

[Summary points from Analysis Report on Financial Institutions' computer System Failures]

1. Introduction

In conjunction with advances in IT, financial institutions are becoming increasingly reliant on computer systems, and risks relating to systems have also become more diverse. Furthermore, as the trend toward digitalization has accelerated in recent years, there has been an emergence of new players, such as cryptoasset exchangers that provide financial services, and also the number of system failures in the sector has increased. In connection with such developments, the establishment of IT risk management systems is becoming increasingly important.

Against this backdrop, we performed an analysis of computer system failures, and found cases where new risks associated with the progress of digitalization have emerged, including third-party risks¹.

In light of this, we have decided to publish trends with failures and specific cases in order to raise awareness at financial institutions, and we hope that our findings can serve as a useful reference when tackling IT risk management.

2. Overview of failure analysis

(1) Key failure trends (industry wide)

[Failures stemming from third parties (responses to new third-party risks)]

At multiple financial institutions, we found cases of errors with the system of one-time password authentication for Internet banking (below, "IB"), resulting in a failure where individuals and corporations were unable to log into their IB accounts. In these cases, CPs directing customers to ATMs or branches were invoked, but they were not particularly effective.

To resolve such issues, it will probably be important to revise CPs to reflect the importance and characteristics of new services and to respond to new third-party risks that are emerging in connection with the march of digitalization.

¹ A third party refers to an organization with which there is a business or contractual relationship.

[Failures stemming from increases in transaction volume]

Transaction volume is increasing as a result, for example, of payments being made by smartphone etc., enhanced convenience thanks to the Zengin System (Japanese Banks' Payment Clearing Network) now being accessible for longer periods, and campaigns and other events. In conjunction with this, there were multiple cases of computer system failures, such as system stopping working, that affected services for customers. These were due to system maximums being exceeded and systems having inadequate processing capacity.

Because of this, and given that transaction volume may also increase temporarily when events such as the 2020 Tokyo Olympic and Paralympic Games take place, it is necessary to verify in advance system maximums, system processing capacity, data storage capacity, and so on.

(2) Key failure trends (sector specific)

[Failures at cryptoasset exchangers]

At cryptoasset exchangers, factors such as program errors and operational mistakes resulted in multiple cases of computer system failure that affected services for customers, making it impossible to perform transactions, for example.

There were few incidents caused by problems specific to cryptoasset technology, with most being due to typical inadequacies of IT system quality control systems, such as potential problems not being considered at the design stage. There were also cases of shortages of IT personnel given the nature of the operations being performed.

Because of this, it is necessary to enhance management systems relating to computer system quality such as by securing appropriate personnel, improving design/manufacturing review processes, analyzing the root causes of failures and proposing measures for preventing recurrences.

[Failures at fund transfer service providers etc.]

At fund transfer service provider etc, we found multiple cases of computer system failures caused by deficiencies that occurred at the time of design/manufacture, such as program errors and requirements not being adequately taken into account, as well as failures, such as operational mistakes during production migration, that

were caused by not preparing work manuals or not having things checked by two different people. These computer system failures affected services for customers by, for example, making it impossible to use settlement services.

Because of this, it is necessary to take action to improve work quality such as by strengthening reviews in the design/manufacturing process, performing tests under the same conditions as the systems will be used, and ensuring that work procedures are prepared and two-person checks are conducted at the time of production migration.

3. Future action by the FSA

We anticipate that the report will serve as a useful reference for financial institutions when they establish and enhance the sophistication of IT risk management systems based on the scale, attributes, etc. of their operations. We also expect the report to encourage, through the sharing of actual examples of computer system failure, financial institutions to become more aware of their own situations and act independently to make improvements.

The FSA will continue to analyze computer system failures, and intend to warn financial institutions about new risks or incidents whenever they emerge.