OPINION

Hwang, Seiwoon

Network Separation Regulations for Financial Companies: Global Practices and Implications for Korea

Korea's network separation regulation for financial companies was initially introduced to minimize security failures in the financial sector, mandating strict physical network separation for many years. Given the rapid development of the ICT industry and the need for financial companies to stay competitive, a significant shift is required for the network separation regulation. The prevalence of cloud-based Software as a Service (SaaS) and the emergence of generative AI are primarily transforming the financial IT network landscape. Financial companies should embrace these changes to reduce costs and provide innovative services. However, strict physical network separation poses a barrier to their utilization of cloud-based technologies and hinders research and development activities.

In contrast to Korea, network separation regulations in the US and Europe are structured as flexible guidelines rather than prescribed mandates, essentially granting financial companies the discretion to select and implement security measures. This approach is rooted in a trust in self-regulation and the tradition of ex-post regulation that holds these companies strictly accountable for security breaches. Under the guidelines, financial companies are encouraged to apply security controls to both internal and external networks. It should be noted that although network segmentation allows for both physical and logical approaches, few companies rely solely on physical separation.

In the long term, Korea's network separation regulation should evolve to permit financial companies to select their preferred separation methods, while holding them strictly accountable for any security breaches. The utilization of regulatory sandbox programs is an important step in improving network separation rules, and

* All opinions expressed in this paper represent the author's personal views and thus should not be interpreted as Korea Capital Market Institute's official position.

* Ph.D., Senior Research Fellow, Fund & Pension Department, Tel: 82-2-3771-0824, E-mail: neptune@kcmi.re.kr

it is necessary to expand the scope of cloud-based solutions such as generative AI and SaaS. In this context, financial companies should establish an independent security system to safeguard sensitive customer and operational data in the evolving regulatory environment. Moreover, financial regulators should regularly inspect these self-regulated security systems and require these companies to take corrective action for security failures.

In recent years, there has been a growing call for reforming the network separation regulation for financial companies in Korea. This regulation was initially introduced to minimize security incidents within financial computing systems, aiming to safeguard critical consumer information and prevent financial losses. As most financial data are managed through computer systems, unintended incidents or cyberattacks can disrupt financial services or lead to data leakage, resulting in substantial financial damages. Moreover, as economic activities increasingly depend on digital systems, it becomes challenging to predict potential security breaches in the financial sector and the scale of damage from such incidents could be significant. In this regard, the network separation regulation for financial companies should remain in place, while it needs further upgrades and optimization to align with evolving market conditions.

Network separation regulations can be designed in various ways, each with its own strengths and limitations. For this reason, it is difficult to evaluate a specific approach as the most effective, and the optimal approach should be selected based on the current financial market landscape and digital technology development. These regulations should not only protect against financial incidents and safeguard financial consumers but also ensure the efficient development and provision of financial services. Against this backdrop, this article examines the key characteristics of the network separation regulation for financial companies in Korea and explores regulatory improvements to foster a robust financial market. Specifically, it identifies existing issues inherent in the Korean network separation framework, compares Korea's approach with those of other countries, and proposes long-term regulatory improvements for financial companies.

Key characteristics and challenges of the network separation regulation for financial companies in Korea

In Korea, network separation for financial companies is governed by the Electronic Financial Supervisory Regulations. Under these regulations, financial companies or electronic financial service providers are required to separate, block, and restrict access to business operation systems connected to their internal communication networks from external networks, such as the Internet (including wireless networks). The primary goal is to protect data processing systems and information and communication networks from electronic security breaches, such as hacking. Specifically, data processing systems housed in data centers and terminals used directly for system operation, development, and security purposes must be physically isolated from external networks, including the Internet.[1] Although this stringent physical isolation is generally mandated, there are exceptions. For example, if a terminal connected to internal networks needs to communicate with external organizations for essential business purposes, an exemption from physical network separation may be granted. Similarly, data processing systems involved in transmitting data to specific external entities, as well as shared systems utilized by affiliates, may also qualify for such exemptions. However, even in cases where exceptions are granted, financial companies or electronic financial service providers are required to conduct internal risk assessments and implement an alternative data security control instead of network separation, which must be approved by their Data Security Committee.[2]

