Compliance Checklist for Financial Institutions in Singapore

Published: February 27, 2018

This document is intended to serve as a guidepost for customers conducting due diligence and risk assessments of Microsoft's Online Services

Customers are responsible for conducting appropriate due diligence, and this document does not serve as a substitute for such diligence or for a customer's risk assessment.

Introduction

Singapore is already delivering on its mission of becoming one of the world's leading "Smart Financial Centers." Cloud computing is fast becoming the norm, not the exception, for financial institutions in Singapore.

Like all technological advancements, cloud computing provides substantial benefits – but it also creates a complex new environment for financial institutions to navigate. These financial institutions rightly want and expect an unprecedented level of assurance from cloud service providers before they move to the cloud.

Microsoft is committed to providing a trusted set of cloud services to financial institutions in Singapore. Our extensive industry experience, customer understanding, research, and broad partnerships give us a valuable perspective and unique ability to deliver the assurance that our financial institutions customers need.

While this document focuses principally on Azure, Office 365, and Dynamics 365, unless otherwise specified, these principles apply equally to all Online Services as defined and referenced in the Data Processing Terms (DPT) of Microsoft's Online Services Terms.

A Compliance Checklist for Financial Institutions in Singapore

This checklist is part of Microsoft's commitment to financial institutions in Singapore. We developed it to help financial institutions in Singapore adopt Microsoft cloud services with confidence that they are meeting the applicable regulatory requirements.

This checklist contains:

- an Overview of the Regulatory Landscape, which introduces the relevant regulatory requirements in Singapore; and
- a Compliance Checklist, which lists the regulatory issues that need to be addressed and maps Microsoft's cloud services against those issues; and details of where you can find further information.

This checklist is aimed at financial institutions[1] in Singapore that want to use Microsoft cloud services, including banks, financial advisers, securities exchanges, futures exchanges, designated clearing houses, securities trading companies, insurance companies, registered insurance brokers, licensed trust companies, capital investment companies, capital services licensees and other regulated service providers in the financial industry.

This checklist applies to Microsoft Office 365, Microsoft Dynamics 365 and Microsoft Azure. You can access relevant information about each of these services at any time via the Microsoft Trust Center:

[1] In this document, "financial institutions" include any entity that is regulated by the Monetary Authority of Singapore (MAS).

- Office 365
- Dynamics 365
- Azure

In Singapore, there is no mandatory requirement for financial institutions to complete a checklist to adopt Microsoft cloud services. However, through conversations with our many cloud customers in Singapore, we understand that a checklist approach like this is helpful – first, as a way of understanding the regulatory requirements; second, as a way of learning more about how Microsoft cloud services can help financial institutions meet those regulatory requirements; third, as an internal framework for documenting compliance; and fourth, as a tool to streamline consultations with the MAS, if they are required. By reviewing and completing the checklist, financial institutions can adopt Microsoft cloud services with confidence that they are complying with the requirements in Singapore.

Using the Checklist

We suggest you begin by reviewing the Overview of the Regulatory Landscape in the next section. This will provide useful context for the sections that follow.

Next, we suggest that you review the questions set out in the Compliance Checklist and the information provided as a tool to measure compliance against the regulatory framework. The information in this document is provided to help you conduct your risk assessment. It is not intended to replace, or be a substitute for, the work you must perform in conducting an appropriate risk assessment but rather to aid you in that process. Additionally, there are a variety of resources Microsoft makes available to you to obtain relevant information as part of conducting your risk assessment, as well as maintaining ongoing supervision of our services. The information is accessible via the Service Trust Portal and, in particular, use of Compliance Manager.

Microsoft provides extensive information enabling self-service audit and due diligence on performance of risk assessments through the Compliance Manager. This includes extensive detail on the security controls including implementation details and explanation of how the third-party auditors evaluated each control. More specifically, Compliance Manager:

- Enables customers to conduct risk assessments of Microsoft cloud services. Combines the detailed information provided by Microsoft to auditors and regulators as part of various third-party audits of Microsoft's cloud services against various standards (such as International Organisation for Standardisation 27001:2013 and ISO 27018:2014) and information that Microsoft compiles internally for its compliance with regulations (such as the EU General Data Protection Regulation or mapping to other required controls) with the customer's own self-assessment of its organisation's compliance with applicable standards and regulations.

- Provides customers with recommended actions and detailed guidance to improve controls and capabilities that can help them meet regulatory requirements for areas they are responsible for.
- Simplifies compliance workflow and enables customers to assign, track, and record compliance and assessment-related activities, which can help an organisation overcome team barriers to achieve their compliance goals. It also provides a secure repository for customers to upload and manage evidence and other artefacts related compliance activities, so that it can produce richly detailed reports in Microsoft Excel that document the compliance activities performed by Microsoft and a customer's organisation, which can be provided to auditors, regulators, and other compliance stakeholders.

If you need any additional support or have any questions, Microsoft's expert team is on hand to support you throughout your cloud project, right from the earliest stages of initial stakeholder engagement through to assisting in any required consultation with the MAS. You can also access more detailed information online, as set out in the Further Information section.

Overview of the Regulatory Landscape

Are cloud services permitted to be used?	Yes, you can consider Microsoft cloud services for the full range of use-cases across your financial institution.
Who are the relevant regulators and authorities?	The Monetary Authority of Singapore (MAS). Banks, insurers, capital market intermediaries, financial advisors, the stock exchange and other financial institutions are regulated by MAS. The MAS website provides links to underlying regulations and guidance.
What regulations and guidance are relevant?	There are several requirements and guidelines that financial institutions should be aware of when moving to the cloud: • MAS Outsourcing Guidelines (updated on 27 July 2016) • MAS Notice on Outsourcing (P018-2014) September 2014 • MAS Technology Risk Management Guidelines June 2013 • MAS Notices on Technology Risk Management • MAS Business Continuity Management Guidelines June 2003 • Notice 634, Banking Act (Cap.19) The latest version of each document can be found on the MAS website. Certification with the InfoComm Media Development Authority's (IMDA) Multi-Tier Cloud Security (MTCS) Tier 3 is generally regarded as necessary for providing cloud services to regulated sectors. Microsoft has the necessary certifications. In August 2016, the Association of Banks in Singapore (ABS) issued a Cloud Implementation Guide, which is designed to help banks with the adoption of cloud services. While this is not binding, it serves as a practical guide for member banks in respect of the implementation of cloud. Microsoft has issued a detailed response to the Outsourcing Guidelines and the ABS Cloud Implementation Guide.
Is regulatory approval required?	No, there is no requirement for prior notification, consultation or approval. However, adverse developments arising from a financial institution's outsourcing arrangements (for example, a data breach incident) must be notified to the MAS as soon as possible.
What is a "material outsourcing arrangement"?	This definition is important, since certain provisions of the Outsourcing 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). An outsourcing arrangement will be "material" if a service failure or breach has the potential to materially affect the institution's business operations or ability to manage risk and comply with applicable laws and regulations. An outsourcing will also 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. However, the definition of "customer information" expressly excludes securely encrypted information. This document includes all the requirements applicable to "material outsourcing arrangements", for the sake of completeness.

Are transfers of data outside of Singapore permitted?	Yes, the use of datacentres outside of Singapore is permitted. Nonetheless, the 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 the MAS to exercise its regulatory oversight. Institutions are also expected to notify MAS if any overseas authority seeks access to customer information. The Personal Data Protection Act (PDPA) requires organisations to put in place safeguards (including contractual measures) to protect data transferred outside of Singapore. Even though Microsoft agrees to contractual terms in line with the relevant requirements and transfers of data outside of Singapore are permitted, many of our financial services customers in Singapore take advantage of the cloud services available from our Singapore datacentres, including Azure, Dynamics 365, and Office 365. We make specific contractual commitments to store categories of data at rest in the Singaporean geography. These are outlined further in the Compliance Checklist below.
Are public cloud services sufficiently secure?	Yes, the Outsourcing Guidelines give a clear green light for the use of cloud services, whether private, public or hybrid cloud, by financial institutions. In fact, public cloud typically enables customers to take advantage of the most advanced security capabilities and innovations because public cloud services generally adopt those innovations first and have a much larger pool of threat intelligence data to draw upon. An example of this type of innovation in Microsoft cloud services is Office 365 Advanced Threat Protection and the Azure Web Application Firewall, which provide a very sophisticated model to detect and mitigate previously unknown malware and provide customers with information security protections and analytics information.
Are there any mandatory terms that must be included in the contract with the services provider?	Yes, the MAS does stipulate some specific points that financial institutions must ensure are incorporated in their cloud services contracts. These are primarily set out in the Outsourcing Guidelines and Notice 634, Banking Act. In Part 2 of the Compliance Checklist, below, we have mapped these against the sections in the Microsoft contractual documents where you will find them addressed.
How do more general Singaporean privacy laws apply to the use of cloud services by financial institutions?	The PDPA applies to personal information collected by financial institutions. When it comes to outsourcing arrangements, the financial institution is likely to be accountable for downstream use of the personal information by its service providers. In Microsoft's experience, privacy compliance is an increasingly important issue for financial institutions and we address the requirements and provide details of how they apply to use of Microsoft cloud services, in the Compliance Checklist below. Additionally, a European privacy law, the General Data Protection Regulation (GDPR), is due to take effect. The GDPR imposes new rules on companies, government agencies, non-profits, and other organisations that offer goods and services to people in the European Union (EU), or that collect and analyse data tied to EU residents. The GDPR applies no matter where you are located. Microsoft is committed to GDPR compliance across its cloud services and provides GDPR related assurances in its contractual commitments.

Compliance Checklist

In the Question/requirement column, we outline the regulatory requirement that needs to be addressed, based on the underlying requirements.
In the Guidance column, we explain how the use of Microsoft cloud services address the requirement. Where applicable, we also provide guidance as to where the underlying requirement comes from and other issues you may need to consider.

Every financial institution and every cloud services project is different. We suggest that you tailor and build on the guidance provided to develop your own responses based on your financial institution and its proposed use of cloud services.

There are two parts to this Compliance Checklist:

- Part 1 addresses the key compliance considerations that apply
- Part 2 lists the contractual terms that must be addressed, and we indicate where these can be found in Microsoft's contract documents.

Part 1: Key Considerations

Part 1 applies to all deployments of Microsoft cloud services (particularly, Azure, Dynamics 365, and Office 365) by financial institutions in Singapore.

