Development of Commercial Bank Information System Based on Risk Management Research

Xiaofei Tang

Science and technology university of Liaoning, liaoning Anshan, 114010, china

Key words: risk management; commercial bank; information system; security

Abstract: In the society, the commercial banks are the enterprises that operate the risks. They are faced with different risks, namely, liquidity, credit, operation, market, reputation, interest rate, law and so on. With the continuous development of science and technology and technology in our country, the business of commercial banks is increasingly dependent on the network and information system. Security management of traditional commercial banks' information systems is generally managed by passive management. The investment is substantial and the benefits are in general. Based on this, this paper based on the risk management model, as a commercial banking information system framework, so that the customary passive information system management into an active, in order to control the bank's investment.

Introduction

In the process of continuous development of shared information, information has become the basic resources of people to participate in economic activities and important assets of enterprises, and can benefit from information technology. Most of the core business of enterprises have been directly based on information systems, and become the majority of the internal digital nerve. Information security, like other assets in the enterprise, is also protected. The value of information systems continues to improve, the information system is also known as some of the illegal personnel to obtain a convenient channel, as a result of the emergence of hacker technology. The security of information systems affects the entire enterprise, so it is necessary to avoid the problem of information security through an effective management model.

The challenges faced by commercial banking information systems

Commercial banks traditional information system development and operational environment are function-oriented, in the banking sector after the demand, the computer sector through the relevant technical resources to achieve, the new financial products arise spontaneously. There is a loosely coupled relationship between products, but there is no connection. Different product development does not exist communication, so that the development team to use their own skills to develop good design products, so the system is also very unique requirements.

Facing the function determines the development of the focus is not safe. The system uses different security measures, so there is no unified security architecture. Only when the problem is identified as solve the problem, this is a passive security management, then it brings the following questions: First, the investment is too large. If each system is using different security programs, products and technologies, it will reduce the interoperability, then it is necessary in each system security alone investment, resulting in investment cannot be shared; Second, the management

complexity. The system has a variety of security technologies, cannot achieve centralized management, resulting in higher management costs; third, passive management. Only in the system when the problem is solved, cannot prevent the security problems, reduce the security level and system security. [1]

China's banking information system has always been in the isolation of the operating environment, resulting in no one knows the structure of the banking information system, application and operation. Most of the traditional banking information systems come from the bank's individual characteristics, including conservative and stable. At present, the traditional banking business has been unable to meet the information system upgrade needs, since the financial reform and development in China, banks have been innovative traditional business obstacles, and gradually enter the market competition, then the banks are faced with a variety of challenges and opportunities. Commercial banks in order to survive,. Is necessary to innovate new financial products and business, and to provide users with quality service. Modern open banking system is mainly for the platform of honest, open network and application structure of the open. Security threats of traditional closed information systems are mainly from within, and now open information systems are mainly from outside and inside, and external threats are more difficult to control. [2]

The traditional bank counter business is carried out by manual, the customer's account is also preserved through the paper, the bank can only through the summary of the document to understand the situation of funds, cross-bank transactions to make the bank through the checks, bills and other data centers to complete. As a result of manual operation, banks can only rely on the network to create to meet customer needs, so there are no excess resources and the ability to develop new derivatives, improve the efficiency of the bank. After the emergence of the computer, the banking business model has undergone enormous changes. China's commercial banks have also innovated the traditional manual business model, the development of the current account-based information business processing model. The customer's account will be saved to the information center host. The customer does not need to pass the paper certificate to the bank exchange. Computer business processing reduces the daily workload of counter staff so that it can concentrate on improving service quality and value-added services. As the customer's account information is stored in the information center host, the banking and management departments can keep track of the operation of the funds, improve the bank's ability to control the funds, but also through the information management system to deal with the daily business of banks. At present, most of the business of the bank is done through the information system, it can be said that the degree of dependence on the information system has reached the limit. [3]

The risk management of commercial bank information system model

The security of the information system of the commercial bank is not an independent event, each level and the link is the interaction and the restriction, if only one-sided processing some security problem, can cause certain influence on the system. The security of bank information system is a dynamic development process, and it is not a simple mechanical problem. The establishment and management of the security of the bank information system are a complicated project. It is necessary in order to combine the planning, technology and management with the change of the idea. In this paper, we use the risk management model to solve the problem of information security.

Risk management refers to the identification, analysis and measurement of a potential security threat and loss, and to develop appropriate strategies to control the safety risk of processed in a reasonable way, in order to ensure the safety of information management. Risk management is a cyclical process, which is divided into identification and analysis, control, tracking and evaluation,

planning and implementation. [4]

As for the bank information system, the sources of security threats are various, and the different security threats are unique to the banking system. Illegal access and denial of service attack. Denial of service attacks can only make the user cannot get the normal system services, does not destroy the data in the system, but illegal access compared to denial of service attacks is very serious. Although the same threat to discrete systems, but the risk is different. To implement risk management, we must first identify and analyze the risks. [5]

Risk identification includes threats, vulnerabilities, assets and consequences:

All risks in the banking system have a source. The general security risk sources include: intentional acts, unintentional acts and non resistance. The data is mainly refers to the intentional acts of illegal access, malicious attacks, computer viruses and social engineering threats; mainly refers to the unintentional behavior is the system itself, software defects and human error operation; non resistance mainly refers to the physical environment threat.

Each system also has a security threat against security vulnerabilities of no threat, no loopholes, security vulnerabilities may exist in the system configuration, products, may also exist in the system, safety management, so as to intensify the recognition of security vulnerabilities.