The current network separation regulation is highly effective in preventing data leakage and external hacking attempts. It also offers cost-saving benefits, as isolating internal data flows reduces the need for comprehensive monitoring across the entire data flow chain.[3] However, it has proven challenging to adapt to changes in the financial market, such as shifts in service delivery models and business operations, under this regulation, which has constantly been criticized for operational inefficiencies.

---

1) Article 15 (Measures to prevent hacking, etc.), Paragraph 1, Subparagraphs 3 and 5 of the Regulation on Supervision of Electronic Financial Transactions.

2) Article 2-2 (Exceptions to network separation) of the Detailed Enforcement Rules of the Regulation on Supervision of Electronic Financial Transactions.

3) Lee, S.H., 2021, Legislative and policy tasks related to digital financial innovation: Focusing on improvements for network separation regulation in the financial sector, NARS Current Issues Analysis No. 202, National Assembly Research Service.

As the introduction of ICT accelerates in the financial services industry, financial companies face an increasing need for rapidly integrating ICT advancements into their services. The most notable trends in the financial market are the transition to cloud-based environments and the rapid growth of AI. Traditionally, financial companies have preferred on-premise software deployment, establishing necessary systems within their own infrastructure. However, it should be noted that the software industry is increasingly shifting from on-premise models to cloud-based Software as a Service (SaaS) solutions. The race to implement generative AI, fueled by Chat GPT, is also reshaping how financial companies deliver services. Going forward, the sustainability of financial companies will depend on their ability to incorporate technological advancements into their business systems quickly and effectively.

As in other industries, the financial sector has seen a steady rise in cloud service adoption. Despite the cost advantages, financial companies have primarily restricted their use of cloud services to simple internal tasks, such as email and internal messaging, or customer service functions. However, there is a growing need for cloud-based software to support critical operations. Financial companies are increasingly utilizing external software not only for non-essential tasks but also for core functions. The demand for cloud services is rising in basic business functions such as customer transaction data analysis, system management, and internet and mobile banking. The adoption of AI, in particular, has played a pivotal role for financial companies seeking to remain competitive. Most generative AI technologies are available in cloud-based internet environments. However, under the current network separation regulation that strictly restricts access to the internet network, financial companies face limitations in integrating generative AI into their core services.

Europe's regulatory approach to network separation for financial companies

Europe provides financial companies with guidelines that outline measures for managing ICT and security risks, while granting them the discretion in selecting specific plans for implementation. In addition to these guidelines, two key regulations that play a critical role in European data security are the General Data Protection Regulation (GDPR) and the Payment Services Directive 2 (PSD2) prepared by the European Banking Authority (EBA).

The General Data Protection Regulation (GDPR) in Europe became enforceable in May 2018 for the protection of the personal data of citizens of member states. It sets out data

security obligations for all companies, including financial companies, and requires any company or organization that handles such personal data to comply with a broad range of privacy regulations. Data controllers or processors subject to the GDPR are required to adopt technical and organizational measures necessary to ensure an adequate level of data protection. These measures include pseudonymization and encryption of personal data, as well as mechanisms for ensuring swift recovery of and access to such data in the event of a physical or technical failure. Additionally, the GDPR mandates that internal control standards be established to safeguard personal information and data, thereby ensuring the compliance of data controllers and processors.[4)]