Ref.	Question / requirement	Guidance
A. OVERVIEW - *This section provides a general overview of Microsoft cloud services in Singapore*		
1.	Who is the service provider?	The service provider is Microsoft Operations Pte. Ltd., the regional licensing entity for, and wholly-owned subsidiary of, Microsoft Corporation, a global provider of information technology devices and services, which is publicly listed in the USA (NASDAQ: MSFT). Microsoft's full company profile is available here and Microsoft's Annual Reports are available here.
2.	Has your organisation assessed this to be a material outsourcing arrangement (as described in the Outsourcing Guidelines)?	Under the Outsourcing Guidelines, some requirements only apply if the outsourcing is *material*. These requirements include the requirement to: (i) perform periodic reviews on material outsourcing arrangements at least on an annual basis; (ii) incorporate contractual clauses to allow the institution and MAS to be granted audit access and access to information and any report or finding made on the service provider and its sub-contractors; and (iii) ensure that material outsourcing arrangements with service providers located outside Singapore are conducted in such a manner so as not to hinder MAS's supervisory efforts. For the sake of completeness, this guidance covers all the requirements under the Outsourcing Guidelines, including those that are only applicable to 'material

		outsourcing arrangements'. However, financial institutions will need to make an assessment as to whether the use of cloud services in a manner is "material." A "material outsourcing arrangement" is defined under the Outsourcing Guidelines as 'an outsourcing arrangement – (a) which, in the event of a service failure or security breach, has the potential to either materially impact an institution's– (i) business operations, reputation or profitability; or (ii) ability to manage risk and comply with applicable laws and regulations, or (b) which 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'. "Customer information" does not include information that is public, anonymised or securely encrypted and, in this respect, please see Question 31 for more detail about the secure encryption provided by Microsoft's cloud services. Annex 2 of the Outsourcing Guidelines lists some considerations in determining whether the outsourcing is "material."
3.	What cloud services are you using?	• Microsoft Office 365 • Microsoft Dynamics 365 • Microsoft Azure
4.	What activities and operations will be outsourced to the service provider? Are these critical to your business or operations?	This Compliance Checklist is designed for financial institutions using Azure, Dynamics 365, and/or Office 365. Each service is different and there are many different options and configurations available for each service. You should tailor your response based on how you are using or intend to use Microsoft cloud services, and you should indicate if the services are critical to your business or operations. Microsoft Azure services typically include: • Virtual Machines • App Service • Cloud Services • Virtual Networks • Azure DNS • VPN Gateway • File Storage • Disk Storage • Site Recovery • SQL Database • Machine Learning • IoT Hub and IoT Edge • Data Catalog • Data Factory • API Management • Security Center • Key Vault • Multi-Factor Authentication • Blockchain Service

		Microsoft Dynamics 365 services typically include: • Dynamics 365 for Customer Service • Dynamics 365 for Field Service • Dynamics 365 for Project Service Automation • Dynamics 365 for Sales and Microsoft Social Engagement • Dynamics 365 for Finance and Operations (Enterprise/Business Editions) • Dynamics 365 for Retail and Microsoft Dynamics 365 for Talent Microsoft Office 365 services typically include: • Office ProPlus (Outlook, Word, Excel, PowerPoint, OneNote and Access) • Exchange Online • OneDrive for Business • SharePoint Online • Microsoft Teams • Yammer Enterprise • Skype for Business
5.	What type of cloud services would your organisation be using?	An understanding of the type of cloud solution may be relevant when determining the risk associated with the solution. With Microsoft cloud services, a range of options exists, including public and hybrid cloud, but given the operational and commercial benefits to customers, public cloud is increasingly seen as the standard deployment model for most institutions. <u>If using public cloud</u> Microsoft Azure, on which most Microsoft business cloud services are built, hosts multiple tenants in a highly-secure way through logical data isolation. Data storage and processing for our tenant is isolated from each other tenants as described in section E. (Technical and Operational Risk Q&A) below. <u>If using hybrid cloud</u> By using Microsoft hybrid cloud, customers can move to multi-tenant cloud at their own pace. Tenants may wish to identify the categories of data that they will store on their own servers using Windows Server virtual machines. All other categories of data will be stored in the multi-tenant cloud. Azure, on which many Microsoft enterprise cloud services are built, hosts multiple tenants in a highly-secure way through logical data isolation. Data storage and processing for our tenants is isolated from each other tenant as described in section E. (Technical and Operational Risk Q&A) below.
6.	What data will be processed/stored by the service provider on behalf of the financial institution? Is the data considered to be sensitive?	When you choose Microsoft cloud services, the types of data affected are within your control, so the guidance below will need to be tailored depending on what data you have selected is relevant to the solution. Pursuant to the terms of the contract in place with Microsoft, all data is treated with the highest level of security so that you can continue to comply with your legal and regulatory obligations and your commitments to customers. You will only collect and process data that is necessary for your business operations in compliance with all applicable laws and regulation and this applies whether you

<table>
<tr>
<td></td>
<td></td>
<td>process the data on your own systems or via a cloud solution. Typically, the types of data that would be processed and stored by Microsoft cloud services include:

<table>
<tr><th>Type of Data</th><th>Processed / Stored / Both</th><th>Sensitive (Y/N)</th></tr>
<tr><td>Customer data (including customer name, contact details, account information, payment card data, security credentials and correspondence)</td><td>Both</td><td>Y</td></tr>
<tr><td>Employee data (including employee name, contact details, internal and external correspondence by email and other means and personal information relating to their employment with the organisation)</td><td>Both</td><td>Y</td></tr>
<tr><td>Transaction data (data relating to transactions in which the organisation is involved)</td><td>Both</td><td>Y</td></tr>
<tr><td>Indices (for example, market feeds)</td><td>Both</td><td>N</td></tr>
<tr><td>Other personal and non-personal data relating to the organisation's business operations as a financial institution</td><td>Both</td><td>Y</td></tr>
</table>
</td>
</tr>
<tr>
<td>7.</td>
<td>How is the issue of counterparty risk addressed through your choice of service provider?</td>
<td>Financial institutions should do their due diligence on the service provider to address risks associated with a service provider failing to meet the terms of any agreement or otherwise to perform as agreed. The following is a summary of the factors that our customers typically tell us are important.

a. Competence. Microsoft is an industry leader in cloud computing. Microsoft cloud services were built based on ISO/IEC 27001 and ISO/IEC 27018 standards, a rigorous set of global standards covering physical, logical, process and management controls. Microsoft offers the most comprehensive set of compliance offerings of any cloud service provider. A list of our current certifications is available online. From a risk assurance perspective, Microsoft's technical and organisational measures are designed to meet the needs of financial institutions globally. Microsoft also makes specific commitments across its cloud services in our Online Services Terms.

b. Track-record. Many of the world's top companies use Microsoft cloud services. There are various case studies relating to the use of Microsoft cloud services at https://customers.microsoft.com. Customers have obtained regulatory approvals (when required) and are using Online Services in all regions of the globe. Office 365 has more than 100 million users, including some of the world's largest organisations and financial institutions. Azure continues to experience more than 90% growth, and over 80% of the largest financial institutions use or have committed to using Azure services.

c. Financial services-specific credentials Financial institution customers in leading markets, including in Australia, Canada, France, Germany, Singapore,</td>
</tr>
</table>

		the United Kingdom, the United States, and many other countries have performed their due diligence and, working with their regulators, are satisfied that Microsoft cloud services meet their respective regulatory requirements. This gives customers confidence that Microsoft can help meet the high burden of financial services regulation and is experienced in meeting these requirements. d. Financial strength of Microsoft Microsoft Corporation is publicly-listed in the United States and is among the world's largest companies by market capitalisation. Microsoft has a strong track record of stable profits. Microsoft's market capitalisation is more than USD $500 billion, making it one of the top three capitalised companies in the world. Microsoft has been one of the top 10 global market capitalised companies since 2000 and is the only company to consistently place in the top 10 over the past twenty years. Accordingly, customers should have no concerns regarding its financial strength.
B. OFFSHORING *Microsoft gives customers the opportunity to choose that certain core categories of data will be stored at-rest within Singapore. The use of datacentres out of Singapore is permitted by the Outsourcing Guidelines.*		
8.	Where are the datacentre(s) of the service provider located? Indicate the datacentre(s) in which your organisation's sensitive data would be stored and/or processed.	*Outsourcing Guidelines, Paragraph 5.10 (Outsourcing outside Singapore). Note that the use of datacentres out of Singapore is permitted by the Outsourcing Guidelines.* Microsoft provides data location transparency and allows customers to choose that certain categories of data will be stored at-rest within Singapore. Microsoft takes a regional approach to hosting of Azure data. Microsoft is transparent in relation to the location of customer data: • Office 365 customers can view data-at-rest storage locations on Microsoft's website. • Dynamics 365 customers can view data-at-rest storage locations on Microsoft's website. • Azure customers can view data-at-rest storage locations on Microsoft's website. You can fill in the table below with your organization's information.

No.	Location of Datacentre	Classification of DC: Tier I, II, III or IV	Storing organisation data (Y/N)

9.	Have you obtained a report on the Threat and Vulnerability Risk Assessment on the physical security and environmental controls available at the datacentre(s)? What were the key risks and security issues raised, and how were they addressed?	*TRM Guidelines, Paragraph 10* To meet the objectives and demands of a robust service, Microsoft regularly conducts penetration testing and vulnerability assessments against the service through its commitment to Security Development Lifecycle and ISO certification. The output of testing is tracked through a risk register which is audited and reviewed on a regular basis to ensure compliance to Microsoft's security practices. To protect both the system and customer data, Microsoft does not provide copies of the testing reports however the tests conducted typically include the OWASP top ten and include the use of independent verified security teams (CREST-certified). Microsoft is happy to make available the ISO and SSAE 16 audit reports which cover vulnerability assessments.
10.	What other risks have been considered in relation to the proposed offshoring arrangement?	The following are the risk areas that our customers consider important: • Political (e.g., cross-broader conflict, political unrest, etc.) o Customers know where their data is hosted. The relevant jurisdictions offer stable political environments. • Country/socioeconomic o Microsoft's datacentres are strategically located around the world, considering country and socioeconomic factors. The relevant locations constitute stable socioeconomic environments. • Infrastructure/security/terrorism o Microsoft's datacentres are secured to the same exacting standards, designed to protect customer data from harm and unauthorised access. This is outlined in more detail on the Microsoft Trust Center and in the information available on the Service Trust Portal. • Environmental (i.e. earthquakes, typhoons, floods) o Microsoft datacentres are built in seismically safe zones. Environmental controls have been implemented to protect the datacentres, including temperature control, heating, ventilation and air-conditioning, fire detection and suppression systems, power management systems, 24-hour monitored physical hardware and seismically-braced racks. These requirements are covered by Microsoft's ISO/IEC 27001 accreditation.

		• Legal ○ Customers have a binding, negotiated contract with Microsoft giving them rights and maintaining MAS' regulatory oversight. The terms are summarised in Part 2.
C. COMPLIANCE WITHIN YOUR ORGANISATION *Although this is a matter for each financial institution, Microsoft provides some guidance, based on its experience of approaches taken by its customers. Ultimately this will need to be tailored for your financial institution to reflect its compliance practices.*		
11.	The financial institution should consider its overall business and strategic objectives prior to outsourcing. Please elaborate on the factors considered and the rationale for entering this outsourcing arrangement.	*Outsourcing Guidelines, Paragraph 5.3 (a financial institution should not engage in outsourcing that results in its risk management, internal control, business conduct or reputation being compromised or weakened).* The MAS expects that management would need to have considered the overall business and strategic objectives. We would suggest including details of the following: (a) your business case for outsourcing the specific operations and the factors considered for using Microsoft cloud services; You should prepare a business case for the use of Microsoft cloud services. Where appropriate, this could include reference to some of the key benefits of Microsoft cloud services: Azure Dynamics 365 Office 365 The factors listed below may be used to prepare a business case for the use of Microsoft cloud services: • **Affordability** Microsoft Online Services make enterprise-class technologies available at an affordable price for small and mid-sized companies. • **Security** Microsoft Online Services include extensive security to protect customer data. • **Availability** Microsoft's datacentres provide first-rate disaster recovery capabilities, are fully redundant, and are geographically dispersed to ensure the availability of data, thereby protecting data from natural disasters and other unforeseen complications. Microsoft also provides a financially

				backed guarantee of 99.9% uptime for most of its Online Services. • IT control and efficiency Microsoft Online Services perform critical IT management tasks—such as retaining security updates and upgrading back-end systems—that allow company IT employees to focus their energy on more important business priorities. IT staff retain control over user management and service configuration. The continuous nature of Microsoft's cloud services in terms of managing updates, addressing security threats, and providing real-time improvements to the service are unmatched relative to traditional legacy private hosted cloud environments. • User familiarity and productivity Because productivity, e-mail, file sharing and other apps are hosted in the cloud, company employees can access information remotely from a laptop, PC, or mobile device.
			(b) internal processes that were carried out;	You need to describe what internal processes were carried out. The factors listed above in (a) may be used in the description of the selection process used to select the service provider (e.g., Microsoft's track record and reputation).
			(c) due diligence review of the chosen service provider, including the ability of the service provider to conduct the business activity on an ongoing basis;	Microsoft provides various materials on the Service Trust Portal to help you to perform and assess the compliance of Microsoft cloud services – including audit reports, security assessment documents, in-depth details of security and privacy controls, FAQs and technical whitepapers.
			(d) who handled the decision-making process, which areas of the business were involved or advised, and any details of external consultants or legal counsel involved;	We suggest having a list of the key people/roles involved in the selection and any decision-making and approvals processes used.
			(e) details of Board approval sought prior to outsourcing the contract;	Various places in the Outsourcing Guidelines state that ultimate responsibility for effective management of risks lies with the Board and that appropriate approvals processes should be put in place.

