Navigating your way to the cloud

A compliance checklist for financial institutions in Hong Kong

Version: May 2020

Contents

Introduction: A compliance checklist for financial institutions in Hong Kong

Overview

Cloud computing is fast becoming the norm, not the exception, for financial institutions in Hong Kong.

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 Hong Kong. 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.

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

What does this checklist contain?

This checklist contains:

1. an **Overview of the Regulatory Landscape**, which introduces the relevant regulatory requirements in Hong Kong;

2. a **Compliance Checklist,** which lists the regulatory issues that need to be addressed and maps Microsoft's Online Services against those issues; and

3. details of where you can find **Further Information**.

Who is this checklist for?

This checklist is aimed at financial institutions in Hong Kong who want to use Microsoft Online Services. We use the term "financial institutions" (“**FIs**”) broadly, to include any entity that is regulated by the Hong Kong Monetary Authority (“**HKMA**”), the Insurance Authority in Hong Kong (“**IA**”) and/or the Securities and Futures Commission ("**SFC**") as the context may dictate. These entities include banks, credit unions, general insurers and life insurers (including virtual insurers), superannuation entities, brokers and dealers, investment advisors, asset managers, automated trading platform providers, and credit rating agencies.

What Microsoft cloud services does this checklist apply to?

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

Office 365:	microsoft.com/en-us/trustcenter/cloudservices/office365
Dynamics 365:	microsoft.com/en-us/trustcenter/cloudservices/dynamics365
Azure:	microsoft.com/en-us/trustcenter/cloudservices/azure

Is it mandatory to complete the checklist?

No. In Hong Kong, there is no mandatory requirement for FIs to complete a checklist to adopt Microsoft Online Services (although the IA has provided in its Guideline on Outsourcing checklists of information that it expects insurers (including virtual insurers) to submit to it for new or significant changes to existing outsourcing arrangements). Through conversations with our many cloud customers in Hong Kong, 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 Online Services can help FIs meet those regulatory requirements; third, as an internal framework for documenting compliance; and fourth, as a tool to streamline consultations with the HKMA, IA and the SFC, if they are required. By reviewing and completing the checklist, FIs can adopt Microsoft Online Services with confidence that they are complying with the requirements in Hong Kong.

How should we use the checklist?

1. 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.

2. Having done so, 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 the 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 Online Services. Combines the detailed information provided by Microsoft to auditors and regulators as part of various third-party audits of Microsoft‘s Online 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 cross team barriers to achieve their compliance goals. It also provides a secure repository for customers to upload and manage evidence and other artifacts 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.

3. 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 HKMA, IA and/or the SFC. You can also access more detailed information online, as set out in the Further Information section.

This document is intended to serve as a guidepost for customers conducting due diligence, including 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. While this paper focuses principally on Azure Core Services (referred to as “Azure”), Office 365 Services (referred to as “Office 365”) and Dynamics 365 Services (referred to as “Dynamics 365”), unless otherwise specified, these principles apply equally to all Online Services as defined and referenced in the Microsoft Online Services Data Protection Addendum (“DPA”) and Microsoft’s Online Services Terms.

Overview of the Regulatory Landscape

Are cloud services permitted?	**Yes.** This means that you can consider Microsoft Online Services for the full range of use-cases across your financial institution.
Who are the relevant regulators and authorities?	The Hong Kong Monetary Authority (“**HKMA”**), the Insurance Authority in Hong Kong (“**IA**”) and the Securities and Futures Commission ("**SFC**"). Banks, credit unions and certain other financial institutions are regulated by the HKMA. The HKMA website at http://www.hkma.gov.hk/eng/index.shtml provides links to underlying regulations and guidance. Insurance companies (including virtual insurance companies) are regulated by the IA. The IA website at https://www.ia.org.hk/en/index.html provides links to underlying regulations and guidance. Brokers and dealers, investment advisors, asset managers, automated trading platform providers, credit rating agencies and other financial institutions conducting SFC regulated activities are regulated by the SFC. The SFC website at www.sfc.hk provides links to underlying regulations and guidance.

What regulations and guidance are relevant?

There are several requirements and publicly available guidelines that FIs should be aware of when moving to the cloud:

1. HKMA’s General Principles for Technology Risk Management (“**Technology Risk Principles**”)

2. HKMA’s Guidelines on Outsourcing (“**Guidelines on Outsourcing**”)

3. The Personal Data (Privacy) Ordinance (the “**PDPO**”) and the Office of the Privacy Commissioner for Personal Data's ("**PCPD**") Information Leaflet on Outsourcing the Processing of Personal Data to Data Processors

4. The IA’s Guideline on Outsourcing (“**GL 14**”)

5. The IA's Guideline on Cybersecurity ("**GL 20**")

6. The IA's Guideline on Enterprise Risk Management ("**GL 21**")

7. SFC's Circular to Licensed Corporations on Use of External Electronic Data Storage dated 31 October 2019 (the "**EDSP Circular**")

8. The IOSCO Principles on Outsourcing of Financial Services for Market Intermediaries endorsed by the SFC in 2005 (the "**IOSCO Principles**")

9. Management, Supervision and Internal Control Guidelines for Persons Licensed by or Registered with the Securities and Futures Commission (the "**SFC Internal Control Guidelines**")

Virtual insurance companies are generally subject to the same requirements of the above guidelines issued by the IA.

There are also guidelines and documents issued by the HKMA to and accessible only by the FIs in this area. Due to the nature of these materials, they are out of the scope of this checklist.

Is regulatory approval required?

No, subject to below.

Under the Guidelines on Outsourcing and the Technology Risk Principles, the HKMA does not require FIs to obtain prior approval before engaging service providers to provide cloud services.

Under GL 14, the IA does not require FIs to obtain prior approval before engaging service providers to provide cloud services. Although there is no approval mechanism in place whether under the HKMA or the IA regulatory regime, prior notification requirements may apply (e.g. under GL14) and FIs may expect some discussions and/or consultations with their regulators. If you are a virtual bank, you should discuss your plans for material outsourcing with the HKMA in advance. Virtual insurance companies are generally subject to the same requirements under GL 14.

Under the EDSP Circular, if the FIs use Microsoft Online Services to keep their regulatory records (as defined in the EDSP Circular) exclusively, the FIs shall seek prior approval from the SFC in respect of the premises (including the data centre locations) for keeping such regulatory records. Also, the FIs shall notify the SFC in respect of changes of record keeping addresses.

Are transfers of data outside of Hong Kong permitted?	**Yes.** There are currently no restrictions on transfers to third countries. There are restrictions in section 33 of the PDPO, but these have not come into effect. In December 2014, the Privacy Commissioner issued a non-binding Guidance Note on Personal Data Protection in Cross- border Data Transfer. However, data users are still required to comply with the general requirements of the PDPO, including Data Protection Principle 3 when transferring personal data overseas (i.e. the transfer must be for a purpose for which the data were to be used at the time of the collection of the data or a directly related purpose; otherwise, express consent will be required in order to use personal data for a "new purpose"). Section 33 of the PDPO, in its current form and assuming it is in force, prohibits organizations from transferring data outside of Hong Kong except in certain circumstances, e.g. if the organization has taken all reasonable precautions and exercised due diligence to ensure that personal data will not be handled overseas in a manner that would be in contravention of the PDPO requirements if it occurred in Hong Kong (commonly referred to as the “Due Diligence Requirement”). Putting in place an enforceable contract between all parties to the transfer is a way to satisfy the Due Diligence Requirement and the Office of the Privacy Commissioner for Personal Data (PCPD) has proposed a set of recommended model clauses to include in such contract. Microsoft's Online Services Terms have in principle covered the core areas of the recommended model clauses.
Are public cloud services sufficiently secure?	**Yes.** Several FIs in Hong Kong are already using public cloud services. 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 Online 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.** These are not set out by HKMA in a comprehensive list, but the Guidelines on Outsourcing and Technology Risk Principles do contain certain provisions which HKMA states should be set out in the FI’s agreement with its service provider. The IA does not specifically mandate contractual requirements that must be agreed by insurances companies with their service providers. However, GL 14 does contain a long list of matters that it says that FIs should “consider” when negotiating the contract. Virtual insurance companies are generally subject to the same requirements under GL 14.

	These are not set out by the SFC in a comprehensive list, but the EDSP Circular does contain certain provisions which the SFC states should be set out in the FI's agreement with its electronic data service providers. In addition, the IOSCO Principles also contain a list of contractual provisions to be included. 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. In addition, under the PDPO, when outsourcing the processing of personal data to data processors, organizations are required to adopt "contractual or other means" of protection to (i) prevent any personal data transferred to the data processor from being kept longer than is necessary for processing of the data; and (ii) prevent unauthorized or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing.
How do general privacy laws apply to the use of cloud services by FIs?	FIs should ensure that the proposed outsourcing arrangement complies with relevant statutory requirements (e.g. the PDPO) and common law customer confidentiality. This will generally involve seeking legal advice. As stated in the Guidelines on Outsourcing, GL 14 and the IOSCO Principles, FIs should notify their customers in general terms of the possibility that their data may be outsourced. They should also give specific notice to customers of significant outsourcing initiatives, particularly where the outsourcing is to an overseas jurisdiction.

Compliance Checklist

How does this Compliance Checklist work?

In the **"Question/requirement"** column, we outline the regulatory requirement that needs to be addressed, based on the underlying requirements, along with other questions that our customers and regulators globally often expect to be addressed.

In the **"Guidance"** column, we explain how the use of Microsoft Online 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.

How should we use the Compliance Checklist?

Every FI 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 circumstances and requirements and its proposed use of cloud services.

Which part(s) do we need to look at?

There are two parts to this Compliance Checklist:

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

Part 1: Key Considerations

Who does this Part 1 apply to?

This Part 1 applies to all deployments of Microsoft Online Services by FIs in Hong Kong.

Ref.	Question / requirement	Guidance
A. OVERVIEW ***This section provides a general overview of the Microsoft Online Services***		
1.	Who is the service provider?	The service provider is 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: microsoft.com/en-us/investor/ Microsoft's Annual Reports are available here: microsoft.com/en-us/Investor/annual-reports.aspx
2.	What cloud services are you using?	Microsoft Office 365: microsoft.com/en-us/trustcenter/cloudservices/office365 Microsoft Dynamics 365: microsoft.com/en-us/trustcenter/cloudservices/dynamics365 Microsoft Azure: microsoft.com/en-us/trustcenter/cloudservices/azure
3.	What activities and operations will be outsourced to the service provider?	This Compliance Checklist is designed for FIs using Office 365, Dynamics 365 and/or Microsoft Azure. Each service is different and there are many different options and configurations available within each service. The response below will need to be tailored depending on how you intend to use Microsoft Online Services. Your Microsoft contact can assist as needed.

