1 June 2022

To:
Electronic Finance Division
Korea Financial Services Commission

RE: ASIFMA response to Draft Amendment to the Regulation on Supervision of Electronic Finance

Dear,

At the outset, ASIFMA is grateful to continue the engagement with the Korea Financial Services Commission (FSC) on regulatory developments pertaining to the use of public cloud in Korea. Specifically, we welcome the opportunity to share our thoughts on the Partial Amendment to the Regulation on Supervision of Electronic Finance.

We applaud the intention to rationalize cloud computing services usage by financial institutions in Korea, and we support the measured and risk-based approach, calibrating the requirements for non-important versus important tasks using cloud computing.

Please find below some detailed feedback and suggestions on some of the amended provisions in the draft Partial Amendment to the Regulation on Supervision of Electronic Finance.

Our suggestions aim to support the regulatory intent for rationalization and simplification, and we very much hope that our feedback will be positively considered and reflected in the final Amendments.

We hope you find the below feedback useful and that this will be reflected in the final Amendments. We would welcome the opportunity for further engagement and remain at your disposal for any further questions you might have. Do not hesitate to reach out to us at lvanderloo@asifma.org or Tel: +65 6622 5972 / M: +65 8514 8215.

Sincerely,

Laurence Van der Loo

Executive Director, Technology & Operations

Asia Securities Industry & Financial Markets Association

Proposed text changes	ASIFMA Comments
Article 14-2 (Procedures for Use, etc. of Cloud Computing Services) (1) Financial companies or electronic financial business operators intending to use cloud computing services under Article 2, subparagraph 3 of the Act on the Development of Cloud Computing and Protection of Its Users shall perform each of the following: 1. Evaluation of the importance of tasks using cloud computing under each of the following standards: d. Risk of subjection to a cloud computing service provider if multiple tasks are outsourced to the same cloud computing service provider; e. Financial companies or electronic financial business operators' ability to internally control the use of cloud computing services and comply with the relevant laws and regulations;	• Having a holistic view of the overall number and nature of engagements with a particular cloud provider is a useful element of an FI's management of third-party risk and a potential decision to outsource. But this is just one of a larger set of considerations that feed into these decisions. Dependence on an individual provider is information that should be taken into consideration but should not in itself be a barrier to the adoption of cloud services. A financial institution should use this information to weigh the costs and benefits of alternative solutions, for example in the use of a different cloud provider, and if those alternatives still align with the institution's business and resilience needs. • Even in light of the criteria for evaluating the importance of tasks in the guidelines used in other major countries, stipulating "subordination risk" as a separate and independent statutory evaluation criterion restricts financial companies' autonomy in cloud computing service usage in some aspects. • Typical examples of benefits that financial companies may enjoy from outsourcing various tasks to a single CSP are (i) enhanced safety when connecting its work system with that of the CSP, (ii) easier internal control such as maintaining confidentiality and managing the outsourced provider, (iii) securing business continuity, (iv) cost reduction, and (v) enhanced security levels through continuous and systematic investment on infrastructures. - Despite these benefits, stipulating "subordination risk" as an independent statutory evaluation criterion may only result in financial companies diversifying their CSPs in a

	way that in fact reduces the overall benefit. For instance, financial companies could enter into agreements with many CSPs merely to avoid strict CSP assessment, business continuity plan and procedures for taking safety measures (without considering the downside of doing so). • As such, we submit that clause d. is not a suitable dimension to assess the importance or criticality of an outsourced service or task and should be removed from the evaluation standards set out in this amendment. • Other more relevant aspects include, among others: data classification, whether the service supports core banking processes, and whether the service carries major financial, operational, strategic, legal and/or regulatory risk to the firm, and/or the firm's customers. • Similarly, item Art. 14-2(1)1.e does not seem like an appropriate input or consideration in determining whether an outsourced task/service is important/critical. Due diligence performed by firms on CSPs serve as part of risk assessment but it does not determine if a task is critical. • As explained in Proposed ASIFMA Principles for Public Cloud Regulation[1], when it comes to potential systemic risks arising from the concentration of third-party services (including cloud services), there must be differentiation between sector-wide concentration risk (where multiple regulated entities use the same CSP) and internal dependency concentration risk (where a financial institution is dependent on a single CSP). We recognize that it is the responsibility

