

## SOUTH KOREA

### CHECKLIST FOR FINANCIAL COMPANIES, ETC. USING CLOUD COMPUTING SERVICE (OFFICE 365)

Last updated: April 2017

#### 1. WHAT DOES THIS CHECKLIST CONTAIN?

This checklist is to confirm compliance with the requirements and procedures under the laws and regulations applicable to the use of cloud computing by financial companies, including banks, insurance companies, financial investment business entities, specialized credit finance business entities and savings banks, etc. ("**Financial Companies**"), and electronic financial business entities regulated by finance related laws (Financial Companies and electronic financial business entities are collectively called "**Financial Companies, etc.**").

Sections 2 to 7 of this checklist explain laws, regulations, and guidelines that are relevant to the use of cloud computing services by the Financial Companies, etc., and Section 8 sets out the items to be confirmed by the Financial Companies, etc. based thereon. Although Financial Companies, etc. using cloud computing services are not required to complete this checklist, this checklist may be used:

- (i) as a reference for ensuring regulatory compliance with the requirements set out in the laws, regulations and guidelines listed in Section 2; and
- (ii) as a reference to aid discussions with the regulator(s) listed in Section 3, should they wish to discuss compliance with their requirements with your company ("**the Company**").

Appendix One also contains a list of the mandatory contractual requirements required by relevant laws, regulations, and guidelines.

Note that this checklist is not drafted with the intention of providing legal or regulatory advice, and should be used only as a reference to efficiently confirm compliance with overall legal or regulatory requirements relating to cloud computing. Therefore, the Company should seek independent legal advice on specific legal or regulatory obligations required in the process of performing cloud-related projects. Also, please note that this checklist is not a warranty or commitment of any sort to the Company.

2. **WHAT LAWS, REGULATIONS AND GUIDELINES ARE RELEVANT?**

**[Laws, Regulations, and Guidelines Applicable to the Use of Cloud Computing Services by Financial Companies, etc.]**



	Relevant Regulations	For Financial Companies		For Electronic Financial Business Entities
1	Regulations relating to outsourcing	Financial Companies which are financial investment business entities	Financial Investment Services and Capital Markets Act (“FSCMA”) is applicable.	The DPO Regulation is applicable.
		Financial Companies which are not financial investment business entities	Regulation on Outsourcing of Data Processing of Financial Companies (“DPO Regulation”) is applicable.	
2	Electronic Financial Supervisory Regulations (“EFSR”)	Only applicable in case of performing electronic financial business		Applicable
3	Guide on Use of Cloud Services in Financial World (“Cloud Guide”)	Commonly applicable (however, in case of not performing electronic financial business, the provisions relating to the EFSR are not applicable)		

※ In case of a financial investment business entity, the provisions relating to outsourcing in the FSCMA prevail over the Regulation Regarding Outsourcing by Financial Institutions (“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 (Article 1 of the Outsourcing Regulation). For your reference, electronic financial business entities are not included in the financial institutions regulated by the Outsourcing Regulation (Article 2(1) of the Outsourcing Regulation).


※ In case of a financial company which does not perform electronic financial business<sup>1</sup>, the EFSR and the provisions in the Cloud Guide relating to the EFSR are not applicable (Article 3(3), Item 1 of the Electronic Financial Transactions Act, Article 5(2) of the Enforcement Decree of the same Act).

[Outline of Laws, Regulations, and Guidelines]

Classification	Relevant Regulations and Outlines	Provisions
<p><b>Regulations relating to outsourcing</b></p>	<p><b>Regulations relating to the FSCMA</b> For financial investment business entities, the FSCMA shall prevail over the Outsourcing Regulation and the DPO Regulation. The term “financial investment business entities” refers to investment-trading business entities, investment brokerage business entities, collective investment business entities, investment consulting business entities, discretionary investment business entities or trust business entities. Even in case where a bank or insurance company also engages in financial investment business, with respect to outsourcing relating to financial investment business, the FSCMA shall prevail over the Outsourcing Regulation and the DPO Regulation.</p>	<p><b>FSCMA, Enforcement Decree of the FSCMA</b></p> <div style="display: flex; justify-content: space-around; align-items: center;"> <div style="text-align: center;">               자본시장과 금융투자업에 관한         </div> <div style="text-align: center;">               자본시장과 금융투자업에 관한         </div> </div> <p>Financial Investment Business Regulation (<a href="#">Please click here</a>)</p>
	<p><b>DPO Regulation</b> DPO Regulation is applicable to the outsourcing of data processing service through cloud computing, etc. by the Financial Companies, etc. Although the Outsourcing Regulation is not directly applicable to such outsourcing of data, as Article 7(1), Item</p>	<p><b>Error! Not a valid link.</b></p>

<sup>1</sup> “Electronic financial services” refers to a Financial Company’s or an electronic financial business entity’s provision of financial products and services through electronic apparatus (Article 2, Item 1 of the Electronic Financial Transaction Act), and whether the relevant company performs electronic financial services or not may differ depending on the specific circumstances. It is stated in p. 4 of 「Interpretation of the EFSR」 (Financial Supervisory Service, December 2009) that, “the inquiry services for credit information, possession of assets, or history of transactions provided through the Internet” also fall under electronic financial business. Therefore, even if there are no transactions where the users make use of “electronic financial business” (electronic financial services) in a non-facing and automated manner (i.e., electronic financial transaction), the EFSR is applicable as long as “electronic financial business” (electronic financial services) are being provided.

	<p>2 of the DPO Regulation requires the “Standards for Operation of Outsourcing of Business” (under Article 3-2 of the Outsourcing Regulation) to be reported to the Governor of the Financial Supervisory Service, the Outsourcing Regulation may be applicable indirectly.</p>	
<p><b>EFSR</b></p>	<p>The EFSR sets forth the matters for securing safety and reliability with respect to the IT sectors, electronic financial business, and authentication methods, etc. of the Financial Companies, etc. engaging in electronic financial transactions. The electronic financial transaction means any transaction whereby the Financial Companies, etc. provide financial products and services through electronic apparatus (“<b>electronic financial business</b>”) and users use such services in a non-facing and automated manner without any direct contact with employees of the Financial Companies, etc., which includes Internet banking, transaction history inquiry system, and trading system, etc. The EFSR is not applicable to the Financial Companies which do not perform electronic financial business.</p> <p>The EFSR sets forth the matters concerning designation of a “non-material data processing system” (Article 14-2) so that the Financial Companies, etc. performing electronic financial business may use cloud computing services. According to the EFSR, only computer rooms with the data processing systems that are designated as non-material data processing systems are exempted from the obligations of (i) installation of computer rooms and disaster recovery centers within Korea (in case of Financial Companies headquartered in Korea) (Article 11, Item 11), (ii) prohibition of installation of a wireless communication network (Article 11, Item 12), and (iii) physical separation of a network (Article 15(1), Item 5). As the data processing system containing any unique identification information of individuals or personal credit information shall not be designated as a non-material data processing system, in order to use cloud computing services for any data processing system using unique identification information of individuals or personal credit information, all of the</p>	<p>EFSR, Detailed Enforcement Rules of the EFSR</p> <div style="display: flex; justify-content: space-around; align-items: center;"> <div style="text-align: center;">  <p>전자금융감독규정.pdf</p> </div> <div style="text-align: center;">  <p>전자금융감독규정 시행세칙.pdf</p> </div> </div>

	<p>abovementioned obligations must be complied with.</p> <p>Meanwhile, the standards for Outside Order under the EFSR shall apply only to cooperation, outsourcing or outside order regarding electronic financial transactions (“<b>Outside Order, etc.</b>”) with an auxiliary electronic financial business entity. <b>As O365 cloud service does not fall under Outside Order, etc. relating to electronic financial transactions, this checklist does not address the matters concerning Outside Order, etc.</b></p>	
<p>Cloud Guide</p>	<p>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 Companies, etc. when using cloud computer services. The Cloud Guide was prepared based on the Act on the Development of Cloud Computing and Protection of its Users, Electronic Financial Transactions Act, Credit Information Use and Protection Act (“<b>Credit Information Act</b>”), Personal Information Protection Act (“<b>PIPA</b>”), and Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. (“<b>Network Act</b>”), and includes the items on data subject to cloud services, introduction of cloud services, use of cloud services, management and <i>expost facto</i> management of cloud services. The Cloud Guide is not legally binding, and is only a recommendation issued by the regulatory authorities.</p>	 <p>[금융보안원] 금융권 클라우드 서</p>

3. **WHO IS/ARE THE RELEVANT REGULATORS?**

- [The Financial Services Commission](#) (“**FSC**”)
- [The Financial Supervisory Service](#) (“**FSS**”)

Note that the FSC is a central administrative body responsible for financial policy and financial supervision. The FSS is a financial regulator that examines and supervises Financial Companies, etc. under the instruction and oversight of the FSC.

4. **IS APPROVAL OF OR REPORT TO REGULATORS REQUIRED?**

Although approval by the regulators is not required, (i) a report on outsourcing, and (ii) in case of designating a non-material data processing system, a report on such designation shall be made to the regulators.

4.1 **Report on outsourcing**

- **Report on outsourcing under the FSCMA:** Financial investment business entities shall report outsourcing to the FSS at least seven days prior to the intended date of performing the outsourced services.
- **Report on outsourcing under the DPO Regulation:** Financial Companies, etc. which are not financial investment business entities and electronic financial business entities shall report to the FSS the below depending on the outsourced information and the location of the outsourcee:

Outsourced information	Location of the Outsourcee	Timing of Report
Financial transaction information which can identify individual customers	Overseas	30 business days prior to the expected date of executing an outsourcing agreement
	Domestic	Seven business days prior to the expected date of executing an outsourcing agreement
Other financial transaction information	Overseas/domestic	Within 10 business days from the date of executing an outsourcing agreement
Information other than financial transaction information	Overseas/domestic	Semiannual report by the end of July of the current year or the end of January the next year

4.2 **Report of designation of a non-material data processing system:** In case where a Financial Company, etc. designates a non-material data processing

system, such company shall report to the FSS within seven days thereafter.

5. **IS/ARE THERE (A) SPECIFIC FORM(S) TO BE COMPLETED?**

Outsourcing by a financial investment business entity that is subject to the FSCMA shall be reported in the form of [Attachment 1] <No. 19> of the Financial Investment Business Regulation (“**FIBR**”), and an outsourcing pursuant to the DPO Regulation shall be reported in the form of [Form 1] under the Outsourcing Regulation.

Designation of a non-material data processing system shall be reported in the form of [Attachment 6] of the Detailed Enforcement Rules of the EFSR.

6. **DOES THE REGULATOR MANDATE SPECIFIC CONTRACTUAL REQUIREMENTS THAT MUST BE ADOPTED IN THE OUTSOURCING AGREEMENT?**

The FSCMA sets forth the matters that must be included in the outsourcing agreement in case of outsourcing by a financial investment business entity, and the DPO Regulation only sets forth the matters that must be included in the outsourcing agreement by the Financial Companies, etc. which are not financial investment business entities and electronic financial business entities. (There used to be a specific standard agreement form required, but it is now deleted.)

