

Information Security Management in Financial Sector Based on Security Baseline

Yanli Xi*

Central University of Finance and Economics, Beijing 102206, China. E-mail: 1580868858@qq.com

Abstract: On the whole, the structure of information security in financial sector will become more complex and diverse, for its system's expansion will, to a certain extent, promote such situation. Thus, such situation will increase the number of key and server applications. If staff makes mistakes in operation, it will inevitably cause adverse obstacles to the normal turnover of the system. In view of the above drawbacks, it is necessary to set up baselines of information security management to cater the needs of the financial sector, and to ensure the safe and effective operation of information systems to the greatest extent. This article studies the above issue and aims to provide some theoretical reference for information security management under the financial environment.

Keywords: Financial Information Security; Security Baseline; Management Methods

1. Introduction

During the development in recent years, security baseline has been applied widely in the financial industry, which has strengthened the overall security coefficient of intranet and information system in the financial industry to a certain degree. Generally speaking, security baseline refers to the minimum standards and indicators of protection capability. It must be met on the basis of ensuring the safe and stable operation of network communication equipment, and must be a complete and unified security baseline. The information security baseline in the financial industry shows the overall information security status of the financial unit at a specific moment, which is the way to summarize the information security level of the unit.

2. Regulate baselines for information security in financial enterprises

In the process of operation and management, enterprises need to have standard system to control risks, and they also need to ensure the effective and strict implementation of these systems. However, as far as the actual situation is concerned, many enterprises have been neglected in the implementation of the system in operation. Problems often happen that human relationship is bigger than regulations, operate without the approval of higher authorities, blindly seek high performance and ignore risks, etc. Besides, they are seriously poor in security responsibility and in system control, which makes information security unable to be fully implemented.

Generally speaking, the security baseline standards adapted to the financial industry involve two major aspects: security management and security technology. The former generally covers the management standards of organizational structure, the safety management of human resources, operation and maintenance processes, confidential information and assets. The latter mainly covers the security of application, host, network, computer room and audit (see **Figure 1**).

Copyright © 2021 Yanli Xi
doi: 10.18686/fm.v6i1.3068

This is an open-access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

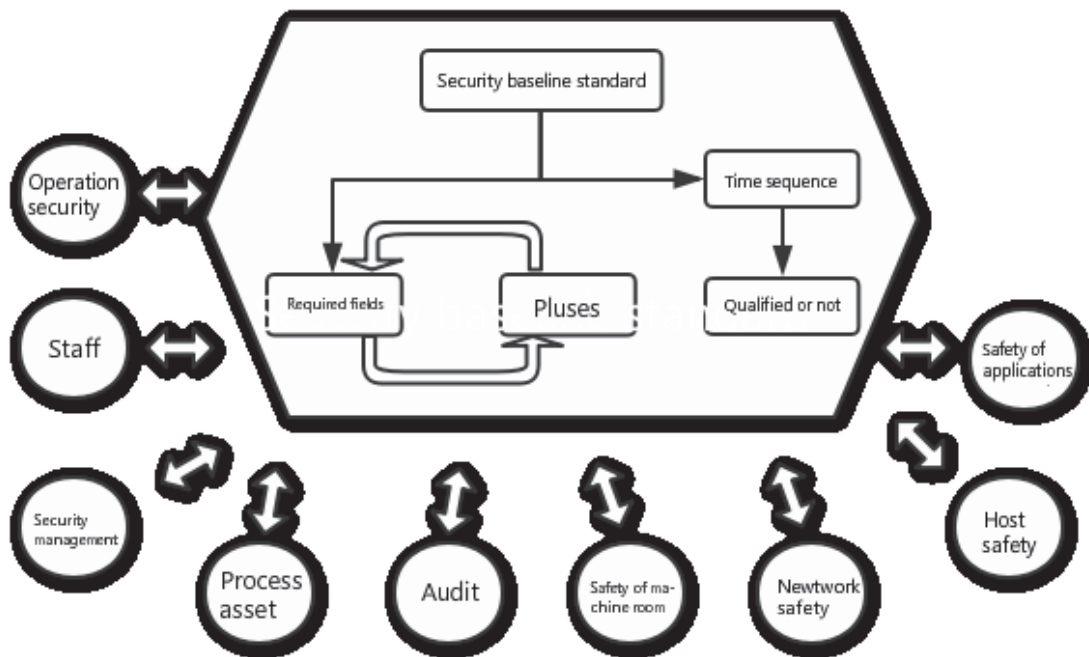


Figure 1. Schematic diagram of standard framework of conventional security baseline

Nowadays, with the reform and innovation of the financial industry, there is a new opportunity to change the security baseline management standard. Supervision, testing and learning contents need to be viewed objectively on an equal level, creating an operating environment that conforms to rules and regulations, and promoting the establishment, perfection, implementation and implementation of the information security baseline standard with the help of the improvement of enforcement^[1].

3. Baseline measurement, security rectification and reporting mechanism

After establishing and perfecting the security baseline specification, it is necessary to refer to these benchmarks to carry out overall safety evaluation and risk measurement. It is also needed to determine the basic safety status in current enterprise operation and the gap between current and safety objectives, strengthen safety rectification and system solidification application and dispel safety risk factors to meet the standard requirements of the baseline.

