



A compliance checklist for financial institutions in Korea

Version: March 2020

Contents

Introduction: A compliance checklist for financial institutions in Korea	Page 3
Overview of the Regulatory Landscape	Page 6
Compliance Checklist	Page 10
<i>Part 1: Key Considerations</i>	<i>Page 11</i>
<i>Part 2: Contract Checklist</i>	<i>Page 54</i>
Further Information	Back

Introduction: A compliance checklist for financial institutions in Korea

Overview

The rapid pace of evolution in artificial intelligence (AI) and Big Data applications, coupled with improvements in computing power and availability of data, have led to growing adoption of AI across all industries. The financial services industry is no exception, with financial institutions adopting AI across a variety of contexts. Cloud computing is essential for such trend, and it is fast becoming the norm, not the exception, for financial institutions in Korea.

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. In its joint press release in December 2018, the Financial Services Commission (FSC) and Financial Supervisory Service (FSS) noted a strong desire to relax the regulations to promote cloud computing to enable digital transformation in the financial services industry and allowed financial institutions to use cloud computing to process even the critical information including Unique Personal Information (UPI) and Personal Credit Information (PCI).

Microsoft is committed to providing a trusted set of cloud services to financial institutions in Korea. 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 Korea. We developed it to help financial institutions in Korea adopt Microsoft cloud services with the confidence that they can meet 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 Korea;
2. a **Compliance Checklist**, which lists the regulatory issues that need to be addressed and maps Microsoft's cloud 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 Korea who want to use Microsoft cloud services. We use the term "financial institutions" broadly, to include any entity that is regulated by FSC and FSS. These entities include banks, general insurers and life insurers.

What Microsoft cloud services does this checklist apply to?

This checklist applies to Microsoft Office 365, Microsoft Dynamics 365 Core Services and Microsoft Azure Core Services, as referenced in Microsoft's Online Services Terms (**OST**). 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 Korea, there is no mandatory requirement for financial institutions to complete a checklist to adopt Microsoft cloud services. However, through conversations with our many cloud customers in Korea, we understand that a checklist approach like this is helpful – first, as a way of understanding the regulatory requirements; second, as a way of learning more about how Microsoft cloud services can help financial institutions meet those regulatory requirements; third, as an internal framework for documenting compliance; and fourth, as a tool to streamline consultations with financial regulators, if they are required. By reviewing and completing the checklist, financial institutions can adopt Microsoft cloud services with confidence that they are complying with the requirements in Korea.

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 cloud services. Combines the detailed information provided by Microsoft to auditors and regulators as part of various third-party audits of Microsoft's cloud services against various standards (such as International Organisation for Standardisation 27001:2013 and ISO 27018:2014) and information that Microsoft compiles internally for its compliance with regulations (such as the EU General Data Protection Regulation or mapping to other required controls) with the customer's own self-assessment of its organisation's compliance with applicable standards and regulations.
 - **Provides customers with recommended actions** and detailed guidance to improve controls and capabilities that can help them meet regulatory requirements for areas they are responsible for.
 - **Simplifies compliance workflow** and enables customers to assign, track, and record compliance and assessment-related activities, which can help an organisation 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 financial regulators. 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 Data Protection Terms (**DPT**) of Microsoft's OST.

Overview of the Regulatory Landscape

<p>Are cloud services permitted?</p>	<p>Yes. This means that you can consider Microsoft cloud services for the full range of use-cases across your financial institution.</p>
<p>Who are the relevant regulators and authorities?</p>	<p>The applicable financial regulators are the Financial Services Commission(FSC) (http://fsc.go.kr/), which is a central Government agency under the Prime Minister, and the Financial Supervisory Service (FSS)(http://fss.or.kr/), which receives instructions/supervision from the FSC.</p>
<p>What regulations and guidance are relevant?</p>	<p>There are several requirements and guidelines that financial institutions should be aware of when moving to the cloud:</p> <ol style="list-style-type: none"> 1. Electronic Financial Transaction Act 2. FSC Regulation on Supervision of Electronic Financial Transactions (Supervisory Regulation) 3. FSC Regulation on Outsourcing of Data Processing of Financial Companies (DPO Regulation)¹ 4. FSC Regulation on Entrustment, etc. of Duties by Financial Institutions (Outsourcing Regulation) 5. Guideline on Use of Cloud Computing Services in Financial Industry” (Cloud Guide)(2019)² http://www.fsec.or.kr/user/bbs/fsec/147/315/bbsDataView/1155.do?page=1&column=&search=&searchSDate=&searchEDate=&bbsDataCategory <p>Please note that the Cloud Guide is not legally binding and is only a recommendation issued by the Financial Security Institute.</p>
<p>Is regulatory approval required?</p>	<p>No. However, financial institutions must report to FSS within at least seven (7) business days prior to the intended date of use of the cloud computing services in any of the following cases:</p> <ol style="list-style-type: none"> 1.If UPI or PCI is processed; or 2.If the matter is expected to have a material impact on the security and reliability of electronic financial transactions

¹ In case of a financial investment business entity, the provisions relating to outsourcing in the Financial Investment Services and Capital Markets Act (“**FSCMA**”) prevail over the Outsourcing Regulation and the DPO Regulation (Article 3(1) of the DPO Regulation).

In case of a Financial Company which does not perform financial investment business, the DPO Regulation prevails over the Outsourcing Regulation with respect to the outsourcing of data processing.

² The Cloud Guide was prepared and distributed by the Financial Security Institute, and its purpose is to protect financial users and to maintain and strengthen financial systems’ safety by recommending certain items to be complied with by the financial institutions, etc. when using cloud computer services. The Cloud Guide includes the items on introduction of cloud services, use of cloud services, management and ex post facto management of cloud services.

<p>Are transfers of data outside of Korea permitted?</p>	<p>Yes except for UPI and PCI.</p> <p>The use of data centers outside of Korea is permitted for the non-critical information processing systems. Unique Personal Information (UPI) and Personal Credit Information (PCI) must be localized in Korea. However, Korean branch offices of foreign financial companies which do not materially affect the safety and reliability of electronic financial transactions and electronic payment gateway providers for Overseas Online Shopping Malls may process UPI and PCI outside of Korea.</p> <p>General privacy legislation (which applies across all sectors, not just to financial institutions) permits transfers of personal data outside of Korea in the context of outsourcing as follows:</p> <ol style="list-style-type: none"> 1. When the Personal Information Protection Act (PIPA) applies: General outsourcing rules apply (no difference between overseas/domestic outsourcing), which is (i) a written outsourcing agreement and (ii) notification/disclosure of the outsourcing arrangement. 2. When Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. ("Network Act") applies: In principle, consent from data subjects is required. However, organisations are exempt from the consent requirements if the use of an outsourcing company is necessary to perform its contractual obligations and enhance users' benefits, and the matters relating to the outsourcing and the overseas transfer are disclosed in the privacy policy or are otherwise notified to the users. Further, it is required to take necessary measures to protect the personal information, including technical and managerial measures to protect the personal information and measures for processing complaints etc. <p>Although data other than UPI and PCI can transfer outside of Korea, many of our Korean financial services customers take advantage of the cloud services available from our Korean data centers, including Azure and Office 365.</p>
<p>Are public cloud services sufficiently secure?</p>	<p>Yes.</p> <p>More and more financial institutions in Korea are 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.</p> <p>An example of this type of innovation in Microsoft cloud services is Office 365 Advanced Threat Protection and the Azure Web Application Firewall, which provide a very sophisticated model to detect and mitigate previously unknown malware and provide customers with information security protections and analytics information.</p>
<p>Are there any mandatory terms that must be included in the contract with the services provider?</p>	<p>Yes.</p> <p>Supervisory Regulation and DPO Regulation do stipulate some specific points that financial institutions must ensure to incorporate in their cloud services contracts. 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.</p>
<p>How do more general Korean privacy laws</p>	<p>The privacy laws applicable to financial institutions include the Credit Information Act, PIPA, and Network Act, which must be complied with according to the type of information outsourced to the cloud service provider (Microsoft, the outsourcee). The</p>

apply to the use of cloud services by financial institutions?

cloud service provider, as the outsourcee to perform personal information processing service, must comply with various requirements under the Credit Information Act (in case of personal credit information), PIPA and the Network Act in relation to processing personal information.

The privacy regulators are **FSC, FSS, the Ministry of the Interior and Safety, the Korea Communications Commission, and the Personal Information Protection Commission.**

Additionally, a European privacy law, the General Data Protection Regulation (**GDPR**), came into effect on 25 May 2018. Of note, the GDPR imposes new rules on companies, government agencies, non-profits, and other organisations that offer goods and services to people in the European Union (**EU**), or that monitor personal behaviour taking place in the EU. In this regard, the GDPR applies on an extraterritorial basis, and not only to entities that are established in the EU. Microsoft is committed to GDPR compliance across its cloud services and provides GDPR related assurances in its contractual commitments. You can learn more about how Microsoft's products help you comply with the GDPR [here](#).

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.

In the "**Guidance**" column, we explain how the use of Microsoft cloud services address the requirement. Where applicable, we also provide *guidance* as to where the underlying requirement comes from and other issues you may need to consider.

How should we use the Compliance Checklist?

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

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 cloud services (particularly, Office 365, Dynamics 365 and Azure) by financial institutions in Korea.

Ref.	Question / requirement	Guidance
A. OVERVIEW		
<i>This section provides a general overview of the Microsoft cloud services</i>		
1.	Who is the service provider?	<p>The service provider is Microsoft Korea Inc., 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).</p> <p>Microsoft's full company profile is available here: microsoft.com/en-us/investor/</p> <p>Microsoft's Annual Reports are available here: microsoft.com/en-us/Investor/annual-reports.aspx</p>
2.	What cloud services are you using?	<p>Microsoft Office 365: microsoft.com/en-us/trustcenter/cloudservices/office365</p> <p>Microsoft Dynamics 365: microsoft.com/en-us/trustcenter/cloudservices/dynamics365</p> <p>Microsoft Azure: microsoft.com/en-us/trustcenter/cloudservices/azure</p>
3.	What activities and operations will be	<p>This Compliance Checklist is designed for financial institutions using Office 365, Dynamics 365 and/or 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 cloud services. Your Microsoft contact can assist as needed.</p>