The EFSR sets forth the matters to be included in the agreement for an Outside Order regarding electronic financial transactions of a Financial Company, etc. performing electronic financial business, and the Cloud Guide provides for the items to be included in the agreement between the Financial Company, etc. and the cloud service provider. This checklist excluded the items to be included in the agreement in case of an Outside Order regarding electronic financial transactions under the EFSR.

Please refer to Appendix One for a list of the items that must be included in the agreements with cloud service providers.

7. **PRIVACY LAW REQUIREMENTS**

7.1 **Privacy law requirements applicable to the Financial Companies, etc.**

The privacy laws applicable to the Financial Companies, etc. include the [Credit Information Act](#), [PIPA](#), and [Network Act](#), and such laws shall be complied

with according to the types of the information outsourced to the cloud service provider (Microsoft, the outsourcee).

The privacy regulators are [FSC](#), [FSS](#), [the Ministry of Government Administration and Home Affairs](#), [the Korea Communications Commission](#), and [the Personal Information Protection Commission](#).

## 7.2 Privacy law requirements applicable to the cloud service provider (i.e. Microsoft)

The 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 credit information), PIPA and the Network Act in relation to processing personal information.

- Credit Information Act
  - In case of outsourcing credit information processing service, the Credit Information Act is applicable. The Credit Information Act provides that credit information processing service may be outsourced to a company whose capital or total amount of capital exceeds KRW 100 million and which has designated a relevant privacy officer (a Credit Information Administrator/Protector (“**CIAP**”) under the Credit Information Act, a Chief Privacy Officer (“**CPO**”) under the PIPA or the Network Act, or a Chief Information Security Officer (“**CISO**”) under the Electronic Financial Transaction Act) (Article 17(2) of the Credit Information Act).
  - The outsourcee is prohibited from using the provided credit information beyond the scope of the outsourced services and, sub-outsourcing is prohibited in principle and is only permitted to the extent that it does not hinder protection and safe processing of the credit information (Articles 17(6) and 17(7) of the Credit Information Act) .
  - With respect to the performance of the services by the outsourcee, Articles 19 through 21, Articles 40, 43, 43-2, and 45 of the Credit Information Act shall apply.
- PIPA
  - The outsourcees are prohibited from using personal information or providing a third party with such information beyond the scope of relevant services outsourced by a personal information manager (Article 26(5) of the PIPA).



- The outsourcees are also required to comply with Articles 15 through 25, 27 through 31, 33 through 38 and 59 of the PIPA (Article 26(7) of the PIPA).
- Network Act
  - The Network Act also sets out various obligations imposed on information and communications service providers in relation to protection of personal information and securing of stability of information and communication network, and the Network Act is applicable to the information collected according to the Network Act.
  - The outsourcee shall not process personal information of the users beyond the personal information processing purposes determined at the time of outsourcing (Article 25(3) of the Network Act).
- There are also administrative rules to be complied with by the cloud service provider, which is the outsourcee, according to the Credit Information Act, the PIPA, and the Network Act.
  - The FSC, as delegated by the Credit Information Act, determines the technical, physical, and managerial security measures to be complied with in case of processing personal credit information in [Attachment 3] of the Credit Information Business Supervisory Regulations.
  - The Ministry of Government Administration and Home Affairs, as delegated by the PIPA, determines the technical, physical, and managerial security measures to be complied with in case of processing personal information in the “Standards of Personal Information Security Measures.”
  - The Korea Communications Commission, as delegated by the Network Act, determines the “Technical and Managerial Safeguards for Personal Information.”
  - The cloud service providers shall comply with the above administrative rules depending on the type of the information outsourced.

※ This checklist focuses on the financial regulatory requirements. For more information about the privacy law requirements, please talk to the Company’s Microsoft contact.

8. CHECKLIST

**Key:**

In blue text, Microsoft has included template responses for the checklist. Some questions are specific to the Company’s own internal operations and processes, and the answers may need to be revised according to the Company’s internal circumstances.

In *red italic*, Microsoft has stated the relevant provisions of the laws and regulations on which the relevant question is based upon, and may be of guidance or assistance to the Company in preparing responses for the checklist questions.

No.	Question/requirement	Template response and guidance
<b>OVERVIEW OF OUTSOURCING ARRANGEMENT</b>		
1.	Who is the cloud service provider (the “Service Provider”)?	<p><i>Article 7(1) Item 7 of the DPO Regulation, Attachment 1 &lt;No. 19&gt; of the Detailed Enforcement Rules of the FIBR</i></p> <p>The Service Provider is Microsoft Korea, Inc., the Korean subsidiary of Microsoft Corporation, a multinational company providing information technology devices and services, which is publicly-listed in the USA NASDAQ.</p> <p>Detailed information of Microsoft is available here:  <a href="https://www.microsoft.com/en-us/news/inside_ms.aspx">https://www.microsoft.com/en-us/news/inside_ms.aspx</a>.</p>
2.	When is the term of this service agreement (or outsourcing agreement)?	<p><i>Attachment 1 &lt;No. 19&gt; of the Detailed Enforcement Rules of the FIBR</i></p> <p><i>Please insert the term of providing the cloud services under the agreement with Microsoft.</i></p>
3.	<b><u>In case of being designated as a non-</u></b>	<i>Article 14-2(1) of the EFSR, Chapter 2, Section 1 of the Cloud Guide</i>

No.	Question/requirement	Template response and guidance
	<p><b>material data processing system]</b> Has the Company assessed this service agreement to be an outsourcing arrangement of a non-material data processing system, considering the followings?</p> <ul style="list-style-type: none"> <li>• Not processing any unique identification information or personal credit information</li> <li>• Importance of the information processed and impact in case of any forgery, falsification, or leakage of the information</li> <li>• Connectivity with other systems, including damage to other systems' business continuity in case of any breach incident or failure</li> <li>• Importance in business of the concerned data processing system, including the recovery time objectives</li> <li>• Usage of the information processing system, including operation, development, and test system, etc.</li> </ul>	<p><i>Please confirm relevant information according to the Company's internal circumstances. However, even in cases of processing unique identification information or personal credit information, , cloud services may be used in processing unique identification information or personal credit information which has been de-identified according to the "Personal Information De-identification Guidelines" or which is irrelevant to electronic financial transactions, such as information on the company employees.</i></p> <p>Yes.</p> <ul style="list-style-type: none"> <li>• Unique identification information or personal credit information is not processed. <i>(Or, even if such information is processed, "it is de-identified according to the "Personal Information De-identification Guidelines.") (Or, even if such information is processed, the unique identification information or personal credit information is not related to electronic financial transactions).</i></li> <li>• Usage of the system: operation system It is the mail system which is a part of the groupware supporting works for business performance among the internal employees and is used for e-mail communication, scheduling, contact information management, and work management, etc.</li> <li>• Data processed: internal information of the company The system processes general business-related communication information which is not relevant to electronic financial transactions and applies technical/managerial protective measures to prevent leakage of unique identification information, personal credit information or internal confidential information, etc.</li> <li>• Users of the system Approximately [ ] employees of the company</li> <li>• Connectivity with other systems: The system is not connected with any electronic financial service system.</li> <li>• Recovery time objectives: One hour or less for Microsoft Exchange Online (e-mail), six hours or less for</li> </ul>

No.	Question/requirement	Template response and guidance
	<ul style="list-style-type: none"> <li>Number of the users of the concerned data processing system according to each type of users (e.g., customers, company employees)</li> </ul>	<p>SharePoint Online (business cooperation)</p>
4.	<p><b><u>[In case of being designated as a non-material data processing system]</u></b> Did the Company comply with the designation procedures under the Cloud Guide when designating a non-material data processing system?</p> <ul style="list-style-type: none"> <li>Deliberation and resolution of the 「Information Protection Committee」 within the financial company</li> <li>Submission of a report stating the standards for evaluation of the importance of information assets, results of designation, and management plans, etc. to the FSS within seven days from the date of designation</li> </ul>	<p><i>Articles 14-2(2) and (3) of the EFSR, Chapter 2, Section 2 of the Cloud Guide</i></p> <p><i>Please confirm relevant information according to the Company's internal circumstances.</i></p> <p><i>Yes.</i></p> <p><i>The Company completed the deliberation and resolution process of the Information Protection Committee according to the Company's internal procedures, which can be confirmed in the relevant minutes of meetings.</i></p>
5.	<p><b><u>[If the Company engages in financial investment business]</u></b> Are the services</p>	<p><i>Proviso of Article 42(1) of the FSCMA, Article 45 of the Enforcement Decree of the same Act</i></p>

No.	Question/requirement	Template response and guidance																					
	<p>that the Company intends to outsource to the Service Provider critical to the license/permit of the Company's financial investment business?</p>	<p><i>The data processing outsourced to Microsoft is limited to the services which are not critical to the business of financial investment business entities under the FSCMA, and the Company can outsource the services only when answer to this question is "no". The services provided by Office 365 are limited to the followings and are not critical to the business of financial investment business entities under the FSCMA.</i></p> <table border="1" data-bbox="786 531 1675 1050"> <thead> <tr> <th data-bbox="786 531 837 608"></th> <th data-bbox="837 531 1487 608">Service(s) to be outsourced</th> <th data-bbox="1487 531 1675 608">Critical (Y/N)</th> </tr> </thead> <tbody> <tr> <td data-bbox="786 608 837 679">1.</td> <td data-bbox="837 608 1487 679">Microsoft Office applications</td> <td data-bbox="1487 608 1675 679">N</td> </tr> <tr> <td data-bbox="786 679 837 751">2.</td> <td data-bbox="837 679 1487 751">Hosted email</td> <td data-bbox="1487 679 1675 751">N</td> </tr> <tr> <td data-bbox="786 751 837 823">3.</td> <td data-bbox="837 751 1487 823">Web conferencing, presence, and instant messaging</td> <td data-bbox="1487 751 1675 823">N</td> </tr> <tr> <td data-bbox="786 823 837 895">4.</td> <td data-bbox="837 823 1487 895">Data and application hosting</td> <td data-bbox="1487 823 1675 895">N</td> </tr> <tr> <td data-bbox="786 895 837 967">5.</td> <td data-bbox="837 895 1487 967">Spam and malware protection</td> <td data-bbox="1487 895 1675 967">N</td> </tr> <tr> <td data-bbox="786 967 837 1050">6.</td> <td data-bbox="837 967 1487 1050">IT support services</td> <td data-bbox="1487 967 1675 1050">N</td> </tr> </tbody> </table>		Service(s) to be outsourced	Critical (Y/N)	1.	Microsoft Office applications	N	2.	Hosted email	N	3.	Web conferencing, presence, and instant messaging	N	4.	Data and application hosting	N	5.	Spam and malware protection	N	6.	IT support services	N
	Service(s) to be outsourced	Critical (Y/N)																					
1.	Microsoft Office applications	N																					
2.	Hosted email	N																					
3.	Web conferencing, presence, and instant messaging	N																					
4.	Data and application hosting	N																					
5.	Spam and malware protection	N																					
6.	IT support services	N																					
6.	<p>List the types of data that would be processed by the Service Provider, and indicate if the data is considered to be sensitive.</p>	<p><i>Article 5(2) of the DPO Regulation</i></p> <p><i>Chapter 2, Section. 1.A.1 of the Cloud Guide</i></p> <p><i>When the Company chooses a Microsoft Office 365 solution, the types of data to be outsourced for processing are within the Company's control so the template response below will need to be tailored depending on what data the Company has selected to be outsourced. In particular, in case of item nos. 1, 3, and 5 below, if any personal credit information of the customers is included, designation as a non-material data processing system (as in question No. 3 above) is prohibited. Therefore, the response below should be</i></p>																					