[1] ASIFMA (2021): https://www.asifma.org/wp-content/uploads/2021/03/final-proposed-asifma-principles-for-public-cloud-regulation-1.pdf

	of each regulated entity to address concentration risk arising from the reliance of certain service providers by that regulated entity and understand this is the risk covered by item Art. 14-2(1)1.d. Regulated entities generally already perform their own concentration risk assessments as part of their ongoing risk management process for outsourcing arrangements. Based on these assessments, the regulated entity may, if necessary, under a risk-based approach, take action to address such concentration risks (e.g. increasing the control and security expectation on the service provider or using two or more regional or global providers for a given service). • For sector-wide concentration risk, we believe that assessment of concentration risk in the sector should be done by authorities in close partnership with the financial services industry. For risks of this nature, authorities (e.g., supervisory bodies) are well positioned to have oversight at an industry level, as compared to FIs individually due to lack of visibility of which CSPs are used by other FIs. We believe, however, that any such assessment should not restrict the choice of outsourcing arrangements or providers available to FIs.
Article 14-2 (Procedures for Use, etc. of Cloud Computing Services) (4) Financial companies or electronic financial business operators shall file a report with the Governor of the FSS within three (3) months from occurrence of any of the following matters, with the reason(s) therefor, relevant materials and response plans attached thereto 1. Where a new cloud computing services agreement is executed;	• We welcome the following: announcement in the 15 April FSC Press release (I, g) : (PROBLEM) Currently, financial companies are required to report to the Financial Supervisory Service when they need to use cloud computing for essential work seven business days prior to the day of the use. However, this reporting rule has been identified as undesirable for the purpose of timeliness.

2. Where there is a material change such as merger, split-off, transfer of contractual status, or subcontracting of the cloud computing service provider; 3. (Same as the current subparagraph 2); 4. Where a material change occurs regarding subparagraph 2 or subparagraph 3 of Paragraph (1).	(SOLUTION) This prior reporting rule will be changed to an ex post facto reporting requirement for using cloud computing. When signing an outsourcing contract for using cloud computing service for essential types of work or when a significant change takes place in their existing contracts, financial companies will be required to report that change within three months from the signing or change taking place. • We note however that under the current regulations, non-material cloud computing arrangements do not have be reported to the FSC. Only material cloud computing currently requires a prior report. However, under the revised regulations as currently drafted, all cloud computing services (both material and non-material) would require an ex-post facto report to the FSC. We submit that under the revised Under the revised Amendments, we submit that only an ex-post report for material cloud services will need to be submitted. This would be in line with the FSC' intention to rationalize the rules and the risk-based approach which differentiates between material and non-material cloud services.
Article 14.2 (1) 2. Assessment of the soundness, safety, etc. of cloud computing service providers (provided, however, that for any tasks classified as non-important tasks through the evaluation under subparagraph 1, only mandatory assessment items among those set forth in <Exhibit 2-2> may be assessed);	• We welcome the fact that global firms could leverage results and evidence from firmwide assessment for completion of FSC/FSS submissions. • Indeed, it is common for a global FI to leverage headquarters' cloud arrangements, and we encourage FSC to recognize the risk assessment performed by the FI at the group level to meet with FSC requirements on risk assessment. Such recognition will not only relieve Korean entities from repetitive and non-value-added work but is also important

	to provide a consistent risk view from FI's perspective to the FSS.
Article 14.2 (4) Financial companies or electronic financial business operators shall file a report with the Governor of the FSS within three (3) months from occurrence of any of the following matters, with the reason(s) therefor, relevant materials and response plans attached thereto. 1. Where a new cloud computing services agreement is executed; 2. Where there is a material change such as merger, split-off, transfer of contractual status, or subcontracting of the cloud computing service provider; 3. (Same as the current subparagraph 2) 4. Where a material change occurs regarding subparagraph 2 or subparagraph 3 of Paragraph (1).	• We would like to confirm with FSS that the Article 14 (4) 1 means "where a new cloud computing service arrangement is executed at platform level". We submit that notifications should be on a platform (critical systems/infrastructure) basis rather than based on specific applications (e.g., SaaS applications, deployments to IaaS environments). Regulators in Singapore, Japan, Australia, Thailand, Philippines, UK, and US already adopt such platform-based approach. We appreciate that platform approval is currently granted by FSC on an ad hoc, bilateral basis to certain firms. We suggest and hope that the FSC will adopt platform-based approval and notification for all financial institutions and clarify this in the final Regulation on Supervision of Electronic Finance. • Also, the current wording which focuses on the cloud computing services agreement may lead to confusion as contractual agreements are usually updated for various reasons without necessarily involving new engagements or arrangements. For example, firms update a contract after some years to reflect the updated regulatory expectations. Reporting on those contractual updates and execution of a slightly different version of contract may overwhelm FSC without focusing on the risks.
Article 14-2 (8) Article 11, subparagraphs 11 and 12 and Article 15, Paragraph (1), subparagraph 5 shall not apply to a computer room where the data processing system of a cloud computing service provider who has completed the procedures set forth in Paragraph (1) is located; provided, however, that Article 11, subparagraph	• During ASIFMA's engagement with FSC and FSS, we have highlighted the importance of cross-border data flow to enable firms to leverage their global cloud. • Free movement of data across border is key to roll out global cloud migration