Ref.	Question / requirement	Guidance
	outsourced to the service provider?	<p>If using Office 365, services would typically include:</p> <ul style="list-style-type: none"> • Microsoft Office applications (Outlook, Word, Excel, PowerPoint, OneNote and Access) • Exchange Online • OneDrive for Business, SharePoint Online, Microsoft Teams, Yammer Enterprise • Skype for Business <p>If using Dynamics 365, services would typically include:</p> <ul style="list-style-type: none"> • 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 <p>If using Microsoft Azure, services would typically include:</p> <ul style="list-style-type: none"> • 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?	<p><i>The nature of the type of cloud services consumed presents different risk profiles, and an understanding of the type of cloud solution may be relevant when determining the risk associated with the solution. With Microsoft cloud services, a range of options exists, including public and hybrid cloud, but given the operational and commercial benefits to customers, public cloud is increasingly seen as the standard deployment model for most institutions.</i></p> <p><u>If using public cloud:</u></p> <p>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 D. (Technical and Operational Risk Q&A) below.</p> <p><u>If using hybrid cloud:</u></p> <p>By using Microsoft hybrid cloud, customers can move to multi-tenant cloud at their own pace.</p> <p>Tenants may wish to identify the categories of data that they will store on their own servers using Windows Server virtual machines.</p> <p>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 D. (Technical and Operational Risk Q&A) below.</p>
5.	What data will be processed by the service provider on behalf of the financial institution?	<p><i>Processing UPI or PCI triggers additional requirements such as prior report to FSS and data localization. It is therefore important to understand what data will be processed through Microsoft cloud services. You will need to tailor this section depending on what data you intend to store or process within Microsoft cloud services. The following are common categories of data that our customers choose to store and process in the Microsoft cloud services.</i></p>

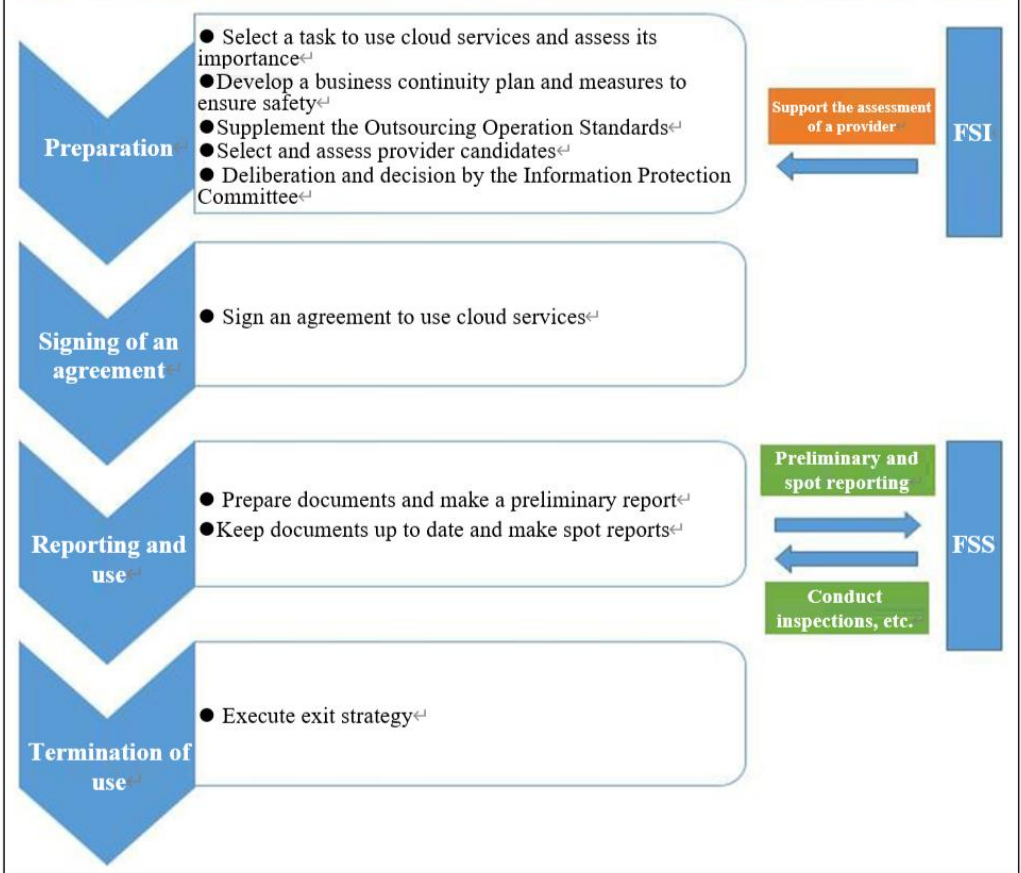
Ref.	Question / requirement	Guidance
		<ul style="list-style-type: none"> • Customer data (including customer name, contact details, account information, payment card data, security credentials and correspondence). • Employee data (including employee name, contact details, internal and external correspondence 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 financial institution. <p>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.</p>
6.	How is the issue of counterparty risk addressed through your choice of service provider?	<p><i>Supervisory Regulation requires financial institutions to assess the soundness and safety of cloud service providers pursuant to Article 14-2, Paragraph (1), Item 2 of the Supervisory Regulation. Regarding the soundness of Microsoft cloud services, 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.</i></p> <p>a. Competence. Microsoft is an industry leader in cloud computing. Microsoft cloud services were built based on ISO/IEC 27001 and ISO/IEC 27018 standards, a rigorous set of global standards covering physical, logical, process and management controls. Microsoft offers the most comprehensive set of compliance offerings of any cloud service provider. A list of 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 financial institutions 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.</p> <p>b. Track-record. Many of the world’s top companies use Microsoft cloud services. There are various case studies relating to the use of Microsoft cloud services at customers.microsoft.com. Customers have obtained regulatory approvals (when required) and are using Online Services in all regions of the globe. Office 365 has grown to have over 100 million users,</p>

Ref.	Question / requirement	Guidance
		<p>including some of the world's largest organisations and financial institutions. Azure continues to experience more than 90% growth, and over 80% of the largest financial institutions use or have committed to use Azure services.</p> <p>c. Specific financial services credentials. Financial institution customers in leading markets, including in the UK, France, Germany, Singapore, Canada, the United States and many other countries have performed their due diligence and, working with their regulators, are satisfied that Microsoft cloud services meet their respective regulatory requirements. This gives customers confidence that Microsoft can help meet the high burden of financial services regulation and is experienced in meeting these requirements.</p> <p>d. 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 market capitalisation is in excess of USD \$1 trillion (as of December 2019), making it one of the top three 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.</p>
<p>B. OFFSHORING</p> <p><i>Microsoft gives customers the opportunity to store certain data at-rest within Korea. This will depend on the configuration of Microsoft cloud services that you select. Your responses will need to be tailored accordingly.</i></p>		
7.	Will the proposed outsourcing require data localization?	<p><i>Supervisory Regulation requires all systems processing any UPI and PCI using cloud shall be localized in Korea. Microsoft provides data location transparency and allows customers to choose data that will be stored at-rest within Korea.</i></p> <p>First, and most importantly, the customer can configure the service such that data for core services are stored at rest within Korea.</p> <p><i>If using Office 365 and/or Dynamics 365:</i></p>

Ref.	Question / requirement	Guidance
		<p>Customers can select to have data for core services stored at rest within Korea. For further detail, please consult the interactive data centers map at http://aka.ms/dcmap (Office365) and o365datacentermap.azurewebsites.net(Dynamics 365).</p> <p><i>If using Azure:</i></p> <p>Customers can configure the service such that data is stored at rest within Korea. For further detail, please consult the interactive data centers map at: azure.microsoft.com/en-us/regions.</p>
8.	How do arrangements with cloud services provider manage offshoring risk?	<p>In relation to the limited categories of data that are stored or processed outside of Korea, customers may become satisfied that any offshoring risk is addressed for the following reasons:</p> <ol style="list-style-type: none"> <li data-bbox="539 727 2029 826">i. Customers know where their data is stored. For the limited categories of data stored or processed outside of Korea, the relevant locations are listed at http://aka.ms/dcmap (for Office365) and o365datacentermap.azurewebsites.net (for Dynamics 365) and at azure.microsoft.com/en-us/regions (for Azure). <li data-bbox="539 834 2029 967">ii. The relevant data centers are strategically located, taking into account a long list of country and socioeconomic factors. Microsoft's data centers are located in jurisdictions that are recognised as stable, safe, and reliable with respect to their legal systems, regulatory regime, technology, and infrastructure. The circumstances under which authorities in these countries may have rights to access information are not considered to be unwarranted. <li data-bbox="539 975 2029 1074">iii. The customer's ability to enforce the agreement against Microsoft is not affected by any use of Microsoft's data centers outside of Korea. Microsoft is a large international organisation with significant resources. It has a presence in many countries (including Korea) and has a long-track record in financial services. <li data-bbox="539 1082 2029 1181">iv. Financial regulators' regulatory oversight and access is not impacted by use of Microsoft's data centers outside of Korea. There are terms in the contract that enable financial regulators to examine Microsoft's facilities, systems, processes and data relating to the services. <li data-bbox="539 1189 2029 1287">v. The customer's ability to access data is not affected by use of Microsoft's data centers outside of Korea. When customers store data in Microsoft cloud services, they retain ownership of that data. They can download a copy of that data at any time and for any reason, without assistance from Microsoft.

Ref.	Question / requirement	Guidance
9.	What risks have been considered in relation to the data offshoring?	<p><i>Unless processing UPI and PCI, data offshoring is allowed. The following are risk areas that our customers typically tell us are important with regards to data offshoring.</i></p> <p>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.</p> <p>b. Country/socioeconomic Microsoft’s data centers are strategically located around the world, taking into account country and socioeconomic factors. The relevant locations constitute stable socioeconomic environments.</p> <p>c. Infrastructure/security/terrorism Microsoft’s data centers 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.</p> <p>d. Environmental (i.e. earthquakes, typhoons, floods) Microsoft data centers are built in seismically safe zones. Environmental controls have been implemented to protect the data centers 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.</p> <p>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 financial regulators’ regulatory oversight. The terms are summarised in Part 2.</p>
C. CLOUD SERVICE USE PROCEDURES		

Ref.	Question / requirement	Guidance
------	------------------------	----------



"FSI" above means "Financial Security Institute" in Korea.