No.	Question/requirement	Template response and guidance																														
		<p><i>drafted consistently with the answers for question No. 3 above.</i></p> <p>We only collect and process data that is necessary for our business operations in compliance with all applicable laws and regulation. Typically the types of data that would be processed and stored by the Office 365 service would include:</p> <table border="1" data-bbox="786 564 2067 1398"> <thead> <tr> <th data-bbox="786 564 837 679"></th> <th data-bbox="837 564 1585 679">Type of Data</th> <th data-bbox="1585 564 1906 679">Processed/Stored/Both</th> <th data-bbox="1906 564 2067 679">Sensitive (Y/N)</th> </tr> </thead> <tbody> <tr> <td data-bbox="786 679 837 831">1.</td> <td data-bbox="837 679 1585 831">Customer data (including customer name, contact details, account information, payment card data, security credentials and communication).</td> <td data-bbox="1585 679 1906 831">Both</td> <td data-bbox="1906 679 2067 831">N</td> </tr> <tr> <td data-bbox="786 831 837 1027">2.</td> <td data-bbox="837 831 1585 1027">Employee data (including employee name, contact details, internal and external communication by email and other means and personal information relating to their employment with the organization).</td> <td data-bbox="1585 831 1906 1027">Both</td> <td data-bbox="1906 831 2067 1027">N</td> </tr> <tr> <td data-bbox="786 1027 837 1139">3.</td> <td data-bbox="837 1027 1585 1139">Transaction data (data relating to transactions in which the organization is involved).</td> <td data-bbox="1585 1027 1906 1139">Both</td> <td data-bbox="1906 1027 2067 1139">N</td> </tr> <tr> <td data-bbox="786 1139 837 1214">4.</td> <td data-bbox="837 1139 1585 1214">Indices (for example, market feeds).</td> <td data-bbox="1585 1139 1906 1214">Both</td> <td data-bbox="1906 1139 2067 1214">N</td> </tr> <tr> <td data-bbox="786 1214 837 1331">5.</td> <td data-bbox="837 1214 1585 1331">Other personal and non-personal data relating to the organization's business operations as a financial institution.</td> <td data-bbox="1585 1214 1906 1331">Both</td> <td data-bbox="1906 1214 2067 1331">N</td> </tr> <tr> <td data-bbox="786 1331 837 1398">6</td> <td data-bbox="837 1331 1585 1398">[Examples of sensitive information]</td> <td data-bbox="1585 1331 1906 1398"></td> <td data-bbox="1906 1331 2067 1398"></td> </tr> </tbody> </table>				Type of Data	Processed/Stored/Both	Sensitive (Y/N)	1.	Customer data (including customer name, contact details, account information, payment card data, security credentials and communication).	Both	N	2.	Employee data (including employee name, contact details, internal and external communication by email and other means and personal information relating to their employment with the organization).	Both	N	3.	Transaction data (data relating to transactions in which the organization is involved).	Both	N	4.	Indices (for example, market feeds).	Both	N	5.	Other personal and non-personal data relating to the organization's business operations as a financial institution.	Both	N	6	[Examples of sensitive information]		
	Type of Data	Processed/Stored/Both	Sensitive (Y/N)																													
1.	Customer data (including customer name, contact details, account information, payment card data, security credentials and communication).	Both	N																													
2.	Employee data (including employee name, contact details, internal and external communication by email and other means and personal information relating to their employment with the organization).	Both	N																													
3.	Transaction data (data relating to transactions in which the organization is involved).	Both	N																													
4.	Indices (for example, market feeds).	Both	N																													
5.	Other personal and non-personal data relating to the organization's business operations as a financial institution.	Both	N																													
6	[Examples of sensitive information]																															

No.	Question/requirement	Template response and guidance
		<p>Ideology/belief, membership of or withdrawal from labor unions/political parties, political view, information relating to physical condition and sex life, etc., genetic information, criminal records</p>
7.	<p>Please provide the background on why the Company has decided to use the service(s) and the Company's expectations for the service(s). What were the business and operational considerations?</p>	<p><i>Article 7(1) Item 4 of the DPO Regulation, Article 4-4(1) Item 1 of the FIBR</i></p> <p><i>In articulating the business and operational considerations that led to the decision of outsourcing using cloud services, the Company may refer to the following.</i></p> <p>Cloud computing enables on-demand network access to a pool of servers, storage and services. In the case of Microsoft Office 365, Microsoft applications are available. The following specific effects are expected.</p> <p>(1) Efficient operation</p> <p>In case of providing services using the facilities and systems in the data center of the Service Provider, the Company does not have to make additional investment in servers or other facilities, systems, and thus can save operation costs and enable efficient operation.</p> <p>(2) Economy of scale and increased productivity</p> <p>The infrastructure, technical expertise and resources of the Service Provider enables the Company to process massive tasks at a low cost, to use a uniform e-mail system within the group and thereby increase uniformity and efficiency of business performance of the Company's employees/officers.</p> <p>(3) Prompt response to changes in IT environment or technologies</p> <p>By using the specialized technical experts and facilities of the Service Provider, the Company may</p>

No.	Question/requirement	Template response and guidance
		promptly respond to the changes in IT environment and technologies, including constant updates of recent security programs.
8.	Will the Service Provider use data obtained in the course of data processing only for the purpose of the original outsourcing?	<p><i>Article 4(5) of the DPO Regulation, Article 4-4(2) Item 2 of the FIBR</i></p> <p>Yes.</p> <p>Microsoft makes a contractual commitment on this point precisely. According to the Online Services Term (“OST”), Microsoft commits only to use the Company’s data for the purpose of providing cloud services (see page 8 of the OST).</p>
9.	Has the Company been subject to at least two institutional warnings or higher sanctions or criminal punishments within the last three years in connection with matters related to inspections by the supervisory authority related to information management of financial users, submission of data related to supervision and etc.?	<p><i>Article 4(2) Item 2 of the DPO Regulation</i></p> <p><i>The Company’s answer to this question should be “No” in order to outsource data processing to a third party.</i></p>
<b>AUDIT</b>		
10.	Does the Service Provider provide the Company with audit rights?	<p><i>Article 4-4(2) Item 3 of the FIBR, Chapter 3 Section 2.A.4 of the Cloud Guide</i></p> <p>Yes.</p>



No.	Question/requirement	Template response and guidance
		<p>The Company may exercise a number of relevant rights according to the contract with Microsoft.</p> <p>In such contract with Microsoft the Company has the opportunity to participate in the Microsoft Online Services Customer Compliance Program, which is a for-fee program that allows the Company (a) to evaluate the services provided and (b) to review Microsoft's internal control environment {see the Financial Services Amendment ("FSA")}. Specifically, this compliance program allows the Company to (a) assess the services' controls and effectiveness, (b) access data related to service operations, (c) maintain insight into operational risks of the services, (d) be provided with additional notification of changes that may materially impact Microsoft's ability to provide the services, and (e) provide feedback on areas for improvement in the services.</p> <p>The Company has access rights (at any time) to the online dashboards, which provide live information in relation to Microsoft's services' performance against performance measures.</p> <p>Under the contract with Microsoft, Microsoft shall also make its Online Information Security Policy available to the Company, along with other information reasonably requested by the Company regarding Microsoft security practices and policies.</p> <p>In addition, as part of Microsoft's certification requirements, Microsoft is required to undergo regular independent third party auditing and share with the Company copies of the independent third party audit reports (see the FSA, section 2c). Through the audit reports, the Company may enjoy the same effect as if the Company had directly exercised audit rights.</p> <p>Finally, the Company has undertaken a thorough due diligence of Microsoft's relevant processes and procedures in relation to the use of Microsoft Office 365 service. The Company is confident that such arrangements provide the Company with the appropriate level of assessment of Microsoft's ability to meet the Company's policy, procedural, security control and regulatory requirements. These examination and inspection rights has been validated by a variety of regulators across the world, including those in Singapore,</p>

No.	Question/requirement	Template response and guidance
		<p>Australia and Europe as being sufficient to meet the regulatory needs in those markets, and as such, the Company is satisfied our rights above are sufficient to meet its obligations under applicable laws and regulations.</p>
11.	<p>Does the Service Provider provide regulatory bodies with audit rights (e.g. supervision and inspection by the FSS in relation to the data processing service)?</p>	<p><i>Article 8(1) of the DPO Regulation, Article 43(2) of the FSCMA, Article 4-4(2) Item 9 of the FIBR, Chapter 3, Section 2.A.4 of the Cloud Guide</i></p> <p><i>Such rights are indeed included in Microsoft's contractual documents, and this is a key advantage of the Microsoft product over competitor products, which often provide only very limited (or no) audit and inspection rights.</i></p> <p>Yes.</p> <p>There are provisions in the Company's contract with Microsoft that enable regulatory authorities to carry out inspection or examination of Microsoft's facilities, systems, processes and data relating to the services (including copies of Microsoft's audit reports and information about findings of Microsoft's independent third party auditors) (see Section 2a of the FSA).</p>
12.	<p>Has the Service Provider obtained any evaluation/certification of a specialized institution in and out of Korea?</p>	<p><i>Chapter 3, Section 1.B of the Cloud Guide</i></p> <p>Yes.</p> <p>As part of Microsoft's certification requirements, they are required to undergo independent third party auditing and Microsoft shares with the Company the relevant audit reports. These include the SSAE16 SOC1 Type II audit and the ISO/IEC 27001, which also includes details about Microsoft's compliance with ISO/IEC 27018.</p>