Ref.	Question / requirement	Guidance
		If using Office 365, services would typically include: • Microsoft Office applications (Outlook, Word, Excel, PowerPoint, OneNote and Access) • Exchange Online • OneDrive for Business, SharePoint Online, Microsoft Teams, Yammer Enterprise • Skype for Business If using Dynamics 365, services would typically include: • Microsoft Dynamics 365 for Customer Service, Microsoft Dynamics 365 for Field Service, Microsoft Dynamics 365 for Project Service Automation, Microsoft Dynamics 365 for Sales and Microsoft Social Engagement • Microsoft Dynamics 365 for Finance and Operations (Enterprise and Business Editions), Microsoft Dynamics 365 for Retail and Microsoft Dynamics 365 for Talent If using Microsoft Azure, services would typically include: • Virtual Machines, App Service, Cloud Services • Virtual Network, Azure DNS, VPN Gateway • File Storage, Disk Storage, Site Recovery • SQL Database, Machine Learning • IoT Hub, IoT Edge • Data Catalog, Data Factory, API Management • Security Center, Key Vault, Multi-Factor Authentication • Azure Blockchain Service

Ref.	Question / requirement	Guidance
4.	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 Online 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.* If using public cloud: 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. If using hybrid cloud: 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. 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 tenants is isolated from each other tenant as described in section E. (Technical and Operational Risk Q&A) below.

Ref.	Question / requirement	Guidance
5.	What data will be processed by the service provider on behalf of the FI?	*It is important to understand what data will be processed through Microsoft Online Services. You will need to tailor this section depending on what data you intend to store or process within Microsoft Online Services. The following are common categories of data that our customers choose to store and process in the Microsoft Online Services.* • Customer data (including customer name, contact details, account information, payment card data, security credentials and correspondence). • 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). • Transaction data (data relating to transactions in which the organisation is involved). • Indices (for example, market feeds). • Other personal and non-personal data relating to the organisation's business operations as a FI. • 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 process the data on your own systems or via a cloud solution.

Ref.	Question / requirement	Guidance
6.	How is the issue of counterparty risk addressed through your choice of service provider?	*The following is a summary of the factors that our customers typically tell us are important. To access more information about Microsoft, visit the* Trust Center*.* **a. Competence.** Microsoft is an industry leader in cloud computing. Microsoft Online 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 its current certifications is available at microsoft.com/en-us/trustcenter/compliance/complianceofferings. From a risk assurance perspective, Microsoft's technical and organisational measures are designed to meet the needs of FIs globally. Microsoft also makes specific commitments across its Online Services in its Online Services Terms available at https://www.microsoft.com/en-sg/Licensing/product-licensing/products.aspx. **Track-record.** Many of the world's top companies use Microsoft Online Services. There are various case studies relating to the use of Microsoft Online Services at customers.microsoft.com. Customers have obtained regulatory approvals (when required) and are using Online Services in all regions of the globe including Asia, North America, Latin America, Europe, Middle East and Africa. Key markets of adoption include, by way of example: the United States, Canada, Hong Kong, Singapore, Australia, Japan, the United Kingdom, France, Germany, Italy, Spain, the Netherlands, Poland, Belgium, Denmark, Norway, Sweden, Czech Republic, Brazil, Luxembourg, Hungary, Mexico, Chile, Peru, Argentina, South Africa, and Israel. Office 365 has grown to have over 100 million users, including some of the world's largest organisations and FIs. Azure continues to experience more than 90% growth, and over 80% of the largest FIs use or have committed to use Azure services.

Ref.	Question / requirement	Guidance
		b. Specific financial services credentials. FI customers in leading markets, including in the UK, France, Germany, Australia, Singapore, Canada, the United States and many other countries have performed their due diligence and, working with their regulators, are satisfied that Microsoft Online 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. **c. Financial strength of Microsoft.** Microsoft Corporation is publicly-listed in the United States and is amongst the world's largest companies by market capitalisation. Microsoft has a strong track record of stable profits. Its substantial market capitalisation makes it one of the top capitalised companies on the planet, Microsoft has been in the top 10 global market capitalised countries since 2000, and, indeed, is the only company in the world to consistently place in the top 10 of global market capitalised firms in the past twenty years. Its full company profile is available here: microsoft.com/en-us/investor/ and its Annual Reports are available here: microsoft.com/en-us/Investor/annual-reports.aspx. Accordingly, customers should have no concerns regarding its financial strength.

Ref.	Question / requirement	Guidance
7.	The FI should develop a framework for assessing the materiality of an outsourcing arrangement. The assessment of what is material may involve qualitative judgement and depends on the circumstances of the FI concerned.	*GL 14, Section 5.4. The IA deems a "material outsourcing" to be "an outsourcing arrangement which if disrupted or falls short of acceptable standards, would have the potential to significantly impact on an FI's financial position, business operation, reputation or its ability to meet obligations or provide adequate services to policy holders or to conform with legal and regulatory requirements." The IA expects you to be able to demonstrate that you have considered the materiality of the outsourcing in relation to at least the following factors:* a. Impact on financial position, business operation and reputation of the FI if the outsourced service is disrupted or falls short of acceptable standards; b. Impact on the ability of the FI to maintain adequate internal controls and comply with legal and regulatory requirements if the outsourced service is disrupted or falls short of acceptable standards; c. Cost of outsourcing as a proportion to the total operating costs of the FI; and

Ref.	Question / requirement	Guidance
		d. Degree of difficulty and time required to find alternative Service Provider or to bring the outsourced service in-house if necessary. Virtual insurance companies are generally subject to the same requirements under GL 14. In the EDSP Circular, the FIs should assess the level of their dependence on the prompt and consistent delivery of services by their service providers as well as the potential operational impact on the FIs and their clients. The IOSCO Principles endorsed by the SFC are applied according to the degree of materiality of the outsourced activity to the FI's business. FIs should therefore assess the materiality, and the IOSCO Principles have set out a non-exhaustive list of factors when determining the materiality of the outsourcing: a. Financial, reputational and operational impact on the outsourcing firm of the failure of a service provider to perform; b. Potential impact of outsourcing on the provision of adequate services to an outsourcing firm’s customers; c. Potential losses to an outsourcing firm's customers on the failure of a service provider to perform; d. Impact of outsourcing the activity on the ability and capacity of the outsourcing firm to conform with regulatory requirements and changes in requirements; e. Cost; f. Affiliation or other relationship between the outsourcing firm and the service provider; g. Regulatory status of the service provider; and h. Degree of difficulty and time required to select an alternative service provider or to bring the business activity in-house, if necessary.

B. OFFSHORING ***This section only applies to the extent that data and services will be hosted outside of Hong Kong. This will depend on the configuration of Microsoft Online Services that you select. Your responses will need to be tailored accordingly.***		
8.	Will the proposed outsourcing require offshoring? If so, from which territory(ies) will the outsourced cloud services be provided?	*Microsoft provides data location transparency. The relevant data locations of various Microsoft Online Services (including Office 365, Dynamics 365 and Microsoft Azure) can be checked at https://www.microsoft.com/en-us/TrustCenter/Privacy/where-your-data-is-located.*
9.	What other risks have been considered in relation to the proposed offshoring arrangement?	*Paragraph 2.9.1 (Additional Concerns in Relation to Overseas Outsourcing), Guidelines on Outsourcing.* *GL 14, Section 5.19 (a).* *EDSP Circular (in particular those provisions relating to the use of non-Hong Kong service providers).* *IOSCO Principles (in particular Part (II)(D), Topic 1 and Topic 2).* **a. Political (i.e. cross-border conflict, political unrest etc.)** Our customers know where their data is hosted. The relevant jurisdictions offer stable political environments. **b. Country/socioeconomic** Microsoft's data centres are strategically located around the world, taking into account country and socioeconomic factors. The relevant locations constitute stable socioeconomic environments. **c. Infrastructure/security/terrorism** Microsoft's data centres around the world are secured to the same exacting standards, designed to protect customer data from harm and unauthorised access. This is outlined in more detail at microsoft.com/en-us/trustcenter/security. **d. Environmental (i.e. earthquakes, typhoons, floods)**

Ref.	Question / requirement	Guidance
		Microsoft data centres are built in seismically safe zones. Environmental controls have been implemented to protect the data centres including temperature control, heating, ventilation and air-conditioning, fire detection and suppression systems and power management systems, 24-hour monitored physical hardware and seismically-braced racks. These requirements are covered by Microsoft's ISO/IEC 27001 accreditation. **e. Legal** Customers will have in place a binding negotiated contractual agreement with Microsoft in relation to the outsourced service, giving them direct contractual rights and maintaining regulatory oversight. The terms are summarised in Part 2.

Ref.	Question / requirement	Guidance
10.	Has a risk assessment been conducted to evaluate the extent and possibility of access to customers' data by overseas authorities taking place? Right of access by such parties may be unavoidable due to compulsion of law. The regulator should be notified if overseas authorities seek access to their customers' data. If such access seems unwarranted the regulator reserves the right to require FIs to take steps to make alternative arrangements for the outsourced activity.	*Paragraph 2.9.2 (Additional Concerns in Relation to Overseas Outsourcing), Guidelines on Outsourcing.* *GL 14, Section 5.19 (b).* *EDSP Circular (in particular those provisions relating to the use of non-Hong Kong service providers).* *IOSCO Principles (in particular Part (II)(D) and Topic 7).* Microsoft recommends that you consider this matter for the jurisdictions in which your data will be stored (refer to the response to Question 8 above), so that you are informed of the extent and the authorities to which you are legally bound to provide information.

