of the factors described above. In the absence of an MAS-mandated questionnaire, Microsoft's checklists can be used to help document compliance on an ongoing basis.

Outsourcing Agreement

Contractual terms governing the arrangements with the service provider should be carefully and properly defined in written agreements

Section 5.5 of the Guidelines

MAS emphasises the importance of a robust contract. MAS expects all of the following to be addressed: the scope of the outsourcing arrangement; performance, operational, internal control and risk management standards; confidentiality and security; business continuity management; monitoring and control; audit and inspection; notification of adverse developments; dispute resolution; default termination and early exit; and subcontracting and applicable laws.

This brings useful clarity to the terms that should be included in any cloud contract. To make the contract review process easier for you, Microsoft provides a contract checklist. This lists the contractual terms that MAS expects to be covered and explains where these terms are addressed in the Microsoft contract.

Risk Management Practices

Confidentiality and Security

Financial institutions should ensure that the service provider is able to protect the confidentiality and security of customer information

Section 5.6 of the Guidelines

The Guidelines state that "public confidence in institutions is a cornerstone in the stability and reputation of the financial industry". MAS emphasises the importance of ensuring that the service provider's security policies, procedures and controls enable the institution to protect confidentiality and security of customer information.

At Microsoft, we believe that confidentiality and security of our customers' information are the core pillars of a trusted cloud environment. With this in mind, Microsoft's cloud services have been engineered with a focus on data confidentiality, security and compliance:

1. Microsoft complies with international standards. Microsoft cloud services meet a broad range of national, international, regional and industry-specific compliance standards, such as MTCS SS 584 (Tier 3) developed by the Infocomm Development Authority of Singapore (IDA, now the Infocomm and Media Development Authority of Singapore or IMDA), ISO/IEC 27001, ISO/IEC 27018, SOC 1 and SOC 2. Independent third-party auditors review Microsoft's adherence to the strict controls set out within these standards annually.
2. Security is built into the Microsoft cloud from the outset and each phase of development. This starts with the Microsoft Security Development Lifecycle (SDL), a mandatory development process that incorporates privacy and security requirements into every phase of the development process. Microsoft also uses various technological safeguards such as encrypted communication of data "at rest" and "in transit" to safeguard customer information.
3. Data that resides in Microsoft's cloud services belongs to the customer, not Microsoft. Microsoft's contractual terms are clear that the financial institution retains ownership of all data stored in the Microsoft cloud. Customer data is not used for unrelated purposes such as advertising.

You can access more detailed information about the robust confidentiality and security at the core of each Microsoft cloud service in the Microsoft Trust Center.

Business Continuity Management

The institution should ensure that its business continuity is not compromised

Section 5.7 of the Guidelines

MAS expects the institution to make sure that it can continue to conduct its business with integrity and competence in the event of a service disruption. In particular, financial institutions should make sure that the service provider has satisfactory business continuity plans in place and proactively seek reassurance from the service provider as to the state of its business continuity preparedness.

We view these principles as helpful and appropriate. Successfully managing business continuity risk sits alongside managing confidentiality and security risk. In this respect, Microsoft believes that international standards can help. The Microsoft Enterprise Business Continuity Management (EBCM) program is based on the Disaster Recovery Institute International Professional Practice Statement and the Business Continuity Institute (BCI) Good Practice Guidelines. Our EBCM program applies across Microsoft's business and drives the development of business continuity plans for our individual cloud services in line with industry best practices. In addition to our own rigorous program, we also provide mechanisms for customers to control backup and recovery themselves.

Business Continuity Management continued

MAS expects institutions to ensure that plans or procedures are in place to address adverse conditions on termination such that the institution will be able to continue business operations.

It is important that financial institutions retain flexibility and choice in respect of their outsourcing arrangements. A financial institution should have contingency plans and consider its exit management arrangements when entering into any outsourcing arrangement. To facilitate this, we made it simple for customers to transition from Microsoft cloud services to alternative arrangements and stand-alone, non-cloud products with similar functionality can be acquired as substitutes. For example, Microsoft makes available a full suite of on-premises Office products that can be used in place of Office 365 when necessary.

MAS expects that all records and documents previously given to the service provider should be promptly removed from the possession of the service provider, deleted or rendered unusable.