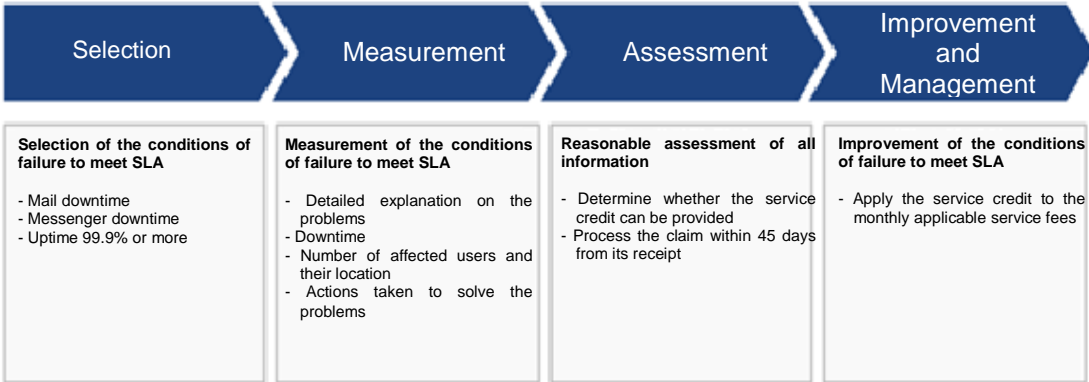
No.	Question/requirement	Template response and guidance
13.	Has the Company obtained comments from a compliance officer or an auditor that the outsourcing contract does not violate any laws or regulations in Korea?	<p><i>Article 7(1)-3 of the DPO Regulation, Article 46(1)-3 of the Enforcement Decree of the FSCMA</i></p> <p><i>The Company should confirm whether the Company has obtained such comments from the compliance officer or the auditor. Please get in touch with the Company's Microsoft contact, if the Company wishes to discuss this requirement.</i></p>
14.	Does the Company have any document that confirms the possibility for the supervisory authority to supervise the operation of data processing by the Service Provider?	<p><i>Article 7(1) Item 6 of the DPO Regulation</i></p> <p><i>It is recommended for the the Company to attach a copy of the Company's contract with Microsoft. The FSA includes provisions which demonstrate that the supervisory authority is able to exercise supervisory rights over the operation of the data processing. Please get in touch with the Company's Microsoft contact, if the supervisory authority requires a written confirmation of acceptance of audit of the outsourcee.</i></p>
<b>RISK ASSESSMENT AND MANAGEMENT</b>		
15.	What measures does the Service Provider take to protect the data?	<p><i>Article 49(2) Item 4 of the Enforcement Decree of the FSCMA and Article 5(1) of the DPO Regulation</i></p> <p>Microsoft is an industry leader in cloud security and implements policies and controls on par with or better than on-premises data centers of even the most sophisticated organizations. Microsoft Office 365 was built based on ISO/IEC 27001 standards, a rigorous set of global standards covering physical, logical, process and management controls.</p> <p>The Microsoft Office 365 security features consist of three parts: (a) built-in security features; (b) security controls; and (c) scalable security. These include 24-hour monitored hardware, isolated customer data, automated operations and lock-box processes, secure networks and encrypted data.</p> <p>Microsoft implements the Microsoft Security Development Lifecycle (“<b>SDL</b>”) which is a comprehensive security process that informs every stage of design, development and deployment of Microsoft software and</p>

No.	Question/requirement	Template response and guidance
		<p>services, including Office 365. Through design requirements, analysis of attack surface and threat modeling, the SDL helps Microsoft predict, identify and mitigate vulnerabilities and threats from before a service is launched through its entire production lifecycle.</p> <p>Networks within the Office 365 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. Client connections to Office 365 use secure sockets layer (“SSL”) for securing Outlook, Outlook Web App, Exchange ActiveSync, POP3, and IMAP. 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”)/SSL. The use of TLS/SSL establishes a highly secure client-to-server connection to help provide data confidentiality and integrity between the customer desktop and the data center. Customers can configure TLS between Office 365 and external servers to protect 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. From a people and internal process standpoint, preventing breach involves auditing all operator/administrator access and actions, zero standing permission for administrators in the service, “Just-In-Time (JET) access and elevation” (that is, elevation is granted on an as-needed and only-at-the-time-of-need basis) for engineer privileges to directly troubleshoot the service, and segregation of the employee email environment from the production access environment. Employees who have not passed background checks are automatically rejected from internal access, and checking employee backgrounds is a highly scrutinized, individual approval process.</p>

No.	Question/requirement	Template response and guidance
		<p>Data is also encrypted. Customer data in Office 365 exists in two states:</p> <ul style="list-style-type: none"> <li>• At rest on storage media</li> <li>• In transit from a data center over a network to a customer device</li> </ul> <p>All email content is encrypted on disk using BitLocker AES encryption. Protection covers all disks on mailbox servers and includes mailbox database files, mailbox transaction log files, search content index files, transport database files, transport transaction log files, and page file OS system disk tracing/message tracking logs.</p> <p>Office 365 also transports and stores secure/multipurpose Internet mail extensions (“<b>S/MIME</b>”) messages. Office 365 will transport and store messages that are encrypted using client-side, third-party encryption solutions such as Pretty Good Privacy (“<b>PGP</b>”).</p>
16.	<p>Has the Company established and applied a set of objective, measurable Service Provider selection criteria? Do they cover all of the following?</p> <ul style="list-style-type: none"> <li>• Security, including response to failure and establishment of a mechanism to respond to breach incidents</li> <li>• Compliance with local laws and regulations by the Service Provider</li> <li>• Applicability of the Company’s</li> </ul>	<p><i>Chapter 3 Section 1.A of the Cloud Guide</i></p> <p><i>Article 7(1) Item 7 of the DPO Regulation</i></p> <p>Yes.</p> <p><b>(1) Security, including response to failure and establishment of a mechanism to respond to breach incidents</b></p> <ul style="list-style-type: none"> <li>- The copies which can be used for data recovery are maintained at least once a week, and the process for recovery is recorded and managed.</li> <li>- In case of failure, the person-in-charge resolves it and carries out recovery according to the documented process.</li> </ul> <p>(In the recovery process, the description of the restored data and where applicable, the person</p>

No.	Question/requirement	Template response and guidance
	<p>internal control process to the cloud</p> <ul style="list-style-type: none"> <li>• Compatibility with the Company's existing data protection systems and security solutions</li> <li>• Compatibility with other clouds so as not to solely depend on a certain cloud provider</li> <li>• Reliability of the Service Provider, including its financial structure, profits and credit ratings, etc.</li> <li>• Other selection criteria that the Company has established</li> </ul>	<p>responsible, and which data had to be input manually in the data recovery process are recorded.)</p> <ul style="list-style-type: none"> <li>- Data recovery procedures are reviewed at least every six months to prevent recurrence of similar interruptions.</li> <li>- Replication and proper separation of the cloud assets are performed so that any failure of a single system does not damage availability of the entire cloud. That is, copies of customer data and data recovery procedures are stored in a different place from where the primary computer equipment processing the customer data is located.</li> <li>- Microsoft performs the process of Incident Response whereby, in case where any breach incident is detected during Microsoft's own operation, the development team and the security team intervene and exactly examine whether any incident occurred, and Breach Response process whereby the incident is notified to the customers by identifying its impact on the customers and the impacted parts after confirming that the incident occurred.</li> </ul> <p><b>(2) Compliance with local laws and regulations by the Service Provider</b></p> <p>MBSA section 11m and the OST state that Microsoft and the customer each commit to comply with all applicable privacy and data protection laws and regulations.</p> <p><b>(3) Reliability of the Service Provider, including its financial structure, profits and credit ratings, etc.</b></p> <ul style="list-style-type: none"> <li>- <b>Financial strength of the Service Provider (i.e., assessment of the past 3 years audited financial statements and other relevant information).</b> Microsoft Corporation is publicly-listed in the United States and is amongst the world's largest companies by market capitalization. Microsoft's audited financial statements indicate that it has been profitable for each of the past three years. Its market capitalization is in the region of USD 280 billion. Accordingly, the Company has no concerns regarding its financial strength.</li> </ul>

No.	Question/requirement	Template response and guidance
		<ul style="list-style-type: none"> <li>- <b>Competence and experience of the Service Provider.</b> Microsoft is an industry leader in cloud computing. Office 365 was built based on ISO/IEC 27001 standards and was the first major business productivity public cloud service to have implemented the rigorous set of global standards covering physical, logical, process and management controls. Microsoft also commits to comply with ISO/IEC 27018, an international standard for personal data stored in the cloud.</li> <li>- <b>Past track-record.</b> 40% of the world's top brands use Office 365. Some case studies are available on the <a href="#">Microsoft website</a>. Financial institution customers in leading markets, including in the UK, France, Germany, Australia, Hong Kong, Canada, the United States and many other countries have performed their due diligence and, working with their regulators, confirmed that Office 365 meets their respective regulatory requirements.</li> </ul>
17.	<p>Does the company establish and implement procedures covering the following items to assess and manage the level of the services of the Service Provider?</p> <ul style="list-style-type: none"> <li>• Designation of the person in charge of assessment and management of the service level and his/her roles and responsibilities by the financial institution and the Service Provider</li> <li>• Cycle of the service level assessment of the Service Provider</li> <li>• Process of report on the assessment results of the Service Provider</li> </ul>	<p><i>Chapter 5 Section 1.B of the Cloud Guide</i></p> <p>Any failure to meet the service level (SLA 99.9%) is compensated with the service credit.</p> <p>The service level (monthly uptime percentage) is calculated as follows.</p> <p><b>Monthly Uptime Percentage</b></p> $\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$ <p>*Service credit: the percentage of the applicable monthly service fees credited to the customers following Microsoft's claim approval</p>

No.	Question/requirement	Template response and guidance
	<ul style="list-style-type: none"> <li>Process of follow-up measures of the Service Provider according to the assessment results, including establishment of cloud improvement plans and report of implementation results</li> </ul>	 <p>The diagram illustrates a four-step process flow for handling SLA failures:</p> <ul style="list-style-type: none"> <li><b>Selection:</b> Selection of the conditions of failure to meet SLA. <ul style="list-style-type: none"> <li>- Mail downtime</li> <li>- Messenger downtime</li> <li>- Uptime 99.9% or more</li> </ul> </li> <li><b>Measurement:</b> Measurement of the conditions of failure to meet SLA. <ul style="list-style-type: none"> <li>- Detailed explanation on the problems</li> <li>- Downtime</li> <li>- Number of affected users and their location</li> <li>- Actions taken to solve the problems</li> </ul> </li> <li><b>Assessment:</b> Reasonable assessment of all information. <ul style="list-style-type: none"> <li>- Determine whether the service credit can be provided</li> <li>- Process the claim within 45 days from its receipt</li> </ul> </li> <li><b>Improvement and Management:</b> Improvement of the conditions of failure to meet SLA. <ul style="list-style-type: none"> <li>- Apply the service credit to the monthly applicable service fees</li> </ul> </li> </ul> <p>In case of a failure to meet the SLA, (i) detailed explanation on the problems, (ii) information of downtime and its period, (iii) the number of affected users and their location, and (iv) explanation on the measures taken to solve the problems when they occurred, etc. are submitted to Microsoft customer center.</p> <p>Microsoft reasonably assesses all the information provided and determines in good faith whether the service credit can be provided, and then applies the service credit to the monthly applicable service fees, if it determines that the service credit can be provided.</p>
<b>VENDOR MANAGEMENT AND MONITORING</b>		
<b>TRANSFER AND CONVERSION PLANS</b>		
18.	Has the Company established and implemented the plans on the scope of	<i>Chapter 3 Section 3.A.1 of the Cloud Guide</i>



No.	Question/requirement	Template response and guidance
	transfer/conversion, including the list of assets to be transferred / converted, for a transfer or conversion to the Service Provider's cloud?	<p><i>Please supplement the answer according to the Company's internal circumstances.</i></p> <p>[Example] The data included in the e-mail service and messenger service currently in use are to be transferred/converted. Specifically, the scope of transfer/conversion mainly includes e-mail data, e-mail archiving history, and messenger archiving history.</p>
19.	Has the Company established and implemented the transfer/conversion plans on the impact on business, including system performance, capacity, and security threats?	<p><i>Chapter 3 Section 3.A.2 of the Cloud Guide</i></p> <p><i>Please supplement the answer according to the Company's internal circumstances.</i></p>
20.	Has the Company established and implemented the transfer/conversion plans on the connection with the business systems within the financial company?	<p><i>Chapter 3 Section 3.A.3 of the Cloud Guide</i></p> <p><i>Please supplement the answer according to the Company's internal circumstances.</i></p> <p>[Example] As only the mail and messenger services are outsourced without any connection with the existing internal systems, there will be no particular connection with the internal business systems.</p>
21.	Has the Company established and implemented the plans on business continuity according to transfer/conversion?	<p><i>Chapter 3 Section 3.A.4 of the Cloud Guide</i></p> <p><i>Please supplement the answer according to the Company's internal circumstances.</i></p> <p>[Example] For business continuity, the plans/projects on the transfer of data between the current service operation environment and the new service operation environment are required, and the entire business continuity is guaranteed with the current service operator, the new service operator, and the previous project</p>