Ref.	Question / requirement	Guidance
11.	Notification to customers FIs should generally notify their customers of the country in which the service provider is located (and of any subsequent changes) and the right of access, if any, available to the overseas authorities.	*Paragraph 2.9.1 (Additional Concerns in Relation to Overseas Outsourcing), Guidelines on Outsourcing.* *GL 14, Section 5.19 (c).* *IOSCO Principles (in particular Topic 4 and Topic 7).* Microsoft recommends that you confirm in this section that you have informed your customers that services will be provided from the relevant data locations (as appropriate according to the specification of your final solution with Microsoft). Microsoft also recommends that you confirm in this section that you have informed your customers of the right of access available to overseas authorities (depending on the specification of your final solution with Microsoft).
C. COMPLIANCE WITHIN YOUR ORGANISATION ***Financial institutions should have internal mechanisms and controls in place to properly manage the outsourcing. Although this is a matter for each FI, Microsoft provides some guidance, based on its experience of approaches taken by its customers. Ultimately this will need to be tailored for your FI to reflect its compliance practices.***		
12.	It is recommended that in assessing the options for outsourcing a material business activity to a third party, a FI should take certain	*Paragraph 2.3 (Ability of Service Providers), Guidelines on Outsourcing (Risk Assessment).* *EDSP Circular (paragraphs 7 and 12).* *IOSCO Principles (Topic 1).*

Ref.	Question / requirement	Guidance	
	steps by way of due diligence (as set out in the next column). How does the FI comply with the steps set out?	*(a) prepared a business case for outsourcing the material business activity;*	You should prepare a business case for the use of Microsoft Online Services. Where appropriate, this could include references to some of the key benefits of Microsoft Online Services, which are described at: • Microsoft Office 365: microsoft.com/en-us/trustcenter/cloudservices/office365 • Microsoft Dynamics 365: microsoft.com/en-us/trustcenter/cloudservices/dynamics365 • Microsoft Azure: microsoft.com/en-us/trustcenter/cloudservices/azure The factors listed below may be used to prepare a business case for the use of Microsoft Online 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 data centres 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.

Ref.	Question / requirement	Guidance	
			• IT control and efficiency. Microsoft Online Services perform basic 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 Online 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 programs like Microsoft Office, Outlook, and SharePoint are hosted on the cloud, company employees can access information remotely from a laptop, PC, or Smartphone.
		(b) undertaken a tender or other selection process for selecting the service provider;	You will need to describe what selection process you had in place. The factors listed 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). Additionally, see below for detail regarding certain specific issues that the HKMA, IA and SFC consider should be taken into account. **(a) Financial Soundness:** Microsoft Corporation is publicly-listed in the United States and is amongst the world's largest companies by market capitalization. Microsoft's audited financial statements indicate that it has been profitable for each of the past three years. Accordingly, you should have no concerns regarding its financial strength.

			(b) Reputation: Microsoft is an industry leader in cloud computing. Microsoft Online Services have been built based on ISO 27001 standards and have implemented the rigorous set of global standards covering physical, logical, process and management controls. Many of the world’s top brands use Microsoft Online Services. Some case studies are available on the Microsoft website. **(c) Managerial skills:** The fact that Microsoft already manages these services for FIs in leading markets around the world and that it has achieved an ISO 27001 accreditation (which, amongst other things, assesses management controls) gives you confidence that it has the necessary managerial skills. **(d) Technical capabilities:** Microsoft’s ISO 27001 accreditation confirms that it has the technical capability required for the service. **(e) Operational capability and capacity:** Microsoft has demonstrated its operational capability through its reputation and its ISO 27001 accreditation and you should have no concerns as to its operational capacity as it is one of the largest providers of cloud computing services in the world. **(f) Disaster recovery and business continuing processes:** Please refer to Question 48 of Microsoft Cloud Compliance Checklist. **(g) Compatibility with the FI’s corporate culture and future development strategies:** We are confident that the use of Microsoft Online Services will align well with your corporate culture and the fact that the service is scalable (i.e. it	

can be expanded or reduced to meet your demand) means that it is compatible with your future development strategy.

(h) **Familiarity with the banking, insurance and securities industries:** FI customers in leading markets, including in the UK, France, Germany, Australia, Hong Kong, Canada, the United States and many other countries have performed their due diligence and, working with their regulators, are satisfied that Microsoft Online Services meet their respective regulatory requirements. This gives you confidence that the service provider is able to help meet the high burden of financial services regulation and is experienced in meeting and understanding these requirements. Insurance company customers in leading markets, including in the UK, France, Germany, Australia, Hong Kong, Canada, the United States and many other countries have performed their due diligence and, working with their regulators, are satisfied that Microsoft Online Services meet their respective regulatory requirements.

(i) **Capacity to keep pace with innovation in the market:** Microsoft has the financial, operational and managerial capacity to lead innovation in the cloud computing market and it has demonstrated this to date.

(j) **Licence, registration, permission or authorization required by law to perform the outsourced service:** We are not aware of any licence, registration, permission or authorization required by us to perform the services that we do not already have in place. We are already providing such services to numerous FIs around the world.

(k) **Subcontracting arrangement:** 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 agreements with customers.

Ref.	Question / requirement	Guidance	
		(c) undertaken a due diligence review of the chosen service provider, including the ability of the service provider to conduct the business activity on an ongoing basis;	You will need to describe your due diligence process. Microsoft provides various materials to help you to perform and assess the compliance of Microsoft Online Services – including audit reports, security assessment documents, in-depth details of security and privacy controls, FAQs and technical white papers – at: microsoft.com/en-us/trustcenter/guidance/risk-assessment.

			(d) involved the Board of the institution, Board committee of the institution, or senior manager of the institution with delegated authority from the Board, in approving the agreement;	We would suggest having a list, setting out the position of the key people involved in the selection and any decision-making and approvals processes used.	
			(e) considered all of the minimum contractual	See Part 2 of this Compliance Checklist.	

Ref.	Question / requirement	Guidance	
		requirements required by HKMA, IA and SFC;	
		(f) established procedures for monitoring performance under the outsourcing agreement on a continuing basis;	See Question 16 for relevant information about the measures offered by Microsoft to enable customers to monitor performance. Such monitoring should cover, inter alia: • contract performance; • material problems encountered by the service provider; and • regular review of the service provider’s financial condition and risk profile and the service provider’s contingency plan, the results of testing thereof and the scope for improving it.
		(g) addressed the renewal process for outsourcing agreements and how the renewal will be conducted;	Yes. 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. Microsoft’s contractual documents anticipate renewal.
		(h) developed contingency plans that would enable	While your financial institution is ultimately responsible for developing its own contingency plans, based on its circumstances, Microsoft has developed a

Ref.	Question / requirement	Guidance
		the outsourced business activity to be provided by an alternative service provider or brought in-house if required? template that can be used to help develop a plan. This is available from the [Microsoft Service Trust Portal]or from your Microsoft contact upon request. Yes. The outsourcing agreement with Microsoft provides customers with the ability to access and extract their customer data stored in each Online Service at all times 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.
13.	Technology service providers should have sufficient resources and expertise to comply with the substance of the FI's IT control policies.	*Paragraph 7.1.1, Technology Risk Principles (Management of Technology Outsourcing).* Microsoft has sufficient resources and expertise to comply with the substance of your requirements. In particular: **a. Competence and experience.** Microsoft is an industry leader in cloud computing. Microsoft Online Services have been built based on, amongst others, ISO 27001 standards and have implemented the rigorous set of global standards covering physical, logical, process and management controls. **b. Past track-record.** Many of the world's top brands use Microsoft Online Services. There are various case studies relating to different Microsoft Online Services, which are available on the [Microsoft website]and Microsoft has amongst its customers some of the world's largest organizations and FIs. **c. Specific financial services credentials.** Financial Institution customers in leading markets, including in the UK, France, Germany, Australia, Hong Kong, Singapore, Canada, the United States and many other countries have performed their due diligence and, working with their regulators, are satisfied that Microsoft Online Services meet their respective

Ref.	Question / requirement	Guidance
		regulatory requirements. This gives confidence that Microsoft is able to help meet the high burden of financial services regulation and is experienced in meeting these requirements. **d. Microsoft's staff hiring and screening process.** All personnel with access to customer data are subject to background screening, 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. User access to data is also limited by user role. For example, system administrators are not provided with database administrative access. **e. Financial strength of Microsoft.** Microsoft Corporation is publicly-listed in the United States and is amongst the world's largest companies by market capitalization. Microsoft's audited financial statements indicate that it has been profitable for each of the past three years. **f. Business resumption and contingency plan.** Microsoft's data centres 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. **g. Security and internal controls, audit, reporting and monitoring.** Microsoft is an industry leader in cloud security and implements policies and controls on par with or better than on-premises data centers of even the most sophisticated organizations. In addition to the ISO 27001 certification, Microsoft Online Services are designed for security. For example, Office 365, Dynamics 365 and Microsoft Azure are designed with BitLocker Advanced Encryption Standard ("AES") encryption that applies to different scenarios and applications.
14.	Does the FI have a policy, approved by the Board, relating to the outsourcing?	*GL 14, Section 5.1 and 5.2. The IA requires that FIs have in place a comprehensive policy on outsourcing duly approved by the board of directors of the FI. This will differ from one organization to another but the IA expects that this will cover the following specific points:*

Ref.	Question / requirement	Guidance
		a. The objectives of the outsourcing and criteria for approving an outsourcing arrangement; b. The framework for evaluating the materiality of outsourcing arrangements; c. The framework for a comprehensive assessment of risks involved in outsourcing; d. The framework for monitoring and controlling outsourcing arrangements; e. The identities of the parties involved and their roles and responsibilities in approving, assessing and monitoring the outsourcing arrangements and how those responsibilities may be delegated and details of any authority limits; and f. The review mechanism to ensure the outsourcing policy and the monitoring and control procedures are capable to accommodate changing circumstances of the FI and cater for market, legal and regulatory developments. The appropriate policy will depend on the type of organisation and the Online Services in question, and will be proportional to the organisation's risk profile and the specific workloads, data, and purpose for using the Online Services. It will typically include: • a framework to identify, assess, manage, mitigate and report on risks associated with the outsourcing to ensure that the organisation can meet its financial and service obligations to its depositors, policyholders and other stakeholders; • the appropriate approval authorities for outsourcing depending on the nature of the risks in and materiality of the outsourcing (the policy itself needing to be approved by the board); • assessing management competencies for developing sound and responsive outsourcing risk management policies and procedures; • undertaking regular review of outsourcing strategies and arrangements for their continued relevance, safety and soundness; • ensuring that contingency plans, based on realistic and probable disruptive scenarios, are in place and tested; and

Ref.	Question / requirement	Guidance
		• ensuring that there is independent review and audit for compliance with the policies. Virtual insurance companies are generally subject to the same requirements under GL 14. You could use the information set out in Question 12 to develop your Board-approved policy. For example, in describing the service provider selection process, you could include in your policy analysis of the factors listed above with respect to Microsoft's reputation and track record. In addition, you may consider including in the policy that, as part of Microsoft's certification requirements, Microsoft is required to undergo regular, independent third-party audits. As a matter of course, Microsoft already commits to annual audits and makes available those independent audit reports to customers. The SFC does not specifically require FIs to have the outsourcing policy to be approved by the Board. However, the senior management of the FIs, including their directors, chief executive officer, managing director or other senior operating management personnel (as the case may be), are ultimately responsible for the adequacy and effectiveness of the corporation's internal control systems. The IOSCO Principles also state that FIs should develop and implement appropriate
15.	What procedures does the FI have in place to ensure that all its relevant business units are fully aware of, and comply with, the outsourcing policy?	You will need to explain how the relevant business units are brought under the scope of the outsourcing policy.