12 shall apply where a financial company or electronic financial business operator (excluding Korean branches of foreign financial companies that do not have a material effect on the safety and reliability of electronic financial transactions, and payment gateway service providers for overseas cybermalls as set forth in Article 50-2) processes unique identification information or personal credit information through cloud computing services, and such data processing system shall be located within Korea.	projects. Global FIs typically consolidate their systems in a single global hub, which offers services to the rest of the firm. In contrast, data localization policies require discrete technological builds in specific jurisdictions, further segregate local systems from global hubs. This exposes FIs to greater cybersecurity risks by creating a more decentralized environment that needs to be safeguarded, which further inhibits central oversight and information sharing across borders. In addition, local processing will negatively impact FIs' global operation, their ability to undertake activities at a global level and cross-border service offering. For example, Financial Stability Board (FSB) started to examine the impact of data framework, including data localization, on cross-border payments to support the G20's priority workstream for faster, cheaper, more transparent, and more inclusive cross-border payment services that are safe and secure. • We have seen positive developments on data connectivity for the financial services industry such as the Monetary Authority of Singapore's Data Connectivity initiatives with the US Treasury, the Bangko Sentral ng Pilipinas (BSP) and the Swiss State Secretariat for International Finance (SIF)[2]. Those Data Connectivity initiatives recognize the importance of cross-border data connectivity in financial services in economic growth and the development of innovative financial services, risk

[2] MAS-UST Joint Statement on Data Connectivity: https://www.mas.gov.sg/news/media-releases/2020/united-states-singapore-joint-statement-on-financial-services-data-connectivity
MAS-BSP Joint Statement on Data Connectivity: https://www.mas.gov.sg/news/media-releases/2020/joint-statement-of-intent-on-data-connectivity-between-bsp-and-mas
MAS-SIF Joint Statement of Intent on Data Connectivity: https://www.mas.gov.sg/news/media-releases/2022/joint-statement-of-intent-between-the-monetary-authority-of-singapore-and-the-swiss-state-secretariat-for-international-finance-to-promote-data-connectivity-for-financial-services

	management and compliance programs. Conversely, data localization requirements may increase cybersecurity risks and other operational risks, hinder risk management and compliance, and inhibit financial regulatory and supervisory access to data. It "enables data flows (including personal information) within financial groups or with business partners, across borders by electronic means provided this activity is for the conduct of the business within the scope of their license, authorization, or registration; and supports the free choice of location for the storage and processing of data as long as financial regulators or supervisors have appropriate access to data necessary to fulfill their regulatory or supervisory mandate[3]". • The industry stands ready to engage with the FSC and FSS on this issue and support the introduction of such initiatives.
Article 15 (1) 3. Separating, blocking and/or prohibiting the internal work system connected with the internal communication network from the Internet (including wireless communication network) and other external communication networks;	• The FSC has previously mentioned in its press release that it will allow firms to use SaaS application in an internal company network for non-essential types of work. However, this exception was not covered in the draft Amendment and we suggest this exemption is included in the final Amendment or ask the FSC to clarify how this exemption for non-essential work will be provided. • This article requires separation from the internet. We are unclear how to execute this requirement this in a cloud environment which is by definition accessible over the internet.
General comment: Some requirements may be overly prescriptive:	• The key objective of these proposed amendments is to "improve regulations

[3] https://www.mas.gov.sg/news/media-releases/2022/joint-statement-of-intent-between-the-monetary-authority-of-singapore-and-the-swiss-state-secretariat-for-international-finance-to-promote-data-connectivity-for-financial-services

	on the use of cloud computing and network separation to promote digital innovation in the financial industry". However, some of the proposed amendments, especially Exhibits 2-4 and 2-5, seem overly prescriptive, and may undermine the intended policy objective.