No.	Question/requirement	Template response and guidance
		performer guaranteeing their business continuity, respectively.
22.	Has the Company established and implemented the plans for analysis on the problems which may arise in each stage of transfer/conversion and the measures to preventive such problems?	<p><i>Chapter 3 Section 3.A.5 of the Cloud Guide</i></p> <p><i>Please supplement the answer according to the Company's internal circumstances.</i></p> <p>[Example] The Company will request the companies performing transfer/conversion projects for a comprehensive analysis of the problems and diagnosis of preventive measures with the support of the current Service Provider and the new Service Provider.</p>
<p><b>IT SECURITY</b></p> <ul style="list-style-type: none"> <li>- <b>PROTECTION OF SENSITIVE/CONFIDENTIAL INFORMATION</b></li> <li>- <b>CONNETION WITH INTERNAL SYSTEMS OF FINANCIAL INSTITUTIONS</b></li> </ul>		
23.	Does the Company separate, block and prohibit access of external institutions' communication network using the same cloud from the non-material data processing system located in the external network of the Service Provider?	<p><i>Chapter 4 Section 2.A of the Cloud Guide</i></p> <p><i>This answer may need to be be amended depending on the specific version that the Company is using. Please refer to the following text if using Office 365 multi-tenanted version:</i></p> <p>Office 365 is a multi-tenant service (that is, multiple customers receiving cloud computing services share the same hardware resources), but it is designed to host multiple tenants in a highly secure way through data isolation. Data storage and processing for each tenant is segregated through Active Directory structure and capabilities specifically developed to help build, manage, and secure multi-tenant environments. Active Directory performs data segregation using security boundaries (also known as silos). This safeguards a customer's data so that the data cannot be accessed or compromised by co-tenants using the same hardware</p>

No.	Question/requirement	Template response and guidance
		<p>resources.</p> <p><i>Please refer to the following text if using Office 365 dedicated version:</i></p> <p>The Company is using a dedicated hosted offering, which means that the Company's data is hosted on hardware dedicated to us.</p>
24.	<p>Does the Company separate, block and prohibit access of, the external communication networks, including the Internet, and the external institutions' communication network using the same cloud from the non-material data processing system located in the internal network of the Service Provider?</p>	<p><i>Chapter 4 Section 2.B of the Cloud Guide</i></p> <p>As Office 365 will be located in the external network of the Service Provider, this question is not applicable.</p>
25.	<p>In case of connecting the Company's business-related terminal units and the data processing system located in the internal network with the internal network of the Service Provider or connecting the Company's management-related terminal units with the Service Provider's cloud, does the Company comply with the rules of the data protection controls alternative</p>	<p><i>Chapter 4 Section 2.C of the Cloud Guide</i></p> <p>In case of Office 365, as the Company's business-related terminal units or the data processing system located in the internal network is not connected with the Service Provider's internal network, this question is not applicable.</p>

No.	Question/requirement	Template response and guidance
	<p>of network separation in &lt;Attachment 7&gt; of the Detailed Enforcement Rules of the EFSR?</p> <p>Also, does the Company use a dedicated line or a virtual dedicated line (e.g., VPN) with the same level of security as a dedicated line for the above connection?</p>	
26.	<p>In case of connecting the Company's business-related terminal units and the data processing system located in the internal network with the external network of the Service Provider, does the Company comply with the rules of the data protection controls alternative of network separation in &lt;Attachment 7&gt; of the Detailed Enforcement Rules of the EFSR?</p>	<p><i>Chapter 4 Section 2.D of the Cloud Guide</i></p> <p>Please demonstrate applicable rules on the data protection controls alternative of network separation of the Company. If you need help from the Service provider, please get in touch with the Company's Microsoft contact.</p>
27.	<p>Does the Company use encrypted telecommunication channels when the Company has to connect the Company's terminal units and data</p>	<p><i>Chapter 4, Section 2.E of the Cloud Guide</i></p> <p>Client connections to Office 365 use secure sockets layer ("SSL") for securing Outlook, Outlook Web App, Exchange ActiveSync, POP3, and IMAP. The Company's (customer) access to services provided over the</p>

No.	Question/requirement	Template response and guidance									
	processing system with the Service Provider's external network?	Internet originates from users' Internet-enabled locations and ends at a Microsoft data center. The Company's (client) connections to the Internet are encrypted using industry-standard transport layer security ("TLS")/SSL. The use of TLS/SSL establishes a highly secure client-to-server connection to help provide data confidentiality and integrity between the desktop and the data center. The Company (customers) can configure TLS between Office 365 and external servers to protect both inbound and outbound email. This feature is enabled by default.									
<b>- DATA CENTER PHYSICAL &amp; ENVIRONMENTAL CONTROLS</b>											
28.	Where are the data center(s) of the Service Provider located? Indicate the data center(s) in which the Company's organization's data would be stored and/or processed.	<p><i>Article 7(1)-7 of the DPO Regulation</i></p> <p>Microsoft informs us that it takes a regional approach to hosting of Office 365 data. Microsoft is transparent in relation to the location of the Company's data. Microsoft data center locations are made public on the Microsoft Trust Center (<a href="https://www.microsoft.com/ko-kr/trustcenter">https://www.microsoft.com/ko-kr/trustcenter</a>).</p> <p><i>The table below would need to be amended depending on the specific solution that the Company is using.</i></p> <table border="1" data-bbox="757 946 2063 1230"> <thead> <tr> <th data-bbox="757 946 801 1018">#</th> <th data-bbox="801 946 1417 1018">Locations of Data Centre</th> <th data-bbox="1417 946 2063 1018">Storing the Company's organization's data (Y/N)</th> </tr> </thead> <tbody> <tr> <td data-bbox="757 1018 801 1126">1.</td> <td data-bbox="801 1018 1417 1126"></td> <td data-bbox="1417 1018 2063 1126"></td> </tr> <tr> <td data-bbox="757 1126 801 1230">2.</td> <td data-bbox="801 1126 1417 1230"></td> <td data-bbox="1417 1126 2063 1230"></td> </tr> </tbody> </table>	#	Locations of Data Centre	Storing the Company's organization's data (Y/N)	1.			2.		
#	Locations of Data Centre	Storing the Company's organization's data (Y/N)									
1.											
2.											
<b>- USER AUTHENTICATION &amp; ACCESS MANAGEMENT</b>											
29.	Does the Service Provider implement access control policies for the	<i>Article 4(3) of the DPO Regulation, Chapter 5, Section 2.A. ① of the Cloud Guide</i>									

No.	Question/requirement	Template response and guidance
	outsourced data?	<p>Yes.</p> <p>Microsoft applies strict controls over which personnel roles and personnel will be granted access to customer data. Personnel access to the IT systems that store customer data is strictly controlled via ① role-based access control (“<b>RBAC</b>”) and ② lock box processes that involve not only approvals from within Microsoft but also explicit approval from the customer. 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 requirements, such as a background screen, fingerprinting, required security training and access approvals. In addition, the access rights are reviewed on a periodic basis to ensure that only users who have appropriate business justification have access to the systems. User access to data is also limited by user role. For example, system administrators are not provided with database administrative access. In emergency situations, a “Just-In-Time (JET) access and elevation system” is used (that is, elevation is granted on an as-needed and only-at-the-time-of-need basis) for engineer privileges to troubleshoot the service.</p>
<b>ASSET MANAGEMENT</b>		
30.	Does the Service Provider detect unauthorized changes of the cloud assets and record and retain history of the assets?	<p><i>Chapter 5 Section 2.A. ② of the Cloud Guide</i></p> <p>All of the cloud assets are registered and managed, and the assets can be accessed only by the personnel authorized to access after completing the relevant process. Unauthorized personnel are not allowed to access by physical controls and multiple access authentications.</p>
31.	Does the Service Provider verify security and compatibility in case of changing the cloud assets?	<p><i>Chapter 5 Section 2.A. ③ of the Cloud Guide</i></p> <p>By satisfying ISO27001 standards and NIST Special Publication 800-88, the Service Provider detects unauthorized changes through the regular monitoring management tool, records and retains history of the</p>

No.	Question/requirement	Template response and guidance
		assets, and discards them in a safe manner in terms of security.
32.	Does the Service Provider perform maintenance to ensure availability and integrity of the cloud assets?	<p><i>Chapter 5 Section 2.A. ④ of the Cloud Guide</i></p> <p>The dedicated team of Microsoft Cloud Infrastructure and Operations (MCIO) automates and monitors asset-related management thereby ensuring security, compatibility, availability, and integrity.</p>
33.	Does the Service Provider prevent, detect, and respond to, malware and immediately provide a patch for security vulnerability?	<p><i>Chapter 5 Section 2.A. ⑤ of the Cloud Guide</i></p> <p>Vulnerability reports, including our operation system and partner solutions, are collected on a monthly basis, and security updates are provided based thereon, and thus, security vulnerability is rapidly minimized.</p>
<b>IT SERVICE AVAILABILITY, DATA BACKUP AND DISASTER RECOVERY</b>		
34.	Does the Company have a disaster recovery or business continuity plan and regularly assess the appropriateness of it? Does the Company prepare/implement troubleshooting or disaster recovery process, including backup and establishment of an emergency communication network? Does the Company perform replication and proper separation of the cloud assets so that any failure of a single system does not damage availability of the	<p><i>Article 4-4(2) Item 6 of the FIBR, Chapter 5 Sections 3.A and 3.B. ① of the Cloud Guide</i></p> <p>Yes.</p> <p>Microsoft offers ① physical redundancy at disk, NIC, power supply and server levels, ② constant content replication, ③ robust backup, restoration and failover capabilities, ④ 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, ⑤ 24/7 on-call engineering teams, and ⑥ contractually-guaranteed 99.9% uptime, hosted out of world class data centers. Microsoft's disaster recovery and business continuity plans cover the following points:</p> <p><u>Redundancy</u></p>

No.	Question/requirement	Template response and guidance
	<p>entire cloud? Does the Company establish and implement the measures to prevent recurrence of failure so as not to repeat similar failure?</p>	<ul style="list-style-type: none"> <li>• Physical redundancy at server, data center, and service levels</li> <li>• Data redundancy with robust failover capabilities</li> <li>• Functional redundancy with offline functionality</li> </ul> <p><b><u>Resiliency</u></b></p> <ul style="list-style-type: none"> <li>• Active load balancing</li> <li>• Automated failover with human backup</li> <li>• Recovery testing across failure domains</li> </ul> <p><i>Chapter 5 Sections 3.A and 3.B.④ of the Cloud Guide</i></p> <p><b><u>Distributed Services</u></b></p> <ul style="list-style-type: none"> <li>• Distributed component services like Exchange Online, SharePoint Online, and Lync Online limit scope and impact of any failures in a component</li> <li>• Directory data replicated across component services insulates one service from another in any failure events</li> <li>• Simplified operations and deployment</li> </ul> <p><b><u>Monitoring</u></b></p>