16.	What monitoring processes does the FI have in place to manage the outsourcing? Responsibility for monitoring the service provider and the outsourced activity should be assigned to staff with appropriate expertise.	*Paragraph 2.6.3 (Control over Outsourced Activities), Guidelines on Outsourcing.* *GL 14, Section 5.15.* *EDSP Circular (in particular paragraph 12).* *IOSCO Principles (Topic 1).* If requested by HKMA or SFC, Microsoft would suggest that you provide details of the relevant personnel and a brief summary of their experience. The guidance below explains how certain features of Microsoft Online Services 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 Online Services and your overall relationship with Microsoft. Microsoft provides access to “service health” dashboards (Office 365 Service Health Dashboard, Azure Status Dashboard and Dynamics 365 Service Health Dashboard)-providing real-time and continuous updates on the status of Microsoft’s Online Services. This provides your IT administrators with information about the current availability of each service or tool

Ref.	Question / requirement	Guidance
	The FI should maintain a central list of the outsourcing arrangements including the name of the Service Provider, service outsourced, commencement date, expiry or renewal date, contact details or key Service Provider personnel. The list should also record similar information relating to any sub-contracting arrangement of the outsourced service.	(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 Online 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 Online 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 data centres that it uses in processing their data (including personal data) for Microsoft Online 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 FI Customer Compliance Program at any time, which enables the customer to have additional monitoring, supervisory and audit rights and additional controls over Microsoft Online Services, such as (a) access to Microsoft personnel for raising questions and escalations relating to Microsoft Online 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 Online 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 Online Services, (d) access to a summary report of the results of Microsoft's third party penetration testing against Microsoft Online 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.

Ref.	Question / requirement	Guidance
17.	In case of outsourcing of critical technology services (e.g. data center operations), FIs are expected to commission a detailed assessment of the technology service provider's IT control environment. The assessment should ideally be conducted by a party independent of the service provider. The independent assessment report should set out clearly the objectives, scope and results of the assessment and should be provided to the regulator for reference.	*Paragraph 7.1.1, Technology Risk Principles (Management of Technology Outsourcing) which sets out some additional controls that FIs should take into account. In the case of a virtual bank, the HKMA expects the virtual bank to commission an independent assessment report on its computer hardware, systems, security procedures and controls from a qualified and independent expert. The general principle is that the security and technology related controls in place should be "fit for purpose", i.e. appropriate to the type of transactions which the virtual bank intends to carry out.* Numerous independent assessments of Microsoft's IT control environment have already been carried out. By way of example, Microsoft Online Services are certified for ISO/IEC 27001. ISO/IEC 27001 is one of the best security benchmarks available across the world. Microsoft Online Services have been built based on, amongst others, ISO 27001 standards and have implemented the rigorous set of global standards covering physical, logical, process and management controls.

18.	FIs should conduct an annual assessment to confirm the adequacy of the IT control environment of the provider of critical technology services.	*Paragraph 7.1.1, Technology Risk Principles (Management of Technology Outsourcing).* The HKMA expects that you repeat your assessment of the adequacy of the Microsoft Online Services at least once a year. In the case of a virtual bank, the HKMA expects you to establish procedures for regular review of your security and technology related arrangements (including but not limited to the cloud service arrangements with Microsoft) to ensure that such arrangements remain appropriate having regard to the continuing developments in technology. The general principle is that the security and technology related controls in place should be “fit for purpose”, i.e. appropriate to the type of transactions which the virtual bank intends to carry out. If you require any input from Microsoft, please do not hesitate to get in touch with your Microsoft contact.

Ref.	Question / requirement	Guidance
19.	Does the FI have access to adequate, independent information in order 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, use of the 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; • the Service Trust Platform, which provides confidential materials, such as third-party audit reports, to current customers and potential customers testing Microsoft's Online Services; • a Financial Services Compliance Program, which 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, Azure Status Dashboard and the Dynamics 365 Service Health Dashboard, which broadcast real-time information regarding the status of Microsoft's Online Services; and

Ref.	Question / requirement	Guidance
		- 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.
20.	How does the FI ensure that it maintains ultimate responsibility for, and control over, any outsourcing and that it avoids placing excessive reliance on a single outside service provider in providing critical technology services?	*Paragraph 2.1.1, Guidelines on Outsourcing (Accountability).* *Paragraph 7.1.1, Technology Risk Principles (Management of Technology Outsourcing).* *GL 14, Sections 4.1 and 4.2.* *EDSP Circular (in particular paragraphs 19, 20 and 22).* *IOSCO Principles (in particular Topic 5)* *You may also want to provide details of any other suppliers you use or intend to use.* The contract with Microsoft provides the customer with legal mechanisms to manage the relationship including appropriate allocation of responsibilities, oversight and remedies and any terms required by the HKMA, IA and SFC. Despite the outsourcing, you retain control over your own business operations, including control of who can access data and how they can use it. At a contractual level, this is dealt with via your contract with Microsoft, which provides you with legal mechanisms to manage the relationship including appropriate allocation of responsibilities, oversight and remedies. At a practical level, the Microsoft Online Services provide you with control over data location, authentication and advanced encryption controls. You will continue to own and retain all rights to your data and your data will not be used for any purpose other than to provide you with the Microsoft Online Services. Additionally, you do have in place contractual rights to exit the arrangements with Microsoft at any time for convenience, which gives you the flexibility to move to another provider (or to revert to a local non-cloud based or hybrid offering) should you choose to do so.

Ref.	Question / requirement	Guidance
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 the HKMA, IA and SFC expect 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 the HKMA, IA and SFC suggest are considered as part of the contractual negotiation but which are not necessarily mandatory contractual terms that should be included in all cases.***		
21.	Are the outsourcing arrangements contained in a documented legally binding written agreement that is signed by all parties and addresses the required matters set out in the Guidelines on Outsourcing and Technology Risk Principles, GL-14, the EDSP Circular and the IOSCO Principles?	*GL 14, Section 5.10.* *EDSP Circular (paragraph 21).* *IOSCO Principles (in particular Topic 2)* Microsoft enters into agreements with each of its financial institution customers for Microsoft Online Services, which includes amongst others a Financial Services Amendment, the Online Services Terms, and the Service Level Agreement. The agreements define the Online Services to be provided. The contractual documents are further outlined in Part 2, below.
22.	Does the outsourcing agreement include a clause that allows the relevant regulator to access documentation and information relating to the outsourcing arrangement? FIs should not outsource to a	*Paragraphs 2.8.1 and 2.8.2 (Access to Outsourced Data), Guidelines on Outsourcing.* *IOSCO Principles (Topic 2 and Topic 7)* Yes. There are terms in the contract that enable a financial services regulator 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 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.

Ref.	Question / requirement	Guidance
	jurisdiction which has secrecy laws that may hamper access to data by the regulator or FIs' external auditors. They should ensure that the regulator has right of access to data	*Paragraph 2.9.1 (Additional Concerns in Relation to Overseas Outsourcing), Guidelines on Outsourcing.* *EDSP Circular (paragraph 7)* Microsoft provides data location transparency (refer to the response to Question 8 above). Customers should consider the laws of those jurisdictions in respect of secrecy laws which may hamper access to data by a regulator or the FI's external auditors in the appropriate circumstances.
23.	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 the Microsoft 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. For information regarding uptime for each Microsoft Online Service, refer to the Service Level Agreement for Microsoft Online Services.
24.	Does the outsourcing agreement also include reporting mechanisms that ensure adequate oversight of IT security risk management by the service provider?	*Paragraph 2.6.4 (Control over Outsourced Activities), Guidelines on Outsourcing.* *IOSCO Principles (in particular Topic 2).* Yes as referenced in Question 19 above.
25.	Is the outsourcing agreement sufficiently flexible to accommodate changes to existing processes and to	Yes. The customer can always order additional services if required. The customer may terminate a Microsoft 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

Ref.	Question / requirement	Guidance
	accommodate new processes in the future to meet changing circumstances?	regulatory requirements, the customer may terminate the applicable Microsoft Online Service without cause by giving 60 days' prior written notice.
26.	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. Upon expiration or termination, the customer can extract its data. As set out in the OST, Microsoft will retain customer data stored in a Microsoft 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 a Microsoft 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

Under various regulatory requirements, including business continuity management and IT security risk requirements (which are not specific to outsourcing but should be considered nonetheless in the context of the outsourcing) FIs need to have in place appropriate measures to address IT risk, security risk, IT security risk and operational risk. This section provides some more detailed technical and operational information about Microsoft Online 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.