It is important that, at the end of the term of a contract, the service provider can be relied on to return and delete all customer data. When you exit a Microsoft cloud service or your subscription expires, we contractually commit to delete your data after giving you a period of 90 days to export your data or renew your subscription. As part of our ISO/IEC 27001 certification, we are certified to have appropriate data deletion practices and are audited against these controls by independent third parties on an annual basis.

Finally, MAS expects regular, complete and meaningful business continuity plan testing.

This is essential and it is another feature that is built into Microsoft's offering from the outset. The Microsoft Business Continuity Planning (BCP) team conducts testing of the business continuity plans and recovery plans at least annually and issues identified during testing are noted and managed to a resolution.

Monitoring and Control of Outsourcing Arrangements

Institutions should monitor and control the outsourcing arrangement on an ongoing basis

Section 5.8 of the Guidelines

MAS expects financial institutions to establish a structure for the management and control of their outsourcing arrangements. MAS acknowledges that the appropriate structure will vary depending on the project.

In our view, institutions will, to a large extent, be dependent on the service provider to assist with and support the necessary monitoring and control. At Microsoft, transparency is one of the core four pillars of our "Trusted Cloud" strategy. Service health of Microsoft cloud services can be monitored through publicly available sources, which helps you assess our performance against our binding, financially backed Service Level Agreements. We also provide service-specific features to assist with ongoing monitoring, providing users with a high level of visibility into user administration, system, and policy actions and events from your Microsoft activity logs. Contractually, we commit to notifying you of security incidents that affect your data, so that you are empowered to take any further mitigation or remediation steps that you deem appropriate.

Risk Management Practices

Audit and Inspection

The arrangements should not interfere with the ability of the financial institution to effectively manage its activities or for MAS to carry out its supervisory functions or objectives

Section 5.9 of the Guidelines

Institutions are expected to ensure that any outsourcing arrangements do not interfere with their ability to manage their activities or for MAS to carry out its supervisory functions and objectives. The Guidelines also include two clarifications concerning the scope of audit rights. The first clarification is that the need to include contractual audit rights in favour of MAS and the service provider applies only to "material outsourcing arrangements". The second clarification is that audits may be carried out by a range of parties and need not necessarily be carried out by the institution itself. MAS confirms that audits may be carried out by the institution's internal or external auditors, the service provider's external auditors and/or by agents appointed by the institution. Copies of all audit reports should be made available to MAS.

We welcome these clarifications and agree that the use of cloud services should not interfere with the institution's ability to maintain effective control over its outsourced operations or its ability to facilitate MAS's supervisory functions. We believe that binding contractual commitments from the service provider to permit monitoring and inspection of the cloud services are key to ensuring that oversight, control and supervision are not affected. It is for this reason that Microsoft extends contract terms that provide the regulator with a right to examine, monitor and audit Microsoft's cloud services. Of course, for arrangements that are not "material", a full audit is unlikely to be necessary or proportionate to the risks and institutions may not always wish to carry out an audit themselves. Every year, we undergo third-party audits by internationally recognised auditors as an independent validation that we comply with our policies and procedures for security, privacy, continuity and compliance. Copies of the reports are made available at the Service Trust Portal.

Outsourcing outside of Singapore

As part of its due diligence on the service provider, the institution should consider the location from which the service provider will provide the services

Section 5.10 of the Guidelines

MAS does not impose any prohibitions on the use of service providers located outside of Singapore. In the case of cloud computing, this means that the use of data centres outside of Singapore is permitted. Nonetheless, MAS is clear that institutions should, if services are provided from outside of Singapore, assess the applicable government policies, political, social and economic conditions, legal and regulatory developments and the institution's ability to effectively monitor the service provider. Some additional considerations apply to material outsourcing arrangements, where the expected standards are higher. These include taking steps to protect confidentiality and the freedom of MAS to exercise its regulatory oversight. Institutions are also expected to notify MAS if any overseas authority seeks access to customer information.

The flow of data across borders is essential in this digital age. However, an institution must have visibility as to where its data will be hosted so that it can undertake the necessary due diligence and feel comfortable with the locations used. It is with these specific considerations in mind that Microsoft is committed to being transparent with the location of its data centres, which are selected based on a detailed set of regulatory, political, socio-economic, geological and environmental factors and are published on the Microsoft Trust Center.