PSD2 is the revised Payment Services Directive prepared by the European Banking Authority (EBA) and has been in force for EU member states since January 2018. The revision aimed to enhance the competitiveness of Europe's financial services industry by allowing non-bank financial entities to engage in payment services. At the same time, it also seeks to foster a secure financial transaction environment by establishing obligations for payment service providers regarding financial consumer protection. Under PSD2, financial companies offering payment services are required to implement financial security systems. Financial authorities in EU member states are responsible for ensuring that these companies have an adequate level of control to manage security risks. As part of these efforts, payment service providers should categorize types of security incidents and develop incident management procedures, based on effective detection mechanisms for each category.[5)]

The most specific security framework for European financial companies is the EBA Guidelines for ICT and Security Risk Management (EBA Guidelines). These guidelines set out essential considerations for ICT security that financial companies should integrate into their operations in order to address the growing complexity of ICT and security risks and the increasing frequency of security failures. In particular, the guidelines also provide specific directives on measures to control security risks as stipulated under Article 95 of Directive 2015/2366/EU(PSD2). The EBA Guidelines focus on establishing an effective internal control system that clearly assigns responsibilities of financial company management for the oversight and mitigation of ICT and security risks. To achieve this, financial companies are required to develop an ICT strategy aligned with their broader operation strategies. When relying on external or third-party ICT

4) General Data Protection Regulation (GDPR), Chapter 4. Article 32.

5) DIRECTIVE (EU) 2015/2366 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2015, Chapter 5, Article 95.

service providers, financial companies should establish effective risk control measures in the form of legally binding agreements.[6)]

US Regulatory approach to network separation for financial companies

Unlike Korea, where a network separation regulation is directly imposed, the US seeks to promote the effectiveness of isolating internal networks and offer fundamental recommendations for network separation by publishing handbooks. Rather than simply focusing on network separation, US regulations promote a broader concept known as network segmentation. Even for systems handling sensitive customer or transaction data, financial companies in the US are encouraged to segregate networks into different layers rather than rigidly implementing network isolation. This regulatory policy allows financial companies to select the most reasonable solutions for network security.

In the US, the primary regulatory framework for network separation is provided in the Information Technology Examination Handbook, Information Security published by the Federal Financial companies Examination Council (FFIEC).[7)] This handbook serves as a key reference for examiners and financial management management when conducting IT examinations. The Information Security Program Management chapter, specifically Section II.C.9 (Network controls), outlines detailed guidance on network separation. According to Section II.C.9, management should secure access to computer networks through multiple layers of access controls. This involves establishing trusted and untrusted zones and applying access controls between them. These trusted and untrusted zones are designated according to the risk profile and criticality of assets contained within the zones, while appropriate access requirements are imposed within and between each zone. Additionally, financial companies are required to maintain accurate network diagrams and data flow charts and implement appropriate controls over wired and wireless networks.

Trusted networks should be protected through appropriate configuration and patch management, privileged access controls, segregation of duties, implementation of effective security policies, and use of perimeter devices and systems to prevent and detect unauthorized access. Tools must also be in place to enforce and detect perimeter protection, including

6) EBA, 2019, *Guidelines on ICT and Security Risk Management*.

7) FFIEC, 2016, *Information Technology Examination Handbook, Information Security*.

routers, firewalls, intrusion detection systems and intrusion prevention systems, and gateways. Internal zones—typically classified as trusted—should segregate various components into distinct areas, each with the level of controls appropriate to the content and function of the assets within the zone. The trusted zone should be further segmented into distinct layers, and each zone should have a security policy appropriate to the characteristics of assets (risk profile, sensitivity of data, and user roles). In summary, US financial regulators provide only broad principles in the form of the FFIEC handbook, without enforcing any specific restrictions on methodologies. While the handbook outlines network segmentation based on information criticality and the implementation of access controls, it does not impose explicit requirements for physical or logical network separation.