27.	Does the FI have a cyber risk policy in place?	*GL 21, Section 7.11. The IA requires that FIs should have a cyber risk policy in place, as part of their enterprise risk management framework, that is commensurate with the scale and complexity of the business, to identify, prevent, detect and mitigate cyber security threats. The cyber risk policy should address the approaches and controls which the FI has in place for the following matters:* *(a) protection of the personal data of its policy holders, and digital or electronic data of its business to ensure continuity of its business operations;* *(b) identification, prevention, detection and mitigation of cyber security threats;* *(c) identification of cyber security threats arising from technology tools and platform such as computer systems, mobile applications, the internet and telecommunication networks;* *(d) periodic testing on the robustness of the mitigation measures to deal with the cyber security threats timely and effectively;* *(e) approach and frequency on monitoring and reporting of cyber risks, including to other law enforcement authorities where applicable; and* *(f) regular review and assessment on the cyber security policies and procedures, as well as monitoring of their implementation.* *The FIs should communicate the cyber risk policy to its staff and as appropriate to other users of the cyber security system concerned.* *Virtual insurance companies are generally subject to the same requirements under GL 21.*

28.	Does the FI establish and maintain a cybersecurity strategy and framework endorsed by the Board?	*GL 20, Sections 4 and 7. The IA requires that FIs should establish and maintain a cybersecurity strategy and framework endorsed by the Board and tailored to mitigate relevant cyber risks that are commensurate with the nature, size and complexity of their business. When establishing the cybersecurity strategy and framework, FIs may make reference to or benchmark with the technology as well as the best available and practicable quality assurance standards such as ISO/IEC 27001.* *The cybersecurity framework should clearly define the FIs' cybersecurity objectives, as well as the requirements for competency of relevant personnel or system users. It should include well-defined processes and technology necessary for managing cyber risks and timely communication of the strategy with all users. FIs should test all elements of their cybersecurity framework to determine their overall effectiveness at least on an annual basis.* *FIs should review and update regularly their cybersecurity strategy to ensure that the strategy remains relevant when there is significant change in their mode of business operation or in the external business environment (including external cyber risk landscape. For example, a review should be undertaken at least on an annual basis, upon the occurrence of cyber incidents to the FI or major external cyber events which potentially could impact the FI, or upon the deployment of new systems or major systems changes.* *Virtual insurance companies are generally subject to the same requirements under GL 20.*
29.	Does the FI have effective monitoring processes for cyber risks?	*GL 20, Section 7. The IA requires that FIs should establish systematic monitoring processes for early detection of cybersecurity incidents; regularly evaluate the effectiveness of internal control procedures; and update the risk appetite and tolerance limit as appropriate. There should be effective monitoring measures including, among others, network monitoring, testing, internal audit and external audit. As part of the monitoring process, FIs should manage the identities and credentials for physical and remote access to information assets. They should recognize signs of a potential cyber risk, or monitor if an actual breach has taken place in their systems.* *Virtual insurance companies are generally subject to the same requirements under GL 20.*
30.	Does the service provider permit audit by the FI and/or the regulators?	*Paragraph 2.5.1, Guidelines on Outsourcing (Customer Data Confidentiality).* *Paragraph 2.6.5 (Control over Outsourced Activities), Guidelines on Outsourcing.*

Ref.	Question / requirement	Guidance
		The HKMA expects that your internal audit function would regularly review the outsourcing arrangement so you will need to confirm this. Yes. Pursuant to the Financial Services Amendment, Microsoft provides the regulators 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 the HKMA or IA requests to examine the Microsoft 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 data centres that it uses in processing customer data for each Microsoft 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.
31.	Are the provider's services subject to any third party audit?	*Paragraph 2.5.1, Guidelines on Outsourcing (Customer Data Confidentiality).* *Microsoft recommends that you do seek legal advice on the use of cloud computing services in relation to statutory/regulatory/common law requirements.* Yes. Microsoft's Online Services are subject to regular independent third party audits, including SSAE16 SOC1 Type II, SSAE SOC Type II, ISO/IEC 27001, ISO/IEC 27002 and ISO/IEC 27018. Rigorous third-party audits, including by Deloitte, validate the adherence of the Online Services to the strict requirements of these standards. 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.

32.	FIs should ensure that the proposed outsourcing	*Paragraph 2.5.1, Guidelines on Outsourcing (Customer Data Confidentiality).*

Ref.	Question / requirement	Guidance
	arrangement complies with relevant statutory requirements (e.g. the Personal Data (Privacy) Ordinance - PDPO) and common law customer confidentiality. This will generally involve seeking legal advice.	*GL 14, Section 5.12.* *Microsoft recommends that you do seek legal advice on the use of cloud computing services in relation to statutory/regulatory/common law requirements.* 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 data centers of even the most sophisticated organizations. In relation to the PDPO, Microsoft Online Services include the following features and commitments from Microsoft to ensure compliance with the requirements of the PDPO: (i) Microsoft will not use your data for any purposes other than providing the services; (ii) Microsoft will not disclose processed data except as you direct, as described in our Data Protection Addendum, or as required by law; (iii) Microsoft has security policies and controls and security measures which are verified by independent auditors. These measures include security features on its hardware, software and physical data center, restricted physical data center access, Microsoft Online Services are ISO 27001 compliant and data is encrypted both at rest and via the network as it is transmitted between data center and a user; (iv) Microsoft will inform you promptly if your data has been accessed improperly; (v) at all times during your subscription, you have the ability to access, extract and delete your data, and your data will be deleted at the end of the service term, once you have been able to take a copy of your data as necessary; (vi) Microsoft contractually ensures that its sub-processors only access and use your data for the services Microsoft has retained them to provide and that they are prohibited from using your data for any other purpose. In addition Microsoft commits to comply with ISO/IEC 27018. In February 2015, Microsoft became the first major cloud provider to adopt the world's first international standard for cloud privacy, ISO/IEC 27018. The standard was developed by the International Organization for Standardization (ISO) to establish a uniform, international approach to protecting privacy for personal data stored in the cloud. The British Standards Institute (BSI) has now independently verified that Microsoft is aligned with the standard's code of practice for the protection of Personally Identifiable Information (PII) in the public cloud. The controls set out in ISO/IEC 27018 match the protections required by the PDPO. ISO/IEC 27018 is specifically referenced in the Hong Kong Privacy Commissioner's Information Leaflet on Cloud Computing.
33.	What security controls are in place to protect	*Paragraph 2.5.2, Guidelines on Outsourcing (Customer Data Confidentiality).*

Ref.	Question / requirement	Guidance
	the transmission and storage of confidential information such as customer data within the infrastructure of the service provider?	*GL 14, Section 5.12.* *EDSP Circular (paragraphs 7(e), 14, 15 and 17).* *IOSCO Principles (Topic 3 and Topic 4).* *Microsoft recommends that you seek legal advice as to PDPO requirements.* 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 data centres of even the most sophisticated organisations. Microsoft Online 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 Online 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 Online 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 data centres 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 data centre. 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

Ref.	Question / requirement	Guidance
		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 scrutinized, 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 Online Services exists in two states: • at rest on storage media; and • in transit from a data centre over a network to a customer device. Microsoft offers a range of built-in encryption capabilities to help protect data at rest. • For Office 365, Microsoft follows industry cryptographic standards such as TLS/SSL and AES to protect the confidentiality and integrity of customer data. For data in transit, all customer-facing servers negotiate a secure session by using TLS/SSL with client machines to secure the customer data. For data at rest, Office 365 deploys BitLocker with AES 256-bit encryption on servers that hold all messaging data, including email and IM conversations,

Ref.	Question / requirement	Guidance
		as well as content stored in SharePoint Online and OneDrive for Business. Additionally, in some scenarios, Microsoft uses file-level encryption. • For Azure, technological safeguards such as encrypted communications and operational processes help keep customers' data secure. Microsoft also provides customers the flexibility to implement additional encryption and manage their own keys. For data in transit, Azure uses industry-standard secure transport protocols, such as TLS/SSL, between user devices and Microsoft data centres. For data at rest, Azure offers many encryption options, such as support for AES-256, giving customers the flexibility to choose the data storage scenario that best meets the customer's needs. • For Dynamics 365, in addition to the ISO 27001 certification, Dynamics 365 is designed for security with encryption features. All email content is encrypted on disk using BitLocker AES encryption. Protection covers all disks on mailbox servers and includes mailbox database files, mailbox transaction log files, search content index files, transport database files, transport transaction log files, and page file OS system disk tracing/message tracking logs. Dynamics 365 also transports and stores S/MIME (as defined above) messages. Dynamics 365 will transport and store messages that are encrypted using client-side, third-party encryption solutions such as PGP. Microsoft Dynamics 365 uses standard Microsoft SQL Server cell level encryption for a set of default entity attributes that contain sensitive information, such as user names and email passwords. This feature can help meet compliance requirements associated with FIPS 140-2. Field-level data encryption is especially important in scenarios that leverage the Microsoft Dynamics CRM Email Router, which must store user names and passwords to enable integration between a Dynamics 365 instance and an email service such as Microsoft Exchange. Additionally, Field-level data encryption is also supported for specific system entity attributes. Such policies and procedures are available through Microsoft's online resources, including the Trust Center and the Service Trust Platform. Regarding the specific safeguards referred to in the HKMA Supervisory Policy Manual:

Ref.	Question / requirement	Guidance
		- **Undertakings by the service provider that the company and its staff will abide by confidentiality rules, including taking account of the data protection principles set out in PDPO:** There are contractual confidentiality terms in your agreements with Microsoft. - **FIs' contractual rights to take action against the service provider in the event of a breach of confidentiality:** You can expect to have a breach of contract claim in this situation. - **Segregation or compartmentalization of FIs' customer data from those of the service provider and its other clients:** Data storage and processing is segregated through Active Directory structure and capabilities specifically developed to help build, manage, and secure multi-tenant environments. Active Directory isolates customers using security boundaries (also known as silos). This safeguards a customer's data so that the data cannot be accessed or compromised by other parties. - **Access rights to FIs' data delegated to authorize employees of the service provider on a need basis:** Microsoft applies strict controls over which personnel roles and personnel will be granted access to customer data. Personnel 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, fingerprinting, 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.
34.	How is the FI's data isolated from other data held by the service provider?	For all of the Microsoft Online Services, data storage and processing is segregated through Active Directory structure and capabilities specifically developed to help build, manage, and secure multi-tenant environments. Active Directory isolates customers using security boundaries (also known as silos). This safeguards a customer's data so that the data cannot be accessed or compromised by other parties.

Ref.	Question / requirement	Guidance
35.	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, Microsoft 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.
36.	What policies does the service provider have in place to monitor employees with access to confidential information?	All personnel with access to customer data are subject to background screening, 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. User access to data is also limited by user role. For example, system administrators are not provided with database administrative access.
37.	How are customers authenticated?	Microsoft Online 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.

