	The Board of Audit and Inspection of Korea	
	Fair Audit **Fair Society**	

Audit on the Current Management and Supervision of Information Protection and Cyber Security in the Financial Sector

Disclosed on 10 April 2014

Background

At present, common activities of most financial businesses, such as accepting deposits and making loans, are carried out through the information communication system. While electronic financial transactions, such as online banking grow each year, cases involving hacking for electronic financial fraud using stolen personal information have evolved into a more sophisticated and upscale form. As a result, confidence in the financial service industries have seriously declined, and the economic damage to the people have also increased, exponentially.

Audit Objectives

The Board of Audit and Inspection (BAI) carried out an inspection on 10 public institutions, including the Financial Services Commission (FSC), in order to detect issues regarding the management and supervision of information protection and cyber security in the financial sector. In addition, the BAI selected a sample of 9 representing financial companies to configure the current state of the security management system in the financial sector.

Audit Findings

A. Evaluation and supervision of information technology in financial companies

1. Inappropriate evaluation methods and evaluation on information technology in financial companies

The Financial Supervisory Service (FSS) prepared regulations on the evaluation of the

IT sector of financial companies with high IT risks or concentrated networks (144 institutions, as of 2012). To better secure the level of security in electronic financial transactions, the regulations provide that an evaluation of the IT sector of those companies should be carried out separately from that of general businesses. However, in practice, the FSS conducted an evaluation on the IT sector, only as a part of its annual review on the overhaul business practices, and did not carry out a separate evaluation specifically focused on the IT sector, itself. Therefore, there are no evaluation records on the IT conditions of 46 financial firms, nor inspection records on the IT sector of 26 financial institutions.

Further, while the FSS is supposed to supervise financial companies for their compliance with the 30 IT security standards stipulated in the Regulations on Supervision of Electronic Financial Transactions, it was found to have failed in fully reflecting the checklist by lacking up to 15 items, including anti-hacking measures.

2. Inappropriate security management of outsourcing companies and operation of relevant regulations

The FSC prepared the standards for financial companies with respect to outsourcing development and operation of the information system.

The aforementioned standards provide that the public sector should run separated development and operation systems, in order to prevent possible information leakage or network paralysis by the personnel of outsourcing businesses. It also requires financial companies to prepare measures for systematic security management of outsourcing partners and comply with them in operation.

However, the current FSC regulations on supervision of electronic financial transactions do not have any provisions for the separation of development and operation systems, nor for the systematic management of external personnel, major data, and facilities. Hence, 5 financial companies subject to inspection were found to have saved their main data in the computers of the outsourcing personnel. Additionally, one financial company was allowing access to its operation system through the development system, resulting in the consumer data being exposed to a high risk of information leakage and arbitrary deletion.

B. Cyber Security Promotion System in the Financial Sector

1. Inadequate knowledge sharing among the institutions in charge of information protection in the financial sector

Currently, the FSC and FSS are operating the “e-Finance Information Sharing and Analysis Center” and the “Electronic Financial Accident Response System”, respectively, for the purpose of responding to any incidents of information infringement in cyber space. Meanwhile, both of the institutions require financial companies to submit their reports on such incidents, redundantly, to each of the aforementioned

systems and did not take any measures against the issues of scaled down or delayed reports.

C. Operation of Electronic Financial Institutions

1. Inappropriate supervision on the security management of mobile applications

With a substantial increase of financial transactions using smart devices, it is necessary to prepare regulations regarding security management of financial institutions in developing and providing mobile applications to counter increased security threats, such as malicious codes. Nonetheless, the FSC has not yet drafted any regulations for this matter. In cooperation with the Korea Internet & Security Agency, the Board discovered that 38 applications among the 72 samples had 54 different vulnerabilities in terms of security.

Recommendations

Accordingly, the BAI notified the FSC of the audit results and recommended the Committee to prepare proper measures to improve the detected issues. The FSC was also requested to pay keener attention to the IT sector of financial companies with heightened supervision.