Ref.	Question / requirement	Guidance
<p><i>Article 14-2 (Procedures for Use, etc. of Cloud Computing Service) of the Supervisory Regulation requires financial institutions to take necessary measures in order to use cloud, and the Cloud Guide shows the procedures as above.</i></p> <p><i>Also, financial institutions should report the use of cloud to FSS, if (i) they process UPI or PCI using cloud, or (ii) safety and reliability of electronic financial transactions are materially impacted by using cloud. The following documents are required when reporting to FSS.</i></p> <ul style="list-style-type: none"> <i>- Documents set forth in each Item of Article 7, Paragraph (1) of the DPO Regulation;</i> <i>- Priority assessment standards and results on data processing work subject to use;</i> <i>- Business continuity plan and measures to ensure safety in connection with the use of cloud services; and</i> <i>-The results of deliberations and resolutions by the Information Protection Committee in connection with the use of cloud services.</i> <p><i>Although this is a matter for each financial institution, Microsoft provides some guidance, based on its experience of approaches taken by its customers. Ultimately this will need to be tailored for your financial institution to reflect its compliance practices.</i></p>		
10.	Select a task to use cloud services and assess its importance	<p><i>If (i) financial institutions process UPI or PCI using cloud or (ii) safety and reliability of electronic financial transactions are materially impacted by using cloud, then financial institutions need to report the use of cloud to FSS.</i></p> <p>Microsoft has implemented and commits to maintaining specified security measures for Customer Data in the Core Online Services, including Asset Inventory and Asset Handling practices and other security commitments set out in the OST and DPA.</p> <p>Additionally, Microsoft has cloud service offerings that leverage data classification and protection technologies to help financial institutions discover, classify, protect and monitor their sensitive data across devices, apps, cloud services and on-premises. Examples of Microsoft Information Protection solutions can be found here, including Azure Information Protection, Office 365 Information Protection, Windows Information Protection, and Microsoft Cloud App Security.</p>

Ref.	Question / requirement	Guidance
		<p>Office 365 / Microsoft 365 also has further advanced capabilities that helps financial institutions meet higher level of assurance and compliance requirements.</p> <p>Examples include:</p> <ul style="list-style-type: none"> • Advanced electronic discovery • Data governance and retention • Bring-your-own service encryption key • Control how Microsoft support engineer access your data • Privileged access management <p>For Azure SQL, there are data security capabilities that support data discovery and classification, along with data masking and encryption.</p>
11.	A business continuity plan and measures to ensure safety	<p><i>These requirements apply whether or not activities are outsourced to third party service providers such as Microsoft. Your Microsoft Account Manager can assist with any questions about Microsoft's disaster recovery arrangements and how they would interface with those of your institution.</i></p> <p>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 real-time issue detection and automated response such that workloads can be moved off any failing infrastructure components with no perceptible impact on the service. Microsoft also maintains 24/7 on-call engineering teams for assistance. See Financial Services Compliance Program and Premier Support; see also Office 365 Support; Premier Support for Enterprise; and Azure Support Plans.</p>

Ref.	Question / requirement	Guidance
		<ul style="list-style-type: none"> • <u>Redundancy</u>. 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. <ul style="list-style-type: none"> ○ For Office 365, Microsoft maintains multiple copies of customer data across data centers for redundancy. ○ For Azure, Microsoft may copy customer data between regions within a given geography for data redundancy or other operational purposes. For example, Azure GRS replicates certain data between two regions within the same geography for enhanced data durability in case of a major data center disaster. • <u>Resiliency</u>. 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. • <u>Distributed Services</u>. Microsoft also offers distributed component services like Exchange Online and SharePoint Online to limit the scope and impact of any failures of a single component. Directory data is also replicated across component services to insulate one service from another in the event of a failure. • <u>Monitoring</u>. 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. • <u>Simplification</u>. Microsoft uses standardised hardware to reduce issue isolation complexities. Microsoft also uses fully automated deployment models and a standard built-in management mechanism.

Ref.	Question / requirement	Guidance
		<ul style="list-style-type: none"> • <u>Human Backup</u>. 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. • <u>Continuous Learning</u>. 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. • <u>Disaster Recovery Tests</u>. Microsoft conducts disaster recovery tests at least once per year.
12.	Supplement the Outsourcing Operation Standards	<p><i>Appendix 2-3 of Supervisory Regulation lists up the supplementary matters for Outsourcing Operation Standards, which are (i) Matters regarding procedures for deciding and terminating outsourcing agreement and re-outsourcing, (ii) Matters regarding monitoring of outsourcing, (iii) Matters regarding emergency plans, (iv) Matters regarding securing investigation and access rights in connection with the outsourced service, and (v) Material matters to be included in outsourcing agreements.</i></p> <p>The appropriate standards 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:</p> <ul style="list-style-type: none"> • 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;

Ref.	Question / requirement	Guidance
		<ul style="list-style-type: none"> • 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 • ensuring that there is independent review and audit for compliance with the policies. <p>For example, in describing the service provider selection process, you could include in your standards 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.</p> <p>For (i) Matters regarding procedures for deciding and terminating outsourcing agreement and re-outsourcing, (ii) Matters regarding monitoring of outsourcing, (iii) Matters regarding emergency plans, please check out Service Trust Portal for resources.</p> <p>For (iii) Matters regarding emergency plans, please see Q11.</p> <p>For (iv) Matters regarding securing investigation and access rights in connection with the outsourced service, please see Q 16.</p> <p>For (v) Material matters to be included in outsourcing agreements, please see Part 2: Contract Checklist.</p>
13.	Select and assess provider candidates	<p><i>Appendix 2-2 of Supervisory Regulation and the Cloud Guide list up the assessment standards, which consist of ‘General protective measures’ and ‘additional protective measures for financial sector’. ‘General protective measures’ is a general security standard required to be complied by all cloud service providers, and ‘additional protective measures for financial sector’ is a specialized standard applicable to the financial industry. The assessment of items of ‘general protective measures’ may be omitted for cloud service provider (services) that obtained and is maintaining the following cloud security certification in domestic and foreign countries. Microsoft has acquired the foreign certifications listed in the Cloud Guide</i></p>

Ref.	Question / requirement	Guidance														
		<p data-bbox="539 336 1973 408"><i>(https://azure.microsoft.com/en-us/overview/trusted-cloud/compliance/) and therefore the assessment of items of 'general protective measures' could be omitted accordingly.</i></p> <table border="1" data-bbox="551 443 1597 1267"> <thead> <tr> <th data-bbox="555 448 745 523">Classification</th> <th data-bbox="745 448 981 523">Certification System</th> <th data-bbox="981 448 1592 523">Grounds for Omission of Assessment</th> </tr> </thead> <tbody> <tr> <td data-bbox="555 523 745 727">Domestic</td> <td data-bbox="745 523 981 727">CSAP</td> <td data-bbox="981 523 1592 727"> <ul style="list-style-type: none"> - Governed by the MSIT, assessed and certified by KISA - Certification obtained by major cloud service providers in the country - Comprised of up to approximately 120 assessment items </td> </tr> <tr> <td data-bbox="555 727 745 1091" rowspan="2">Foreign</td> <td data-bbox="745 727 981 874">FedRAMP (High)(U.S.)</td> <td data-bbox="981 727 1592 874">Governed by the government (FedRAMP Program Management Office) - Comprised of up to approximately 400 assessment items</td> </tr> <tr> <td data-bbox="745 874 981 1091">CSA STAR (Gold)(Global)</td> <td data-bbox="981 874 1592 1091"> <ul style="list-style-type: none"> - Governed by CSA* joined by approximately 400 cloud service providers * CSA : Cloud Security Alliance- Comprised of up to approximately 300 assessment items </td> </tr> <tr> <td data-bbox="555 1091 745 1267"></td> <td data-bbox="745 1091 981 1267">MTCS (Level 3) (Singapore)</td> <td data-bbox="981 1091 1592 1267">Governed and certified by the Info-communications Media Development Authority (IMDA)</td> </tr> </tbody> </table> <p data-bbox="539 1315 2029 1382"><i>Fundamentally, financial institutions are the principal subject to perform assessment of the cloud service provider, and organizations responding to breach incidents (i.e. "Financial Security Institute") may assist for such assessment at the request</i></p>	Classification	Certification System	Grounds for Omission of Assessment	Domestic	CSAP	<ul style="list-style-type: none"> - Governed by the MSIT, assessed and certified by KISA - Certification obtained by major cloud service providers in the country - Comprised of up to approximately 120 assessment items 	Foreign	FedRAMP (High)(U.S.)	Governed by the government (FedRAMP Program Management Office) - Comprised of up to approximately 400 assessment items	CSA STAR (Gold)(Global)	<ul style="list-style-type: none"> - Governed by CSA* joined by approximately 400 cloud service providers * CSA : Cloud Security Alliance- Comprised of up to approximately 300 assessment items 		MTCS (Level 3) (Singapore)	Governed and certified by the Info-communications Media Development Authority (IMDA)
Classification	Certification System	Grounds for Omission of Assessment														
Domestic	CSAP	<ul style="list-style-type: none"> - Governed by the MSIT, assessed and certified by KISA - Certification obtained by major cloud service providers in the country - Comprised of up to approximately 120 assessment items 														
Foreign	FedRAMP (High)(U.S.)	Governed by the government (FedRAMP Program Management Office) - Comprised of up to approximately 400 assessment items														
	CSA STAR (Gold)(Global)	<ul style="list-style-type: none"> - Governed by CSA* joined by approximately 400 cloud service providers * CSA : Cloud Security Alliance- Comprised of up to approximately 300 assessment items 														
	MTCS (Level 3) (Singapore)	Governed and certified by the Info-communications Media Development Authority (IMDA)														

Ref.	Question / requirement	Guidance
		<p><i>of financial institutions. Microsoft has already gone through the assessment process by the Financial Security Institute, and is ready to support financial institutions' assessment. For the assistance of the assessment process, please reach out to your Microsoft contact.</i></p>
14.	<p>The deliberations and resolutions by the Information Protection Committee in connection with the use of cloud services</p>	<p><i>Article 14-2 (2) of Supervisory Regulation requires financial institutions to have the following matters deliberated and resolved by the Information Protection Committee.</i></p> <ul style="list-style-type: none"> - <i>Results of assessment on the importance of the company's data processing work</i> - <i>Results of assessment on the soundness and safety, etc. of cloud service providers</i> - <i>Internal Outsourcing Operation Standards</i> <p>For the assessment on the soundness of cloud service providers, please see Q6.</p> <p>For assessment on the safety of cloud service providers, please see Q13.</p> <p>For the Outsourcing Operation Standards please see Q12.</p>
15.	<p>Documents required for FSS report</p>	<p><i>If (i) financial institutions process UPI or PCI using cloud or (ii) safety and reliability of electronic financial transactions are materially impacted by using cloud, then financial institutions need to report the use of cloud to FSS.</i></p> <p><i>Below are the documents required for the FSS report:</i></p> <ul style="list-style-type: none"> - <i>Documents set forth in each Item of Article 7, Paragraph (1) of the DPO Regulation;</i> - <i>Priority assessment standards and results on data processing work subject to use;</i> - <i>Business continuity plan and measures to ensure safety in connection with the use of cloud services; and</i>