38.	What are the procedures for identifying, reporting and responding to suspected security incidents and violations? Additionally, FIs should establish reporting procedures which can promptly escalate problems relating to the outsourced activity to the attention of the management of the FI and their service providers. The FI should then take appropriate rectification actions forthwith if deficiencies are identified.	*Paragraph 2.6.4 (Control over Outsourced Activities), Guidelines on Outsourcing.* *GL 14, Section 5.16.* *GL 20, Section 8* *Virtual insurance companies are generally subject to the same requirements under GL 14 and GL 20.* 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. Data centre 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. 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.

Ref.	Question / requirement	Guidance
		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, the Office 365 Service Health Dashboard, and the Dynamics 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 leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to customer data, Microsoft notifies affected parties without unreasonable delay (refer to the Online Services Terms, under the heading 'Security Incident Notification'). 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 Online 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:

Ref.	Question / requirement	Guidance
		• 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. For more information regarding Microsoft's security incident management, refer to http://aka.ms/SecurityResponsepaper. • *Minimising Service Disruptions—Redundancy*. Microsoft makes every effort to minimise service disruptions, including by implementing physical redundancies at the disk, Network Interface Card ("NIC"), 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.

Ref.	Question / requirement	Guidance
		- *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, the Office 365 Service Health Dashboard and the Dynamics 365 Service Health Dashboard, among other online resources, which allow customers to monitor security threats on the cloud service provider's server. Service Provider Escalation As part of the support you receive from Microsoft you have access to a technical account manager who is responsible for understanding your challenges and providing expertise, accelerated support and strategic advice tailored to your organization. This includes both continuous hands-on assistance and immediate escalation of urgent issues to speed resolution and keep mission-critical systems functioning.
39.	How is end-to-end application encryption security implemented to protect PINs and other	Microsoft Online Services use industry-standard secure transport protocols for data as it moves through a network—whether between user devices and Microsoft data centres or within data centres themselves. To help protect data at rest, Microsoft offers a range of built-in encryption capabilities.

Ref.	Question / requirement	Guidance
	sensitive data transmitted between 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 your 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: a. Transport Layer Security (TLS), which uses symmetric cryptography based on a shared secret to encrypt communications as they travel over the network. b. 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. c. 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. d. 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. e. 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

Ref.	Question / requirement	Guidance
		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. f. 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. g. 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. h. Transparent Data Encryption (TDE) encrypts data at rest when it is stored in an Azure SQL database. i. 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). j. 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). k. Dynamics 365 is designed for security with encryption features. All email content is encrypted on disk using BitLocker AES encryption. Protection covers all disks on mailbox servers and includes mailbox database files, mailbox transaction log files, search content index files, transport database files, transport transaction log files, and page file OS system disk tracing/message tracking logs. Dynamics 365 also transports and stores S/MIME (as defined above) messages. Dynamics 365 will transport and store messages that are encrypted using client-side, third-party encryption solutions such as PGP. Microsoft Dynamics 365 uses standard Microsoft SQL Server cell level encryption for a set of default entity attributes that contain sensitive information, such as user names and email passwords. This feature can help meet compliance requirements associated with FIPS 140-2. Field-level data encryption is especially important in scenarios that leverage the Microsoft Dynamics CRM Email Router, which must store user names and passwords to enable integration between a Dynamics 365 instance and an email service such as Microsoft Exchange. Additionally, Field-level data encryption is also supported for specific system entity attributes.

Ref.	Question / requirement	Guidance
		3. Secure apps and data: The specific controls for each Microsoft cloud service are described in more detail at microsoft.com/en-us/trustcenter/security/encryption.
40.	Are there procedures established to securely destroy or remove the data when the need arises (for example, when the contract terminates)?	*Paragraph 2.5.4, Guidelines on Outsourcing (Customer Data Confidentiality).* *GL 14, Section 5.13.* Yes. Microsoft uses best practice procedures and a wiping solution that is NIST 800-88, ISO/IEC 27001, ISO/IEC 27018, SOC 1 an 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.
41.	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 data centres are monitored using motion sensors, video surveillance and security breach alarms.

Ref.	Question / requirement	Guidance
42.	Are there documented security procedures for safeguarding hardware, software and data in the data centre?	Yes. These are described at length in the Microsoft Trust Center at microsoft.com/trust. For information on: • design and operational security see https://www.microsoft.com/en-us/trustcenter/security/designopsecurity • network security see https://www.microsoft.com/en-us/trustcenter/security/networksecurity • encryption see https://www.microsoft.com/en-us/trustcenter/security/encryption • threat management see https://www.microsoft.com/en-us/trustcenter/security/threatmanagement • identify and access management see https://www.microsoft.com/en-us/trustcenter/security/identity
43.	How are privileged system administration accounts managed? Describe the procedures governing the issuance (including emergency usage), protection, maintenance and destruction of these accounts. Please describe how the privileged accounts are subjected to dual control (e.g. password is split into 2 halves and each given to a different staff for custody).	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. For more information regarding Microsoft identity and access management, see https://www.microsoft.com/en-us/trustcenter/security/identity. 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. An internal, independent Microsoft team audits the log at least once per quarter, and customers have access to such

Ref.	Question / requirement	Guidance
		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.
44.	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.	Yes. An internal, independent Microsoft team will audit the log at least once per quarter. More information is available at microsoft.com/en-us/trustcenter/security/auditingandlogging.
45.	Are the audit/activity logs protected against tampering by users with privileged accounts? Describe the safeguards implemented.	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. 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. 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.

Ref.	Question / requirement	Guidance
46.	Is access to sensitive files, commands and services restricted and protected from manipulation? Provide details of controls implemented.	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. For more information regarding Microsoft identity and access management, see https://www.microsoft.com/en-us/trustcenter/security/identity.

47.	What remote access controls are implemented?	Administrators who have rights to applications have no physical access to the production systems. So administrators have to 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. For more information regarding Microsoft identity and access management, see https://www.microsoft.com/en-us/trustcenter/security/identity.

Ref.	Question / requirement	Guidance
48.	Does the service provider have a disaster recovery or business continuity plan? Have you considered any dependencies between the plan(s) and those of your FI? Procedures should be in place for regular reviews and testing of the contingency plan. In establishing a viable contingency plan, FIs should consider, among other things, the availability of alternative service providers or the possibility of bringing the outsourced activity	*Paragraph 7.1.1 (Management of Technology Outsourcing), Technology Risk Principles.* *Paragraph 22, EDSP Circular* *GL 14, Section 5.17.* You are expected to have a contingency plan in place, covering disaster recovery/business continuity. This would usually include: • performing a business impact analysis of a disaster situation; • considering the internal mechanisms to deal with such a situation; and • considering the relevant Microsoft's Online Service's own disaster recovery and business continuity safeguards. *Paragraph 2.7.2 (Contingency Planning), Guidelines on Outsourcing.* *The HKMA requirements indicate the importance of you understanding the disaster recovery/business continuity safeguards forming part of the Microsoft Online Services. As such, if you have any questions about these, please do not hesitate to get in touch with your Microsoft contact.* - Microsoft makes every effort to minimise service disruptions, including by implementing physical redundancies at the disk, NIC, power supply, and server levels; constant content replication; robust backup, restoration, and failover capabilities; and

Ref.	Question / requirement	Guidance
	back in-house in an emergency, or any other alternative arrangements to ensure operational resilience.	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, data centre, 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 data centres 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 data centre 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 controllers (ADC/load balancing) functionality. Load balancing is also provided by Power BI Services, the Gateway, and Azure API Management roles. • *Distributed Services*. Microsoft also offers distributed component services like Exchange Online, SharePoint Online, and Skype for Business 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.

Ref.	Question / requirement	Guidance
		- *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.
49.	What are the recovery time objectives (RTO) of systems or applications outsourced to the service provider?	The RTO for each Microsoft Online Service is specified in the Service Level Agreement (SLA) here: http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=37 -
50.	What are the recovery point objectives (RPO) of systems or	- **Office 365:** Peer replication between data centres 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

Ref.	Question / requirement	Guidance
	applications outsourced to the service provider?	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. Information on each Office 365 service available from the Office 365 Trust Center: https://www.microsoft.com/en-us/trustcenter/cloudservices/office365 ○ 45 minutes or less for Microsoft Exchange Online ○ 2 hours or less for SharePoint Online • **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: microsoft.com/en-us/trustcenter/cloudservices/azure ○ 1 minute of less for Virtual Storage
51.	What are the data backup and recovery arrangements for your organisation's data that resides with the service provider?	**Redundancy** • Physical redundancy at server, data centre, and service levels. • Data redundancy with robust failover capabilities. • 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. Additionally, 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 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 replicates certain data between two regions within the same location for enhanced data durability in case of a major data centre disaster.

Ref.	Question / requirement	Guidance
		Resiliency • Active/active load balancing. • Automated failover with human backup. • 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. **Distributed Services** • Distributed component services like Exchange Online, SharePoint Online, and Skype for Business limit scope and impact of any failures in a component. • Directory data replicated across component services insulates one service from another in any failure events. • Simplified operations and deployment. **Monitoring** • Internal monitoring built to drive automatic recovery. • Outside-in monitoring raises alerts about incidents. • Extensive diagnostics provide logging, auditing, and granular tracing.

Ref.	Question / requirement	Guidance
		Simplification • Standardised hardware reduces issue isolation complexities. • Fully automated deployment models. • Standard built-in management mechanism. **Human Backup** • Automated recovery actions with 24/7 on-call support. • Team with diverse skills on the call provides rapid response and resolution. • Continuous improvement by learning from the on-call teams. **Continuous Learning** • If an incident occurs, Microsoft does a thorough post-incident review every time. • Microsoft's post-incident review consists of analysis of what happened, Microsoft's response, and Microsoft's plan to prevent it in the future. • If the organisation was affected by a service incident, Microsoft shares the post-incident review with the organisation. **Disaster recovery tests** • Microsoft conducts disaster recovery tests at least once per year.
52.	How frequently does the service provider conduct disaster recovery tests?	Microsoft conducts disaster recovery tests at least once per year. By way of background, Microsoft maintains physical redundancy at the server, data center, 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.