Security baseline specification corresponds to security baseline report, which relates to specific standards of different branches of financial enterprises based on the baseline. It is composed of a comprehensive report of safety status, which is generally composed of a group of safety configuration items. The configuration items describe in detail the information security status of a certain unit at a certain time point, which is a process of quantifying the overall level of information security of this unit. Different time points of risk assessment will inevitably lead to differences in the versions of information security baseline reports. The set of security baseline reports in a specific time series can better reflect the information security change trend of this unit in this time period^[2].

3.1 Security assessment and risk assessment

Based on the relevant standards of security baseline, the head office of financial enterprises can refer to the dynamic state of information security of its branches for effective inspection and evaluation. The office evaluates the gap between the security status of each branch and the baseline standards to provide information reference for subsequent information security rectification and dynamic adjustment.

3.2 Security rectification

With reference to the evaluation report and information data, the project that does not meet the standard should be properly rectified to avoid the potential risks of information security, implement the security status and meet the specification requirements of the baseline standard.

3.3 Establish and improve the security baseline reporting system

The security control unit of a financial enterprise needs to inquire regularly or dynamically the security reports of branches at a specific time point, in order to understand the information security situation and risk distribution of the institution, and to clarify the development trend of security changes^[3].

4. Enhance the management of scientific and technological change based on security baseline

After the security baseline report being confirmed to meet the standard, it is proved that the information security status of the unit has met the baseline standard at this time. In order to have a long-term and stable safe operation state, it is necessary to strengthen the related work of scientific and technological change based on the security baseline.

As far as the current situation is concerned, although there have been many templates for enterprise management units to plan safety baselines, which have become the industry security baseline guidelines, there are still some unreasonable problems. In this regard, it is necessary for financial enterprises to report the changes and adjustments of the information security baseline in time, so that the superior management can clearly and master the information security work of subordinate units at any time. In view of the practical problems that are difficult to solve in the short term, subordinate units must also analyze the causes practically, make effective improvements, integrate the problems arising during the improvement period, the specialized technical means involved, the required equipment cost investment, etc., and feed them back to the corresponding departments in time. On the whole, as the baseline of information security, to initialize the management of science and technology, it is necessary to ensure a high degree of scientificity and rationality. The higher-level examination and approval and the lower-level report all need to strengthen the inspection process, and timely and effective inspection and regular review should be made for the change of security standards^[4].

5. Long-term management of baseline operation and maintenance of financial information security

5.1 Comprehensive and dynamic operation and maintenance monitoring management

With reference to the relevant standards of safety baseline, dynamically monitor the safety status and reasonable configuration of the system, environment and various parts of equipment. Once any behavior that does not meet the requirements in the baseline specification is found, timely warn and remind, and dynamically summarize and analyze the data according to the indicators of safety operation and maintenance.

5.2 Track potential risks immediately

With the help of the effective management strategy of information security baseline of branches, we can better quantify the information security level of each unit, monitor the overall information security situation at any time, and track the security requirements and information security risks that have not yet reached the standard, so as to better strengthen emergency management.

5.3 Set up an automated baseline management database

With the help of the baseline safety management system, the goal of automatically uploading reports by branch companies can be effectively achieved, and the demand of headquarters to query the baseline reports in the time series of branch companies can be met.

5.4 Dynamic updating of safety baseline standards

According to the above analysis, it can be found that the safety baseline standard is not fixed after its establishment, but should be constantly updated and improved during the development process. Therefore, if the system and application change, the safety baseline must be adjusted in time.

5.5 Build better long-term security mechanism

Regular comprehensive audit, system update and information reporting process are applied to effectively strengthen the controllability of information security baseline and meet the manageable requirements of security baseline.

5.6 Improve the assessment and effective evaluation of safety work

At present, for most large financial enterprises in China, it is necessary for the headquarters to assume the responsibility of controlling the information security of different branches. In this process, strengthening the effective assessment of information security work is the key way to stimulate development, and the report on the security baseline is one of the key basis for assessment^[5].

6. Conclusion

In summary, the application of information security management system based on security baseline in China's financial industry can better provide new management ideas on information security for various financial enterprises. In organizational security baseline management, it is necessary to refer to its own actual situation and the dynamic changes of the market and incorporate it into daily operation and maintenance management because the security baseline itself is the product of balancing security costs and security needs. In-depth and further researches on security system of financial information and scientific planning can improve the safety of financial information system and promote the rational development of financial market.

References

1. Zhang G. Information security management and control strategies of small and medium-sized banks in the financial technology age (in Chinese). *China Banking* 2019; (12): 33 - 35.
2. Jia H, Xie Z. Standard framework of financial cybersecurity management based on comprehensive risk management perspective. *China Quality and Standards Review* 2018; (8): 24 - 28.
3. Zhang Y, Lin W, Hu J. Improving the management level of science and technology based on information security baseline (in Chinese). *Financial Computerizing* 2014; (1): 79 - 80.
4. Tang Q. Discussion on the defense system of information security management of basic-leveled central banks — take change branch as an example. *Financial Technology Time* 2019; (7): 63 - 65, 80.
5. Li Y, Wang X. Financial information security management method based on security baseline (in Chinese). *Financial Computerizing* 2013; (10): 61 - 62.