			Each organisation of course has its own internal approval processes. Where this includes Board sign-off, this will not be an issue. Where it does not, you will need to briefly explain how the sign-off processes work (e.g., how right of approval has been delegated by the Board). Again, details of the relevant decision-makers should be included here.
		(f) acknowledgement of the risks by the Board of Directors or a relevant committee of the Board;	Outsourcing Guidelines, Paragraph 5.2 states the responsibilities of the Board including approving the framework for evaluating risks. Paragraph 3 of the Technology Risk Management Guidelines is also relevant.
		(g) vetting of the outsourcing agreement by a competent authority;	Outsourcing Guidelines, Paragraph 5.5.1 states that the outsourcing agreement should be vetted by a competent authority on its legality and enforceability. If it hasn't, explain why.
		(h) established procedures for monitoring performance under the outsourcing agreement on a continuing basis;	See Question 15 for relevant information about the measures offered by Microsoft to enable customers to monitor performance.
		(i) the renewal process for outsourcing agreements and how the renewal will be conducted;	The outsourcing agreement with Microsoft runs on an ongoing basis. Customers may also terminate an Online Service at the express direction of a regulator with reasonable notice or to ensure regulatory compliance and by giving 60 days' prior written notice. Microsoft's contractual documents anticipate renewal.
		(j) contingency plans that would enable the outsourced business activity to be provided by an alternative service provider or brought in-house if required	While your financial institution is ultimately responsible for developing its own contingency plans, based on its circumstances, Microsoft has developed a template that can be used to help develop a plan. This is available from the Service Trust Portal or from your Microsoft contact upon request. The outsourcing agreement with Microsoft provides customers with the ability to access and extract their customer data stored in each Online Service always during their subscription. Microsoft will retain customer data stored in the Online Service in a limited function account for 90 days after expiration or termination of customer's subscription so that the customer may

		extract the data. No more than 180 days after expiration or termination of the customer's use of an Online Service, Microsoft will disable the account and delete customer data from the account.
12.	Has a compliance check for the proposed outsourcing arrangement been performed against the Outsourcing Guidelines and the TRM Guidelines?	If any "compliance gaps" were identified as part of your risk management processes then these need to be detailed, indicating how the relevant issues have been resolved. Customers should review the MAS Guidelines on Outsourcing and the Technology Risk Management Guidelines and can obtain confirmation from Microsoft that Microsoft can help customers comply with these guidelines. Internally, they should ensure that their own processes also comply with the guidelines.
13.	Will all identified security and control gaps be resolved prior to the commencement of this outsourcing arrangement? If not, please explain why and state when they can be resolved.	If any "compliance gaps" were identified as part of your risk management processes then you need to state whether these gaps will be resolved, and if they won't be, why not.
14.	Has your organisation performed a risk assessment of this outsourcing arrangement, including security risk assessment against the latest security threats? Please elaborate on the key risks and threats that have been identified for this outsourcing arrangement	MAS expects that your organisation would have carried out a risk assessment. Outsourcing Guidelines, Paragraph 5.3 lists the factors that should be considered in a framework for risk evaluation. The TRM Guidelines also list the key principles and an indication of what the MAS would consider to be a "proper risk assessment." You should ensure that you have carried out comprehensive due diligence on the nature, scope and complexity of the outsourcing to identify the key risks and risk mitigation strategies. We have made suggestions regarding common issues below and you will need to expand on our guidance to describe what you see as the key risks and what risk processes you have carried out as part of this project. You may also want to refer to data isolation here (in the context of a multi-tenanted solution – noting that logical isolation is expressly permitted by the Outsourcing Guidelines). • identify the role of outsourcing in the overall business strategy and objectives of the institution;

	and the actions that have been or will be taken to address them.	• risk identification; • analysis and quantification of the potential impact and consequences of these risks; • risk mitigation and control strategy; and • ongoing risk monitoring and reporting. If you have any questions when putting together a risk assessment, please do not hesitate to get in touch with your Microsoft contact. The following should be considered in your risk assessment: 1. Data security By transferring certain data processing operations to a third-party, customers should be aware that they need to ensure that their selected outsourcing partner has in place appropriate and reasonable technical and organisational measures to protect the data. This is necessary both from a financial services regulatory perspective as well as the organisation's compliance with data protection legislation. This should be of utmost importance to customers and therefore they should carry out a robust assessment as part of their selection process. Customers that select Microsoft as an outsourcing partner take heavily into account the fact that it is an industry leader in cloud security and implements policies and controls on par with or better than on-premises datacentres of even the most sophisticated organisations. Microsoft is ISO/IEC 27001 and ISO/IEC 27018 accredited. In addition, the Microsoft cloud services achieved the highest-level certification (Tier 3) of the MTCS SS 584 which builds upon recognised international standards such as ISO/IEC 27001, and covers such areas as data retention, data sovereignty, data portability, liability, availability, business continuity, disaster recovery, and incident management. The Microsoft cloud services security features (being the product that the organisation will be using) consist of three parts: (a) built-in security features including encryption of data when in transit and at rest; (b) security controls; and (c) scalable security. These include 24-hour monitored physical hardware, isolated customer data, automated operations and lock-box processes, secure networks and encrypted data. 2. Access and audit In addition to ensuring that relevant security and other safeguards are put in place up front, it is essential that the outsourcing arrangement provides for customers to ensure that such standards and commitments and regulatory requirements are adhered to in practice. Customers should be aware that audit and access to verify this can be a difficult issue in outsourcing and therefore should make this a high priority requirement as part of their outsourcing. Another reason for the selection of Microsoft in this case is that it permits regulator audit and inspection of its datacentres and in agreed circumstances inspection rights for its financial services customers. 3. Control The handing over of a certain amount of day to day responsibility to an outsourcing provider does present certain challenges in relation to control of data. What is essential to customers is that despite the outsourcing they retain control over their own business operations, including control of who can access

		data and how they can use it. At a contractual level, customer would have dealt with this via their agreement with Microsoft, which provides them with legal mechanisms to manage the relationship including appropriate allocation of responsibilities, oversight and remedies. At a practical level, customers select Microsoft cloud services because they provide customers with control over data location, access and authentication and advanced encryption controls. Customers continue to own and retain all rights to their data and their data will not be used for any purpose other than to provide them with the Microsoft cloud services.
15.	Is there a vendor management process to monitor the performance of the service provider? Does your organisation have a process to audit the service provider to assess its compliance with your policies, procedures, security controls and regulatory requirements and obtain reports and findings made on the service provider?	Outsourcing Guidelines, Paragraph 5.8 contains detailed requirements in relation to monitoring and control of outsourced activities. In addition to your own internal processes, you may in this context also wish to consider the contractual vendor management rights that you have under your agreements with Microsoft, including the rights of audit and inspection. Outsourcing Guidelines, Paragraph 5.9 sets out the audits that MAS expects financial institutions to be conducting. It is not required that the FSI conducts the audit itself and it may rely on independent third-party audit by obtaining copies of such finding/audit made on the service provider and its subcontractors. This is a question about your own internal processes, although it is of course relevant in this context to mention that Microsoft permits audit and inspection both by their financial institution's customers and regulators. The guidance below sets out certain features of Microsoft cloud services that can make monitoring easier for you. In addition, you may sign up for Premier Support, in which a designated Technical Account Manager serves as a point of contact for day-to-day management of the Microsoft cloud services and your overall relationship with Microsoft. Microsoft provides access to "service health" dashboards (Office 365 Service Health Dashboard and Azure Status Dashboard) providing real-time and continuous updates on the status of Microsoft's Online Services. This provides our IT administrators with information about the current availability of each service or tool (and history of availability status), details about service disruption or outage and scheduled maintenance times. The information is provided online and via an RSS feed. As part of its certification requirements, Microsoft is required to undergo independent third-party auditing, and it shares with the customer the independent third-party audit reports. As part of the Financial Services Amendment that Microsoft offers to regulated financial services institutions, Microsoft gives them a right to examine, monitor and audit its provision of Microsoft cloud services. Specifically, Microsoft: (i) makes available a written data security policy that complies with certain control standards and frameworks, along with descriptions of the security controls in place for Microsoft cloud services and other information that the customer reasonably requests regarding Microsoft's security practices and policies; and (ii) causes the performance of audits, on the customer's behalf, of the security of the computers, computing environment and physical datacentres that it uses in processing their data (including personal data)

		for Microsoft cloud services and provides the audit report to the customer upon request. Such arrangements should provide the customer with the appropriate level of assessment of Microsoft's ability to facilitate compliance against the customer's policy, procedural, security control and regulatory requirements. The Microsoft Financial Services Amendment further gives the customer the opportunity to participate in the optional financial institution Customer Compliance Program at any time, which enables the customer to have additional monitoring, supervisory and audit rights and additional controls over Microsoft cloud services, such as: (a) access to Microsoft personnel for raising questions and escalations relating to Microsoft cloud services, (b) invitation to participate in a webcast hosted by Microsoft to discuss audit results that leads to subsequent access to detailed information regarding planned remediation of any deficiencies identified by the audit, (c) receipt of communication from Microsoft on: (1) the nature, common causes, and resolutions of security incidents and other circumstances that can reasonably be expected to have a material service impact on the customer's use of Microsoft cloud services, (2) Microsoft's risk-threat evaluations, and (3) significant changes to Microsoft's business resumption and contingency plans or other circumstances that might have a serious impact on the customer's use of Microsoft cloud services, (d) access to a summary report of the results of Microsoft's third-party penetration testing against Microsoft cloud services (e.g. evidence of data isolation among tenants in the multi-tenanted services); and (e) access to Microsoft's subject matter experts through group events such as webcasts or in-person meetings (including an annual summit event) where roadmaps of planned developments or reports of significant events will be discussed and where customers will have a chance to provide structured feedback and/or suggestions regarding the FSI Customer Compliance Program and its desired future evolution.
16.	Does the financial institution have access to adequate, independent information to appropriately monitor the cloud service provider and the effectiveness of its controls?	All customers and potential customers have access to information for monitoring the effectiveness of Microsoft's controls, including through the following online sources: • the information on the Service Trust Portal, and in particular, the use of Compliance Manager provides extensive information enabling self-service audit and due diligence; • a publicly available Trust Center for Microsoft's Online Services that includes non-confidential compliance information; • a Financial Services Compliance Program that provides access to a team of specialists in banking, insurance, asset management, and financial services treasury and remediation services; • the Azure Security Center and Office 365 Advanced Threat Analytics, which enable customers to seamlessly obtain cybersecurity-related information about Online Services deployments;

