Financial Services Commission

Press Release

April 15, 2022

FSC Introduces Improvements to Cloud Computing and Network Separation Rules in Financial Sector

The FSC unveiled its plans to improve regulations on cloud computing and network separation in financial sectors on April 14. The financial industry has been raising concerns about difficulties in adopting and using new digital technologies as a result of excessive regulations on cloud computing and network separation. Therefore, in order to support the financial sectors' efforts for digital transformation in a stable manner, the authorities have introduced a set of measures to improve regulations on cloud computing and network separation. On cloud computing, the changes will focus on (a) clarifying the scope (and types) of work that can make use of cloud computing, (b) overhauling the usage process to remove redundancies and similarities and (c) making a transition from the current prior reporting requirement to ex post facto reporting. On network separation, the uniform application of the network separation rules will be eased in stages starting with the development and test servers.

Background

The acceleration of digital transformation in financial services has been pushing up demand for new digital technologies such as cloud computing, big data analytics and artificial intelligence (AI). However, there have been continuous complaints from the industry that the current regulations on data security in the financial sector regarding cloud computing and network separation have been too strict, thereby hindering the adoption and use of new digital technologies. In order to address this issue, after taking into account various opinions from the financial industry,[1] the FSC has prepared the measures for improving regulations on the use of cloud computing and network separation to promote digital innovation in the financial industry.

Overview of Current Regulation on Cloud Computing and Network Separation

I. Regulation on Cloud Computing

(Usage Status) The financial sector has thus far been using cloud computing[2] for back office (non-essential types of work) purposes including for internal email and messaging systems and for customer services including marketing. More recently, however, the use of cloud computing for data analysis, system management and online and mobile banking has been increasing for front office functions (essential types of work).

[1] FSC Chairman held talks with the fintech industry and pledged support for financial innovation. Please click here to see the press release dated December 9, 2021.

[2] Instead of building its own network system, cloud computing allows a company to outsource network management to an IT specializing company in a flexible manner according to its own needs.

(USAGE PROCESS) Financial companies are able to make use of cloud computing for their front office functions (or essential types of work) as well as for back office functions (or non-essential types of work). However, financial companies need to carry out the following—(a) assessment on the level of work significance, (b) establishment of a business continuity plan, (c) establishment of safety assurance measures, (d) establishment of supplemental measures for work outsourcing standards and (e) safety assessment on the cloud service provider (CSP)—prior to (f) signing a cloud computing outsourcing contract with a CSP after a deliberation by their own internal data protection committee and (g) report to the Financial Supervisory Service (FSS) prior to using cloud computing service.[3]

(EVALUATION) Due to unclear standards and excessive reporting procedures, however, it has been indicated that there are limits in the current regulatory system for more effectively and flexibly responding to the demand of financial companies. Also, even for non-essential types of work including back office functions, financial companies are currently bound to follow the same level of rules and procedures that need to be observed for carrying out essential types of work.

II. REGULATION ON NETWORK SEPARATION

(BACKGROUND) The network separation rule is a network security measure that requires the maintenance of separate networks between the internal network and the external network for the purpose of protecting internal system resources from external attacks. The methods for network separation include the physical network separation method using two separate computers (hardware) and the logical network separation method based on a single computer (hardware) but which keeps networks separate through virtualization technology using cloud computing.

(REGULATION STATUS) In the aftermath of a large-scale network disruption that took place in the financial sectors in 2013, the government adopted a network separation rule in the financial sector and decided to enforce the physical network separation method. As such, financial companies and electronic financial businesses have been required to physically separate their network system and hardware connected to the internal network from the external network.

(EVALUATION) Since the introduction of the network separation rule, the authorities found that hackings and cyber accidents involving financial network disruptions have declined significantly, providing safe protection for the financial system.[4] However, the uniform application of the physical network separation rule across all financial sectors without making distinctions for disparities between different companies and types of work has been impeding the level of efficiency for the development and testing[5] types of work and posing difficulties in making use of

[3] Ex post facto reporting for non-essential types of work

[4] Even in the face of the 2017 ransomware attack that caused damages worldwide, domestic financial sectors were unharmed.