Although it is not a regulatory guideline, the Payment Card Industry Data Security Standard (PCI DSS) also plays a significant role in managing computer security for financial companies.[8)] PCI DSS is a widely recognized information security standard for the credit card industry, aiming to protect the personal information of cardholders. It was first established in 2004 by the PCI Security Standards Council, which consists of major global card companies including VISA, MasterCard, American Express, Discover, and JCB. Since its inception, PCI DSS has been regularly updated, with the latest version, PCI DSS v.4.0.1, released in June 2024 and has been widely adopted by the credit card industry. The standard recommends separating the Cardholder Data Environment (CDE) from other networks within card companies. This segregation could reduce the technical complexity and the cost of complying with PCI DSS. If the card company network operates as a flat network without the appropriate level of segmentation, PCI DSS requirements would apply to the entire network, potentially increasing management costs. Network segmentation can be achieved through a variety of physical or logical methods, and credit card companies can choose the optimal approach that suits their CDE operational needs.

Insights from global practices and regulatory improvements in network separation for Korea's financial companies

An analysis of global cases finds that overseas financial authorities and companies take a more flexible and comprehensive approach to network separation regulations. In the US and

8) Payment Card Industry Security Standard Council, 2024, *Payment Card Industry Data Security Standard, Requirements and Testing Procedures*.

Europe, regulators do not view network separation as a requirement for computer network security, but rather as one of the options for protecting trusted zones (internal networks). This perception also leads to a different approach to network separation. The US and Europe primarily aim to control access within networks, while Korea focuses on isolating internal networks from external ones.

Another characteristic observed in overseas network separation regulations is the discretion granted to financial companies. Despite this flexibility, few financial companies opt for physical network separation. In the US and Europe, financial companies typically implement security controls on internal and external networks according to relevant guidelines. It is notable that network segmentation adopted by these countries allows both physical and logical approaches. Although some companies employ physical separation methods, most of them utilize various methods of logical separation to maintain financial computer network security. It is worth noting that even though physical separation is permitted, few companies rely solely on it. It is even rare to find large financial companies that utilize physical separation exclusively.

Korea can benefit from global network separation frameworks and the strategies employed by global financial companies, highlighting the need for a more rational adjustment to Korea's current regulations. In the long term, the regulatory approach should grant financial companies the flexibility to opt for their network separation methods, while strictly holding them accountable for any security incidents. Notably, the on-premise model increasingly transitions into subscription-based software solutions and cloud services become prevalent. Given these trends, it becomes evident that uniform physical network separation has limitations in developing financial services. As observed in global practices, it is inevitable to allow financial companies to select their own data security methods that align with their security needs, considering that the evolving ICT market is correlated with the changing financial service landscape. Although overseas financial companies are permitted to implement physical network separation with security effects, they rarely choose it. Given that logical network separation is not necessarily less costly than the physical approach, this trend carries crucial implications for Korea's network separation regulation.

When financial companies are granted discretion in selecting their network separation methods, it is crucial to establish a regulatory framework that holds them strictly accountable in the event of security failures. Financial companies are structurally incentivized to underinvest

in information security. As security expenditure can be viewed as a burden by management, especially in the absence of immediate incidents, financial companies with discretion over IT security methods may risk reducing investments in security. Although security breaches within financial entities occur infrequently, their impact can be extensive and severe, affecting a large number of customers. Therefore, it is imperative to impose heavy liability for security breaches and levy substantial fines, preventing financial companies from reducing their security investments and creating a stable security environment. In this light, it is necessary to require them to reinforce internal controls over data security and to enhance organizational construction by imposing significant liability on management for material security failures.

A regulatory shift in network separation should be gradually implemented. Currently, many of Korea's financial companies may lack the capacity to operate an autonomous and flexible data security system. These companies have long relied on physical network separation as their primary security measure. As physical separation provides straightforward security benefits, it has shielded these companies from more complex IT security challenges. Even if various options including logical network separation are permitted, financial companies may experience significant trials and errors without the capabilities to address complex challenges. This, in turn, is likely to expose financial consumers to undue risks. Therefore, it is desirable to adopt regulatory sandbox programs to allow financial companies time to adapt to relaxed regulations on network separation. This will motivate them to build the expertise required for autonomous information security management.