Ref.	Question / requirement	Guidance				
		<p data-bbox="539 331 1962 392"><i>-The results of deliberations and resolutions by the Information Protection Committee in connection with the use of cloud services.</i></p> <p data-bbox="539 435 1697 464"><i>Documents set forth in each Item of Article 7, Paragraph (1) of the DPO Regulation are as follows;</i></p> <ul style="list-style-type: none"> <li data-bbox="595 507 1016 536"><i>(a) Copies of outsourcing contracts</i> <li data-bbox="595 547 1682 576"><i>(b) Outsourcing Operation Standards according to Article 3-2 of the Outsourcing Regulation</i> <li data-bbox="595 587 2024 655"><i>(c) Copies of the review opinions and related materials of the compliance officer (who, if there is no compliance officer, is equivalent to an auditor, etc.) that the contract of entrustment does not violate relevant laws and regulations</i> <li data-bbox="595 667 1218 695"><i>(d) Necessity for outsourcing and expected outcome</i> <li data-bbox="595 707 1447 735"><i>(e) Main changes of task handling process according to the outsourcing</i> <li data-bbox="595 746 1697 775"><i>(f) Documents confirming the regulators' ability to supervise the operation of data processing</i> <li data-bbox="595 786 2007 898"><i>(g) Matters concerning the party to which outsourcing will be entrusted (including the subprocessor party in case of subcontract of the outsourcing), such as trade name, amount of capital, location, main type of business, and in case of natural persons, personal information of the representative;</i> <li data-bbox="595 909 1352 938"><i>(h) Remedy process in case of security incident or data leakage</i> <table border="1" data-bbox="539 938 2018 1319"> <tbody> <tr> <td data-bbox="539 938 887 1090"><i>(a) Copy of the outsourcing contracts</i></td> <td data-bbox="887 938 2018 1090">Please see Part 2 of this Compliance Checklist.</td> </tr> <tr> <td data-bbox="539 1090 887 1319"><i>(b) Outsourcing Operation Standards according to Article 3-2 of the Outsourcing Regulation</i></td> <td data-bbox="887 1090 2018 1319">Please see Q12.</td> </tr> </tbody> </table>	<i>(a) Copy of the outsourcing contracts</i>	Please see Part 2 of this Compliance Checklist.	<i>(b) Outsourcing Operation Standards according to Article 3-2 of the Outsourcing Regulation</i>	Please see Q12.
<i>(a) Copy of the outsourcing contracts</i>	Please see Part 2 of this Compliance Checklist.					
<i>(b) Outsourcing Operation Standards according to Article 3-2 of the Outsourcing Regulation</i>	Please see Q12.					

Ref.	Question / requirement	Guidance	
		<p>(c) <i>Necessity for outsourcing and expected outcome</i></p>	<p>You should prepare a business case for the use of Microsoft cloud services. Where appropriate, this could include references to some of the key benefits of Microsoft cloud services, which are described at:</p> <ul style="list-style-type: none"> • 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 <p>The factors listed below may be used to prepare a business case for the use of Microsoft Online Services:</p> <ul style="list-style-type: none"> • <u>Affordability.</u> Microsoft Online Services make enterprise-class technologies available at an affordable price for small and mid-sized companies. • <u>Security.</u> Microsoft Online Services include extensive security to protect customer data. • <u>Availability.</u> Microsoft’s data centers 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. • <u>IT control and efficiency.</u> 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.

Ref.	Question / requirement	Guidance	
			<p>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.</p> <ul style="list-style-type: none"> • <u>User familiarity and productivity.</u> 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.
		(f) Documents confirming the regulators' ability to supervise the operation of data processing	<p>There are terms in the contract that enable financial regulators 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.</p>
		(g) Matters concerning the party to which outsourcing will be entrusted (including the subprocessor party in case of subcontract of the outsourcing), such as trade name, amount of capital, location, main type	<p>Microsoft Korea Inc. 12th fl. Tower A, the K-Twin Towers, 50 Jongno 1gil, Jongno-Gu, Seoul 03142 Korea Representative director: Alfred Soon Dong Koh</p>

Ref.	Question / requirement	Guidance	
		of business, and in case of natural persons, personal information of the representative	
		(h) Remedy process in case of security incident or data leakage	The Incident Management Implementation Guidance for Azure and Office 365 is a comprehensive document customers can use to harden the security posture of their Microsoft cloud environment. It outlines the best methods for configuring the tenant for optimal security incident management: prevention, detection, alerts, anomalous activity monitoring, and post-incident investigations, made possible by in-product logging capability. Microsoft's Office 365 Security Incident Management and Azure Security Response program documents also help you assess Microsoft's own incident management capabilities, policies and processes.

D. TECHNICAL AND OPERATIONAL RISK Q&A

Under Security Assessment Standards Items from the Cloud Guide (Appendix. Standards for Provision of Cloud Computing Services in the Finance Sector) which specifies its 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), financial institutions 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 cloud services which should address many of the technical and operational questions that may arise. If other questions arise, please do not hesitate to get in touch with your Microsoft contact.

16.	Does the service provider permit audit by the financial institution and/or financial regulators?	<p><i>Appendix 2-3 of Supervisory Regulation and Article 4 (3) of DPO Regulation.</i></p> <p>Yes. Pursuant to the Financial Services Amendment, Microsoft provides financial 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 financial regulators requests to examine the Online Services operations in order to meet their supervisory obligations. Microsoft will cause the</p>	
-----	--	---	--

Ref.	Question / requirement	Guidance
		<p>performance of audits of the security of the computers, computing environment and physical data centers that it uses in processing customer data for each Online Service. Customers may also participate in the optional Financial Services Compliance Program to have additional monitoring, supervisory and audit rights and additional controls over the Online Services. See Part 2 below, in relation to Section 29(h), Outsourcing Standards for further detail.</p>
17.	<p>Are the provider's services subject to any third party audit?</p>	<p>Yes. Microsoft's cloud services are subject to regular independent third party audits, including SSAE16 SOC1 Type II, SSAE SOC2 Type II, ISO/IEC 27001, ISO/IEC 27002 and ISO/IEC 27018. Rigorous third-party audits, 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 Compliance Program at any time, which enables them to (amongst other things) participate in an annual 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. A recording of this webcast will also be made available for members of the Financial Services Compliance Program.</p>
18.	<p>What security controls are in place to protect the transmission and storage of confidential information such as customer data within the infrastructure of the service provider?</p>	<p>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 organisations. Microsoft cloud services were built based on ISO/IEC 27001 and ISO/IEC 27018 standards, a rigorous set of global standards covering physical, logical, process and management controls.</p> <p>The Microsoft cloud services security features consist of three parts: (a) built-in security features; (b) security controls; and (c) scalable security. These include 24-hour monitored physical hardware, isolated customer data, automated operations and lock-box processes, secure networks and encrypted data.</p> <p>Microsoft implements the Microsoft Security Development Lifecycle (SDL) which is a comprehensive security process that informs every stage of design, development and deployment of Microsoft cloud services. Through design requirements, analysis of attack surface and threat modelling, the SDL helps Microsoft predict, identify and mitigate vulnerabilities and threats from before a service is launched through its entire production lifecycle.</p>

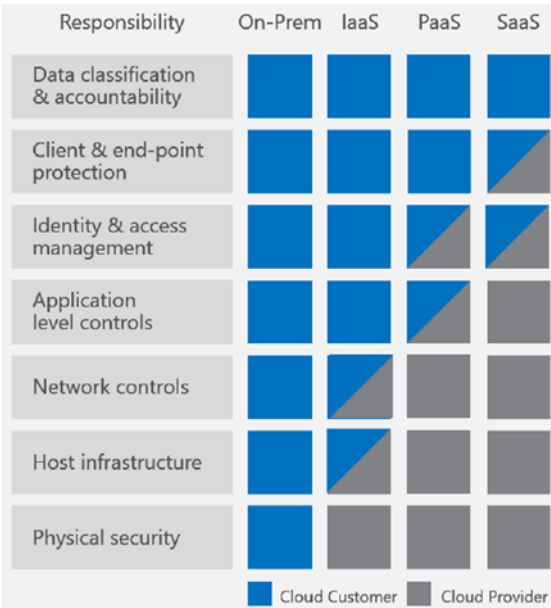
Ref.	Question / requirement	Guidance
		<p>Networks within Microsoft’s data centers are segmented to provide physical separation of critical back-end servers and storage devices from the public-facing interfaces. Edge router security allows the ability to detect intrusions and signs of vulnerability. Customer access to services provided over the Internet originates from users’ Internet-enabled locations and ends at a Microsoft data center. These connections are encrypted using industry-standard transport layer security TLS. The use of TLS establishes a highly secure client-to-server connection to help provide data confidentiality and integrity between the desktop and the data center. Customers can configure TLS between Microsoft cloud services and external servers for both inbound and outbound email. This feature is enabled by default.</p> <p>Microsoft also implements traffic throttling to prevent denial-of-service attacks. It uses the “prevent, detect and mitigate breach” process as a defensive strategy to predict and prevent security breaches before they happen. This involves continuous improvements to built-in security features, including port-scanning and remediation, perimeter vulnerability scanning, OS patching to the latest updated security software, network-level DDOS detection and prevention and multi-factor authentication for service access. Use of a strong password is enforced as mandatory, and the password must be changed on a regular basis. From a people and process standpoint, preventing breach involves auditing all operator/administrator access and actions, zero standing permission for administrators in the service, “Just-In-Time (JIT) access and elevation” (that is, elevation is granted on an as-needed and only-at-the-time-of-need basis) of engineer privileges to troubleshoot the service, and isolation of the employee email environment from the production access environment. Employees who have not passed background checks are automatically rejected from high privilege access, and checking employee backgrounds is a highly scrutinised, manual-approval process. Preventing breach also involves automatically deleting unnecessary accounts when an employee leaves, changes groups, or does not use the account prior to its expiration.</p> <p>Data is also encrypted. Customer data in Microsoft cloud services exists in two states:</p> <ul style="list-style-type: none"> • at rest on storage media; and • in transit from a data center over a network to a customer device.

Ref.	Question / requirement	Guidance
		<p>Microsoft offers a range of built-in encryption capabilities to help protect data at rest.</p> <ul style="list-style-type: none"> 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, 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 centers. 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. <p>Such policies and procedures are available through Microsoft's online resources, including the Trust Center and the Service Trust Portal.</p>
19.	How is the financial institution's data isolated from other data held by the service provider?	For all of its Online Services, Microsoft logically isolates customer data from the other data Microsoft holds. Data storage and processing for each tenant is segregated through an "Active Directory" structure, which isolates customers using security boundaries ("silos"). The silos safeguard the customer's data such that the data cannot be accessed or compromised by co-tenants.
20.	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

Ref.	Question / requirement	Guidance
		<p>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.</p> <p>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.</p> <p>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.</p>
21.	What policies does the service provider have in place to monitor employees with access to confidential information?	For certain core services of Office 365 and Azure, personnel (including employees and subcontractors) with access to customer data content are subject to background screening, security training, and access approvals as allowed by applicable law. Background screening takes place before Microsoft authorises the employee to access customer data. To the extent permitted by law, any criminal history involving dishonesty, breach of trust, money laundering, or job-related material misrepresentation, falsification, or omission of fact may disqualify a candidate from employment, or, if the individual has commenced employment, may result in termination of employment at a later day.
22.	How are customers authenticated?	Microsoft cloud services use two-factor authentication to enhance security. Typical authentication practices that require only a password to access resources may not provide the appropriate level of protection for information that is sensitive or vulnerable. Two-factor authentication is an authentication method that applies a stronger means of identifying the user. The Microsoft phone-based two-factor authentication solution allows users to receive their PINs sent as messages to their phones, and then they enter their PINs as a second password to log on to their services.
23.	Does the service provider have	<i>Article 14-2 (1) Supervisory Regulation and Cloud Guide requires financial institutions to assess the safety of the cloud services before they use cloud. For the detailed report which shows how Microsoft cloud services meet the Security Assessment Standards Items from the Cloud Guide, please reach out to your Microsoft contact.</i>