We believe that the institution is best placed to respond to any request for data and, as such, we undertake to re-route any such request to the institution, unless we are legally prohibited from doing so. This means that in the event that an authority seeks to access customer data, an institution will still be able to notify MAS.

Cloud Computing: "A Green Light for Cloud in Singapore"

Section 6 of the Guidelines

For the first time, the Guidelines include specific guidance on the use of cloud services. The Guidelines are clear that the use of cloud services by financial institutions is permitted, whether private, public or hybrid cloud. Microsoft welcomes the forward-looking approach taken by MAS on this subject and responds to this important section of the Guidelines below.

Cloud offers "a number of advantages"

Sections 6.1 to 6.4 of the Guidelines

The Guidelines outline the many benefits of cloud services, including economies of scale, cost savings, access to quality service administration, uniform security standards, scalability and agility. MAS also acknowledges that the distributed nature of cloud series may enhance system resilience during location-specific disasters or disruptions.

It is important that MAS has acknowledged the benefits of cloud and thereby dispelled the myth that MAS does not approve of cloud. By emphasising these benefits, the Guidelines will help financial institutions with their decision-making at a time when they are reassessing their technology strategies to adapt to changes in the industry. We regard this move as part of a wider shift in approach, evidenced by other positive developments such as the appointment of an MAS Chief Fintech Officer, the Fintech Sandbox Initiative and the inaugural MAS Fintech Festival of November 2016.

Different cloud models provide for "distinct operational and security trade-offs"

Section 6.3 of the Guidelines

MAS notes that cloud service deployment may take the form of private, public or hybrid cloud and suggests that the different cloud models provide for distinct operational and security trade-offs.

In our view, a particular cloud deployment model need not involve a trade-off in security. It is important to note that public cloud services are not inherently riskier than on-premises, community or private cloud alternatives. The risks associated with cloud services should be assessed based on the actual service provider and its ability to provide a robust and secure cloud environment, rather than purely on the cloud deployment model.

Cloud is just another form of outsourcing

Sections 6.5, 6.6 and 6.8 of the Guidelines

MAS considers that cloud services is "a form of outsourcing". No additional rules apply to cloud computing, and institutions are expected to apply the same risk management framework as they would to any other technology procurement.

This is a much-needed clarification. Despite the uptake of cloud services by financial institutions in Singapore, prior to the Guidelines there was a misconception that the use of cloud was restricted or even prohibited. The Guidelines now leave no doubt that the use of cloud services by financial institutions is permitted.

In multi-tenanted solutions, strong physical or logical controls should be applied

Section 6.7 of the Guidelines

MAS expects financial institutions to ensure that the service provider possesses the ability to clearly identify and segregate customer data using strong physical or logical controls.

The confirmation that logical controls are an acceptable means to separate the data of one customer from that of another is important and helpful. It means that financial institutions are free to unlock the benefits of public cloud solutions provided that the service provider has the right controls in place. Since many of the benefits of cloud, including scalability and economies of scale, are connected to public cloud services, this is positive news for the industry. Microsoft has long recognised the importance of strong data isolation controls and these are built into Microsoft's cloud services from the ground up. More information about these controls is available via the Microsoft Trust Center.

Part 2: Microsoft's Response to the ABS Cloud Implementation Guidelines

About the ABS Guide

How the ABS Guide applies

On 2 August 2016, immediately after the publication of the Guidelines, ABS released the ABS Guide, which is a set of practical guidelines to help Singapore banks with their cloud procurement. Importantly, the ABS Guide applies only to banks and not to other categories of financial institution. Being an industry-developed document, the ABS Guide constitutes a set of non-binding guidance rather than a set of regulatory requirements.

How the ABS Guide is structured

Section 1

of the ABS Guide provides an overview of the different cloud deployment models. Section 1 is general in nature and is not addressed in this paper.

Section 2

of the ABS Guide focuses on what is likely to constitute "material" and "non-material" outsourcing.

Section 3

of the ABS Guide recommends a set of due diligence and vendor management activities for banks to consider.

Section 4

of the ABS Guide recommends a set of baseline controls that service providers should have in place when working with banks.