Ref.	Question / requirement	Guidance
		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 datacenters 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 datacenter 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. For more information, refer to Microsoft’s white paper “Data Resiliency in Microsoft Office 365,” available at https://aka.ms/Office365DR.
53.	The Board of Directors and management of FIs should ensure that the proposed outsourcing arrangement has been subject to a comprehensive risk assessment (in respect of operational, legal, reputation and cyber risks) and that all the risks identified have been	*Paragraph 2.2.1, Guidelines on Outsourcing (Risk Assessment)* *GL 14, Section 5.6.* *GL 20, Section 6.1* The HKMA and IA expect that your organization would have carried out a risk assessment. In summary, this would need to include: • 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.

Ref.	Question / requirement	Guidance
	adequately addressed before launch.	Ideally this should also include all of the items listed in the next section. If you have any questions when putting together a risk assessment, please do not hesitate to get in touch with your Microsoft contact.
54.	Specifically, the risk assessment should cover inter alia the following:	
	a. the importance and criticality of the services to be outsourced;	*Paragraph 2.2.1, Guidelines on Outsourcing (Risk Assessment).* You should identify here the importance and criticality of the services to be outsourced, and how risks are managed. For example, risks could be managed through: • the choice of service provider, being the result of a formal selection process that amongst other things covers competence and track record, financial services credentials, hiring and screening processes, financial and parent company strength, inputs from its customers and its approach to continuity planning; • the controls in place to manage the relationship with the service provider (for example, your contractual agreement with Microsoft, service levels and the rights of audit and inspection that are in place); and • your own internal controls should an issue arise (for example, your disaster recovery planning process).
	b. Reasons for the outsourcing (e.g. cost and	*Paragraph 2.2.1, Guidelines on Outsourcing (Risk Assessment).*

Ref.	Question / requirement	Guidance
	benefit analysis); and	You should identify the reasons for your choice of the Microsoft Online Services (e.g., the Microsoft Online Services have been chosen specifically for these services because it is capable of delivering benefits in terms of operating costs, service standard and security).

	c. the impact on the FI's risk profile (in respect of operational, legal, reputation and cyber risks) of the outsourcing.	*Paragraph 2.2.1, Guidelines on Outsourcing (Risk Assessment).* *GL 14, Section 5.6.* *GL 20, Section 6.1* • **Operational risk:** This is managed this through the choice of service provider, the controls in place to manage your relationship with the service provider (for example, your contractual agreement, service levels, access to a Microsoft technical account manager and the regulator rights of audit and inspection that are in place) and your own internal controls (for example, your business continuity and disaster recovery plans). • **Legal risk:** You have in place with Microsoft a legally-binding agreement regarding your respective roles and responsibilities in respect of the outsourcing. • **Reputational risk:** Microsoft has been chosen because of its reputation in this sector. It is an industry leader in cloud computing. Microsoft Online Services have been built based on ISO 27001 standards and have implemented the rigorous set of global standards covering physical, logical, process and management controls. • **Cyber risk:** 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. • **Risk of loss to customers in the event of a failure:** The outsourcing will not involve critical functions so the risks

Ref.	Question / requirement	Guidance
55.	After FIs implement an outsourcing plan, they should regularly re-perform this assessment.	*Paragraph 2.2.2, Guidelines on Outsourcing (Risk Assessment). The Guidelines do not specify exactly how often this needs to be done but the HKMA may wish to know how often you plan to re-perform the assessment (e.g. annually may be a good suggestion and/or whenever any material changes occur).* In the case of a virtual bank, you should establish procedures for regular review of your security and technology related arrangements to ensure that such arrangements remain appropriate having regard to the continuing developments in technology. *GL 20, Section 6.2. FIs should regularly review and assess if changes to cyber risk mitigation processes are necessary when significant changes to organizational and operational structure and systems take place. For example, the review should be on an annual basis or upon major deployment of systems.*

F. PRIVACY		
56.	FIs should ensure that the proposed outsourcing arrangement complies with relevant statutory requirements (e.g. the Personal Data (Privacy) Ordinance (“**PDPO**”)) and common law customer confidentiality.	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 data centers of even the most sophisticated organizations. In relation to the PDPO, the Microsoft Online Services include the following features and commitments from Microsoft to ensure compliance with the requirements of the PDPO: (i) Microsoft will not use your data for any purposes other than providing the services; (ii) Microsoft will not disclose processed data except as you direct, as described in our Data Protection Addendum, or as required by law; (iii) Microsoft has security policies and controls and security measures which are verified by independent auditors. These measures include security features on its hardware, software and physical data center, restricted physical data center access, the Microsoft Online Services are ISO/IEC 27001 compliant and data is encrypted both at rest and via the network as it is transmitted between data center and a user; (iv) Microsoft will inform you promptly if your data has been accessed improperly; (v) at all times during your subscription, you have the ability to access, extract and delete your data, and your data will be deleted at the end of the service term, once we have been able to take a copy of your data as necessary; (vi) Microsoft contractually ensures that its sub-processors only access and use your data for the services Microsoft has retained them to provide and that they are prohibited from using your data for any other purpose. In addition Microsoft commits to comply with ISO/IEC 27018. In February 2015, Microsoft became the first major cloud provider to adopt the world’s first international standard for cloud privacy, ISO/IEC 27018. The standard was developed by the International Organization for Standardization (ISO) to establish a uniform, international approach to protecting privacy for personal data stored in the cloud. The British Standards Institute (BSI) has now independently verified that Microsoft is aligned with the standard’s code of practice for the protection of Personally Identifiable Information (PII) in the public cloud. The controls set out in ISO/IEC 27018 match the protections required by the PDPO. Microsoft offers access and audit rights, thereby allowing you to comply with your regulatory obligations in this respect. ISO/IEC 27018 is specifically referenced in the Hong Kong Privacy Commissioner's Information Leaflet on Cloud Computing.

G. The SFC's powers to request for information to conduct supervisory compliance inspections and investigations under *the SFO and the AMLO*		
Ref.	**Question / requirement**	**Guidance**

57.	What are the SFC powers to request for information stored with the service providers like Microsoft?	**Powers to request for information for compliance supervision of Licensed Corporations ("LCs"):** The SFC has a broad range of powers to perform its supervisory functions to ascertain if the LCs are in compliance with the applicable laws and regulations: (i) **Section 180 of the SFO**: In order to ensure that the LCs are in ongoing compliance with their statutory and regulatory obligations under relevant SFO provisions and their licensing conditions etc., the SFC has the power to request for access to or production of records and documents, or make inquiries thereof, regarding the businesses and transactions conducted by such LCs. (ii) **Section 9 of the AMLO**: As part of its ongoing powers to conduct supervisory checks over the LCs to ensure their compliance with relevant AMLO laws and regulations, the SFC has the power to request for access to or production of records and documents, or make inquiries thereof, regarding the businesses and transactions conducted by such LCs. In general, the powers to request for production of information, documents and records above may be exercised not only against the relevant LCs, but also against "any person", whether or not connected to such entities, which the SFC has reasonable cause to be believe has **possession** of the relevant information. The term "**possession**" is defined under *Schedule 1 to the SFO* to include "custody, control and power" over the relevant matter. Having said that, in the ordinary context where the SFC conducts its routine inspections, in general, the SFC will only be able to request information from such persons other than the LCs (e.g., service providers such as Microsoft) where the SFC has reasonable cause to believe that the information required cannot first be obtained by an exercise of its power against the LCs. **Request for information in conjunction with SFC investigations against LCs:** The SFC has a range of powers to conduct investigations: (i) **Section 183 of the SFO:** The SFC has the power to request for, amongst others, production of any records or documents which may be relevant to a regulatory investigation conducted pursuant to section 182 of the SFO (such as investigations regarding an offence or market misconduct under the SFO, or where there is suspicion of fraud, misfeasance or other misconduct in connection with certain SFC regulated activities). (ii) **Section 12 of the AMLO:** The SFC has the power to request for, amongst others, production of any record or document which may be relevant to a regulatory investigation conducted pursuant to section 11 of the AMLO (such as investigations regarding a suspected offence under the AMLO).

		The power can be exercised on the LCs as well as such other persons whom the SFC has reasonable cause to believe has in his **<u>possession</u>** any record or document which contains, or which is likely to contain, information relevant to the investigation. **Search warrants:** *Section 191 of the SFO* provides that where a magistrate is satisfied that there are reasonable grounds to suspect that there is, or is likely to be, on specified premises any record or document which may be required to be produced under *Part VIII of the SFO*, the magistrate may issue a warrant authorizing a person specified in the warrant, a police officer, or such other persons as may be necessary to assist in the execution of the warrant to:- (i) enter the specified premises, if necessary by force, at any time within the period of 7 days beginning on the date of the warrant; and (ii) search for, seize and remove any record or document which the person specified in the warrant or the police officer has reasonable cause to believe may be required to be produced under Part VIII of the SFO.

Part 2: Contract Checklist

What are our contract documents?

The HKMA and IA require that all outsourcing arrangements must contain certain provisions in a documented legally binding agreement, signed by all parties to it before the outsourcing arrangement commences. The SFC has also set out certain contractual requirements in a documented legally binding agreement in respect of cloud services, and also there are some general requirements under the IOSCO Principles. There are various parts to your signed contract with Microsoft. Your Microsoft Account Manager can walk you through the relevant parts if helpful. The following table sets out the relevant Microsoft documents:

Core Microsoft contract documents Microsoft Business and Services Agreement (**MBSA**); Enterprise Agreement (**EA**); and the enabling **Enrollment**, which is likely to be either an Enterprise Enrollment or a Server and Cloud Enrollment.	**Documents incorporated in Microsoft contracts**[1] Online Service Terms (**OST**) Data Protection Addendum (**DPA**) including GDPR Terms and the EU Model Clauses; **Product Terms**
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**[2] Materials available from the relevant **Trust Center**

What does this Part 2 cover?

The HKMA's General Principles for Technology Risk Management ("**Technology Risk Principles**"), the HKMA's Guidelines on Outsourcing ("**Guidelines on Outsourcing**"),the GL 14 and the EDSP Circular, provide that your agreement with the cloud services provider must address specified matters. This Part 2 sets out those specific items that must be addressed in your agreement (as well as other terms that we often see customers and regulators identify as important to include in agreements), and the third column indicates how and where in the Microsoft contractual documents the mandatory requirement is covered.

[1] Available at www.microsoft.com/contracts.
[2] Available at www.microsoft.com/trustcenter.