Ref.	Question / requirement	Guidance
	sufficient information security capability?	<p>There are several avenues through which financial institutions can assess the information security capability of Microsoft and evaluate the design of the information security controls of Microsoft cloud services. Together they ensure that you can meet your regulatory requirements and supervise the cloud services.</p> <p>First, Microsoft provides many built-in service capabilities to help you examine and verify access, control and service operation as part of your regular assurance processes. These include:</p> <ul style="list-style-type: none"> • Service Trust Portal – for deep technical trust and compliance information, including recent audit reports for our services, as well as the International Standards Organisation (ISO) Statements of Applicability • Compliance Manager – a tool that provides detailed information about our internal controls, including test status and most recent test dates, and allows you to create your own assessments and monitor your own controls • Office 365 Audited Controls – for detailed information about our internal control set, including mapping to international standards, and the most recent test dates • Office 365 Management Activity API – for visibility of user, admin, system and policy actions and events from your Office 365 and Azure Active Directory activity logs • Office 365 Health Dashboard – to immediately check service health, including current known services issues and ongoing resolution plans in progress • Azure Security Center – for visibility into the security state of your Azure resources and the ability to respond to threats and vulnerabilities • Azure Advisor – for continuous intelligent recommendation for how to further secure your Azure environment

Ref.	Question / requirement	Guidance
		<ul style="list-style-type: none"> • Microsoft Trust Center – for information about data protection and security, including the location of our primary and backup data centers, subcontractor lists, and rules for when Microsoft service administrators have access to customer data. <p>Furthermore, our extended contract terms for financial services customers add the ability for your internal compliance officers to examine the service more deeply to meet regulatory requirements. Through the optional Financial Services Compliance Program, customers have the opportunity to examine the control framework of the service, review its risk management framework, hold one-to-one discussions with Microsoft’s auditors and obtain in-depth views directly from Microsoft subject matter experts.</p> <p>The Microsoft Security Policy Governance White Paper provides an overview of Microsoft’s Security Policy Framework, with links to the key Microsoft Security Policy documents.</p> <p>Customers can refer to the Azure Response on Security, Privacy and Compliance to assess Microsoft security capability for Azure, and underpinning Office 365 / Microsoft 365 and Dynamics 365 cloud services.</p>
24.	Does the financial institution have an information security policy framework? If so, does it address the responsibilities of the service provider?	<p>Microsoft cloud services comply with several security frameworks, such as ISO 27001, PCI- DSS and FedRAMP etc. These frameworks mandate Microsoft to implement a comprehensive Vulnerability Management Framework for continuous assessment of known and unknown threats. Microsoft cloud security policy framework compliance offerings are committed in the “<i>Security Practices and Policies</i>” section of the Online Services Terms and are summarised at the Trust Center Compliance Offerings page.</p> <p>A financial institution’s information security policy framework should include roles for Microsoft, as cloud services provider, consistent with the customer-side and service-side controls in the shared responsibility model (see diagram below), and with contractual commitments in the Online Services Terms.</p>

Ref.	Question / requirement	Guidance																																								
		<p>The figure below describes how shared responsibility works across the cloud service models.</p>  <table border="1" data-bbox="555 387 1104 997"> <thead> <tr> <th>Responsibility</th> <th>On-Prem</th> <th>IaaS</th> <th>PaaS</th> <th>SaaS</th> </tr> </thead> <tbody> <tr> <td>Data classification & accountability</td> <td>Cloud Customer</td> <td>Cloud Customer</td> <td>Cloud Customer</td> <td>Cloud Customer</td> </tr> <tr> <td>Client & end-point protection</td> <td>Cloud Customer</td> <td>Cloud Customer</td> <td>Cloud Customer</td> <td>Cloud Customer / Cloud Provider</td> </tr> <tr> <td>Identity & access management</td> <td>Cloud Customer</td> <td>Cloud Customer</td> <td>Cloud Customer / Cloud Provider</td> <td>Cloud Customer / Cloud Provider</td> </tr> <tr> <td>Application level controls</td> <td>Cloud Customer</td> <td>Cloud Customer</td> <td>Cloud Customer / Cloud Provider</td> <td>Cloud Provider</td> </tr> <tr> <td>Network controls</td> <td>Cloud Customer</td> <td>Cloud Customer / Cloud Provider</td> <td>Cloud Provider</td> <td>Cloud Provider</td> </tr> <tr> <td>Host infrastructure</td> <td>Cloud Customer</td> <td>Cloud Customer / Cloud Provider</td> <td>Cloud Provider</td> <td>Cloud Provider</td> </tr> <tr> <td>Physical security</td> <td>Cloud Customer</td> <td>Cloud Provider</td> <td>Cloud Provider</td> <td>Cloud Provider</td> </tr> </tbody> </table> <p>For more information, see our White Paper on Shared Responsibilities for Cloud Computing and related Blog Post.</p>	Responsibility	On-Prem	IaaS	PaaS	SaaS	Data classification & accountability	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer	Client & end-point protection	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer / Cloud Provider	Identity & access management	Cloud Customer	Cloud Customer	Cloud Customer / Cloud Provider	Cloud Customer / Cloud Provider	Application level controls	Cloud Customer	Cloud Customer	Cloud Customer / Cloud Provider	Cloud Provider	Network controls	Cloud Customer	Cloud Customer / Cloud Provider	Cloud Provider	Cloud Provider	Host infrastructure	Cloud Customer	Cloud Customer / Cloud Provider	Cloud Provider	Cloud Provider	Physical security	Cloud Customer	Cloud Provider	Cloud Provider	Cloud Provider
Responsibility	On-Prem	IaaS	PaaS	SaaS																																						
Data classification & accountability	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer																																						
Client & end-point protection	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer / Cloud Provider																																						
Identity & access management	Cloud Customer	Cloud Customer	Cloud Customer / Cloud Provider	Cloud Customer / Cloud Provider																																						
Application level controls	Cloud Customer	Cloud Customer	Cloud Customer / Cloud Provider	Cloud Provider																																						
Network controls	Cloud Customer	Cloud Customer / Cloud Provider	Cloud Provider	Cloud Provider																																						
Host infrastructure	Cloud Customer	Cloud Customer / Cloud Provider	Cloud Provider	Cloud Provider																																						
Physical security	Cloud Customer	Cloud Provider	Cloud Provider	Cloud Provider																																						
25.	What are the procedures for detecting, responding to and reporting information security incidents?	<p>The Incident Management Implementation Guidance for Azure and Office 365 is a comprehensive document customers can use to harden the security posture of their Microsoft cloud environment. It outlines the best methods for configuring the tenant for optimal security incident management: prevention, detection, alerts, anomalous activity monitoring, and post-incident investigations, made possible by in-product logging capability. Microsoft's Office 365 Security Incident Management and Azure Security Response program documents also help you assess Microsoft's own incident management capabilities, policies and processes.</p> <p>Microsoft also supports your compliance through its "Security Incident Notification" commitments in the Online Services Terms:</p>																																								

Ref.	Question / requirement	Guidance
		<p>“Security Incident Notification</p> <p>If Microsoft becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data or Personal Data while processed by Microsoft (each a “Security Incident”), Microsoft will promptly and without undue delay (1) notify Customer of the Security Incident; (2) investigate the Security Incident and provide Customer with detailed information about the Security Incident; (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident ...</p> <p>Microsoft shall make reasonable efforts to assist Customer in fulfilling Customer’s obligation under GDPR Article 33 or other applicable law or regulation to notify the relevant supervisory authority and data subjects about such Security Incident.”</p> <p>“Microsoft has implemented and will maintain for Customer Data in the Core Online Services the following security measures: ...</p> <p>Incident Response Process</p> <ul style="list-style-type: none"> • Microsoft maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, to whom the breach was reported, and the procedure for recovering data. • For each security breach that is a Security Incident, notification by Microsoft (as described in the “Security Incident Notification” section above) will be made promptly and without undue delay after Microsoft becomes aware of the incident. • Microsoft tracks, or enables Customer to track, disclosures of Customer Data, including what data has been disclosed, to whom, and at what time. <p>Service Monitoring. Microsoft security personnel continuously monitors logs to detect anomalies and to propose remediation efforts if necessary.</p> <p>Furthermore, the optional Financial Services Compliance Program provides for deeper information sharing by Microsoft about information security incidents and potential threats, including their nature, common causes and resolutions.</p>

Ref.	Question / requirement	Guidance
		<p>Microsoft Threat Protection (MTP), and other Microsoft security products and capabilities, help financial institutions to comply with this obligation. MTP provides protection across Identities, Endpoint, User Data, Cloud Apps and Infrastructure.</p> <p>Microsoft facilitates compliance with the obligation to annually review and test the Microsoft cloud service information security response plans, to ensure they remain effective and fit-for-purpose, through our “Auditing Compliance” contractual commitments in the Online Services Terms, described further in item 26 below.</p>
26.	<p>What procedures are in place to test, and conduct internal audits of, the effectiveness of information security controls, including those maintained by the service provider?</p>	<p>Microsoft facilitates compliance with these regulations with respect to tests of the Microsoft cloud services thoughts its “Auditing Compliance” contractual commitments in the Online Services Terms:</p> <p>“Auditing Compliance</p> <p>Microsoft will conduct audits of the security of the computers, computing environment and physical data centers that it uses in processing Customer Data and Personal Data, as follows:</p> <ul style="list-style-type: none"> • Where a standard or framework provides for audits, an audit of such control standard or framework will be initiated at least annually. • Each audit will be performed according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework. • Each audit will be performed by qualified, independent, third party security auditors at Microsoft’s selection and expense. <p>Each audit will result in the generation of an audit report (Microsoft Audit Report), which Microsoft will make available at https://servicetrust.microsoft.com/ or another location identified by Microsoft. The Microsoft Audit Report will be Microsoft’s Confidential Information and will clearly disclose any material findings by the auditor. Microsoft will promptly remediate issues raised in any Microsoft Audit Report to the satisfaction of the auditor.”</p> <p>Furthermore, our extended contract terms for regulated financial services customers add the ability to examine the service more deeply to meet regulatory requirements. Regulated financial services customers that opt to join the Financial Services Compliance Program (including their internal and external auditors) have the right to conduct audits on Microsoft business</p>