No.	Question/requirement	Template response and guidance
		<ul style="list-style-type: none"> <li>• Internal monitoring built to drive automatic recovery</li> <li>• Outside-in monitoring raises alerts about incidents</li> <li>• Extensive diagnostics provide logging, auditing, and granular tracing</li> </ul> <p><b><u>Simplification</u></b></p> <ul style="list-style-type: none"> <li>• Standardized hardware reduces issue isolation complexities</li> <li>• Automated deployment models</li> <li>• Standard built-in management mechanism</li> </ul> <p><b><u>Human backup</u></b></p> <ul style="list-style-type: none"> <li>• Automated recovery actions with 24/7 on-call support</li> <li>• Team with diverse skills on the call provides rapid response and resolution</li> <li>• Continuous improvement by learning from the on-call teams</li> </ul> <p><i>Chapter 5 Sections 3.A and 3.B.③ of the Cloud Guide</i></p> <p><b><u>Continuous learning</u></b></p> <ul style="list-style-type: none"> <li>• If an incident occurs, Microsoft does a thorough post-incident review every time</li> <li>• Microsoft's post-incident review consists of analysis of what happened, Microsoft's response, and</li> </ul>

No.	Question/requirement	Template response and guidance
		<p>Microsoft’s plan to prevent it in the future</p> <ul style="list-style-type: none"> <li>In the event the customer was affected by an incident, Microsoft shares the post-incident review with the customer</li> </ul>
35.	What are the recovery time objectives (“RTO”) of systems or applications outsourced to the Service Provider?	<p><i>Chapter 5 Section 3.B. ② of the Cloud Guide</i></p> <p>1 hour or less for Microsoft Exchange Online, 6 hours or less for SharePoint Online.</p>
36.	How frequently does the Service Provider conduct disaster recovery tests?	<p><i>Chapter 5 Section 3.A of the Cloud Guide</i></p> <p>At least once per year.</p>
37.	Does the Service Provider establish and implement breach incident response procedures, including a report process in the event of a breach incident and an incident resolution process, etc.?	<p><i>Chapter 5 Section 3.C. ① of the Cloud Guide</i></p> <p>Yes.</p> <p>Microsoft performs (1) the process of Incident Response whereby, in case where any breach incident is detected, the development team and the security team intervene and exactly examine whether any incident occurred, and (2) Breach Response process whereby the incident is notified to the customers by identifying its impact on the customers and the impacted parts after confirming that the incident occurred.</p> <p>Microsoft maintains security breach records along with the details, period, and results of a breach, name of the reporter, the person-in-charge who received a report of breach, and description of the data recovery process, and notifies the customers of any security violation which constitutes a security incident as set forth in the provisions of the “security incident notification.”</p>

No.	Question/requirement	Template response and guidance
38.	In the event of a breach incident, does the Service Provider promptly deal with the incident and perform recovery?	<p><i>Chapter 5 Section 3.C.② of the Cloud Guide</i></p> <p>In case of failure, the person-in-charge resolves such failure and carries out recovery according to the documented process. In the recovery process, the description of the restored data and where applicable, the person responsible, and which data had to be input manually in the data recovery process are recorded.</p>
<b>EXIT STRATEGY</b>		
39.	In the event of contract termination with the Service Provider, either on expiry or prematurely, is the Company able to have all IT information and assets promptly returned, removed or destroyed and procure a written confirmation of destruction?	<p><i>Chapter 6 Sections 1.A, 1.B, and 1.C of the Cloud Guide</i></p> <p>Yes.</p> <p>Microsoft uses best practice procedures and a wiping solution that is NIST 800-88 compliant. For hard drives that can't 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 utilize approved media storage and disposal management services. Paper documents are destroyed by approved means at the pre-determined end-of-life cycle.</p> <p>"Secure disposal or re-use of equipment and disposal of media" is covered under the ISO/IEC 27001 standard against which Microsoft is certified.</p> <p>Microsoft can provide a written confirmation that our data have been destroyed according to the relevant contract.</p>
40.	Is the Company able to demand the Service Provider to actively cooperate in	<p><i>Chapter 6 Section 1.D of the Cloud Guide</i></p>

No.	Question/requirement	Template response and guidance
	conversion and termination of the cloud?	The customer can access or extract its customer data stored in each online service at all times during its regular subscription period. Microsoft retains customer data in a limited function account for 90 days after expiration or termination of the term of the contract.
41.	Is the Company able to demand the Service Provider to carry out mock training for the cloud conversion and termination process upon consultation?	<p><i>Chapter 6 Section 1.E of the Cloud Guide</i></p> <p><i>Please get in touch with the Company's Microsoft contact if the Company wishes to discuss this requirement.</i></p>

## APPENDIX ONE

### MANDATORY CONTRACTUAL REQUIREMENTS

This table sets out the specific items that must be covered in the financial institution's agreement with the Service Provider.

Most of the requirements are also found in the Checklist in Section 8 (above) but the specific items are extracted separately in this appendix.

#### Key:

Where relevant, a cross-reference is included in *red italic* to the underlying regulation that sets out the contractual requirement.

In *blue text*, Microsoft has provided the Company with a reference to where in the agreement the contractual requirement is covered for ease of reference.

Terms used below as follows:

**OST** = *Online Services Terms*

**EA** = *Enterprise Agreement*

**Enrolment** = *Enterprise Enrolment*

**FSA** = *Financial Services Amendment*

**MBSA** = *Microsoft Business and Services Agreement*

**PUR** = *Product Use Rights*

**SLA** = *Online Services Service Level Agreement*

No.	Requirement	Microsoft Agreement reference
1.	Does the outsourcing agreement have provisions to address the scope of the outsourcing arrangement (scope of provision of the cloud)?	<p><i>Chapter 3 Section 2.A.1 of the Cloud Guide</i></p> <p>Microsoft's contractual documents comprehensively set out the scope of the outsourcing arrangement and the respective commitments of the parties. The services are broadly described, along with the applicable usage rights, in the Product List and OST. The services are described in more detail in the OST, which includes a list of service functionality and core features of the Office 365 services in particular.</p> <p>The SLA contains Microsoft's service level commitment, as well as the remedies for the customer in the event that Microsoft does not meet the commitment. The terms of the SLA current at the start of the applicable term of the Enrollment (or the renewal term, if the Enrollment is renewed) are fixed for the duration of that term.</p> <p>Please find a copy of the OST at:  <a href="http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&amp;DocumentTypeId=46">http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&amp;DocumentTypeId=46</a></p> <p>Please find a copy of the SLA at:  <a href="http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&amp;DocumentTypeId=37">http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&amp;DocumentTypeId=37</a></p>
2.	Does the outsourcing agreement have provisions to address security requirements necessary for performance of the outsourced services, operational, internal control and other risk management?	<p><i>Chapter 3 Section 2.A.10 of the Cloud Guide</i></p> <p>All of these aspects of the outsourced services are covered in the OST and the SLA. The OST contains the privacy and security practices and internal controls that Microsoft implements, and the SLA contains Microsoft's service level commitment, as well as the remedies for the customer in the event that Microsoft does not meet the commitment. The terms of the SLA are fixed for the period from the effective date to the termination of the Enrollment (except when it is renewed).</p>

No.	Requirement	Microsoft Agreement reference
3.	Does the outsourcing agreement have provisions to address roles and responsibilities (including mutual joint and several responsibilities) for data protection and confidentiality according to the provision of the cloud?	<p><i>Chapter 3, Section 2.A.3 of the Cloud Guide</i></p> <p><i>Article 4(7) of the DPO Regulation</i></p> <p><i>Article 42(2) of the FSCMA, Article 46(2) Item 3 of the Enforcement Decree of the FSCMA, and Article 4-4(2) Item 5 of the FIBR</i></p> <p><i>Customer information should be used by the Service Provider and its staff strictly for the purpose of the contracted service. For this, (i) access to customer data is limited to employees of the Service Provider who strictly require the information to perform their duties; (ii) customer data is used strictly for a specified and disclosed purpose; and (iii) further disclosure of customer data to any other party is restricted unless required by law.</i></p> <p>MBSA section 3 deals with confidentiality. Under this section Microsoft commits not to disclose the Company(customer)'s confidential information (which includes the Company's data) to third parties and to only use the customer's confidential information for the purposes of Microsoft's business relationship with the customer. Further, Microsoft commits to take reasonable steps to protect the customer's confidential information, to notify the customer if there is any unauthorized use or disclosure of the customer's confidential information and to cooperate with the customer to help to regain control of the Company's confidential information and prevent further unauthorized use or disclosure of it.</p> <p>MBSA section 11m and the OST state that Microsoft and the customer each commit to comply with all applicable privacy and data protection laws and regulations.</p> <p>The customer owns its data that is stored on Microsoft cloud services at all times. The customer also retains the ability to access its customer data at all times, and Microsoft will deal with customer data in accordance with the terms and conditions of the Enrollment and the OST. Following termination,</p>

No.	Requirement	Microsoft Agreement reference
		<p>Microsoft will (unless otherwise directed by the customer) delete the customer data after a 90-day retention period (see OST, page 5).</p> <p>Microsoft makes specific commitments with respect to safeguarding customer data in the OST. In summary, Microsoft commits that:</p> <ol style="list-style-type: none"><li>1. Ownership of customer data remains at all times with the customer (see OST, page 8).</li><li>2. Customer data will only be used to provide the online services to the Company and the Company's data will not be used for any other purposes, including for advertising or other commercial purposes.</li><li>3. Microsoft will not disclose customer data to supervisory authorities unless it is legally obliged to do so, and only after not being able to redirect the supervisory authority's request for disclosure from Microsoft to the customer (see OST, page 8).</li><li>4. Microsoft will implement and maintain appropriate technical and organizational measures, internal controls, and information security routines intended to protect customer data against accidental, unauthorized or unlawful access, disclosure, alteration, loss, or destruction. Technical support personnel are only permitted to have access to customer information when needed (for detailed information, see OST, pages 8 and 11 through 13).</li><li>5. Microsoft will notify the customer if it becomes aware of any security incident, and will take reasonable steps to mitigate the effects and minimize the damage resulting from the security incident (see OST, page 9).</li></ol> <p><i>Regarding the obligation of the party liable for the relevant losses in the event of a breach of security or confidentiality and the Service Provider to inform the relevant authorities.</i></p>