		• Office 365 Secure Score, which provides insight into the strength of customers' Office 365 deployment based on the customer's configuration settings compared with recommendations from Microsoft, and Azure Advisor, which enables customers to optimise their Azure resources for high availability, security, performance, and cost; • the Office 365 Service Health Dashboard and Azure Status Dashboard, which broadcast real-time information regarding the status of Microsoft's Online Services; and • Office 365 Advanced Threat Protection and the Azure Web Application Firewall, which protect customer email in real-time from cyberattacks and provide customers with information security protections and analytics information.
D. THE NEED FOR AN APPROPRIATE OUTSOURCING AGREEMENT ***Note: See also Part 2 of this Compliance Checklist for a list of the standard contractual terms that MAS expects to be included in the outsourcing agreement and how these are addressed by the Microsoft contractual documents. This section D also includes reference to certain issues that MAS suggests are considered as part of the contractual negotiation, but which are not necessarily mandatory contractual terms that should be included in all cases.***		
17.	Are the outsourcing arrangements contained in a documented legally binding agreement that is signed by all parties and addresses the required matters set out in the Outsourcing Guidelines?	Microsoft enters into agreements with each of its financial institution customers for Online Services, which includes a Financial Services Amendment, the Online Services Terms, and the Service Level Agreement. The agreements clearly define the Online Services to be provided. The contractual documents are further outlined in Part 2, below.
18.	Does the outsourcing agreement include a clause that allows MAS and its agents to carry out an inspection or examination of the service provider and its sub-contractors, and to obtain copies of reports	*Outsourcing Guidelines, Paragraph 5.9.2 requires the inclusion of access to information, inspection and examination rights in favour of MAS. Such rights are indeed included in Microsoft's contractual documents.* Yes, there are provisions in the contract that enable MAS to carry out inspection or examination of Microsoft's facilities, systems, processes and data relating to the services. As part of the Financial Services Amendment that Microsoft offers to regulated financial services institutions, Microsoft will, upon a regulator's request, provide the regulator a direct right to examine the relevant service, including the ability to conduct an on-premises examination; to meet with Microsoft personnel

	made on the service provider or reports or information given to, stored at or processed by the service provider and its sub-contractors?	and Microsoft's external auditors; and to access related information, records, reports and documents. Under the outsourcing agreement, Microsoft commits that it will not disclose customer data to the regulator except as required by law or at the direction or consent of the customer.
19.	Does the outsourcing agreement provide a guarantee of access to the minimum IT assets required to operate under a disaster scenario?	Yes, the uptime guarantee given by Microsoft applies to all IT assets, not just a minimum number required to operate in a disaster situation. Microsoft guarantees 99.9% of uptime for most of its Online Services. Uptime guarantees are set forth in Microsoft's contracts with its customers, and if service levels are not maintained, customers may be eligible for a credit towards a portion of their monthly service fees.
20.	Does the outsourcing agreement also include reporting mechanisms that ensure adequate oversight of IT security risk management by the service provider?	Yes, as referenced in Question 16 above.
21.	Is the outsourcing agreement sufficiently flexible to accommodate changes to existing processes and to accommodate new processes in the future to meet changing circumstances?	Yes, customers can always order additional services, if required. The customer may terminate an Online Service at the express direction of a regulator with reasonable notice. Additionally, to ensure regulatory compliance, Microsoft and the Customer may contemplate adding additional products or services, or if these are unable to satisfy the customer's new regulatory requirements, the customer may terminate the applicable Online Service without cause by giving 60 days' prior written notice.

22.	In the event of termination, do transitional arrangements address access to, and ownership of, documents, records, software and hardware, and the role of the service provider in transitioning the service?	Yes, at any time during a subscription or upon termination thereof, the customer can extract their data. As set out in the OST, Microsoft will retain customer data stored in the Online Service in a limited function account for 90 days after expiration or termination of the customer's subscription so that the customer may extract the data. After the 90-day retention period ends, Microsoft will disable the customer's account and delete the customer data. Microsoft will disable the account and delete customer data from the account no more than 180 days after expiration or termination of customer's use of an Online Service. Ownership of documents, records and other data remain with the customer and at no point transfer to Microsoft or anyone else, so this does not need to be addressed through transition. Being a cloud services solution, ownership of software and hardware used to provide the service remains with Microsoft.
E. TECHNICAL AND OPERATIONAL RISK Q&A *This section provides some more detailed technical and operational information about Microsoft cloud services which should address many of the technical and operational questions that may arise. If other questions arise, please do not hesitate to get in touch with your Microsoft contact.*		
23.	Does the service provider permit audit by the financial institution and/or MAS?	Yes, pursuant to the Financial Services Amendment, Microsoft provides MAS with a direct right to examine the Online Services, including the ability to conduct an on-premise examination, to meet with Microsoft personnel and Microsoft's external auditors, and to access any related information, records, reports and documents, in the event that MAS requests to examine the Online Services operations in order to meet their supervisory obligations. Microsoft will cause the performance of audits of the security of the computers, computing environment and physical datacentres that it uses in processing customer data for each Online Service. Customers may also participate in the optional Customer Compliance Program to have additional monitoring, supervisory and audit rights and additional controls over the Online Services. See Part 2 below for further detail.
24.	Are the provider's services subject to any third-party audit?	*Outsourcing Guidelines, Paragraph 5.9* Yes, Microsoft's cloud services are subject to regular independent third-party audits, including SSAE16 SOC1 Type II, SSAE SOC2 Type II, ISO/IEC 27001, ISO/IEC 27002 and ISO/IEC 27018. Rigorous third-party audits validate the adherence of the cloud services to the strict requirements of these standards. Copies of these audit reports are available for download from the Service Trust Portal. In addition, the Financial Services Amendment further gives customers the opportunity to participate in the optional Financial Services Customer Compliance Program at any time, which enables them to (amongst other things) participate in a webcast hosted by Microsoft to discuss audit results that leads to subsequent access to

		detailed information regarding planned remediation of any deficiencies identified by the audit.
25.	What security controls are in place to protect the transmission and storage of confidential information such as customer data within the infrastructure of the service provider? How does your organisation protect your networks and systems from the potential threats arising from the system connectivity?	*Outsourcing Guidelines, Paragraph 5.6* *TRM Guidelines, Paragraph 9 (operational infrastructure security management), Paragraph 10 (datacentres protection and controls) and Paragraph 11 (access control)* You need to demonstrate that you protect your networks and systems from the potential threats arising from the system connectivity. We have made suggestions regarding measures taken below and you will need to expand on our guidance to describe any further measures taken by your organisation. Microsoft as an outsourcing partner is an industry leader in cloud security and implements policies and controls on par with or better than on-premises datacentres of even the most sophisticated organisations. Microsoft cloud services were built based on ISO/IEC 27001 and ISO/IEC 27018 standards, a rigorous set of global standards covering physical, logical, process and management controls. The Microsoft cloud services security features consist of three parts: (a) built-in security features; (b) security controls; and (c) scalable security. These include 24-hour monitored physical hardware, isolated customer data, automated operations and lock-box processes, secure networks and encrypted data. Microsoft implements the Microsoft Security Development Lifecycle (SDL) which is a comprehensive security process that informs every stage of design, development and deployment of Microsoft cloud services. Through design requirements, analysis of attack surface and threat modelling, the SDL helps Microsoft predict, identify and mitigate vulnerabilities and threats from before a service is launched through its entire production lifecycle. Networks within Microsoft's datacentres are segmented to provide physical separation of critical back-end servers and storage devices from the public-facing interfaces. Edge router security allows the ability to detect intrusions and signs of vulnerability. Customer access to services provided over the Internet originates from users' Internet-enabled locations and ends at a Microsoft datacentre. These connections are encrypted using industry-standard transport layer security TLS. The use of TLS establishes a highly secure client-to-server connection to help provide data confidentiality and integrity between the desktop and the datacentre. Customers can configure TLS between Microsoft cloud services and external servers for both inbound and outbound email. This feature is enabled by default.

		Microsoft also implements traffic throttling to prevent denial-of-service attacks. It uses the "prevent, detect and mitigate breach" process as a defensive strategy to predict and prevent security breaches before they happen. This involves continuous improvements to built-in security features, including port-scanning and remediation, perimeter vulnerability scanning, OS patching to the latest updated security software, network-level DDoS detection and prevention and multi-factor authentication for service access. Use of a strong password is enforced as mandatory, and the password must be changed on a regular basis. From a people and process standpoint, preventing breach involves auditing all operator/administrator access and actions, zero standing permission for administrators in the service, "Just-In-Time (JIT) access and elevation" (that is, elevation is granted on an as-needed and only-at-the-time-of-need basis) of engineer privileges to troubleshoot the service, and isolation of the employee email environment from the production access environment. Employees who have not passed background checks are automatically rejected from high privilege access, and checking employee backgrounds is a highly scrutinised, manual-approval process. Preventing breach also involves automatically deleting unnecessary accounts when an employee leaves, changes groups, or does not use the account prior to its expiration. Data is also encrypted. Customer data in Microsoft cloud services exists in two states: at rest on storage media; and in transit from a datacentre over a network to a customer device. Microsoft offers a range of built-in encryption capabilities to help protect data at rest. For example, for customer data at rest, Microsoft Azure uses BitLocker and DM-Crypt, and Microsoft Office 365 uses BitLocker, Azure Storage Service Encryption, Distributed Key Manager (DKM), and Customer Key. For customer data in transit, Azure, Office 365, Microsoft Commercial Support, Microsoft Dynamics 365, Microsoft Power BI, and Visual Studio Team Services use industry-standard secure transport protocols, such as Internet Protocol Security (IPsec) and Transport Layer Security (TLS), between Microsoft datacentres and between user devices and Microsoft datacentres. See Question 31 for further information on encryption.
26.	Does the service provider employ a system architecture that involves multi-tenancy and data commingling for the outsourced service(s)? If so, how is the financial institution's data isolated from other data held	*Outsourcing Guidelines expressly permit logical segregation. Outsourcing Guidelines, Paragraph 6.7 contains requirements that institutions should be aware of the typical characteristics of cloud computing, such as multi-tenancy and data commingling.* *TRM Guidelines, Paragraph 5.2.3 (Management of IT outsourcing risks) contains requirements for service providers to isolate and clearly identify their customer data and other information system assets for protection.* Microsoft cloud services are multi-tenant services (that is, data from different customers shares the same hardware resources) but they are designed to host

	by the service provider?	multiple tenants in a highly secure way through data isolation. For Online Services, Microsoft isolates customer data from the other data Microsoft holds. Multiple forms of protection have been implemented throughout Office 365 to prevent customers from compromising Office 365 services or applications or gaining unauthorized access to the information of other tenants or the Office 365 system itself, including: • Logical isolation of customer content within each tenant for Office 365 services is achieved through Azure Active Directory authorization and role-based access control. • SharePoint Online and OneDrive for Business provide data isolation mechanisms at the storage level. • Microsoft uses rigorous physical security, background screening, and a multi-layered encryption strategy to protect the confidentiality and integrity of customer content. All Office 365 datacentres have biometric access controls, with most requiring palm prints to gain physical access. In addition, all U.S.-based Microsoft employees are required to successfully complete a standard background check as part of the hiring process. • Office 365 uses service-side technologies that encrypt customer content at rest and in transit Together, the above-listed protections provide robust logical isolation controls that provide threat protection and mitigation equivalent to that provided by physical isolation alone.
27.	How are the service provider's access logs monitored?	Microsoft provides monitoring and logging technologies to give its customers maximum visibility into the activity on their cloud-based network, applications, and devices, so they can identify potential security gaps. The Online Services contain features that enable customers to restrict and monitor their employees' access to the services, including the Azure AD Privileged Identify Management system and Multi-Factor Authentication. In addition, the Online Services include built-in approved Windows PowerShell Scripts, which minimise the access rights needed and the surface area available for misconfiguration. Microsoft logs, or enables customers to log, access and use of information systems containing customer data, registering the access ID, time, authorisation granted or denied, and relevant activity. An internal, independent Microsoft team audits the log at least once per quarter, and customers have access to such audit logs. In addition, Microsoft periodically reviews access levels to ensure that only users with appropriate business justification have access to appropriate systems.
28.	What policies does the service provider have in place to monitor employees with	For certain core services of Office 365 and Azure, personnel (including employees and subcontractors) with access to customer data content are subject to background screening, security training, and access approvals as allowed by applicable law. Background screening takes place before Microsoft authorises the employee to access customer data. To the extent permitted by law, any criminal