Ref.	Question / requirement	Guidance
		premises, examine the control framework of the service, review its risk management framework, hold one-to-one discussions with Microsoft’s independent auditors and obtain in-depth views directly from Microsoft subject matter experts.
27.	Are there any measures to immediately notify to financial companies and organizations responding to breach incidents, and to make response in an appropriate manner upon occurrence of computer system failure, electronic breach, etc.?	<p><i>2.1. Of the Additional protective measures for financial sector from the Cloud Guide Security Assessment.</i></p> <p><i>Article 73 of the Supervisory Regulation requires financial institutions to report to FSS:</i></p> <ol style="list-style-type: none"> <i>1. Suspension or delay of the operation of computer for not less than 10(ten) minutes due to any breakdown in the information processing system or communications lines;</i> <i>2. Financial incidents related to manipulation of computer data or programs;</i> <i>3. Information processing system failures due to any electronic trespass, or monetary damage sustained by users as a result of such system failures communicated to the financial company or electronic financial business operator;</i> <i>4. Accidents provided for in Article 9 (1) of the Electronic Financial Transaction Act</i> <p><i>Article 21-5 (1) of the Electronic Financial Transaction Act (Notification, etc. of Infringement Incidents) requires financial institutions to immediately report to the FSC in case an incident, such as disturbance or paralysis of electronic financial infrastructure, occurs due to an electronic infringement.</i></p> <p>Microsoft supports compliance through its “Security Incident Notification” commitments in the Online Services Terms, which are excerpted in item 25 above.</p> <p>When Microsoft notifies the financial institution of an information security incident, the financial institution then “becomes aware” of the incident, and so must notify FSS as soon as possible after receiving notice from Microsoft and evaluating</p>

Ref.	Question / requirement	Guidance
		<p>whether the incident requires FSC notification under Article 21-5 of the Electronic Financial Transaction Act and FSS notification under Article 73 of the Supervisory Regulation³.</p> <p>Furthermore, the optional Financial Services Compliance Program provides for deeper information sharing by Microsoft about information security incidents and potential threats, including their nature, common causes and resolutions.</p> <p>It is important to note that security incident monitoring is a shared responsibility. Microsoft cloud customers are responsible to detect some types of security incidents, and are not dependent upon Microsoft to detect those incidents. Microsoft provides the tools and resources outlined in item 25 above to empower our customers to identify security concerns and detect security incidents.</p>
28.	How is end-to-end application encryption security implemented to protect PINs and other sensitive data transmitted between terminals and hosts?	<p>Microsoft cloud services use industry-standard secure transport protocols for data as it moves through a network—whether between user devices and Microsoft data centers or within data centers themselves. To help protect data at rest, Microsoft offers a range of built-in encryption capabilities.</p> <p>There are three key aspects to Microsoft's encryption:</p> <ol style="list-style-type: none"> 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 unauthorized access to our data. Proper key

³ Article 42 of the Regulation on Examination and Sanctions Against Financial Institutions (Report of Important Information Items) requires financial institutions to report important matters or incidents, if deemed necessary to be reported, to the FSS.

Ref.	Question / requirement	Guidance
		<p>management is an essential element in encryption best practices, and Microsoft helps ensure that encryption keys are properly secured. Protocols and technologies examples include:</p> <ol style="list-style-type: none"> 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 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.

Ref.	Question / requirement	Guidance
		<ul style="list-style-type: none"> 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). <p>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.</p>
29.	Are there procedures established to securely destroy or remove the data when the need arises (for example, when the contract terminates)?	<p><i>12.1.6. of the General Protective Measures from the Cloud Guide Security Assessment Standard Items</i></p> <p>Yes. Microsoft uses best practice procedures and a wiping solution that is NIST 800-88, ISO/IEC 27001, ISO/IEC 27018, SOC 1 and SOC 2 compliant. For hard drives that cannot be wiped it uses a destruction process that destroys it (i.e. shredding) and renders the recovery of information impossible (e.g., disintegrate, shred, pulverize, or incinerate). The appropriate means of disposal is determined by the asset type. Records of the destruction are retained.</p> <p>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.</p> <p>“Secure disposal or re-use of equipment and disposal of media” is covered under the ISO/IEC 27001 standards against which Microsoft is certified.</p>
30.	Are there documented security procedures for safeguarding premises and	<p><i>8. of General Protective Measures from the Cloud Guide Security Assessment Standard Items</i></p>

Ref.	Question / requirement	Guidance
	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 centers are monitored using motion sensors, video surveillance and security breach alarms.
31.	Are there documented security procedures for safeguarding hardware, software and data in the data center?	<p><i>8. of General Protective Measures from the Cloud Guide Security Assessment Standard Items</i></p> <p>Yes. These are described at length in the Microsoft Trust Center at microsoft.com/trustcenter.</p> <p>For information on:</p> <ul style="list-style-type: none"> • 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
32.	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	<p><i>Various parts from the Cloud Guide Security Assessment Standard Items.</i></p> <p>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.</p>

Ref.	Question / requirement	Guidance
	<p>privileged accounts are subjected to dual control (e.g. password is split into 2 halves and each given to a different staff for custody).</p>	<p>Microsoft provides monitoring and logging technologies to give customers maximum visibility into the activity on their cloud-based network, applications, and devices, so they can identify potential security gaps. The Online Services contain features that enable customers to restrict and monitor their employees' access to the services, including the Azure AD Privileged Identify Management system and Multi-Factor Authentication. Microsoft logs, or enables customers to log, access and use of information systems containing customer data, registering the access ID, time, authorisation granted or denied, and relevant activity (see Online Services Terms, page 13). An internal, independent Microsoft team audits the log at least once per quarter, and customers have access to such audit logs. In addition, Microsoft periodically reviews access levels to ensure that only users with appropriate business justification have access to appropriate systems.</p> <p>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.</p> <p>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.</p>
33.	<p>Are the activities of privileged accounts captured (e.g. system audit logs) and reviewed regularly? Indicate the party reviewing</p>	<p><i>2.6.of the Additional protective measures for financial sector from the Cloud Guide Security Assessment asks “Is there any system that cooperates with and assists for automatic recording and maintenance of (i) record on access to data processing system (date and time, accessing person, access confirmation), (ii) record on access to computer data (date and time, user, access confirmation), (iii) record on processing of computer data (user login, access log, etc.), regardless of succeeding in access?”</i></p>

Ref.	Question / requirement	Guidance
	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 .
34.	Are the audit/activity logs protected against tampering by users with privileged accounts? Describe the safeguards implemented.	<p><i>10.1 of General Protective Measures from the Cloud Guide Security Assessment Standard Items</i></p> <p>Yes. Microsoft logs, or enables customers to log, access and use of information systems containing customer data, registering the access ID, time, authorization granted or denied, and relevant activity (see Online Services Terms, page 13). An internal, independent Microsoft team audits the log at least once per quarter, and 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.</p>
35.	Is access to sensitive files, commands and services restricted and protected from manipulation? Provide details of controls implemented.	<p><i>10.1 of General Protective Measures from the Cloud Guide Security Assessment Standard Items</i></p> <p>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.</p> <p>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</p>

Ref.	Question / requirement	Guidance
		<p>information regarding Microsoft identity and access management, see https://www.microsoft.com/en-us/trustcenter/security/identity.</p>
36.	<p>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 financial institution?</p>	<p><i>Various obligations regarding disaster recovery and business continuity management that apply to financial institutions are set out in the Cloud Guide: Business Continuity Management. These requirements apply whether or not activities are outsourced to third party service providers such as Microsoft. Your Microsoft Account Manager can assist with any questions about Microsoft's disaster recovery arrangements and how they would interface with those of your institution.</i></p> <p>Yes. 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 real-time issue detection and automated response such that workloads can be moved off any failing infrastructure components with no perceptible impact on the service. Microsoft also maintains 24/7 on-call engineering teams for assistance. See Financial Services Compliance Program and Premier Support; see also Office 365 Support; Premier Support for Enterprise; and Azure Support Plans.</p> <ul style="list-style-type: none"> • <i>Redundancy.</i> 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. <ul style="list-style-type: none"> ○ For Office 365, Microsoft maintains multiple copies of customer data across data centers for redundancy. ○ For Azure, Microsoft may copy customer data between regions within a given geography for data redundancy or other operational purposes. For example, Azure GRS replicates certain data between two regions within the same geography for enhanced data durability in case of a major data center disaster.

Ref.	Question / requirement	Guidance
		<ul style="list-style-type: none"> • <u>Resiliency</u>. 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. • <u>Distributed Services</u>. Microsoft also offers distributed component services like Exchange Online, SharePoint Online, and Lync Online to limit the scope and impact of any failures of a single component. Directory data is also replicated across component services to insulate one service from another in the event of a failure. • <u>Monitoring</u>. 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. • <u>Simplification</u>. Microsoft uses standardised hardware to reduce issue isolation complexities. Microsoft also uses fully automated deployment models and a standard built-in management mechanism. • <u>Human Backup</u>. 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. • <u>Continuous Learning</u>. 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. • <u>Disaster Recovery Tests</u>. Microsoft conducts disaster recovery tests at least once per year.

Ref.	Question / requirement	Guidance
37.	What are the recovery time objectives (RTO) of systems or applications outsourced to the service provider?	<p><i>Additional Protective Measures for Financial Sector from the Cloud Guide Security Assessment Standards Items requires that there are to be cooperation and assistance systems that enable compliance with the recovery time objective (RTO) designated for each service by financial companies. Article 23(9) of the Supervisory Regulation set forth that the RTO for core business shall be less than 3(three) hours and that for core business of insurance companies under the Insurance Business Act, less than 24 hours.</i></p> <ul style="list-style-type: none"> • Azure: Please refer to the Service Level Agreement (SLA) here: http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeld=37 <p>The responsibility of designing applications for resilience is a shared responsibility with the customer. Microsoft Azure provides the platform of resilience with various design and configurations that utilize Availability Sets, Availability Zones and geo-redundant Azure Regions, however it is the responsibility of the customer to design/architect their application for the resiliency/available requirements.</p> <ul style="list-style-type: none"> • Office 365 operates using an active/active configuration. For example Exchange Online operates using an Active:Active:Active:Active configuration with 24hr lagged online copy of data. This configuration allows the service to meet a high resilience design and cope with blackswan events such as total loss of data center(s). RTO/RPO is not considered a valid metric for evaluating active/active configurations or for services like Exchange Online, as this service is built to targets for near instant failover and zero data loss.
38.	What are the recovery point objectives (RPO) of systems or applications	<p><i>Additional Protective Measures for Financial Sector from the Cloud Guide Security Assessment Standards Items include cooperation and assistance systems that enable compliance with the recovery time objective (RTO) designated for each service by financial companies. Article 23(9) of the Supervisory Regulation sets forth that the RTO for core business shall be less than 3 (three) hours and that for core business of insurance companies under the Insurance Business Act, less than 24 hours.</i></p>