Since the ABS Guide was published in parallel with the Guidelines there is some overlap between the two documents. The ABS Guide builds upon the high-level principles set out in the Guidelines by adding a layer of recommendations for banks to consider in the context of cloud services specifically. We will not comment at length on aspects of the ABS Guide that are already addressed in our response to the Guidelines, set out in Part 1.

Outsourcing Classification

Section 2 of the ABS Guide

The ABS Guide provides suggestions as to what is likely to constitute "material" and "non-material" outsourcing in the context of cloud.

Factors Influencing Materiality

Section 2 of the ABS Guide

As described in Part 1 of this paper, the Guidelines introduce a new and broader concept of "material outsourcing arrangement" and a new definition of "customer information", which excludes information that is anonymised, encrypted or public. The ABS Guide provides guidance to help banks and service providers with the interpretation of these definitions. It splits cloud adoptions into those that are "likely to be material" and those that are "likely to be non-material" and introduces various factors to consider in reaching a conclusion on materiality. Importantly, the ABS Guide recognises that a key factor to consider in an outsourcing classification is whether the "customer information" being stored or processed as part of the cloud adoption is encrypted. Cloud solutions that apply secure encryption are, according to the ABS Guide, "likely to be non-material".

We agree with ABS's interpretation that cloud solutions that apply secure encryption are "likely to be non-material". We believe that where data is securely encrypted it is well protected. All of Microsoft's cloud services apply secure encryption by default. This means that, under the ABS Guide, the use of Microsoft's cloud services is unlikely to constitute a material outsourcing arrangement. However, banks should be mindful that, under the Guidelines, an outsourcing arrangement can potentially still be "material", even if encryption is used, where a service failure or breach has the potential to materially affect the institution's ability to manage risk and/or comply with applicable laws and regulations.

Scenario Based Cloud Control Guidance Matrix

Section 2 of the ABS Guide

The ABS Guide maps various cloud deployment scenarios (for example, internet banking, fraud prevention, microsites, data rooms, data analytics) against key controls set out in section 4 of the ABS Guide and suggests whether, for each deployment scenario, controls are "strongly recommended", "recommended" or only "discretionary". This is referred to as the "Scenario Based Cloud Control Guidance Matrix".

The matrix will act as a helpful starting point for banks as they approach the adoption of cloud services. Overall, we agree with the list of controls and the way in which they are classified in the matrix. For example, we strongly agree that encryption should be a baseline requirement in the vast majority of cloud deployment scenarios and it is for this reason that Microsoft enables encryption by default across its cloud services. The only control that we believe requires further consideration is "Collaborative Disaster Recovery Testing", which is "strongly recommended" or "recommended" by the matrix in certain scenarios. In our view, joint recovery testing is not necessary if the service provider undertakes such testing, is certified against the relevant global industry standards and shares the findings of third-party audit reports that are required as part of the certification.

Activities recommended as part of due diligence and vendor management

Section 3 of the ABS Guide

The ABS Guide builds on the due diligence and vendor management requirements of the MAS Guidelines by addressing matters such as contractual considerations in more detail. In this section, Microsoft comments on the suggestions and provides information about Microsoft's vendor management tools and assistance during due diligence.

Contractual Considerations

Section 3.1 of the ABS Guide

The ABS Guide builds on the minimum contractual terms set out in the Guidelines. Overall, most of the suggestions mirror those set out in the Guidelines and provide for six core contractual recommendations:

1. The contract should ensure that the bank can contractually enforce agreed and measurable information security and operational requirements.
2. The contract should state the responsibilities of the contracting parties to ensure the adequacy and effectiveness of security policies and practices, including the circumstances under which these security requirements may be changed.
3. The contract should limit material changes to the service structure.
4. The contract should state that, where a service provider uses subcontractors for material functions, they should ensure that the bank is notified and that the service provider remains accountable.
5. There should be enforceable SLAs, with accompanying governance terms.
6. There should be enforceable termination rights.