	access to confidential information?	history involving dishonesty, breach of trust, money laundering, or job-related material misrepresentation, falsification, or omission of fact may disqualify a candidate from employment, or, if the individual has commenced employment, may result in termination of employment at a later day.
29.	How are customers authenticated?	Microsoft cloud services use two-factor authentication to enhance security. Typical authentication practices that require only a password to access resources may not provide the appropriate level of protection for information that is sensitive or vulnerable. Two-factor authentication is an authentication method that applies a stronger means of identifying the user. The Microsoft phone-based two-factor authentication solution allows users to receive their PINs sent as messages to their phones, and then they enter their PINs as a second password to log on to their services.
30.	What are the procedures for identifying, reporting and responding to suspected security incidents and violations?	First, there are robust procedures offered by Microsoft that enable the prevention of security incidents and violations arising in the first place and detection if they do occur. Specifically: a. Microsoft implements 24 hour monitored physical hardware. Datacentre access is restricted 24 hours per day by job function so that only essential personnel have access to customer applications and services. Physical access control uses multiple authentication and security processes, including badges and smart cards, biometric scanners, on-premises security officers, continuous video surveillance, and two-factor authentication. b. Microsoft implements "prevent, detect, and mitigate breach", which is a defensive strategy aimed at predicting and preventing a security breach before it happens. This involves continuous improvements to built-in security features, including port scanning and remediation, perimeter vulnerability scanning, OS patching to the latest updated security software, network-level DDOS (distributed denial-of-service) detection and prevention, and multi-factor authentication for service access. In addition, Microsoft has anti-malware controls to help avoid malicious software from gaining unauthorised access to customer data. Microsoft implements traffic throttling to prevent denial-of-service attacks and maintains a set of Security Rules for managed code to help ensure that application cybersecurity threats are detected and mitigated before the code is deployed. c. Microsoft employs some of the world's top experts in cybersecurity, cloud compliance, and financial services regulation. Its Digital Crimes Unit, for example, employs cyber experts, many of whom previously worked for law enforcement, to use the most advanced tools to detect, protect, and respond to cybercriminals. Its Cyber Defense Operations Center brings together security response experts from across Microsoft to help protect, detect, and respond 24/7 to security threats against Microsoft's infrastructure and Online Services in real-time. General information on cybersecurity can be found here. d. Microsoft conducts a risk assessment for Azure at least annually to identify internal and external threats and associated vulnerabilities in the Azure environment. Information is gathered from numerous data sources within Microsoft through interviews, workshops, documentation review, and analysis

		of empirical data. The assessment follows a documented process to produce consistent, valid, and comparable results year over year. e. Wherever possible, human intervention is replaced by an automated, tool-based process, including routine functions such as deployment, debugging, diagnostic collection, and restarting services. Microsoft continues to invest in systems automation that helps identify abnormal and suspicious behaviour and respond quickly to mitigate security risk. Microsoft is continuously developing a highly effective system of automated patch deployment that generates and deploys solutions to problems identified by the monitoring systems—all without human intervention. This greatly enhances the security and agility of the service. f. Microsoft allows customers to monitor security threats on their server by providing access to the Azure Security Center, Office 365 Advanced Threat Analytics, Azure Status Dashboard, and the Office 365 Service Health Dashboard, among other online resources. g. Microsoft maintains 24-hour monitoring of its Online Services and records all security breaches. For security breaches resulting in unlawful or unauthorised access to Microsoft's equipment, facilities, or customer data, Microsoft notifies affected parties without unreasonable delay. Microsoft conducts a thorough review of all information security incidents. h. Microsoft conducts penetration tests to enable continuous improvement of incident response procedures. These internal tests help Microsoft cloud services security experts create a methodical, repeatable, and optimised stepwise response process and automation. In addition, Microsoft provides customers with the ability to conduct their own penetration testing of the services. This is done in accordance with Microsoft's rules of engagement, which do not require Microsoft's permission in advance of such testing. Second, if a security incident or violation is detected, Microsoft Customer Service and Support notifies customers by updating the Service Health Dashboard. Customers would have access to Microsoft's dedicated support staff, who have a deep knowledge of the service. Microsoft provides Recovery Time Objective (RTO) commitments. These differ depending on the applicable Microsoft service and are outlined further below. Finally, after the incident, Microsoft provides a thorough post-incident review report (PIR). The PIR includes: • An incident summary and event timeline. • Broad customer impact and root cause analysis. • Actions being taken for continuous improvement. If the customer is affected by a service incident, Microsoft shares the post-incident review with them. Microsoft's commitment to cybersecurity and data privacy, including restrictions on access to customer data, are set forth in Microsoft's contracts with customers. In summary:

		• **Logical Isolation** Microsoft logically isolates customer data from the other data Microsoft holds. This isolation safeguards customers' data such that the data cannot be accessed or compromised by co-tenants. • **24-Hour Monitoring & Review of Information Security Incidents** Microsoft maintains 24-hour monitoring of its Online Services and records all security breaches. Microsoft conducts a thorough review of all information security incidents. For security breaches resulting in unlawful or unauthorised access to Microsoft's equipment, facilities, or customer data, Microsoft notifies affected parties without unreasonable delay. • **Minimising Service Disruptions—Redundancy** Microsoft makes every effort to minimise service disruptions, including by implementing physical redundancies at the disk, network, power supply, and server levels; constant content replication; robust backup, restoration, and failover capabilities; and real-time issue detection and automated response such that workloads can be moved off any failing infrastructure components with no perceptible impact on the service. • **Resiliency** Microsoft's Online Services offer active load balancing, automated failover and human backup, and recovery testing across failure domains. • **Distributed Services** Microsoft offers distributed component services to limit the scope and impact of any failures of a single component, and directory data is replicated across component services to insulate one service from another in the event of a failure. • **Simplification** Microsoft uses standardised hardware to reduce issue isolation complexities. Microsoft also uses fully automated deployment models and a standard built-in management mechanism. • **Human Backup** Microsoft's Online Services include automated recovery actions with 24/7 on-call support; a team with diverse skills on call to provide rapid response and resolution; and continuous improvement through learning from the on-call teams. • **Disaster Recovery Tests** Microsoft conducts disaster recovery tests at least once per year. Customers also have access to the Azure Security Center, Office 365 Advanced Threat Analytics, Azure Status Dashboard, and the Office 365 Service Health Dashboard, among other online resources, which allow them to monitor security threats on the cloud service provider's server.
31.	How is end-to-end application encryption security implemented to protect PINs and other sensitive data transmitted between	*TRM Guidelines, Paragraph 9.1 and Appendix E (Paragraph E.2.5)* Microsoft cloud services use industry-standard secure transport protocols for data as it moves through a network—whether between user devices and Microsoft datacentres or within datacentres themselves. To help protect data at rest, Microsoft offers a range of built-in encryption capabilities.

	terminals and hosts?	There are three key aspects to Microsoft's encryption: 1. Secure identity: Identity (of a user, computer, or both) is a key element in many encryption technologies. For example, in public key (asymmetric) cryptography, a key pair—consisting of a public and a private key—is issued to each user. Because only the owner of the key pair has access to the private key, the use of that key identifies the associated owner as a party to the encryption/decryption process. Microsoft Public Key Infrastructure is based on certificates that verify the identity of users and computers. 2. Secure infrastructure: Microsoft uses multiple encryption methods, protocols, and algorithms across its products and services to help provide a secure path for data to travel through the infrastructure, and to help protect the confidentiality of data that is stored within the infrastructure. Microsoft uses some of the strongest, most secure encryption protocols in the industry to provide a barrier against unauthorised access to customer data. Proper key management is an essential element in encryption best practices, and Microsoft helps ensure that encryption keys are properly secured. Protocols and technologies examples include: • Transport Layer Security (TLS), which uses symmetric cryptography based on a shared secret to encrypt communications as they travel over the network. • Internet Protocol Security (IPsec), an industry-standard set of protocols used to provide authentication, integrity, and confidentiality of data at the IP packet level as it's transferred across the network. • Office 365 servers using BitLocker to encrypt the disk drives containing log files and customer data at rest at the volume-level. BitLocker encryption is a data protection feature built into Windows to safeguard against threats caused by lapses in controls (e.g., access control or recycling of hardware) that could lead to someone gaining physical access to disks containing customer data. • BitLocker deployed with Advanced Encryption Standard (AES) 256-bit encryption on disks containing customer data in Exchange Online, SharePoint Online, and Skype for Business. Advanced Encryption Standard (AES)-256 is the National Institute of Standards and Technology (NIST) specification for a symmetric key data encryption that was adopted by the US government to replace Data Encryption Standard (DES) and RSA 2048 public key encryption technology. • BitLocker encryption that uses AES to encrypt entire volumes on Windows server and client machines, which can be used to encrypt Hyper-V virtual machines when a virtual Trusted Platform Module (TPM) is added. BitLocker also encrypts Shielded VMs in Windows Server 2016, to ensure that fabric administrators cannot access the information inside the virtual machine. The Shielded VMs solution

		includes the Host Guardian Service feature, which is used for virtualization host attestation and encryption key release. • Office 365 offers service-level encryption in Exchange Online, Skype for Business, SharePoint Online, and OneDrive for Business with two key management options—Microsoft managed and Customer Key. Customer Key is built on service encryption and enables customers to provide and control keys that are used to encrypt their data at rest in Office 365. • Microsoft Azure Storage Service Encryption encrypts data at rest when it is stored in Azure Blob storage. Azure Disk Encryption encrypts Windows and Linux infrastructure as a service (IaaS) virtual machine disks by using the BitLocker feature of Windows and the DM-Crypt feature of Linux to provide volume encryption for the operating system and the data disk. • Transparent Data Encryption (TDE) encrypts data at rest when it is stored in an Azure SQL database. • Azure Key Vault helps easily and cost-effectively manage and maintain control of the encryption keys used by cloud apps and services via a FIPS 140-2 certified cloud-based hardware security module (HSM). • Microsoft Online Services also transport and store secure/multipurpose Internet mail extensions (S/MIME) messages and transport and store messages that are encrypted using client-side, third-party encryption solutions such as Pretty Good Privacy (PGP).
32.	Are there procedures established to securely destroy or remove the data when the need arises (for example, when the contract terminates)?	*TRM Guidelines, Paragraph 5.2.4 (Management of IT outsourcing risks)* *Outsourcing Guidelines, Paragraph 5.7.2(c) requires financial institutions to ensure that there are plans and procedures in place to address the need to have all relevant IT information and assets promptly removed and destroyed upon termination.* Yes, Microsoft uses best practice procedures and a wiping solution that is NIST 800-88, ISO/IEC 27001, ISO/IEC 27018, SOC 1 and SOC 2 compliant. For hard drives that cannot be wiped it uses a destruction process that destroys it (i.e. shredding) and renders the recovery of information impossible (e.g., disintegrate, shred, pulverize, or incinerate). The appropriate means of disposal is determined by the asset type. Records of the destruction are retained. All Microsoft online services utilise approved media storage and disposal management services. Paper documents are destroyed by approved means at the pre-determined end-of-life cycle. In its contracts with customers, Microsoft commits to disabling a customer's account and deleting customer data from the

		account no more than 180 days after the expiration or termination of the Online Service. "Secure disposal or re-use of equipment and disposal of media" is covered under the ISO/IEC 27001 standards against which Microsoft is certified.
33.	Are there documented security procedures for safeguarding premises and restricted areas? If yes, provide descriptions of these procedures.	Yes, physical access control uses multiple authentication and security processes, including badges and smart cards, biometric scanners, on-premises security officers, continuous video surveillance and two-factor authentication. The datacentres are monitored using motion sensors, video surveillance and security breach alarms.
34.	Are there documented security procedures for safeguarding hardware, software and data in the datacentre?	Yes. These are described at length on the Microsoft Trust Center: • Design and operational security • Network security • Encryption • Threat management • Identify and access management
35.	Does the service provider have privileged access or remote access to perform system/user administration for the outsourced service? If so, does the service provider have access to your organisation's sensitive data? Please provide details on the controls implemented to mitigate the risks of unauthorised access to	*TRM Guidelines, Paragraphs 10.2 (physical security) and 11 (access control)* Yes, Microsoft applies strict controls over access to customer data. Access to the IT systems that store customer data is strictly controlled via role-based access control (RBAC) and lock box processes. Access control is an automated process that follows the separation of duties principle and the principle of granting least privilege. This process ensures that the engineer requesting access to these IT systems has met the eligibility requirements, such as a background screen, required security training, and access approvals. In addition, the access levels are reviewed on a periodic basis to ensure that only users who have appropriate business justification have access to the systems. This process ensures that the engineer requesting access to these IT systems has met the eligibility requirements. In addition, the Online Services include built-in approved Windows PowerShell Scripts, which minimise the access rights needed and the surface area available for misconfiguration.