Ref.	Question / requirement	Guidance
	outsourced to the service provider?	<ul style="list-style-type: none"> Azure: Please refer to the Service Level Agreement (SLA) here: http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=37 <p>The responsibility of designing applications for resilience is a shared responsibility with the customer. Microsoft Azure provides the platform of resilience with various design and configurations that utilize Availability Sets, Availability Zones and geo-redundant Azure Regions, however it is the responsibility of the customer to design/architect their application for the resiliency/available requirements.</p> <ul style="list-style-type: none"> Office 365: Office 365 operates using an active/active configuration. For example Exchange Online operates using an Active:Active:Active:Active configuration with 24hr lagged online copy of data. This configuration allows the service to meet a high resilience design and cope with blackswan events such as total loss of data center(s). RTO/RPO is not considered a valid metric for evaluating active/active configurations or for services like Exchange Online, as this service is built to targets for near instant failover and zero data loss.
39.	What are the data backup and recovery arrangements for your organisation's data that resides with the service provider?	<p><i>2.7.of the Additional Protective Measures for Financial Sector from the Cloud Guide Security Assessment Standards Items include establishment of Network Duplexing and Data Backup Systems.</i></p> <p><u>Redundancy</u></p> <ul style="list-style-type: none"> Physical redundancy at server, data center, and service levels. Data redundancy with robust failover capabilities. Functional redundancy with offline functionality. <p>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,</p>

Ref.	Question / requirement	Guidance
		<p>Microsoft maintains multiple copies of customer data across for redundancy. For Azure, Microsoft provides configuration options to enable customers to duplicate copies of data into a paired region in the same jurisdiction. Some services may replicate metadata between paired regions for resilience purposes.</p> <p><u>Resiliency</u></p> <ul style="list-style-type: none"> • Active load balancing. • Automated failover with human backup. • Recovery testing across failure domains. <p>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.</p> <p><u>Distributed Services</u></p> <ul style="list-style-type: none"> • Distributed component services like Exchange Online, SharePoint Online, and Skype for Business Online 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. <p><u>Monitoring</u></p> <ul style="list-style-type: none"> • Internal monitoring built to drive automatic recovery. • Outside-in monitoring raises alerts about incidents.

Ref.	Question / requirement	Guidance
		<ul style="list-style-type: none"> • Extensive diagnostics provide logging, auditing, and granular tracing. <p><u>Simplification</u></p> <ul style="list-style-type: none"> • Standardised hardware reduces issue isolation complexities. • Fully automated deployment models. • Standard built-in management mechanism. <p><u>Human Backup</u></p> <ul style="list-style-type: none"> • 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. <p><u>Continuous Learning</u></p> <ul style="list-style-type: none"> • 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. <p><u>Disaster recovery tests</u></p> <ul style="list-style-type: none"> • Microsoft conducts disaster recovery tests at least once per year.
40.	How frequently does the service provider	<p><i>Even upon emergencies such as failure, disaster, strike and terrorism, are there measures for securing service continuity to prevent suspension of services that it established and complies with (such as procedures for responding to each event, disaster recovery plan, composition and operation of organization for responding to emergency, mock training, emergency</i></p>

Ref.	Question / requirement	Guidance
	conduct disaster recovery tests?	<p><i>contract system, emergency provision of personnel upon strike, and service manual)? Also, does it conduct regular inspection?(2.7.of the Additional Protective Measures for Financial Sector from the Cloud Guide Security Assessment Standards Items)</i></p> <p>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.</p> <p>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 data centers for redundancy. For Azure, Microsoft provides configuration options to enable customers to duplicate copies of data into a paired region in the same jurisdiction. Some services may replicate metadata between paired regions for resilience purposes.</p> <p>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.</p>

Part 2: Contract Checklist

What are our contract documents?

Appendix 2-3 of the Supervisory Regulation and Article 4 of the DPO Regulation list up items which must be contained in an outsourcing agreement. 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:

<p>Core Microsoft contract documents</p> <p>Microsoft Business and Services Agreement (MBSA);</p> <p>Enterprise Agreement (EA); and the enabling Enrollment, which is likely to be either an Enterprise Enrollment or a Server and Cloud Enrollment.</p>	<p>Documents incorporated in Microsoft contracts⁴</p> <p>Online Service Terms (OST), incorporating the Data Protection Addendum (DPA) including GDPR terms;</p> <p>Product Terms</p> <p>Online Services Service Level Agreement (SLA).</p>
<p>Amendment provided by Microsoft to add to core contract documents for financial services customers</p> <p>Financial Services Amendment</p>	<p>Supporting documents and information that do not form part of the contract⁵</p> <p>Materials available from the Trust Center</p>

What does this Part 2 cover?

- I. Appendix 2-3 of the Supervisory Regulation and Article 4 of the DPO Regulation provide that, at a minimum, 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, and the second column indicates how and where in the Microsoft contractual documents the mandatory requirement is covered.

⁴ Available at www.microsoft.com/contracts.

⁵ Available at www.microsoft.com/trustcenter.

Appendix 2-3 of the Supervisory Regulation

1. Key items required in outsourcing agreements

	Key items required in outsourcing agreements	How and where is this deal with in Microsoft's contract?	Applicable laws and regulations
1.	Physical location where cloud computing services are provided	<p>Relevant terms are stipulated under the “Data Transfers and Location” section (DPA, p. 8)” of the Data Protection Addendum (DPA), which is an addendum to the Microsoft Online Services Terms (OST) executed between Microsoft and a financial customer.</p> <p>Storage location for Customer Data in Korea is available in the link below. http://azuredatacentermap.azurewebsites.net/</p>	
2.	Matters requiring consent from financial companies or electronic financial business entities, such as re-outsourcing or changes related to re-outsourcing	<p>The current re-outsourcer and its services can be viewed at Service Trust Portal, and the Customer is deemed to have consented to such re-outsourcer’s processing.</p> <p>In cases where Microsoft newly re-outsources, Microsoft gives Customer notice thereof in advance (at least 6 months prior to providing a Subprocessor with access to Customer Data, 14 days for providing that Subprocessor with access to Personal Data other than that which is contained in Customer Data). The Customer may terminate related services by submitting a written notice if the Customer does not approve the new re-outsourcer (DPA, p.9).</p>	<ul style="list-style-type: none"> • Matters concerning restrictions on the re-outsourcing of credit information processing (3(d) of Appendix 4 in the Regulations on the Supervision of Credit Information Business) • Matters concerning the report on the outsourcer in cases where the outsourcer subcontracts the outsourced work (3(e) of Appendix 4 in the Regulations on the Supervision of Credit Information Business) • Matters concerning restrictions on re-outsourcing (Article 28(1)2 of the Enforcement Decree of the Personal Information Protection Act)

3.	Matters concerning outsourced work and data	<p>[Outsourced work]</p> <p>The contract pack comprehensively sets out the scope of the arrangement and the respective commitments of the parties. The online services are ordered under the EA Enrollment, and the order will set out the online services and relevant prices.</p> <p>Microsoft enters into agreements with each of its financial institution customers for Online Services, which includes a Financial Services Amendment, the Online Services Terms, Data Protection Addendum and the Service Level Agreement. The agreements clearly define the Online Services to be provided.</p> <p>The services are broadly described, along with the applicable usage rights, in the Product Terms and the OST, particularly in the OST “Core Online Services” commitments.</p> <p>[Matters concerning data]</p> <p>Under the DPA, 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.</p> <p>Microsoft also makes specific commitments with respect to customer data in the DPA. In summary, Microsoft commits that:</p> <ol style="list-style-type: none"> 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 and for “Microsoft’s legitimate business operations” (as further provided in the “Nature of Processing; Ownership” section of the DPA), each as incident to delivery of the Online Services to Customer. Customer data will not be used for any other purposes, including for advertising or other commercial purposes. 	<ul style="list-style-type: none"> • The scope and purposes of providing and using the credit information provided (1(a) of Appendix 4 in the Regulations on the Supervision of Credit Information Business) • Matters concerning the use of credit information provided for purposes other than prescribed business purposes, and prohibition of disclosing credit information to a third party (1(b) of Appendix 4 in the Regulations on the Supervision of Credit Information Business) • Prohibition of personal information processing for purposes other than the outsourced purpose (Article 26(1)1 of the Personal Information Protection Act) • The scope and purpose of the outsourced work (Article 28(1)1 of the Enforcement Decree of the Personal Information Protection Act)
----	---	---	---

		<p>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.</p> <p>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.</p> <p>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.</p> <p>6. The MBSA deals with confidentiality. 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.</p>	
4.	Matters requiring notification to financial companies or electronic financial business entities such as important changes related to outsourcing	<p>The current re-outsourcer and its services can be viewed at Service Trust Portal, and the Customer is deemed to have consented to such re-outsourcer's processing.</p> <p>In cases where Microsoft newly re-outsources, Microsoft gives Customer notice thereof in advance (at least 6 months prior to providing a Subprocessor with access to Customer Data, 14 days for providing a Subprocessor with access to Personal Data other than that which is contained in Customer Data). The Customer may terminate related services by</p>	<ul style="list-style-type: none"> • Matters concerning restrictions on the re-outsourcing of credit information processing (3(d) of Appendix 4 in the Regulations on the Supervision of Credit Information Business) • Matters concerning the report on the outsourcer in cases where the outsourcer subcontracts the outsourced work (3(e) of Appendix 4 in the Regulations on

	agreements and re-outsourcing	submitting a written notice if the Customer does not approve the new re-outsourcer (DPA, p.9).	<p>the Supervision of Credit Information Business)</p> <ul style="list-style-type: none"> • Matters concerning restrictions on re-outsourcing (Article 28(1)2 of the Enforcement Decree of the Personal Information Protection Act)
5.	Obligation to accommodate supervisory authorities or internal and external auditors to access for inspection (including onsite visits)	There are terms in the contract that enable financial regulators 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.	<ul style="list-style-type: none"> • The outsourcee's obligation to accommodate supervision and inspection of supervisory authorities (Article 4(3) of the Regulations on the Outsourcing of Data Processing Services by Financial Companies)
6.	Matters concerning the transfer and return of outsourced work in cases of annulment or termination of an agreement, or in cases where the effective implementation of the outsourced work is difficult	Microsoft retains Customer Data that remains stored in Online Services under a limited-function account for 90 days after the expiration or termination of the Agreement. After the 90 days, Microsoft disables the Customer's account and deletes the Customer Data and Personal Data within an additional 90 days, unless Microsoft is permitted or required by applicable law, or authorized under the DPA to retain such data (DPA, p. 9). Microsoft's Financial Services Amendment provides for business continuity and exit provisions, including rights for the customer to obtain exit assistance at market rates from Microsoft Consulting Services. Customers should work with Microsoft to build such business continuity and exit plans. Microsoft's flexibility in offering hybrid solutions further facilitate transition from cloud to on-premise solutions more seamlessly.	<ul style="list-style-type: none"> • Matters concerning the disposal and return of credit information during and after the use and retention period of credit information (1(e) of Appendix 4 in the Regulations on the Supervision of Credit Information Business)