Reference	Requirement	How and where is this dealt with in Microsoft's contract?
Paragraph 2.4.1, Guidelines on Outsourcing (Outsourcing Agreement), **Paragraph 7.1.1, Technology Risk Principles (Management of Technology Outsourcing)** **and** **GL 14, Section 5.10.**	(a) The scope of the arrangement and services to be supplied	The contract pack comprehensively sets out the scope of the arrangement and the respective commitments of the parties. The services are described, along with the applicable usage rights, in the Product Terms, the OST, the DPA and the SLA.
Paragraph 2.4.2, Guidelines on Outsourcing (Outsourcing Agreement) **and**	(b) Commencement and end dates	Standard EA Enrollments have a three-year term and may be renewed for a further three-year term.

Reference	Requirement	How and where is this dealt with in Microsoft's contract?
GL 14, Section 5.10 (c).		
Paragraph 2.4.2, Guidelines on Outsourcing (Outsourcing Agreement)	(c) Review provisions	The customer may monitor the performance of the Online Services via the administrative dashboard, which includes information as to Microsoft compliance with its SLA commitments. The DPA specifies the control standards and frameworks that Microsoft will comply with for each Microsoft Online Service. The DPA also provides for independent audits of compliance of those Online Services, Microsoft remediation of issues raised by the audits and availability to customers of the audit reports and Microsoft information security policies. The HKMA seems to expect that you review your arrangements at least once per year. If you require any input from Microsoft, please do not hesitate to get in touch with your Microsoft contact.
Paragraphs 2.3.2, Guidelines on Outsourcing (Ability of Service Providers) and paragraphs 2.6.1 and 2.6.2 (Control over Outsourced Activities)	(e) Service levels and performance requirements	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 Enrollment: *"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.

Reference	Requirement	How and where is this dealt with in Microsoft's contract?
Paragraph 7.1.1, Technology Risk Principles **and** **GL 14, Section 5.10 (e).**		
GL 14, Section 5.10. **Paragraph 21, EDSP Circular**	(f) The form in which data is to be kept and clear provisions identifying ownership and control of data and assets, including after the termination of the contract	The customer will have the ability to access and extract its Customer Data stored in each Online Service at all times during the subscription and for a retention period of at least 90 days after it ends (see OST and DPA). Microsoft also makes specific commitments with respect to customer data in the DPA and the OST. In summary, Microsoft commits that: 1. Ownership of customer data remains at all times with the customer. 2. Customer data will only be used to provide the online services to the customer. Customer data will not be used for any other purposes, including for advertising or other commercial purposes. 3. Microsoft will not disclose customer data to law enforcement unless it is legally obliged to do so, and only after not being able to redirect the request to the customer.

Reference	Requirement	How and where is this dealt with in Microsoft's contract?
		4. Microsoft will implement and maintain appropriate technical and organisational measures, internal controls, and information security routines intended to protect customer data against accidental, unauthorised or unlawful access, disclosure, alteration, loss, or destruction. 5. 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. MBSA section 3 deals with confidentiality. Under this section Microsoft commits not to disclose confidential information (which includes customer data) to third parties (unless required by law) and to only use confidential information for the purposes of Microsoft's business relationship with the customer. If there is a breach of the contractual confidentiality obligations by Microsoft, the customer would be able to bring a claim for breach of contract against Microsoft.
GL 14, Section 5.10.	(g) Reporting requirements, including content and frequency of reporting	The customer may monitor the performance of the Online Services via the administrative dashboard at any time, which includes information as to Microsoft's compliance with its SLA commitments. Microsoft also commits to providing the customer with Microsoft's audit reports, resulting from audits performed by a qualified, independent, third party security auditor that measure compliance against Microsoft's standards certifications (see the DPA).
GL 14, Section 5.10.	(h) Audit and monitoring procedures	The DPA 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 DPA. 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

Reference	Requirement	How and where is this dealt with in Microsoft’s contract?
		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. For more information regarding penetration testing, see https://technet.microsoft.com/en-us/mt784683.aspx. Microsoft makes available certain tools through the Service Trust Platform to enable customers to conduct their own virtual audits of the Microsoft 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 Microsoft Online Services, respectively. In addition, the Financial Services Amendment details the examination and audit rights that are granted to the customer and regulators. 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 Microsoft Online Service and other information reasonably requested by the customer regarding Microsoft security practices and policies.

Reference	Requirement	How and where is this dealt with in Microsoft's contract?
		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 data centres that it uses in processing customer data for each Microsoft Online Service. Pursuant to the terms in the DPA, Microsoft will provide Customer with each Microsoft Audit Report. **3. Customer Compliance Program** The customer also has the opportunity to participate in the Customer 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.
	(i) Business continuity management	Business Continuity Management forms part of the scope of the accreditation that Microsoft maintains in relation to the online services, and Microsoft commits to maintain specified business continuity management practices (under the DPA). Business continuity management also forms part of the scope of Microsoft's industry standards compliance commitments and regular third party compliance audits.
Paragraph 2.5.1, Guidelines on Outsourcing	(j) Confidentiality, privacy and security of information	The contractual documents include various confidentiality, privacy and security protections. The DPA states that Microsoft and the customer each commit to comply with all applicable privacy and data protection laws and regulations. The customer owns its data that is stored on Microsoft Online Services at all times. The customer also retains the ability to access its customer data at all times, and Microsoft will deal with customer data in accordance with the terms and conditions of the

Reference	Requirement	How and where is this dealt with in Microsoft's contract?
(Customer Data Confidentiality) **Paragraph 2.5.2, Guidelines on Outsourcing (Customer Data Confidentiality)**		Enrollment and the DPA. Microsoft will retain customer data stored in the Microsoft 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 a Microsoft Online Service, Microsoft will disable the account and delete customer data from the account. Microsoft makes specific commitments with respect to safeguarding your data in the DPA. 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. 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. 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. Technical support personnel are only permitted to have access to customer information when needed. The DPA 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.

Reference	Requirement	How and where is this dealt with in Microsoft’s contract?
		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 (DPA).
GL 14, Section 5.10. **Paragraph 21, EDSP Circular**	(k) Default arrangements and termination provisions	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. Micosoft’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.
GL 14, Section 5.10.	(l) Dispute resolution arrangements	In the event that a FI and Microsoft have a dispute, the choice-of-law and dispute resolution provisions would be clearly described in the agreement between Microsoft and the FI. The MBSA contains terms that describe how a dispute under the contract is to be conducted.
Paragraph 2.4.1, Guidelines on Outsourcing	(m) Liability and indemnity	MBSA deals with liability. MBSA sets out Microsoft’s obligation to defend the regulated entity against third party infringement claims.
Paragraph 7.1.1, Technology Risk Principles (Management of Technology Outsourcing),	(n) A notification or an approval requirement for significant sub-contracting of services and a provision that the original technology service provider is still responsible for its sub-contracted services	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 agreements with customers. To ensure subcontractor accountability, Microsoft requires all of 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,

Reference	Requirement	How and where is this dealt with in Microsoft’s contract?
GL 14, Section 5.10. **And** **GL 14, Section 5.20.**		more information regarding Microsoft’s Supplier Security and Privacy Program, see https://www.microsoft.com/en-us/procurement/msp-requirements.aspx. 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 (refer to the DPA). In addition, Microsoft’s ISO/IEC 27018 certification requires Microsoft to ensure that its subcontractors are subject to the same security controls as Microsoft. 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 Microsoft 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. (refer to the DPA)
GL 14, Section 5.10.	(o) Insurance	Microsoft maintains self-insurance arrangements for most of the areas where third party insurance is typically obtained and can make certificates of insurance available upon request. Microsoft has taken the commercial decision to take this approach, and considers that this does not detrimentally affect its customers, given Microsoft’s financial position set out in Microsoft’s Annual Reports (see Part 1, Section 1 above).

Reference	Requirement	How and where is this dealt with in Microsoft's contract?
	(p) To the extent applicable, offshoring arrangements (including through subcontracting)	The DPA provides commitments on the location at which Microsoft will store customer data at rest (refer to the DPA). Microsoft also makes GDPR specific commitments (under the DPA) to all customers effective May 25, 2018.
Paragraph 2.8.2, Guidelines on Outsourcing **and** **GL 14, Section 5.10.**	(q) Supervisory inspection or review of the operations and controls of the service provider as they relate to the outsourced activity	The DPA specifies the audit mechanisms that Microsoft puts in place in order to verify that the online services meet appropriate security and compliance standards. This commitment is reiterated in the FSA. In addition, the FSA detail the examination and influence rights that are granted to the customer and HKMA. It sets out a process which can culminate in the regulator's examination of Microsoft's premises, and gives the customer the opportunity to participate in the Microsoft Online Services Customer Compliance Program, which is a for-fee program that facilitates the customer's ability to (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 additional 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.
Paragraph 2.9.1, Guidelines on Outsourcing **GL 14, Section 5.10.** **and** **GL 14, Section 5.19 (f).**	(r) Governing Law	MBSA deals with what laws apply if there is a legal dispute. The governing law is that of Ireland, however the parties have the ability to bring proceedings in the locations as follows: • If Microsoft brings the action, the jurisdiction will be where the customer is located; • If the customer brings the action, the jurisdiction will be Ireland; and • Both parties can seek injunctive relief with respect to a violation of intellectual property rights or confidentiality obligations in any appropriate jurisdiction.

Reference	Requirement	How and where is this dealt with in Microsoft's contract?
GL 14, Section 5.10 (b).	(s) Location where the outsourced services will be performed	The DPA contain 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 DPA. Also, as noted in the DPA: "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 DPA". Commitments on the location of data at rest is discussed in the DPA, and may depend on where a customer provisions its service tenancy or specify as a Geo for the online service. More details are set out, non-contractually, at the Trust Centers for each applicable online service.

Further Information

- **Navigating Your Way to the Cloud: microsoft.com/en-sg/apac/trustedcloud**
- **Trust Center: microsoft.com/trust**
- **Service Trust Portal: aka.ms/trustportal**
- **Customer Stories: customers.microsoft.com**
- **Online Services Terms: microsoft.com/contracts**
- **Service Level Agreements: microsoft.com/contracts**
- **SAFE Handbook: aka.ms/safehandbook**

This document is not legal or regulatory advice and does not constitute any warranty or contractual commitment on the part of Microsoft. You should seek independent legal advice on your cloud services project and your legal and regulatory obligations.