	sensitive data by the service provider, or other parties.	Microsoft provides monitoring and logging technologies to give customers maximum visibility into the activity on their cloud-based network, applications, and devices, so they can identify potential security gaps. The Online Services contain features that enable customers to restrict and monitor their employees' access to the services, including the Azure AD Privileged Identify Management system and Multi-Factor Authentication. Microsoft logs, or enables customers to log, access and use of information systems containing customer data, registering the access ID, time, authorisation granted or denied, and relevant activity (see Online Services Terms, page 13). An internal, independent Microsoft team audits the log at least once per quarter, and customers have access to such audit logs. In addition, Microsoft periodically reviews access levels to ensure that only users with appropriate business justification have access to appropriate systems. Microsoft provides customers with information to reconstruct financial transactions and develop audit trail information through two primary sources: Azure Active Directory reporting, which is a repository of audit logs and other information that can be retrieved to determine who has accessed customer transaction information and the actions they have taken with respect to such information, and Azure Monitor, which provides activity logs and diagnostic logs that customers can use to determine the "what, who, and when" with respect to changes to customer cloud information and to obtain information about the operation of the Online Services, respectively. In emergency situations, a "JIT (as defined above) access and elevation system" is used (that is, elevation is granted on an as-needed and only-at-the-time-of-need basis) of engineer privileges to troubleshoot the service.
36.	Are the activities of privileged accounts captured (e.g. system audit logs) and reviewed regularly? Indicate the party reviewing the logs and the review frequency.	*TRM Guidelines, Paragraph 11.1.4 (Access Controls)* Yes, an internal, independent Microsoft team audits the logs at least once per quarter.
37.	Are the audit/activity logs protected against tampering by users with privileged accounts? Describe the	*TRM Guidelines, Paragraph 11 (Access Controls)* Yes, Microsoft logs, or enables customers to log, access and use of information systems containing customer data, registering the access ID, time, authorization granted or denied, and relevant activity (see Online Services Terms, page 13). An internal, independent Microsoft team audits the log at least once per quarter, and

	safeguards implemented.	customers have access to such audit logs. In addition, Microsoft periodically reviews access levels to ensure that only users with appropriate business justification have access to appropriate systems. All logs are saved to the log management system which a different team of administrators manages. All logs are automatically transferred from the production systems to the log management system in a secure manner and stored in a tamper-protected way.
38.	Is access to sensitive files, commands and services restricted and protected from manipulation? Are integrity checks implemented to detect unauthorised changes to databases, files, programs and system configuration? Provide details of controls implemented.	*TRM Guidelines, Paragraph 11 (Access Controls)* *Yes, system level data such as configuration data/file and commands are managed as part of the configuration management system. Any changes or updates to or deletion of those data/files/commands will be automatically deleted by the configuration management system as anomalies.* Further, Microsoft applies strict controls over access to customer data. Access to the IT systems that store customer data is strictly controlled via role-based access control (RBAC) and lock box processes. Access control is an automated process that follows the separation of duties principle and the principle of granting least privilege. This process ensures that the engineer requesting access to these IT systems has met the eligibility requirements, such as a background screen, required security training, and access approvals. In addition, the access levels are reviewed on a periodic basis to ensure that only users who have appropriate business justification have access to the systems. This process ensures that the engineer requesting access to these IT systems has met the eligibility requirements. In addition, the Online Services include built-in approved Windows PowerShell Scripts, which minimise the access rights needed and the surface area available for misconfiguration.
39.	Are password controls for the outsourced systems and applications reviewed for compliance on a regular basis?	*TRM Guidelines, Paragraph 11.1.5 (Access Controls)* Yes, all access to production and customer data requires multi-factor authentication. Use of strong passwords is enforced as mandatory, and password must be changed on a regular basis.
40.	Are access rights for the outsourced systems and applications reviewed for compliance on a regular basis?	*TRM Guidelines, Paragraph 11 (Access Controls) It is recommended that financial institutions implement strong controls over remote access by privileged users.*

		Administrators who have rights to applications have no physical access to the production systems. They must securely access the applications remotely via a controlled, and monitored remote process called lockbox. All operations through this remote access facility are logged. Further, Microsoft applies strict controls over access to customer data. Access to the IT systems that store customer data is strictly controlled via role-based access control (RBAC) and lock box processes. Access control is an automated process that follows the separation of duties principle and the principle of granting least privilege. This process ensures that the engineer requesting access to these IT systems has met the eligibility requirements, such as a background screen, required security training, and access approvals. In addition, the access levels are reviewed on a periodic basis to ensure that only users who have appropriate business justification have access to the systems. This process ensures that the engineer requesting access to these IT systems has met the eligibility requirements. In addition, the Online Services include built-in approved Windows PowerShell Scripts, which minimise the access rights needed and the surface area available for misconfiguration.
41.	Does the service provider have a disaster recovery or business continuity plan and what is the service availability? For your organisation's data residing at the service provider, what are the backup and recovery arrangements?	*Outsourcing Guidelines, Paragraph 5.7* *TRM Guidelines, Paragraphs 8.1 (Systems Availability), 8.2 (Disaster Recovery Plan), 8.3 (Disaster Recovery Testing) and 8.4 (Data Backup Management)* *Business Continuity Management Guidelines, Principle 2* Yes, Microsoft makes every effort to minimise service disruptions, including by implementing physical redundancies at the disk, network, power supply, and server levels; constant content replication; robust backup, restoration, and failover capabilities; and real-time issue detection and automated response such that workloads can be moved off any failing infrastructure components with no perceptible impact on the service. Microsoft also maintains 24/7 on-call engineering teams for assistance. See Financial Services Compliance Program and Premier Support; see also Office 365 Support; Premier Support for Enterprise; and Azure Support Plans. Redundancy Microsoft maintains physical redundancy at the server, datacentre, and service levels; data redundancy with robust failover capabilities; and functional redundancy with offline functionality. Microsoft's redundant storage and its procedures for recovering data are designed to attempt to reconstruct customer data in its original or last-replicated state from before the time it was lost or destroyed. For Office 365, Microsoft maintains multiple copies of customer data across datacentres for redundancy. For Azure, Microsoft may copy customer data between regions within a given location for data redundancy or other operational purposes. For example, Azure GRS replicates certain data between two regions

		within the same location for enhanced data durability in case of a major datacentre disaster. **Resiliency** To promote data resiliency, Microsoft's Online Services offer active load balancing, automated failover and human backup, and recovery testing across failure domains. For example, Azure Traffic Manager provides load balancing between different regions, and the customer can use network virtual appliances in its Azure Virtual Networks for application delivery controller functionality. Load balancing is also provided by Power BI Services, the Gateway, and Azure API Management roles. Office 365 services have been designed around specific resiliency principles that are designed to protect data from corruption, to separate data into different fault zones, to monitor data for failing any part of the ACID test, and to allow customers to recover on their own. **Distributed Services** Microsoft also offers distributed component services like Exchange Online, SharePoint Online, and Lync Online to limit the scope and impact of any failures of a single component. Directory data is also replicated across component services to insulate one service from another in the event of a failure. **Monitoring** Microsoft's Online Services include internal monitoring to drive automatic recovery; outside-in monitoring to raise alerts about incidents; and extensive diagnostics for logging, auditing, and granular tracing. **Simplification** Microsoft uses standardised hardware to reduce issue isolation complexities. Microsoft also uses fully automated deployment models and a standard built-in management mechanism. **Human Backup** Microsoft's Online Services include automated recovery actions with 24/7 on-call support; a team with diverse skills on call to provide rapid response and resolution; and continuous improvement through learning from the on-call teams. **Continuous Learning** If an incident occurs, Microsoft conducts a thorough post-incident review. This post-incident review consists of an analysis of the events that occurred, Microsoft's response, and Microsoft's plan to prevent a similar problem from occurring in the future. Microsoft will share the post-incident review with any organization affected by the service incident. **Disaster Recovery Tests** Microsoft conducts disaster recovery tests at least once per year. If the organisation is affected by a service incident, Microsoft shares the post-incident review with the organisation.
42.	What are the recovery time objectives (RTO) of systems or applications outsourced to	*Outsourcing Guidelines, Paragraph 5.7.2(a). TRM Guidelines, Paragraph 8.2.4. Business Continuity Management Guidelines, Principle 4 (financial*

	the service provider?	*institutions should develop recovery strategies and set recovery time objectives for critical business functions).* The SLA for each Microsoft Online Service is specified in the Service Level Agreement (SLA).
43.	What are the recovery point objectives (RPO) of systems or applications outsourced to the service provider?	*Outsourcing Guidelines, Paragraph 5.7.2(a). TRM Guidelines, Paragraph 8.2.4. Business Continuity Management Guidelines, Principle 4 (financial institutions should develop recovery strategies and set recovery time objectives for critical business functions)* Azure Backup and resiliency RPO is provided on a service-by-service basis, with information on each Azure service available from the Azure Trust Center. Office 365 Peer replication between datacentres ensures that there are always multiple live copies of any data. Standard images and scripts are used to recover lost servers, and replicated data is used to restore customer data. Because of the built-in data resiliency checks and processes, Microsoft maintains backups only of Office 365 information system documentation (including security-related documentation), using built-in replication in SharePoint Online and our internal code repository tool, Source Depot. System documentation is stored in SharePoint Online, and Source Depot contains system and application images. Both SharePoint Online and Source Depot use versioning and are replicated in near real-time.
44.	How frequently does the service provider conduct disaster recovery tests?	*Outsourcing Guidelines, Paragraph 5.7.2(b) (financial institutions should ensure that the service provider regularly tests its business continuity plans and that the tests validate the feasibility of the RTOs and the resumption operating capacities. The service provider should also be required to notify the financial institution of any test finding that may affect the service provider's performance). TRM Guidelines, Paragraph 8.3, contains details around expectations of disaster recovery tests (with paragraph 8.3.2 referring to this being done at least annually). Business Continuity Management Guidelines, Principle 3.* Microsoft conducts disaster recovery tests at least once per year. By way of background, Microsoft maintains physical redundancy at the server, datacentre, and service levels; data redundancy with robust failover capabilities; and functional redundancy with offline functionality. Microsoft's redundant storage and its procedures for recovering data are designed to attempt to reconstruct customer data in its original or last-replicated state from before the time it was lost or destroyed.