7.	Obligation to comply with applicable laws related to outsourcing and outsourced work, and to cooperate on voluntary self-regulation.	Microsoft will comply with all laws and regulations applicable to its provision of the Online Services, including security breach notification law and Data Protection Requirement (DPA, p. 5).	
8.	Matters concerning cooperation on emergency response training (including disaster recovery and transition training), vulnerability analysis and evaluation, breach incident response training, etc.	<p>Microsoft establishes and distributes documented official procedures related to breach response procedures (DPA, Appendix A – Security Measures).</p> <p>The content regarding the vulnerability analysis and evaluation is available in reports such as Penetration Test Summary under the “Data Protection Resources” section on https://servicetrust.microsoft.com.</p>	
9.	Matters concerning assistance on the monitoring of outsourced work	<p>Financial institutions may monitor the performance of the Online Services via the administrative dashboard, which includes information as to Microsoft compliance with its SLA commitments.</p> <p>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.</p>	<ul style="list-style-type: none"> • Matters concerning the management and supervision of the outsourcee (3(b) of Appendix 4 in the Regulations on the Supervision of Credit Information Business) • Matters concerning supervision including inspection on the management status of personal information retained for the outsourced work (Article 28(1)4 of the Enforcement Decree of the Personal Information Protection Act)

		<p>Microsoft also conducts regular penetration testing to increase the level of detection and protection throughout the Microsoft cloud. Microsoft makes available to customers penetration testing and other audits of its cybersecurity practices, and customers also may conduct their own penetration testing of the services. This is done in accordance with Microsoft's rules of engagement, which do not require Microsoft's permission in advance of such testing. For more information regarding penetration testing, see https://technet.microsoft.com/en-us/mt784683.aspx.</p> <p>Microsoft makes available certain tools through the Service Trust Portal to enable customers to conduct their own virtual audits of the Online Services. Microsoft also provides customers with information to reconstruct financial transactions and develop audit trail information through two primary sources: Azure Active Directory reporting, which is a repository of audit logs and other information that can be retrieved to determine who has accessed customer transaction information and the actions they have taken with respect to such information, and Azure Monitor, which provides activity logs and diagnostic logs that can be used to determine the “what, who, and when” with respect to changes to customer cloud information and to obtain information about the operation of the Online Services, respectively.</p> <p>In addition, the Financial Services Amendment details the examination and audit rights that are granted to the customer and financial 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:</p> <p>1. Online Services Information Policy</p> <p>Microsoft makes each Information Security Policy available to the customer, along with descriptions of the security controls in place for the applicable Online</p>	
--	--	--	--

		<p>Service and other information reasonably requested by the customer regarding Microsoft security practices and policies.</p> <p>2. Audits of Online Services</p> <p>On behalf of the customer, Microsoft will cause the performance of audits of the security of the computers, computing environment and physical data centers that it uses in processing customer data for each Online Service. Pursuant to the terms in the DPA, Microsoft will provide Customer with each Microsoft Audit Report.</p> <p>3. Financial Services Compliance Program</p> <p>The customer also has the opportunity to participate in the Financial Services Compliance Program, which is a for-fee program that facilitates the customer’s ability to audit Microsoft, including: (a) assess the services’ controls and effectiveness, (b) access data related to service operations, (c) maintain insight into operational risks of the services, (d) be provided with notification of changes that may materially impact Microsoft’s ability to provide the services, and (e) provide feedback on areas for improvement in the services.</p> <p>In relation to the Outsourcing Standards 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.</p>	
10.	Security requirements such as the data protection obligation for transmitted information and assurance of service continuity	<p>[Data protection obligation for transmitted information]</p> <p>Microsoft protects data according to internal security policies and ISO 27001, ISO 27002, ISO 27018, SSAE 18 SOC 1 Type II, and SSAE 18 SOC 2 Type II. As for data security policies and specific security measures, refer to the “Data Security” section and “Appendix A – Security Measures” in the DPA.</p> <p>[Assurance of service continuity]</p>	<ul style="list-style-type: none"> • Access control on data (Article 4(3) of the Regulations on the Outsourcing of Data Processing Services by Financial Companies) • Matters concerning measures to ensure safety, including limitations on access to personal information (Article 28(1)3 of the Enforcement Decree of the

		<p>The SLA sets out 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.</p> <p>For information regarding uptime for each Online Service, refer to the Service Level Agreement for Microsoft Online Services.</p>	<p>Personal Information Protection Act)</p> <ul style="list-style-type: none"> • Accurate description of security measures for personnel, equipment, and data and compensation for damages against information leakage and unfair business operators in written agreement (including a bid announcement) and task instructions written in order to clearly communicate the requirements of financial companies or electronic financial business entities to business operators (Appendix 5-2 linked to Article 9-2(1) of the Detailed Enforcement Rules of the Regulations on the Supervision of Electronic Financial Activities) • Matters concerning the prevention of information leakage when transmitting and receiving credit information (1(d) of Appendix 4 in the Regulations on the Supervision of Credit Information Business) • Matters concerning confidentiality and protection of credit information owner (3(c) of Appendix 4 in the Regulations on the Supervision of Credit Information Business) • Matters concerning technical and managerial safeguards for personal information (Article
--	--	--	--

			26(1)2 of the Personal Information Protection Act)
11	Matters concerning the obligation of a cloud service provider to manage and supervise re-outsourcing	<p>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 conduct as if it was Microsoft's.</p> <p>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, and to bring vendor business processes and systems into compliance with those of Microsoft. For more information regarding Microsoft's Supplier Security and Privacy Program, see https://www.microsoft.com/en-us/procurement/msp-requirements.aspx.</p> <p>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 (DPA, p. 9). 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.</p> <p>Microsoft provides a website that lists subcontractors authorised to access customer data in the Online Services as well as the limited or ancillary services they provide. At least 6 months before authorising any new subcontractor to access Customer Data, Microsoft will update the website and provide the customer with a mechanism to obtain</p>	<ul style="list-style-type: none"> • Matters concerning restrictions on the re-outsourcing of credit information processing (3(d) of Appendix 4 in the Regulations on the Supervision of Credit Information Business) • Matters concerning restrictions on re-outsourcing (Article 28(1)2 of the Enforcement Decree of the Personal Information Protection Act)

		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 which may include 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. (DPA, p. 9)	
12	Matters concerning the right of the original outsourcer to terminate the contract in cases where services may be adversely affected due to an increase in security risks caused by re-outsourcing or re-outsourcing changes	Microsoft provides a website that lists subcontractors authorised to access customer data in the Online Services as well as the limited or ancillary services they provide. At least 6 months before authorising any new subcontractor to access Customer Data, Microsoft will update the website and provide the customer with a mechanism to obtain notice of that update. If the customer does not approve of a new subcontractor, then the customer may terminate the affected Online Service without penalty by providing, before the end of the notice period, written notice of termination which may include 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. (DPA, p. 9).	<ul style="list-style-type: none"> • Matters concerning restrictions on the re-outsourcing of credit information processing (3(d) of Appendix 4 in the Regulations on the Supervision of Credit Information Business) • Matters concerning restrictions on re-outsourcing (Article 28(1)2 of the Enforcement Decree of the Personal Information Protection Act)

II. Key items required in outsourcing agreements, excluding items included in Section I

1. Article 4(3) of the Regulations on the Outsourcing of Data Processing Services by Financial Companies

	Key items required in outsourcing agreements	How and where is this deal within Microsoft's contract?
1	Liabilities of the outsourcer and outsourcee for damage suffered by Customer due to a computer system failure, etc.	The MBSA contains clauses which deal with liability.

		The MBSA sets out Microsoft's obligation to defend the regulated entity against third party infringement claims.
2	Jurisdiction of the outsourcee during the course of dispute resolution	In the event that a financial institution and Microsoft have a dispute, the choice-of-law and dispute resolution provisions would be clearly described in the agreement between Microsoft and the financial institution. The MBSA contains terms that describe how a dispute under the contract is to be conducted including the jurisdiction.

2. Article 60(1)7 of the Regulations on the Supervision of Electronic Financial Activities and Appendix 5-2 linked to Article 9-2(1) of the Detailed Enforcement Rules on the Regulations on the Supervision of Electronic Financial Activities

	Key items required in outsourcing agreements	How and where is this deal within Microsoft's contract?
1	<p>In cases where confidentiality is required for the data and equipment being used in the service business, a confidentiality agreement shall be prepared separately from a service execution agreement.</p> <p>* The confidentiality agreement must specify the scope of confidential information, security compliance items, liability for compensation in case of violation, issues of intellectual property rights, return of data, etc.</p>	A separate non-disclosure agreement is available upon a customer's request.
2	It shall be specified that personnel engaging in the service business may not be arbitrarily replaced by the service provider without prior consent of the financial company or electronic financial business entity.	DPA sets that Microsoft shall not engage another processor without specific or general prior written authorization from Customer.

3	Security measures for personnel, equipment, and data and compensation for damages against information leakage and unfair business operators shall be accurately described in written agreement (including a bid announcement) and task instructions written in order to clearly communicate the requirements of financial companies or electronic financial business entities to service providers.	Refer to Table I. 10. and Table II. 1.1.
---	---	--

3. Appendix 4 of the Regulations on the Supervision of Credit Information Business– Security Management Measures for Credit Information to Be Included in Agreement of Credit Information Provision (related to Article 21), Article 17(5) of the Credit Information Use and Protection Act and Article 14 (5) of the Enforcement Decree thereof

	Key items required in outsourcing agreements	How and where is this deal within Microsoft's contract?
1	(1)c Matters concerning restrictions of users of the credit information provided and appointment of a dedicated manager	DPA sets out security measures including physical access to facilities and access authorization.
2	(3)g Matters concerning responsibility and punishment in cases of violation of the above matters	Refer to Table II. 1.1.
※ Article 17(5) of the Credit Information Use and Protection Act and Article 14 (5) of the Enforcement Decree thereof		
3	Provision of education/training to the outsourcee's officers/employees for at least once a year	Through security training, Microsoft informs its personnel about relevant security procedures and their respective roles. Microsoft also informs its personnel of possible consequences of breaching the security rules and procedures.(DPA, Appendix A -Security Measures)

4. Article 26(1) of the Personal Information Protection Act and Article 28(1) of the Enforcement Decree of the Personal Information Protection Act

	Key items required in outsourcing agreements	How and where is this deal with-in Microsoft's contract?
1	Matters concerning liabilities such as compensation in cases of a breach of compliance obligations of the outsourcee under Article 26(2) of the Act	Refer to Table II. 1.

Further Information

- **Korea Regulatory Compliance for Financial Services Customers:** <https://www.microsoft.com/en-sg/apac/trustedcloud/korea-financial-service.aspx>
- **Asia Regulatory Compliance for Financial Services Customers:** aka.ms/asiafs
- **Trust Center:** microsoft.com/trust
- **Service Trust Portal:** aka.ms/trustportal
- **Customer Stories:** customers.microsoft.com
- **Online Service Terms:** microsoft.com/contracts
- **Service Level Agreements:** microsoft.com/contracts
- **SAFE Handbook:** aka.ms/safehandbook

© Microsoft Corporation 2019 . 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.