[5] Development and testing nowadays often take place not in a closed source environment but in an open source environment via the internet.

innovative technologies.[6]

MEASURES FOR IMPROVEMENT

I. REGULATORY IMPROVEMENTS ON THE USE OF CLOUD COMPUTING

a) Clarifying assessment standards for determining the level of work significance for making use of cloud computing service

(PROBLEM) When using cloud computing, an assessment should take place to determine the level of work significance, but it has been indicated that the assessment standards have been rather unclear. Under the current regulation, the level of work significance is determined by the factors such as the handling of personal credit information and whether it has grave impact on the safety and reliability of electronic financial transactions, but there have been difficulties in terms of its applicability in practice.
(SOLUTION) The authorities will prepare a more detailed set of standards for assessing the level of work significance while taking into account examples from overseas.[7] The assessment for the level of work significance will be determined through a deliberation by financial companies' internal data protection committee.

b) Reducing the number of assessment criteria for cloud service providers (CSPs) from 141 to 54 criteria

(PROBLEM) Financial companies are required to conduct a soundness and stability assessment on the cloud service provider prior to using a cloud computing service. The current assessment comprises of too many criteria, up to 141[8] in total with overlapping items, posing the utmost burden on financial companies throughout the whole process.
(SOLUTION) The authorities have made a simplification and reduced the number of CSP assessment criteria down to 54 in total that are made up of 16 essential criteria and 38 alternate criteria. For non-essential types of work, a further simplification is provided with financial companies being required to carry out assessment on CSPs on only the 16 essential criteria.[9]

c) Differentiating the process for cloud computing usage based on the level of work significance

(PROBLEM) Currently, even the types of work that have been classified[10] as back

[6] AI and big data analytics are made available in open source, thus connection to the internet is inevitable.
[7] For instance, the Monetary Authority of Singapore has the following standards for assessing the level of work significance: (a) level of contribution to earnings and profits made by the outsourced work; (b) potential impact of outsourcing on income, payment capability and liquidity; (c) cost resulting from a failure in outsourcing; (d) proportion of outsourcing cost relative to the institution's total operating costs; and (e) impact on customers when contractor suspends its service and a breach of confidential and security matters takes place.
[8] Includes 109 criteria for general protection measures which follow the Ministry of Science and ICT's security certification criteria for cloud computing service and 32 criteria for additional protection measures in the financial sector which evaluate the soundness and additional security items of CSPs.
[9] While easing requirements on CSP assessment, the authorities will ensure accountability of financial companies by requiring them to set up and operate their own internal deliberation committee for data protection.
[10] Via an assessment on the level of work significance

office functions (non-essential types of work) also need to abide by the same usage process as those that have been classified as front office functions (essential types of work). As such, even though financial companies can freely make adjustments on certain criteria for non-essential types of work in their business continuity plans, in practice, the non-essential types of work have been treated in a similar way as the essential types of work.

<Comparison on the current usage process for essential and non-essential types of work>

	Establishment of business continuity plan	Establishment of safety assurance measures	Supplemental measures for outsourcing standards	CSP assessment	Deliberation by data protection committee
Essential types of work	○	○	○	○	○
Non-essential types of work	△	△	△	○	○

* △ indicates assessment items that can be autonomously adjusted by financial companies.

(SOLUTION) The authorities will ease the usage process for making use of cloud computing service for non-essential types of work by lifting some portions of the CSP assessment requirements. The authorities will also introduce separate standards for non-essential types of work when establishing business continuity plans and safety assurance measures in order to make a clear procedural distinction between essential types of work and non-essential types of work.

<Comparison on the current usage process for essential and non-essential types of work>

	Establishment of business continuity plan	Establishment of safety assurance measures	Supplemental measures for outsourcing standards	CSP assessment	Deliberation by data protection committee
Essential types of work	○	○	X	○	○
Non-essential types of work	△	△	X	△[11]	○

* △ indicates assessment items that can be autonomously adjusted by financial companies.

d) Introducing a uniform assessment system on CSPs to reduce burdens on financial companies

(PROBLEM) Currently, when financial companies “A” and “B” wish to use cloud computing service provided by a CSP “a,” financial companies “A” and “B” each have to make an assessment on the CSP “a” separately. The problem of procedural inefficiency has been identified in this regard.
(SOLUTION) A uniform CSP assessment will be carried out by the Financial Security Institute (FSI) representing financial companies, the result of which can be used by financial companies “A” and “B” alike.

e) Drawing up a distinctive set of assessment standards for SaaS

(PROBLEM) The current CSP assessment criteria are not readily fit for assessing Software as a Service (SaaS) applications that have gained more traction for use

[11] With eased standards

recently.[12]

(SOLUTION) The authorities will prepare a separate set of assessment criteria for SaaS businesses in a similar way as the cloud security assurance program (CSAP).

f) Simplifying the paperwork required for submission such as the "work consignment operational standards"

(PROBLEM) In order for financial companies to make use of cloud computing, the industry has made complaints that the paperwork required for submission is redundant and excessive. Currently, the "work consignment operational standards"[13] that financial companies need to submit when using cloud computing are posing burdens as there exists redundancy with the items also reflected in their "business continuity plans."