		Microsoft maintains multiple live copies of data at all times. Live data is separated into "fault zones," which ensure continuous access to data. For Office 365, Microsoft maintains multiple copies of customer data across datacentres for redundancy. For Azure, Microsoft may copy customer data between regions within a given location for data redundancy or other operational purposes. For example, Azure Globally-Redundant Storage ("GRS") replicates certain data between two regions within the same location for enhanced data durability in case of a major datacentre disaster. To promote data resiliency, Microsoft's Online Services offer active load balancing, automated failover and human backup, and recovery testing across failure domains. For example, Azure Traffic Manager provides load balancing between different regions, and the customer can use network virtual appliances in its Azure Virtual Networks for application delivery controllers (ADC/load balancing) functionality. Load balancing is also provided by Power BI Services, the Gateway, and Azure API Management roles. Office 365 services have been designed around specific resiliency principles that are designed to protect data from corruption, to separate data into different fault zones, to monitor data for failing any part of the ACID test, and to allow customers to recover on their own.
45.	Do you have the right to terminate the SLA in the event of default, ownership change, insolvency, change of security or serious deterioration of service quality?	*Outsourcing Guidelines, Paragraph 5.5.2(i), which states that the agreement should contain provisions for default termination and early exit.* The SLA is only one part of the contractual arrangement with Microsoft. It is not terminable as a stand-alone document (the remedies available to customers under the SLA are financial). The customer may terminate an Online Service at the express direction of a regulator with reasonable notice. Additionally, to ensure regulatory compliance, Microsoft and the customer may contemplate adding additional products or services, or if these are unable to satisfy the customer's new regulatory requirements, the customer may terminate the applicable Online Service without cause by giving 60 days' prior written notice.
F. PRIVACY *In addition to the sector-specific requirements imposed by MAS, the financial institution also needs to comply with the Personal Data Protection Act in respect of any personal information that Microsoft hosts for the financial institution in the course of providing the Microsoft cloud services.*		
46.	Will use of the cloud service enable the institution to continue	The Personal Data Protection Act 2012 (PDPA) will generally apply to personal information collected by financial institutions. Yes, Microsoft has prepared a mapping document which indicates how Microsoft's compliance with ISO/IEC 27018 enables the customer to continue to comply with its key privacy obligations under the PDPA.

	complying with the PDPA?	
47.	Does the service provider agree to comply with the PDPA?	The financial institution is likely to be accountable for downstream use of the personal information by its service providers and, for information transferred outside of Singapore, the financial institution will need to ensure that it obtains sufficient commitments from its service provider to ensure that it complies with the PDPA. Yes, Microsoft will comply with the PDPA in respect of any personal information hosted by Microsoft while providing the cloud services. More general principles that are expressly stated in the Microsoft online services contract include commitments that: • Microsoft will use customer data only for the purposes of providing the services; • Customers retain all rights in, and effective control of, their data; and • Customers can extract, verify, amend or delete their data at any time. • Microsoft will not provide any third-party access to customer data except as directed by a customer or required by law; and • After a customer terminates its use of the service, customer data is held for at least 90 days to allow data to be extracted or migrated to a new service, and after this period it is deleted. The Microsoft online services contract also includes the standard contractual data protection clauses created by the European Union (called the "EU Model Clauses"), and the contract has also expressly been endorsed by the Article 29 Working Group (which comprises representatives from the Data Protection Authorities of the EU member states). Microsoft is also committed to GDPR compliance across their cloud services when enforcement begins on May 25, 2018, and that is why we provide GDPR related assurances in our contractual commitments. More information regarding GDPR compliance can be found here. Microsoft's contractual commitments, in combination with its independent certification process and the functionality of the Microsoft online services, collectively represent binding commitments which meet the threshold required by the PDPA.

Part 2: Contract Checklist

Core Microsoft contract documents	Documents incorporated in Microsoft contracts
Microsoft Business and Services Agreement (MBSA); Enterprise Agreement (EA); and the enabling Enrolment, which is likely to be either an Enterprise Enrolment or a Server and Cloud Enrolment	Online Service Terms (OST), incorporating the Data Processing Terms (DPT) including the EU Model Clauses; Product Terms Online Services Service Level Agreement (SLA)
Amendment provided by Microsoft to add to core contract documents for financial services customers Financial Services Amendment	Supporting documents and information that do not form part of the contract Materials available from the Trust Center

Part 2 sets out the specific items that should be covered in the financial institution's outsourcing agreement with the service provider, pursuant to the Outsourcing Guidelines and Notice 634, Banking Act (Appendix). It also contains useful information on how Microsoft's contractual documents address each of said items. Microsoft is pleased to conclude that all relevant requirements specified in the Guidelines on Outsourcing and Notice 634, Banking Act are addressed in Microsoft's contractual documents, as shown below.

Reference	Requirement	How and where is this dealt with in Microsoft's contract?
Outsourcing Guidelines, Paragraphs 5.5.2	(a) The outsourcing agreement should address the risks identified at the risk evaluation and due diligence stages.	This depends on the results of your risk evaluation and due diligence exercises.
Outsourcing Guidelines, Paragraphs 5.5.2	(b) The outsourcing agreement should allow for timely renegotiation and renewal to enable the institution to retain an appropriate level of control over the outsourcing arrangement and the right to intervene with appropriate measures to meet its legal and regulatory obligations.	In order to facilitate your continued and ongoing legal and regulatory compliance needs, and as part of its standard offering to you (i.e. the FSA that automatically applies to regulated financial services institution customers), Microsoft agrees to discuss how to meet new or additional requirements imposed on you should you become subject to Future Applicable Law (as defined in the FSA). Furthermore, Microsoft's contractual documents anticipate renewal. More information on your termination rights is available under Requirement (k) below. Meanwhile, Microsoft enables financial institution customers to retain an appropriate level of control to meet their legal and regulatory obligations. Not only do you have full control and ownership over your data at all times, under the FSA Microsoft (i) makes available to you the written cloud services

Reference	Requirement	How and where is this dealt with in Microsoft's contract?
		data security policy that complies with certain control standards and frameworks, along with descriptions of the security controls in place for Azure and other information that you reasonably request regarding Microsoft's security practices and policies; and (ii) causes the performance of audits, on your behalf, of the security of the computers, computing environment and physical datacentres that it uses in processing your data (including personal data) for the cloud services, and provides the audit report to you upon request. These arrangements are offered to you to provide you with the appropriate level of assessment of Microsoft's ability to facilitate compliance against your policy, procedural, security control and regulatory requirements. You can further elect to participate in the FSI Customer Compliance Program. This program allows you to engage with Microsoft during the term of the outsourcing contract to ensure that you have oversight over the services to ensure that the services meet your legal and regulatory obligations. Specifically, it enables you to have additional monitoring, supervisory and audit rights and additional controls over the cloud services, such as: (a) access to Microsoft personnel for raising questions and escalations relating to the cloud services, (b) invitation to participate in a webcast hosted by Microsoft to discuss audit results and subsequent access to detailed information regarding planned remediation of any deficiencies identified by the audit, (c) receipt of communication from Microsoft on: (1) the nature, common causes, and resolutions of security incidents and other circumstances that can reasonably be expected to have a material service impact on your use of the cloud services, (2) Microsoft's risk-threat evaluations, and (3) significant changes to Microsoft's business resumption and contingency plans or other circumstances that might have a serious impact on your use of Azure, (d) access to a summary report of the results of Microsoft's third-party penetration testing against the cloud services (e.g., evidence of data isolation among tenants), and (e) access to Microsoft's subject matter experts through group events such as webcasts or in-person meetings (including an annual summit event) where roadmaps of

Reference	Requirement	How and where is this dealt with in Microsoft's contract?
		planned developments or reports of significant events will be discussed, and you will have a chance to provide structured feedback and/or suggestions regarding the FSI Customer Compliance Program and its desired future evolution. The group events will also give you the opportunity to discuss common issues with other regulated financial institutions and raise them with Microsoft.
Outsourcing Guidelines, Paragraph 5.5.2(a)	(c) The outsourcing agreement should have provisions to address the scope of the outsourcing arrangement.	Microsoft's contractual documents comprehensively set out the scope of the outsourcing arrangement and the respective commitments of the parties. Microsoft enters into agreements with each of its financial institution customers for Online Services, which includes a Financial Services Amendment, the Online Services Terms, and the Service Level Agreement. The agreements clearly define the Online Services to be provided. The services are broadly described, along with the applicable usage rights, in the Product Terms and the OST, particularly in the OST "Core Features" commitments.
Outsourcing Guidelines, Paragraph 5.5.2(b)	(d) The outsourcing agreement should have provisions to address performance, operational, internal control and risk management standards.	All these aspects are covered in the OST and the SLA. The OST contains the privacy and security practices, and internal controls that Microsoft implements, and the SLA sets outs Microsoft's service level commitments for online services, as well as the service credit remedies for the customer if Microsoft does not meet the commitment. The SLA is fixed for the initial term of the Enrolment. *"We will not modify the terms of your SLA during the initial term of your subscription; however, if you renew your subscription, then the version of this SLA that is current at the time of renewal will apply for your renewal term."* For information regarding uptime for each Online Service, refer to the Service Level Agreement for Microsoft Online Services.

Outsourcing Guidelines, Paragraph 5.5.2(c)	(e) The outsourcing agreement should have provisions to address confidentiality and security.	The OST states that Microsoft and the customer each commit to comply with all applicable privacy and data protection laws and regulations. The customer always owns its data that is stored on Microsoft cloud services. The customer also always retains the ability to access its data, and Microsoft will deal with customer data in accordance with the terms and conditions of the Enrolment and the OST. Microsoft will retain customer data stored in the Online Service in a limited function account for 90 days after expiration or termination of customer's subscription so that the customer may extract the data. No more than 180 days after expiration or termination of the customer's use of an Online Service, Microsoft will disable the account and delete customer data from the account. *Outsourcing Guidelines, Paragraph 5.6.2(a). The outsourcing agreement should address the issue of access to and disclosure of customer information by the service provider. Customer information should be used by the service provider and its staff strictly for the purpose of the contracted service* *and* *Notice 634, Banking Act, Paragraph 8 of the Appendix. The agreement should contain obligations relating to the following: (i) access to customer data is limited to employees of service provider who strictly require the information to perform their duties: (ii) customer data is used strictly for a specified and disclosed purpose; and (iii) further disclosure of customer data to any other party is restricted unless required by law* Microsoft makes specific commitments with respect to safeguarding your data in the OST. In summary, Microsoft commits that: 1. Your data will only be used to provide the online services to you and your data will not be used for any other purposes, including for advertising or similar commercial purposes. (OST, page 7) 2. Microsoft will not disclose your data to law enforcement unless required by law. If law enforcement contacts Microsoft with a demand for your data, Microsoft will attempt to redirect the law enforcement agency to request that data directly from you. (OST, page 7)

		3. Microsoft has implemented and will maintain appropriate technical and organisational measures, internal controls, and information security routines intended to protect your data against accidental, unauthorised or unlawful access, disclosure, alteration, loss, or destruction. (OST, page 36) Technical support personnel are only permitted to have access to customer information when needed. (OST, page 13) *Outsourcing Guidelines, Paragraph 5.6.2(a). The outsourcing agreement should address the issue of the party liable for losses in the event of a breach of security or confidentiality and the service provider's obligation to inform the institution* The OST states the responsibilities of the contracting parties that ensure the effectiveness of security policies. To the extent that a security incident results from Microsoft's failure to comply with its contractual obligations, and subject to the applicable limitations of liability, Microsoft reimburses you for reasonable and third-party validated, out-of-pocket remediation costs you incurred in connection with the security incident, including actual costs of court- or governmental body-imposed payments, fines or penalties for a Microsoft-caused security incident and additional, commercially-reasonable, out-of-pocket expenses you incurred to manage or remedy the Microsoft-caused security incident (FSA, Section 3). Applicable limitation of liability provisions can be found in the MBSA. Microsoft further agrees to notify you if it becomes aware of any security incident, and to take reasonable steps to mitigate the effects and minimise the damage resulting from the security incident (OST).
Outsourcing Guidelines, Paragraphs 5.5.2(d) and 5.7.2 and Notice 634, Banking Act, Paragraph 11 of the Appendix	(f) The outsourcing agreement should have provisions to address business continuity management.	Business Continuity Management forms part of the scope of the accreditation that Microsoft retains in relation to the online services, and Microsoft commits to maintain a data security policy that complies with these accreditations (DPT, see OST page 13). Business Continuity Management also forms part of the scope of Microsoft's industry standards compliance commitments and Microsoft's annual third-party compliance audit. Business Continuity Plans (BCPs) are documented and reviewed at least annually, and the BCPs provide roles and responsibilities and detailed procedures for recovery and reconstitution of systems to a known state per

		defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). Microsoft also maintains emergency and contingency plans for the facilities in which Microsoft information systems that process customer data are located. Microsoft's redundant storage and its procedures for recovering data are designed to attempt to reconstruct customer data in its original or last-replicated state from before the time it was lost or destroyed. Data Recovery Procedures: • On an ongoing basis, but in no case less frequently than once a week (unless no customer data has been updated during that period), Microsoft maintains multiple copies of customer data from which customer data can be recovered. • Microsoft stores copies of customer data and data recovery procedures in a different place from where the primary computer equipment processing the customer data is located. • Microsoft has specific procedures in place governing access to copies of customer data. • Microsoft reviews data recovery procedures at least every six months, except for data recovery procedures for Azure Government Services, which are reviewed every twelve months. Microsoft logs data restoration efforts, including the person responsible, the description of the restored data and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process.
Outsourcing Guidelines, Paragraphs 5.5.2(e) and 5.8.1	(g) The outsourcing agreement should have provisions to address monitoring and control.	The OST allows customer to have the ability to access and extract customer data and specifies the audit and monitoring mechanisms that Microsoft puts in place to verify that the online services meet appropriate security and compliance standards. Microsoft also conducts regular penetration testing to increase the level of detection and protection throughout the Microsoft cloud. Microsoft makes available to customers penetration testing and other audits of its cybersecurity practices, and customers also may conduct their own penetration testing of the services. This is done in accordance with Microsoft's rules of engagement, which do not require Microsoft's permission in advance of such testing. In addition, the Financial Services Amendment details the examination and audit rights that are granted to the customer and MAS. The "Regulator Right to Examine" sets

		out a process which can culminate in the regulator's examination of Microsoft's premises. To enable the customer to meet its examination, oversight and control, and audit requirements, Microsoft has developed specific rights and processes that provide the customer with access to information, Microsoft personnel and Microsoft's external auditors. Microsoft will provide the customer with the following rights: 1. Online Services Information Policy Microsoft makes each Information Security Policy available to the customer, along with descriptions of the security controls in place for the applicable Online Service and other information reasonably requested by the customer regarding Microsoft security practices and policies. 2. Audits of Online Services On behalf of the customer, Microsoft will cause the performance of audits of the security of the computers, computing environment and physical datacentres that it uses in processing customer data for each Online Service. Pursuant to the terms in the OST, Microsoft will provide customer with each Microsoft Audit Report. 3. Financial Services Compliance Program The customer also can participate in the Financial Services Compliance Program, a for-fee program that facilitates the customer's ability to audit Microsoft. This program allows you to engage with Microsoft during the term of the outsourcing contract to ensure that you have oversight over the services to ensure that the services meet your legal and regulatory obligations. Specifically, it enables you to have additional monitoring, supervisory and audit rights and additional controls over Azure, such as (a) access to Microsoft personnel for raising questions and escalations relating to Azure, (b) invitation to participate in a webcast hosted by Microsoft to discuss audit results and subsequent access to detailed information regarding planned remediation of any deficiencies identified by the audit, (c) receipt of communication from Microsoft on (1) the nature, common causes, and resolutions of security incidents and other circumstances that can reasonably be expected to have a material service impact on your use of Azure, (2) Microsoft's risk-threat evaluations, and (3) significant changes to Microsoft's business resumption and contingency plans or other circumstances that might have a serious impact on your use of Azure, (d) access to a

		summary report of the results of Microsoft's third-party penetration testing against Azure (e.g. evidence of data isolation among tenants), and (e) access to Microsoft's subject matter experts through group events such as webcasts or in-person meetings (including an annual summit event) where roadmaps of planned developments or reports of significant events will be discussed and you will have a chance to provide structured feedback and/or suggestions regarding the FSI Customer Compliance Program and its desired future evolution. The group events will also give you the opportunity to discuss common issues with other regulated financial institutions and raise them with Microsoft.
Outsourcing Guidelines, Paragraphs 5.5.2(f), 5.9.2 and 5.10.2(b), for material outsourcing and Notice 634, Banking Act, Paragraph 8a of the Appendix	(h) The outsourcing agreement should have provisions to address audit and inspection.	The DPT specifies the audit and monitoring mechanisms that Microsoft puts in place to verify that the Online Services meet appropriate security and compliance standards. Rigorous third-party audits validate the adherence of Microsoft's Online Services to these strict requirements. Upon request, Microsoft will provide each Microsoft audit report to a customer to verify Microsoft's compliance with the security obligations under the DPT Microsoft also conducts regular penetration testing to increase the level of detection and protection throughout the Microsoft cloud. Microsoft makes available to customers penetration testing and other audits of its cybersecurity practices, and customers also may conduct their own penetration testing of the services. This is done in accordance with Microsoft's rules of engagement, which do not require Microsoft's permission in advance of such testing. Microsoft makes available certain tools through the Service Trust Portal to enable customers to conduct their own virtual audits of the Online Services. Microsoft also provides customers with information to reconstruct financial transactions and develop audit trail information through two primary sources: Azure Active Directory reporting, which is a repository of audit logs and other information that can be retrieved to determine who has accessed customer transaction information and the actions they have taken with respect to such information, and Azure Monitor, which provides activity logs and diagnostic logs that can be used to determine the "what, who, and when" with respect to changes to customer cloud information and to obtain information about the operation of the Online Services, respectively.

		In addition, the Financial Services Amendment details the examination and audit rights that are granted to the customer and the MAS. The "Regulator Right to Examine" sets out a process which can culminate in the regulator's examination of Microsoft's premises. To enable the customer to meet its examination, oversight and control, and audit requirements, Microsoft has developed specific rights and processes that provide the customer with access to information, Microsoft personnel and Microsoft's external auditors. Microsoft will provide the customer with the following rights: 1. Online Services Information Policy Microsoft makes each Information Security Policy available to the customer, along with descriptions of the security controls in place for the applicable Online Service and other information reasonably requested by the customer regarding Microsoft security practices and policies. 2. Audits of Online Services On behalf of the customer, Microsoft will cause the performance of audits of the security of the computers, computing environment and physical datacentres that it uses in processing customer data for each Online Service. Pursuant to the terms in the OST, Microsoft will provide Customer with each Microsoft Audit Report. 3. Financial Services Compliance Program The customer also has the opportunity to participate in the Financial Services Compliance Program, which is a for-fee program that facilitates the customer's ability to audit Microsoft, including: (a) assess the services' controls and effectiveness, (b) access data related to service operations, (c) maintain insight into operational risks of the services, (d) be provided with notification of changes that may materially impact Microsoft's ability to provide the services, and (e) provide feedback on areas for improvement in the services. In relation to the Outsourcing Guidelines requirement that requires the regulated entity to obtain examination and access rights from the service provider, Microsoft believes that the Financial Services Amendment meets this requirement.
Outsourcing Guidelines, Paragraphs 5.5.2(g) and 4.2	(i) The outsourcing agreement should have provisions to address notification of	Microsoft will notify the customer if it becomes aware of any security incident and will take reasonable steps to mitigate the effects and minimise the damage resulting from the security incident (see OST).

	adverse developments.	
Outsourcing Guidelines, Paragraph 5.5.2(h)	(j) The outsourcing agreement should have provisions to address dispute resolution.	If a financial institution and Microsoft have a dispute, the choice-of-law and dispute resolution provisions would be clearly described in the agreement between Microsoft and the financial institution. MBSA clauses 10(g) and 10(h) contains terms that describe how a dispute under the contract is to be conducted.
Outsourcing Guidelines, Paragraph 5.5.2(i) and Notice 634, Banking Act, Paragraph 10 of the Appendix	(k) The outsourcing agreement should have provisions to address default termination and early exit.	Microsoft agreements are usually subject to terms of 12-36 months, which may be extended at the customer's election. They also include rights to terminate early for cause and without cause. Microsoft's Financial Services Amendment provides for business continuity and exit provisions, including rights for the customer to obtain exit assistance at market rates from Microsoft Consulting Services. Customers should work with Microsoft to build such business continuity and exit plans. Microsoft's flexibility in offering hybrid solutions further facilitate transition from cloud to on-premise solutions more seamlessly.
Outsourcing Guidelines, Paragraph 5.5.2(j)	(l) The outsourcing agreement should have provisions to address sub-contracting.	Microsoft commits that its subcontractors will be permitted to obtain customer data only to deliver the services Microsoft has retained them to provide and will be prohibited from using customer data for any other purpose. Microsoft remains responsible for its subcontractors' compliance with Microsoft's obligations in the OST, which Microsoft considers complies with section 30 of the Outsourcing Guidelines[2] (OST, page 9). To ensure subcontractor accountability, Microsoft requires all its vendors that handle customer personal information to join the Microsoft Supplier Security and Privacy Assurance Program, which is an initiative designed to standardise and strengthen the handling of customer personal information, and to bring vendor business processes and systems into compliance with those of Microsoft. Microsoft will enter into a written agreement with any subcontractor to which Microsoft transfers customer data that is no less protective than the data processing terms in the customer's contracts with Microsoft (DPT, see OST, page 11). In addition, Microsoft's ISO/IEC 27018 certification requires Microsoft to ensure that its subcontractors are subject to the same security controls as Microsoft.

[2] Section 30 of the Outsourcing Guidelines provides "*A regulated institution that outsources a material business activity must ensure that its outsourcing agreement includes an indemnity to the effect that any subcontracting by a third-party service provider of the outsourced function will be the responsibility of the third-party service provider, including liability for any failure on the part of the sub-contractor.*"

		Microsoft's ISO 27001 certification provides a layer of additional controls that impose stringent requirements on Microsoft's subcontractors to comply fully with Microsoft's privacy, security, and other commitments to its customers, including requirements for handling sensitive data, background checks, and non-disclosure agreements. Microsoft provides a website that lists subcontractors authorised to access customer data in the Online Services as well as the limited or ancillary services they provide. At least 6 months before authorising any new subcontractor to access Customer Data, Microsoft will update the website and provide the customer with a mechanism to obtain notice of that update. If the customer does not approve of a new subcontractor, then the customer may terminate the affected Online Service without penalty by providing, before the end of the notice period, written notice of termination that includes an explanation of the grounds for non-approval. If the affected cloud computing service is part of a suite (or similar single purchase of services), then any termination will apply to the entire suite. After termination, Microsoft will remove payment obligations for the terminated Online Services from subsequent customer invoices. (DPT, see OST, page 11)
Outsourcing Guidelines, Paragraph 5.5.2(k)	(m) The outsourcing agreement should have provisions to address applicable laws	MBSA (Section 10.h) sets out the applicable law provision.
Outsourcing Guidelines, Paragraphs 5.5.3 and 5.10.2(b)	(n) The outsourcing agreement should be tailored to address issues arising from country risks and potential obstacles in exercising oversight and management of the outsourcing arrangements made with a service provider outside Singapore.	The DPT provides commitments on the location at which Microsoft will store customer data at rest (see OST, page 11). Microsoft cloud services offer data-location transparency so that the organisations and regulators are informed of the jurisdiction(s) in which data is hosted. The datacentres are strategically located around the world considering country and socioeconomic factors. Microsoft's datacentre locations are selected to offer stable socioeconomic environments. The OST contains general commitments around data location. Microsoft commits that customer data transfers out of the EU will be governed by the EU Model Clauses set out in the OST to represent a high standard of care in relation to data transfers. Also, as noted in the OST, "*Any subcontractors to whom Microsoft transfers Customer Data, even those used for storage purposes, will have entered into written agreements with Microsoft that are no less protective than the Data Processing Terms*."

		Microsoft also makes GDPR specific commitments (Attachment 4, OST) to all customers effective May 25, 2018.

References and Resources

- A Cloud for Global Good
- Customer Stories
- ISO 27018 and Singaporean Privacy Compliance
- Microsoft Trust Center
- Microsoft's response to the Outsourcing Guidelines and the ABS Cloud Implementation Guide
- Navigating Your Way to the Cloud
- Online Services Terms and Service Level Agreements
- SAFE Handbook
- Service Trust Portal