We agree that all of these terms should be included in any cloud contract to protect the bank and are pleased to confirm that Microsoft's contractual terms address all of these matters:

1. We agree that security and operational commitments need to be binding and enforceable. The Microsoft contract includes binding, enforceable security and operational protections in favour of the bank.
2. At Microsoft, we are firmly of the view that security is central to any trusted cloud solution and must be backed up by contractual commitments. Microsoft commits that: (i) it will implement and maintain appropriate security controls to protect customer data; (ii) it will notify the customer if it becomes aware of any security incident; and (iii) it will take reasonable steps to mitigate the damage resulting from the security incident.
3. We agree that the contract should limit material changes to the service structure because we recognise that banks require certainty. Microsoft's online service terms and service level terms are locked in for the period of the subscription.
4. Imposing controls on subcontractors is a prudent step for any cloud customer to take. At Microsoft, we commit that subcontractors will be bound by terms no less protective than those we agree with our customer and we remain contractually responsible for ensuring compliance. We publish a list of subcontractors on the Microsoft Trust Center and, if our customer does not approve of a subcontractor on the list, it has the ability to terminate the services.

Contractual Considerations continued

5. The ability to measure and enforce service levels is key to driving performance in any outsourcing arrangement and cloud services are no different. We provide SLA commitments in relation to all of our cloud services, with specified remedies if we fail to meet those commitments.
6. Whilst any outsourcing arrangement should look to the long term, it is prudent to build in a process for bringing the service to an end. With this in mind, our contracts provide rights for the customer to terminate in a range of circumstances, including in the case of material breach or for convenienc

Data Centres

Section 3.2 of the ABS Guide

The ABS Guide suggests that the bank should consider the city and country where data is processed. A threat and vulnerability risk assessment should be conducted on data centres and an appropriate policy put in place to reduce the risk of data leakage in the data centre. Like MAS, ABS acknowledges that an independent third-party audit is a suitable alternative to the bank carrying out the audit itself.

We support these suggestions and strongly believe in the importance of providing transparency as to the location(s) in which data will be stored and processed. Microsoft is committed to being transparent with the location of its data centres, which are selected based on a detailed set of regulatory, political, socio-economic, geological and environmental factors, and are published on the Microsoft Trust Center.

Data Sovereignty

Section 3.3 of the ABS Guide

Like the Guidelines, the ABS Guide acknowledges that there should be no restrictions on the use of data centres outside of Singapore. The ABS Guide suggests that agreed data locations should not be changed without the bank's approval and that the service provider should notify the bank if there is a request from a third party to disclose data.

These suggestions largely mirror the requirements of the Guidelines and we agree with the approach. We strongly believe that banks should retain control of their data when stored in the cloud and customer data should never be used by a cloud provider for any purpose other than providing the cloud service. Microsoft's commitments as to the handling of data on termination are summarised in the Microsoft contract checklist, available from your Microsoft contact upon request.

Activities recommended as part of due diligence and vendor management

Governance

Section 3.5 of the ABS Guide

The ABS Guide emphasises the importance of good relationship governance between a bank and its service provider. It suggests that expectations should be agreed between the service provider and the bank, and key activities, inputs and outputs should be defined. Periodic reviews of key performance indicators and key risk indicators should be held and the service provider should have an outsourcing risk register in place to demonstrate that internal governance exists to regularly review its risk profile and risk management decisions. SLAs should have enforceable penalty clauses included.

Microsoft agrees that a collaborative approach between a bank and its cloud provider is central to a healthy working relationship and a successful cloud project. To facilitate collaboration, Microsoft offers access to technical account managers, continuous hands-on assistance and immediate escalation of urgent issues to speed up resolution and keep mission-critical systems functioning. In the event of service level degradation, Microsoft is contractually committed via the Service Level Agreement to provide service credits to affected customers. Microsoft's extended compliance program for regulated financial institutions provides a platform for even deeper engagement between the bank and Microsoft.

Exit Plan

Section 3.5 of the ABS Guide

The ABS Guide includes various matters to be taken into account when it comes to exit management. These include an agreed procedure for deletion of data upon exit and transferability of outsourced services (e.g. to a third party or to the bank) to ensure service continuity.