No.	Requirement	Microsoft Agreement reference
		<p>The OST states the responsibilities of the contracting parties that ensure the effectiveness of security policies. To the extent that a security incident results from Microsoft's failure to comply with its contractual obligations, and subject to the applicable limitations of liability, Microsoft reimburses the customer for ① reasonable and third-party validated, out-of-pocket costs the customer incurred in connection with the security incident, including actual costs of court- or governmental body-imposed payments, fines or penalties for a Microsoft-caused security incident and ② additional, commercially-reasonable, out-of-pocket expenses the customer incurred to manage or remedy the Microsoft-caused security incident (FSA, Section 3). Applicable limitation of liability provisions can be found in the MBSA.</p> <p>MBSA section 6 deals with liability. MBSA section 5 expressly sets out Microsoft's obligation to defend the customer against third party infringement and breach of confidence. Subject to the terms of the MBSA, Microsoft's liability under section 5 is unlimited.</p>
4.	Does the outsourcing agreement have provisions to address management and supervision over the outsourcee?	<p><i>Article 42(2) of the FSCMA, Article 46(2) Item 3 of the Enforcement Decree of the FSCMA, Article 4-4(2) Item 3 of the FIBR, Chapter 3 Section 2.A.4 or 2.A.5 of the Cloud Guide</i></p> <p>(1) Third-Party Audit Report</p> <p>The customer has the ability to access and extract customer data under the OST. The OST specifies the audit and monitoring mechanisms that Microsoft puts in place in order to verify that the online services are provided in accordance with the appropriate security and compliance standards.</p> <p>(2) Compliance Program</p> <p>The FSA further gives financial institution customers, i.e. us, the opportunity to participate in the Microsoft Customer Compliance Program. This program allows the customer to engage with Microsoft during the term of the outsourcing contract and have oversight rights over the services in</p>

No.	Requirement	Microsoft Agreement reference
		<p>order to ensure compliance with the customer’s legal and regulatory obligations. Specifically, it enables the customer to have additional monitoring, supervisory and audit rights and additional controls over Office 365, such as (a) access to Microsoft personnel for raising questions and escalations relating to Office 365, (b) invitation to participate in a webcast hosted by Microsoft to discuss audit results and subsequent access to detailed information regarding planned remediation of any deficiencies identified by the audit, (c) receipt of communication from Microsoft on ① the nature, common causes, and resolutions of security incidents and other circumstances that can reasonably be expected to have a material service impact on the customer’s use of Office 365, ② Microsoft’s risk-threat evaluations, and ③ significant changes to Microsoft’s business resumption and contingency plans or other circumstances that might have a serious impact on the customer’s use of Office 365, (d) access to a summary report of the results of Microsoft’s third party penetration testing against Office 365 (e.g. evidence of data isolation among tenants in the multi-tenanted services), and (e) access to Microsoft’s subject matter experts through group events such as webcasts or in-person meetings (including an annual summit event) where roadmaps of planned developments or reports of significant events will be discussed and the customer will have a chance to provide structured feedback and/or suggestions regarding the financial service institution Customer Compliance Program and its desired future evolution. The group events will also give the customer the opportunity to discuss common issues with other regulated financial institutions and raise them with Microsoft.</p>
5.	Does the agreement cover legal requirements and policy compliance regarding data protection?	<p><i>Chapter Section 2.A.5 of the Cloud Guide</i></p> <p>Yes.</p> <p>MBSA section 11m and the OST state that Microsoft and the customer each commit to comply with all applicable privacy and data protection laws and regulations.</p>

No.	Requirement	Microsoft Agreement reference													
		<p>In addition, under section 2a of the FSA, Microsoft and the customer commit to consult with each other in good faith to comply with any requests from a supervisory authority.</p>													
6.	<p>Did the Company discuss with the Service Provider the following service levels considering the Company's internal regulations and system characteristics, etc. so as not to cause any disturbance to the smooth performance of business while using the cloud? (If necessary, possible to be reflected in the SLA)</p> <ul style="list-style-type: none"> <li>- Cloud availability, including the ratio of the hours of operating the cloud without failure to the available time of the cloud required by the Company</li> <li>- Cloud continuity, including the number of cases of failure, average time of failure, and the time required to resolve failure</li> <li>- Cloud performance, including average response time, the number of cases of exceeding maximum response time, and the maximum number of the concurrently connected users</li> <li>- Data backup and recovery, including backup cycle, backup compliance rate, recovery time for backup data, and retention period of backup data</li> </ul>	<p><i>Chapter 5 Section 1.A of the Cloud Guide</i></p> <p>Yes.</p> <p>All of these aspects of service levels, performance targets, service availability, reliability, stability and upgrade are covered in the SLA. The SLA contains Microsoft's service level commitment, as well as the remedies for the customer in the event that Microsoft does not meet the commitment. The terms of the SLA current at the start of the applicable term of the Enrollment (or the renewal term, if the Enrollment is renewed) are fixed for the duration of that term. Please find a copy of the SLA at:</p> <p><a href="http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&amp;DocumentTypeId=37">http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&amp;DocumentTypeId=37</a></p> <p>Cloud availability</p> <p>In case of mail (Exchange Online), 99.9% of uptime is guaranteed, and, if the monthly uptime percentage is less than 99.9%, it is compensated with the service credit (the percentage of the applicable monthly service fees credited to the customers following Microsoft's claim approval). For more information, please refer to the SLA.</p> <p>Cloud continuity/performance: The global uptime percentage of Office 365 is as follows:</p> <table border="1" data-bbox="837 1254 2060 1409"> <thead> <tr> <th data-bbox="837 1254 1008 1331">2014</th> <th colspan="3" data-bbox="1008 1254 1711 1331">2015</th> <th colspan="2" data-bbox="1711 1254 2060 1331">2016</th> </tr> </thead> <tbody> <tr> <td data-bbox="837 1331 1008 1409">99.99%</td> <td data-bbox="1008 1331 1182 1409">99.99%</td> <td data-bbox="1182 1331 1357 1409">99.95%</td> <td data-bbox="1357 1331 1532 1409">99.98%</td> <td data-bbox="1532 1331 1711 1409">99.98%</td> <td data-bbox="1711 1331 1886 1409">99.98%</td> <td data-bbox="1886 1331 2060 1409">99.98%</td> </tr> </tbody> </table>	2014	2015			2016		99.99%	99.99%	99.95%	99.98%	99.98%	99.98%	99.98%
2014	2015			2016											
99.99%	99.99%	99.95%	99.98%	99.98%	99.98%	99.98%									

No.	Requirement	Microsoft Agreement reference						
	<ul style="list-style-type: none"> <li>- Security management, including the number of breach incident, the number of security violations, and breach detection rate</li> <li>- User support, including average time required to process user requests, user request processing rate, and frequency of user education</li> </ul>	Q4	Q1	Q2	Q3	Q4	Q1	Q2
		<p><a href="#">Data recovery process</a></p> <ul style="list-style-type: none"> <li>- Multiple copies of customer data which can be used for customer data recovery are maintained at least once a week, and copies of customer data and data recovery procedures are stored in a different place from where the primary computer equipment processing the customer data is located. Also, the procedures applicable to the access to the customer data copies are continuously managed, and the data recovery procedures are reviewed at least every six months.</li> </ul> <p><a href="#">Security management</a></p> <p>The operator is regularly provided with analysis of the current situation and checkup of the usual response status by the external institution with respect to the situations regarding security threats and submits a report (e.g., End of Year Security Report and Penetration Test Summary).</p> <p><a href="#">User support</a></p> <p>Any inquiry or request regarding failure can be directly made on the administrator's page or by telephone (only by the administrator, 24X7 available).</p> <p>Requests can be made 24X7. However, the response time depends on their seriousness, as the response is provided for significantly serious requests within one hour, and for highly serious requests, by the next day. Also, for the requests which are not highly serious, the response time is not guaranteed.</p>						

No.	Requirement	Microsoft Agreement reference
		<p>As for education, online education is basically provided through the web at all times, and in-person education is provided as necessary (e.g., annually) through a separate agreement.</p>
7.	<p>Has the Company included in the outsourcing contracts the matters concerning the obligation to accept the request for submission of materials regarding the concerned outside order and inspection made by the Company or the financial authorities to the Service Provider?</p>	<p><i>Articles 7(1) Item 6 and 8(1) of the DPO Regulation, and Chapter 3 Section 2.A.4 of the Cloud Guide</i></p> <p><i>Article 42(2) of the FSCMA, Article 46(2) Item 3 of the Enforcement Decree of the FSCMA, and Article 4-4 Item 9 of the FIBR</i></p> <p>Yes.</p> <p>The OST specifies the audit and monitoring mechanisms that Microsoft puts in place in order to verify that the online services meet appropriate security and compliance standards. This commitment is reiterated in the FSA as a standard offering to regulated financial institutions. Under the FSA, Microsoft gives the customer a right to examine, monitor and audit its provision of Office 365. Specifically, Microsoft (i) makes available to the customer the written Office 365 data security policy that complies with certain control standards and frameworks, along with descriptions of the security controls in place for Office 365 and other information that the customer reasonably request regarding Microsoft's security practices and policies; and (ii) causes the performance of audits, on the customer's behalf, of the security of the computers, computing environment and physical data centers that it uses to process the customer's data (including personal data) for Office 365, and provides the audit report to the customer upon request. These arrangements are offered to the Company in order to provide the Company with the appropriate level of assessment of Microsoft's ability to facilitate compliance against the Company's policy, procedural, security control and regulatory requirements. Please refer to the optional financial institution Customer Compliance Program for opportunities to gain further visibility and influence into Microsoft's practices.</p> <p>The FSA further describes that if the customer request, Microsoft will provide the supervisory authorities</p>

No.	Requirement	Microsoft Agreement reference
		<p>a direct right to conduct an examination of Microsoft locations; to examine the relevant service; to interview Microsoft personnel and Microsoft's external auditors; and to access related information, records, reports and documents. Microsoft will not disclose customer data to the supervisory authorities except as described in the OST. Customer will at all times have access to its data using the standard features of Office 365, and may delegate its access to its data to representatives of the supervisory authorities (see FSA, Section 2a).</p> <p>Section 2a of the FSA details the examination and influence rights that are granted to the customer and the regulator. The process can culminate in the regulator's examination of Microsoft's services, records, reports and premises. This examination and inspection right has been validated by a variety of regulators across the world, including those in Singapore, Australia and Europe as being sufficient to meet the regulatory needs in those markets, and as such, the Company is satisfied the rights the Company has agreed are sufficient to meet the Company's regulatory obligations.</p> <p>In addition, under section 2a of the FSA, Microsoft and the customer commit to consult with each other in good faith to comply with any requests from a supervisory authority.</p>
8.	<p>Does the Company establish and implement procedures covering the following items to assess and manage the level of the services of the Service Provider?</p> <ul style="list-style-type: none"> <li>• Designation of the person in charge of assessment and management of the service level of the Company and the Service Provider, and his/her roles and responsibilities</li> </ul>	<p><i>Chapter 5, Section 1.B of the Cloud Guide</i></p> <p>Yes.</p> <p>The SLA contains the performance measures.</p> <p>The SLA evaluation and management is performed according to the following procedures:</p> <p><u>In case of a failure to meet the SLA</u>, (i) detailed explanation on the problems, (ii) information of downtime and its period, (iii) the number of affected users and their location, and (iv) explanation on the measures taken to solve the problems when they occurred, etc. are submitted to Microsoft customer</p>