The banking system is mainly composed of many subsystems. Each system has different asset value, different systems have different importance to the bank service. In order to effectively control the risk, it is necessary to carry out modest assets to balance the value of assets, and control risk.

Different security threats will have different consequences and impact on the system. These consequences and effects can make us grasp the seriousness of the risk, which determines the remedial measures to control risk. [6]

The risk analysis is through the model and analysis of information system security threats and vulnerabilities of the system will be a loss, in order to be able to determine what kind of tools and techniques to control risk, the risk and cost control balance in the economy. Risk analysis is commonly used in two ways: quantitative and qualitative. Quantitative analysis is performed through the mathematical model, qualitative is judged by intuition and experience, in order to classify threats and assets.

The mathematical model of quantitative analysis:

SLE=AV*EF

ALE=SLE*ARO

E=P*I

SLE said a loss of expectations, AV said the value of the assets, EF said the coefficient of the exposed ALE said a year; the loss of expectation, ARO said a year probability of occurrence; E said security exposure value, P said the probability of occurrence of I, said the impact of risk. [7]

Develop and implement risk control plan

Prior to the development of a risk control plan, we should pay heed to the higher risk according to the priority level, so as to reasonably control the risk and improve the security of the bank information system effectively. Since most of the security threats are active attacks, it is not possible to eliminate the threat source, but we can eliminate security threats or vulnerabilities, in order to control the risk. The form of security threat is diverse, but the root cause is the same, a risk factor can start another risk. If we can control the root cause of the risk or the risk factors that depend on it, we can increase the efficiency and effectiveness of risk control. The development of control risk plan includes three steps:

First, mitigation plan. Mitigation plan is used before the occurrence of security risks, can control

the occurrence of risk, or effectively reduce the incidence of risk on the system. For example, the use of enhanced password protection strategy to reduce the risk of security attacks by password guessing;

Second, risk triggers management. In the implementation of risk control, it is necessary to inform the user that the security risk is imminent or has occurred through the trigger, so there is sufficient time to develop plans. Ideally, before a security risk causes a systemic problem, the trigger captures the security event and notifies the staff. General trigger threshold type, there are many parameters in the information system and safety is closely related, if these parameters exceed the normal value, so the security of the system is changed, and a security incident. If the trigger threshold decision effectively, so the setting time to a detailed study of the threshold set too strict would make the threshold lose its role, if set too wide would lose its threshold value;

Third, contingency plans. Contingency plans for reactive planning, in the implementation of mitigation plans, but no effect, you can through the security risk contingency plan. The emergency plan is mainly for safety accidents including reflect, what should be done if there is a threat, if a threat to the system there is a problem what should be done, and if that can affect the information system and the banking business has been to the lowest. All security threats should be targeted to develop contingency plans, including operational control plan risk. [8]

In the development of risk control plan, it is necessary in order to formulate the corresponding remedial measures according to the steps of the plan, mainly to strengthen the information system technology and modify the bank safety management, in order to achieve risk control.

After the completion of the development of remedial measures, to test the remediation plan strictly, including the emergency and mitigation plan, in order to make the risk control plan to complete and effective, and also make the risk control after the implementation will not affect the operation of the system. A comprehensive review of the risks related to remedial actions, including system vulnerabilities and security threats to the system. Test whether the trigger can capture the security of the system in the process of changing the security time, and timely for the relevant personnel and users to send a notice. The rehearsal of emergency plan, the normal operation and the bank can in the shortest possible time to restore the bank information system in the event of accidents related to business.

On the basis of the effectiveness of the risk control plan and remedial measures, according to the level of risk and the priority of the implementation of the plan, the implementation of the whole process is step by step. [9]

Conclusion

Through the above description, the paper studies the application of risk management model in China's banking information system, its main advantage is that he can meet the requirements of information security and to carry out the business of the bank, into the information security management in bank risk prevention, safety to protect the information of commercial banks in our country, to promote its integration with the international bank the pace of. On the basis of cost control, risk management has an obvious effect, which can effectively improve the safety level of commercial banks.

References

[1] Zheng Lei. Evaluation of internal control of commercial banks based on risk management [D]. Southwestern University of Finance and Economics, 2011

[2].Zhang Weizhen .Research on credit risk management of commercial banks based on the perspective of comprehensive risk management [D]. Nanchang University, 2012

[3]Zang yafeng.Study on the internal control of commercial banks based on operational risk management[D]. Shanxi University of Finance and Economics ,2007

[4] Liu Xiaoxing VaR of the Commercial Bank of [J]. risk management based on Economic Research Guide, 2006 (6): 69-72.

[5] Peng Jiangping. Research and development of risk management theory of commercial banks based on risk value [D]. Central South University

[6].Liu Xiaoxing, He Jianmin,Zhao Lihang.Research on credit risk management of commercial bank based on [J]. VaR contemporary education and culture, 2004, 17 (3): 31-35.

[7] Hu Jirong, Liu Huifang. Study on the function of internal audit of commercial banks based on comprehensive risk management [J]. accounting monthly, 2008 (33): 65-66.

[8] Rong Yuanhong. Safety risk management of commercial bank information system research based on [D]. of Tongji University, 2005

[9] Liu Xinyu. Study on the internal control of Chinese Commercial Banks Based on comprehensive risk management [D]. Liaoning University, 2011

About the author: Tang Xiaofei, 1971,09, female, Tianjin, master, lecturer, research direction: Software Engineering