At Microsoft, we support these requirements because we recognise that banks need to retain flexibility and choice in their technology arrangements and this requires planning for exit and transition. We also agree it is important that, at the end of the term, the service provider can be relied on to delete the data. When you exit a Microsoft cloud service or your subscription expires, we contractually commit to delete your data after giving you a period of 90 days to export it or renew your subscription. Requirements relating to deletion of data are part of the global standards such as ISO/IEC 27001, ISO/IEC 27018 and MTCS SS 584 that Microsoft complies with and is audited against by independent third parties.

Financial and Continuity Risk

Section 3.7 of the ABS Guide

The ABS Guide suggests that the service provider should be reviewed for its financial and operational capabilities at least annually.

At Microsoft, we firmly believe that transparency is a core pillar of a trusted cloud environment and this is why ongoing oversight and review is built into all of Microsoft's cloud offerings. We arrange for independent third parties to audit our operational capabilities against international standards annually and copies of these audit reports are made available to you; our financial reports, published quarterly, provide regular updates on our company's overall performance; our service dashboards provide you with real-time service information; and our extended compliance program for financial institutions enables deeper and ongoing engagement.

Key controls recommended when entering a cloud outsourcing arrangement

Section 4 of the ABS Guide

Section 4 is an important section because it recommends a set of baseline controls that service providers should have in place when working with banks. We are pleased to provide an overview of the key baseline controls and how Microsoft addresses them.

Encryption

Section 4.1 of the ABS Guide

The ABS Guide states that encryption should be an integral control to secure sensitive information such as authentication credentials, personally identifiable information, credit card information, financial information, emails and computer source code. It goes on to provide a list of "good practice" steps that service providers should take. These include ensuring that sensitive data should be subjected to appropriate encryption controls both "in transit" and "at rest" and that the location, ownership and management of the encryption keys and hardware security modules are agreed between the bank and the service provider.

Microsoft agrees that encryption is an integral control in securing customer data and notes that the Guidelines and the ABS Guide both recognise this. Microsoft cloud services use encryption to help safeguard all customer data, whether or not such data is sensitive. Customer data is encrypted in transit, at rest and when it moves between our data centres. More information about the encryption controls enabled by Microsoft cloud services can be found in the Microsoft Trust Center.

Tokenisation

Section 4.2 of the ABS Guide

The ABS Guide confirms that controls for encryption and tokenisation can be used interchangeably, so they are combined in the guidance matrix and can be used on a complementary or stand-alone basis.

As described above, Microsoft uses world-class encryption technology in its cloud services to help safeguard customer data.

Dedicated Equipment or "Private Cloud"

Section 4.3 of the ABS Guide

The ABS Guide suggests that, in certain circumstances, logical segregation may be bypassed or, in the event of system failure, data may be accessible by exploiting data dumps and accessing infrastructure shared memory. The ABS Guide goes on to elaborate that for situations where particularly sensitive information assets are used, a bank may consider dedicated equipment or "private cloud".

In our view, a particular cloud deployment model need not involve a trade-off in security. Public cloud services are not inherently risker than on-premises, community or private cloud solutions and indeed companies, institutions and governments around the world already use public cloud services for even very sensitive categories of data. In our view, the risks associated with any cloud service should be assessed based on the capabilities of the service provider to provide a secure and trusted cloud environment, rather than purely on the type of deployment model.

Change Management and Privileged User Access Management (PUAM)

Section 4.4 of the ABS Guide

Banks should maintain control over their data, and service providers should have controls in place to facilitate management of privileged accounts as well as near-real-time capability to review any privileged activities. Service providers can help banks maintain appropriate oversight of material changes by establishing dedicated compliance programs that facilitate deep engagement between the bank and the service provider.

We agree that banks should maintain ownership and control over their data. Under Microsoft's contract, when a bank stores its data in Microsoft cloud, the bank retains ownership and control of that data. Microsoft cloud services are certified against ISO/IEC 27018, an international set of privacy standards for public cloud services that specifically require that cloud customers have control over how their information is used.

We also agree that privileged accounts must be managed carefully. In Microsoft cloud services, access to the systems that store customer data is strictly controlled via role-based access measures. Microsoft maintains a record of security privileges of individuals having access to customer data and uses industry-standard procedures to identify and authenticate users who attempt to access information. More information about these controls is available via the Microsoft Trust Center.