No.	Requirement	Microsoft Agreement reference				
	<ul style="list-style-type: none"> <li>• Cycle of the service level assessment of the Service Provider</li> <li>• Process of report of the assessment results of the Service Provider</li> <li>• Process of follow-up measures of the Service Provider according to the assessment results, including establishment of service improvement plans and report of implementation results</li> </ul>	<p><u>center.</u></p> <p>Microsoft reasonably assesses all the information provided and determines in good faith whether the service credit can be provided, and then <u>applies the service credit to the monthly applicable service fees, if it determines that the service credit can be provided.</u></p> <div data-bbox="837 638 2000 1136" data-label="Diagram"> <pre> graph LR     A[Selection] --&gt; B[Measurement]     B --&gt; C[Assessment]     C --&gt; D[Improvement and Management]   </pre> <table border="1"> <tr> <td data-bbox="882 820 1144 1082"> <b>Selection of the conditions of failure to meet SLA</b>            - Mail downtime            - Messenger downtime            - Uptime 99.9% or more         </td> <td data-bbox="1151 820 1413 1082"> <b>Measurement of the conditions of failure to meet SLA</b>            - Detailed explanation on the problems            - Downtime            - Number of affected users and their location            - Actions taken to solve the problems         </td> <td data-bbox="1420 820 1682 1082"> <b>Reasonable assessment of all information</b>            - Determine whether the service credit can be provided            - Process the claim within 45 days from its receipt         </td> <td data-bbox="1688 820 1951 1082"> <b>Improvement of the conditions of failure to meet SLA</b>            - Apply the service credit to the monthly applicable service fees         </td> </tr> </table> </div> <p>The OST specifies the audit and monitoring mechanisms that Microsoft puts in place in order to verify that the online services meet appropriate security and compliance standards. This commitment is reiterated in the FSA.</p> <p>In addition, the FSA gives the customer the opportunity to participate in the Microsoft Online Services Customer Compliance Program, which is a for-fee program that facilitates the customer's ability to (a)</p>	<b>Selection of the conditions of failure to meet SLA</b> - Mail downtime - Messenger downtime - Uptime 99.9% or more	<b>Measurement of the conditions of failure to meet SLA</b> - Detailed explanation on the problems - Downtime - Number of affected users and their location - Actions taken to solve the problems	<b>Reasonable assessment of all information</b> - Determine whether the service credit can be provided - Process the claim within 45 days from its receipt	<b>Improvement of the conditions of failure to meet SLA</b> - Apply the service credit to the monthly applicable service fees
<b>Selection of the conditions of failure to meet SLA</b> - Mail downtime - Messenger downtime - Uptime 99.9% or more	<b>Measurement of the conditions of failure to meet SLA</b> - Detailed explanation on the problems - Downtime - Number of affected users and their location - Actions taken to solve the problems	<b>Reasonable assessment of all information</b> - Determine whether the service credit can be provided - Process the claim within 45 days from its receipt	<b>Improvement of the conditions of failure to meet SLA</b> - Apply the service credit to the monthly applicable service fees			

No.	Requirement	Microsoft Agreement reference
		<p>assess the services' controls and effectiveness, (b) access data related to service operations, (c) maintain insight into operational risks of the services, (d) be provided with additional notification of changes that may materially impact Microsoft's ability to provide the services, and (e) provide feedback on areas for improvement in the services. Under this program, customers can raise issues directly and immediately with Microsoft where corrective measures are required.</p>
9.	<p>Does the agreement cover sub-contracting (i.e. restrictions on sub-contracting and clauses governing confidentiality of data)?</p>	<p><i>Article 4(4) of the DPO Regulation, Chapter 3 Section 2.A.7 of the Cloud Guide</i></p> <p><i>Article 42(2) of the FSCMA, Article 46(2) Item 3 of the Enforcement Decree of the FSCMA, and Article 4-4 Item 10 of the FIBR</i></p> <p>Yes.</p> <p>See page 9 of the OST for selection of subcontractors by Microsoft.</p> <p>The confidentiality of the customer's data is protected when Microsoft uses subcontractors because 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" (OST, page 9).</p> <p>Microsoft commits to have its subcontractors enter into written agreements with Microsoft that are no less protective than the data processing terms in the OST (OST, page 11).</p> <p>Under the terms of the OST, Microsoft remains contractually responsible (and therefore liable) for its subcontractors' compliance with Microsoft's obligations in the OST (OST, page 9).</p> <p>Finally, Microsoft maintains a list of authorized subcontractors that have access to the Company's data through the online services that the Company uses and provides us with a mechanism to obtain the list</p>



No.	Requirement	Microsoft Agreement reference
		<p>and notice of any updates to that list (OST, page 10). The actual list is published on the applicable Trust Center (<a href="https://www.microsoft.com/ko-kr/trustcenter">https://www.microsoft.com/ko-kr/trustcenter</a>). If the Company has any objection to the subcontractor that is added to the list, then the Company is entitled to terminate the affected online services.</p>
10.	<p>Does the agreement cover emergency plans including the security of the back-up system in order to secure the continuance of the business?</p>	<p><i>Article 42(2) of the FSCMA, Article 46(2) Item 3 of the Enforcement Decree of the FSCMA, and Article 4-4 Item 6 of the FIBR, Chapter 3 Section 2.A.10 of the Cloud Guide</i></p> <p>Yes.</p> <p>Business Continuity Management forms part of the scope of the accreditation that Microsoft retains in relation to the online services, and Microsoft contractually commits to maintain a data security policy that complies with these accreditations (see OST, page 13). Business Continuity Management also forms part of the scope of Microsoft's annual third party audit. Microsoft offers contractually-guaranteed 99.9% uptime.</p>
11.	<p>Does the agreement cover termination of the agreement?</p>	<p><i>Chapter 3 Section 2.A.8 of the Cloud Guide</i></p> <p><i>Article 42(2) of the FSCMA, Article 46(2) Item 2 of the Enforcement Decree of the FSCMA</i></p> <p>Yes.</p> <p>The contract allows us to terminate the arrangement with Microsoft for convenience (MBSA section 8) by providing 60 calendar days prior written notice.</p> <p>This means in effect the Company has the right to terminate as long as the Company provides 60 days prior notice, even in the event of default including change of ownership, insolvency or where there is a breach of security or confidentiality or demonstrable deterioration in the ability of the Service Provider to</p>

No.	Requirement	Microsoft Agreement reference
		<p>perform the service as contracted.</p> <p>The Company may also terminate the contract if Microsoft is in material breach or default of any obligation that is not cured within 30 calendar days' notice of such breach (MBSA section 8).</p> <p>It is also worth noting that the Company at all times has control over the data the Company loads into the online service. In addition, termination rights for the Enrollment are set out in the Enrollment itself, and in section 6 of the EA. If the Enrollment is terminated, this will terminate all products and services ordered under the Enrollment (except to the extent that the Company has perpetual rights).</p>
12.	Does the agreement cover the Company's ownership, copyright, and intellectual property right to the data generated while using the cloud?	<p><i>Chapter 3 Section 2.A.2 of the Cloud Guide</i></p> <p><i>Article 42(2) of the FSCMA, Article 46(2) Item 3 of the Enforcement Decree of the FSCMA, Article 4-4 Item 4 of the FIBR</i></p> <p>Yes.</p> <p>Ownership of Customer Data remains at all times with us (see OST, page 8).</p> <p>The customer's data will only be used to provide the online services to us and the Company's data will not be used for any other purposes, including for advertising or other commercial purposes (see OST, page 8).</p> <p>Finally, the customer retains the ability to access the customer's data at all times (OST, page 11).</p>
13.	Does the agreement include the matters concerning secure destruction and return of the data in case of conversion or termination of the	<p><i>Chapter 3 Section 2.A.9 of the Cloud Guide</i></p>

No.	Requirement	Microsoft Agreement reference
	cloud?	<p>Yes.</p> <p>Microsoft commits to retain the Company's data stored in the Online Service for 90 days after expiration or termination of the term so that the Company may extract the data (other functions of the Company's account are restricted). After the 90 day retention period ends, Microsoft will disable the Company's account and delete the Company's data (OST, page 5).</p>
14.	Does the agreement contain provisions regarding indemnity, insurance, and dispute resolution methods (arbitration or mediation, etc.)?	<p><i>Article 42(2) of the FSCMA, Article 46(2) Item 3 of the Enforcement Decree of the FSCMA, Article 4-4 Item 7 of the FIBR</i></p> <p>Yes.</p> <p>MBSA section 6 deals with liability. MBSA section 5 expressly sets out Microsoft's obligation to defend the customer against third party infringement and breach of confidence. Subject to the terms of the MBSA, Microsoft's liability under section 5 is unlimited.</p> <p>Microsoft will maintain industry-appropriate insurance coverage at all times. Microsoft will provide Customer with evidence of its coverage on request.</p> <p>The MBSA covers dispute resolution process (Section 10.e.), warranties (Section 5), defense of third party claims (Section 6), limitation of liability (Section 7), and term and termination (Section 9). It further offers country-specific provisions determined by applicable law (Section 11).</p> <p>A customer that has elected to participate in the Microsoft Online Services Customer Compliance under the OST may raise issues with Microsoft through this program.</p> <p>MBSA section 11e sets out the jurisdictions in which parties should bring their actions. Microsoft must bring actions against the customer in the country where the contracting party is headquartered. The</p>

No.	Requirement	Microsoft Agreement reference
		customer must bring actions against Microsoft: (a) in Ireland courts if the action is against a Microsoft affiliate in Europe; or (b) in the U.S. Washington State courts if the action is against a Microsoft affiliate outside of Europe.
15.	Does the agreement include provisions for damage compensation?	<p><i>Chapter 3 Section 2.A.8 of the Cloud Guide</i></p> <p>To the extent that a security incident results from Microsoft's failure to comply with its contractual obligations, and subject to the applicable limitations of liability, Microsoft reimburses the customer for ① reasonable and third-party validated, out-of-pocket costs the customer incurred in connection with the security incident, including actual costs of court- or governmental body-imposed payments, fines or penalties for a Microsoft-caused security incident and ② additional, commercially-reasonable, out-of-pocket expenses the customer incurred to manage or remedy the Microsoft-caused security incident (FSA, Section 3). Applicable limitation of liability provisions can be found in the MBSA.</p>
16.	Does the agreement contain provisions for providing information, including the country where the Company's data are stored?	<p><i>Chapter 3 Section 2.A.6 of the Cloud Guide</i></p> <p>The OST contains provisions for the regions where the data are stored, which are also available at Trust Center (<a href="https://www.microsoft.com/ko-kr/trustcenter">https://www.microsoft.com/ko-kr/trustcenter</a>).</p>
17.	<p><b><u>[For financial investment business entities]</u></b></p> <p>Does the agreement contain provisions for limitation of liability of the Service Provider, which is the outsourcee?</p>	<p><i>Article 42(2) of the FSCMA, Article 46(2)-3 of the Enforcement Decree of the FSCMA, Article 4-4, Item 8 of the FIBR</i></p> <p>Yes, MBSA section 6 deals with limitation of liability.</p>
18.	<p><b><u>[For financial investment business entities]</u></b></p> <p>Does the agreement contain provisions for</p>	<p><i>Article 42(2) of the FSCMA, Article 46(2) Item 2 of the Enforcement Decree of the FSCMA</i></p>

No.	Requirement	Microsoft Agreement reference
	outsourcing fees, etc. of the Service Provider?	Yes, the relevant provisions are contained within agreement executed with Microsoft.