(SOLUTION) The authorities will simplify the redundancy and similarity to help ease financial companies' burdens of preparing and submitting the necessary paperwork.[14]

g) Making a transition from the current requirement of prior reporting to an ex post facto reporting for the use of cloud computing

(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.

(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.

II. REGULATORY IMPROVEMENTS ON NETWORK SEPARATION

a) Exemption of network separation rules for development and test servers

(PROBLEM) With the uniform application of the physical network separation rule on development and test servers which do not hold personal credit information and thus have relatively lower level of importance in electronic financial transactions, there has been concern about low efficiency for development and test environment.

(SOLUTION) For development and test servers, an exemption will be granted for easing the physical network separation rule. However, supplemental measures will be taken to minimize potential malware attacks and require additional control

[12] The CSP assessment criteria are mostly made up of material requirements as Infrastructure as a Service (IaaS) businesses provide cloud computing services with servers and storage facilities. Therefore, applying the same criteria on SaaS businesses that are not equipped with the infrastructure at an equivalent level would be rather difficult.

[13] Matters related to decisions regarding consignment contracts, monitoring of work being outsourced, emergency plans, reservation of the right to investigate and access work being outsourced as prescribed by the supervisory regulation on electronic financial transactions.

[14] The overlapping items in the "work consignment operational standards" will be integrated into the "business continuity plans," while essential elements such as key details of consignment contracts will be maintained.

measures for data protection.[15]

b) Exemption of network separation rules for non-electronic financial work and SaaS

(PROBLEM) There has been continuous call for the need to ease the network separation rule for the types of work that are not relevant to electronic financial transactions and for the operating systems that do not handle information about customers and their transactions such as information systems that provide support for business management including personnel management and groupware and other related systems. The network separation rule has been a source of inconvenience when using Software as a Service (SaaS) applications even for non-essential types of work.
(SOLUTION) Through the financial regulatory sandbox program, the authorities will grant an exemption for the physical network separation requirement for the types of work that are not relevant to electronic financial transactions and those that do not handle information about customers and their transactions. For non-essential types of work, the authorities will permit the use of SaaS applications in an internal company network.[16]

c) Step-by-step deregulation of network separation over medium to long term

(PROBLEM) Currently, the network separation rule is applied uniformly regardless of the scope of the work of financial companies. For instance, asset management businesses that do not necessarily hold information about their customers but focus solely on managing their assets are subject to the equivalent level of network separation rule as banks even though the need for such regulation is relatively lower for asset management businesses vis-à-vis other financial companies.
(SOLUTION) Over a medium to long term, the authorities will seek deregulation of network separation after reviewing certain conditions such as ensuring accountability from financial companies and strengthening security oversight by the FSI. Deregulatory measures will focus on (a) downsizing the types of work that are subject to the network separation rule and (b) granting financial companies an option to choose network separation in both physical and logical terms.

FURTHER PLAN

The authorities will promptly work to revise the Enforcement Decree of the Electronic Financial Transactions Act and its supervisory regulation with an aim to begin the enforcement of the changed rules starting in 2023.[17] At the same time, the authorities will also prepare a revision to the guideline on the use of cloud computing service in the financial sector to help provide specific procedures and standards for practical reference in the financial sector. Beginning in May 2022, the FSC along with the FSS, FSI and relevant industry groups will operate a joint support team providing authoritative interpretations on the changed rules to facilitate early adaptation to the

[15] e.g. Restriction on the use of customer's personal credit data or ledger data, establishment and implementation of internal standards for accessing and using open source, etc.
[16] For data protection, additional internal control measures will be required through a supplemental condition of the financial regulatory sandbox program.
[17] Expected to be put up for public notice within April.

improved system. The contents of authoritative interpretations will be put together and shared with all financial institutions which will also be reflected in the revised guideline on the use of cloud computing service in the financial sector. Since financial companies' internal control measures on a voluntary basis are crucial for the changed rules to take root in the industry, the authorities will carry out inspections on their internal control mechanisms such as the establishment and operation of an internal data protection deliberation body in the second half of this year.

# # #

For press inquiry, please contact Foreign Media Relations at fsc_media@korea.kr.