Finally, we support the suggestion that service providers should establish dedicated compliance programs. The Microsoft compliance program for regulated financial institutions provides a platform for deeper and ongoing engagement between the bank and Microsoft. This helps customers to maintain oversight of the services throughout the contract period.

Virtualised Environment Security

Section 4.5 of the Cloud Guidelines

The ABS Guide suggests that virtualisation may introduce new threats and recommends that measures are in place to ensure the confidentiality and integrity of data in virtualised cloud architecture.

We agree that, in virtualised, multi-tenanted public cloud architecture, appropriate technical controls should be put in place to help ensure that the data of one cloud customer cannot be accessed by another cloud customer. Microsoft's public cloud services were built with exactly these controls in mind. Microsoft cloud services are designed to host multiple tenants in a highly secure way through controls such as data isolation. Data storage and processing for each tenant is segregated through Active Directory controls specifically developed to help build, manage and secure multi-tenant environments. This helps safeguard a customer's data so that it cannot be accessed or compromised by co-tenants. With such measures in place to protect data in a virtualised cloud environment, we believe that public cloud services should not be viewed as inherently riskier than on-premises, community or private cloud solutions.

Key controls recommended when entering a cloud outsourcing arrangement

User Access Management and Segregation of Duties

Section 4.6 of the ABS Guide

The ABS guide suggests that user access management provides controlled access to information and allows customers and their partners to perform their business activities, while protecting the information and systems from unauthorised access.

At Microsoft, we support this recommendation. Microsoft identity and access management solutions are designed to help control access to applications and resources across the data centre and in the cloud, providing additional levels of validation and security, such as multi-factor authentication and conditional access policies. Monitoring suspicious activity through advanced security reporting, auditing and alerting also helps mitigate potential security issues.

Collaborative Disaster Recovery Testing

Section 4.7 of the ABS Guide

The ABS Guide suggests that the bank should plan and perform their own simulated disaster recovery testing, jointly with the service provider where possible. Service providers should obtain necessary certifications (e.g. ISO/IEC 27001 and validated against ISO/IEC 27018) and their processes should be audited by independent third parties, with such audit reports being made available to the bank.

Simulated disaster recovery testing is essential and it is another feature that is built into Microsoft's offering from the outset. The Microsoft BCP team conducts testing of the business continuity plans and recovery plans at least annually. Issues identified during testing are noted and managed to a resolution. In our view, joint recovery testing is not necessary as Microsoft complies with the relevant global industry standards (i.e. ISO/IEC 27001 and ISO/IEC 27018). These address disaster recovery testing and Microsoft is audited against them each year by independent third parties. This provides customers with comfort that Microsoft has the necessary disaster recovery controls in place.

Security Events Monitoring and Incident Management

Section 4.8 of the ABS Guide

The ABS Guide suggests that there should be effective monitoring of the IT systems and timely detection of security events. Tight integration with incident response and management process can allow security incidents to be remediated speedily.

In our view, institutions will, to a large extent, be dependent on their service provider to assist with and support the necessary monitoring and control. With this in mind, we have built various monitoring and control features into Microsoft cloud services. For example, service health can be monitored through publicly available sources, which allow you to monitor performance against Microsoft's financially backed availability guarantees. At a contractual level, we commit to notifying you of security incidents that affect your data, so that you can take any necessary mitigation or remediation steps that you deem appropriate.

Penetration Testing and Vulnerability Management

Section 4.9 of the ABS Guide

The ABS Guide recommends regular vulnerability assessments and penetration tests. ABS also publishes separate Penetration Testing guidelines that provide more detail as to the requirements.

Penetration testing has an important role to play in providing assurances to cloud customers as to the security status of a cloud offering. Microsoft conducts regular penetration testing to test and improve security controls and processes. We also understand that security assessment is an important part of our customers' own application development and deployment onto the cloud.

Administrative Remote Access

Section 4.10 of the ABS Guide

The ABS Guide suggests that remote access tools carry an inherent risk of information and physical security controls of the data centre being bypassed. It therefore recommends that strict controls, including VPN encryption, are required if remote access is to be used.

Remote access is necessary in order to enjoy many of the benefits of cloud services. Microsoft enables remote access but only on the basis of strict controls. Built-in cryptographic technology enables you to encrypt communications. Administrator access to virtual machines is always encrypted. Industry-standard secure protocols such as SSTP and IPsec are fully supported. All of these practices have been designed and implemented to help safeguard against information and physical security controls of the data centre being bypassed.

Secure Software Development Life Cycle and Code Reviews

Section 4.11 of the ABS Guide

The ABS Guide points out that deployment of applications via cloud services requires a different approach from the traditional software development life cycle as the applications are no longer deployed on an on-premises infrastructure "with implicit security, compliance, control, operational transparency and perceived service level requirements".

We agree with this recommendation and note that Microsoft incorporates security methodology into each phase of development through the Microsoft Security Development Lifecycle (SDL). The SDL is a software development process that helps developers build more secure software and address security and privacy compliance requirements while reducing development costs. The SDL consists of seven phases and one of the key steps is threat modelling and attack surface analysis, where potential threats are assessed and evaluated, and the attack surface is minimised by restricting services or eliminating unnecessary functions. Controls are then fully tested to mitigate the potential threats, so customers can have confidence in the final service release of any software/platform. All of our cloud services use SDL to ensure that the relevant service is safe and secure and addresses privacy and data protection issues from the outset.

Securing Logs and Backups

Section 4.12 of the ABS Guide

The ABS Guide suggests that logs and backups are often overlooked and should be secured to ensure confidentiality, integrity and availability of data.

We agree that logs and backups, like all categories of data, need to be secured to ensure their confidentiality, integrity and availability. At Microsoft, we believe that cloud services can provide enhanced log and back-up features when compared to existing, tape-based, on-premises solutions. In Microsoft cloud services, historical backups are geo-replicated to ensure distribution across multiple locations to manage risk. Robust security controls, as demonstrated by our compliance with international standards such as ISO/IEC 27001 and 27018, are in place to protect log and back-up data. When it comes to availability, backups are available online and restoring a file can be done quickly, directly from the cloud. There is no "unexpected logging of data". We apply controls such as role-based access and two-factor authentication, with activities performed in the production service environment being logged and audited regularly. Data is used only for the purpose of providing the service.

Conclusion: “A Smart Financial Centre”

The Guidelines and the ABS Guide are a welcome step in Singapore’s continued journey of being a “Smart Financial Centre”.

The MAS Guidelines substantially streamline the process for technology adoption, provide clarity on the regulator’s expectations and address many of the misconceptions that had previously slowed the financial industry’s adoption of cloud. In taking this welcomed step, MAS has opened the door for financial institutions to benefit from new technologies in a manner that manages applicable risk and compliance requirements.

The specific recommendations of the ABS Guide build on the principles set out in the MAS Guidelines and will be an invaluable tool for banks as they implement cloud solutions. By relying on our comprehensive approach to risk assurance in the cloud, we are confident that financial institutions in Singapore can move to Microsoft’s cloud in a manner that is not only consistent with the Guidelines and ABS Guide but that can also provide customers with a more advanced security risk management profile than many on-premises solutions.

We look forward to continuing to be at the forefront of those conversations for the benefit of our financial institution customers in Singapore and around the world.

Annex: Microsoft’s compliance program for regulated financial institutions

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

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

Microsoft has also developed various materials that directly map its cloud services against the applicable MAS regulatory criteria, including a checklist populated with detailed information about Microsoft’s cloud services and contractual terms, which is available from your Microsoft contact upon request.

Microsoft has 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. Microsoft has a long and consistent history of being the first cloud services provider to implement major new cloud standards, including recent or forthcoming examples such as ISO/IEC 27018 and ISO/IEC 19086. Microsoft has already implemented the forthcoming FIDO 2.0 authentication standard (expected to be formally adopted in early 2017) in its core client and server operating systems with Windows Hello and Windows Passport as well in its Azure Active Directory cloud service.

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 Singapore on the types of issues they should consider. Microsoft, the Microsoft logo, Active Directory, Azure, Dynamics, Office 365, Windows Hello and Windows Intune are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.

This document is also not intended to be and does not constitute legal advice; rather it is intended to be a summary of the key issues in the Guidelines and the ABS Guide, and to provide general guidance to financial institutions in Singapore on how Microsoft facilitates financial institutions to meet the requirements set out in these guidelines. 18991-1116/Microsoft