International Journal of Security and Its Applications
Vol. 10, No. 3 (2016), pp.245-258
http://dx.doi.org/10.14257/ijsia.2016.10.3.23

Overview of Risk Management System of Commercial Bank Data Center

Zheng Li[1,2], Shanlin Yang[2] and Zhenyao Li[1]

[1] *Bank of China Limited, Beijing 100818,China*
[2] *School of Management of Hefei University of Technology, Hefei 230009,China*
leeching3668813@sina.com

Abstract

In nowadays, the trend of the economic globalization is increasing evidently. Without exception, all of the global banking industries take information technology as a necessary condition for survival in the future and the core of the competition. Aimed at two risks, 'operational risk' and 'compliance risk', which commercial banks data center must face to, this article constructs a risk management system, represents a management style of 'One management framework, One set of risk baseline, Three kinds of control methods, Three improvement mechanisms', establishes risk baselines as the basic of risk management, consolidates risk assessment experience, raises the standardization level of the risk assessment, improves risk baselines with continuous effort to adapt the updated security environment, identifies operational risk and compliance risk comprehensively within the unified management framework, achieves risk management standardized and sustainable, provides strong support to the commercial bank on the development and robust operation around the whole world.

Keywords*: Data Center, Risk Management System, Management Framework, Operational Risk, Compliance Risk*

1. Introduction

In nowadays, the trend of the economic globalization is increasing evidently, the high integration of commercial banks' business process and information technology brings great improvement to the effective and core competition. The expansion of commercial banks' operation, the extension of the service objects, the improvement of the globalization level bring profound changes and long-term impact on the IT management and operation system of commercial banks:

(1) High integration of commercial banks' business process and information technology [1]. With emerge of large numbers of technologies such as internet, mobile communication, and intelligent terminal, traditional business model is broken thoroughly. In recent years, the new businesses banks pushed out such as "Financing against accounts Receivable Insurance from BOC", "Trade of ICBC", bring more procedures on the processing flow, data exchange, linking and transaction path between the information system and the relevant enterprise systems. Redefine the business procedure will increase the bank's operation pressure inevitably. At the same time, bank's business systems are highly reliable on the information technology; the banks' business process and information technology are highly integrated. The correspondence of information technology and business process becomes more and more complicated as while as the occupation of the market increases, even the boundary of business and technology management is becoming blur and the management content is overlapping.

(2) The situation of network security is becoming increasingly serious [2]. At present, the banking service system's dependence on the electronic channels such as on-line

ISSN: 1738-9976 IJSIA

banking is increasing day by day; the average rate of the main bank electronic banking transactions has reached 62.6%. At the same time, the network attacks are developed from show off and personal behavior to economic interests and organization behavior. Under the network environment, customer information protection becomes the most concern of the public. Any defect of the procedure or any leak hole may lead to customer information leakage or improper user, and then produce a serious reputation risk or legal risk, even the stability of the whole financial industry.

(3) The operational scale grows rapidly [3]. Up to end of 2011, there are 501 data centers from 255 key financial institutions. Total investment in science and technology reaches 69.87 billion, up 38.3%. The number of information systems is increased rapidly. The structures of these systems are more complicated, the correspondence among software, hardware, infrastructure, services, data, interfaces and customer is more complicated. It is not rare that an application system supports multiple channels and interacts with several application systems [4-5].

(4) The pressure of compliance is increasing steeply [6]. Economic globalization prompts numerous of commercial banks to face to great challenges which are caused by the difference of supervision requirements from different countries and regions. A domestic commercial bank, whose branches are around the world, needs to satisfy the different supervision requirements from 34 countries and regions for operation and maintenance. There are various IT supervision requirements (up to 260 policies). Although the contents of these policies are similar, the focal points are different. There are many special requirements. If we can't identify, control, avoid and defuse compliance risk, we will face legal sanctions, supervision punishment, financial loss and loss of reputation. All of these will make irreparable damages. The above generates two risks which commercial banks have to face: operational risk and compliance risk. To enhance the reputation and operation efficiency of commercial bank, satisfy the supervision requirements, defuse the security threats which may affect the normal business, commercial bank needs to increase the risk control for data center [7] [8].

The research of the risk control for commercial bank data center still exists several problems:

(1) The research of operational risk for the commercial bank data center is lack of comprehensiveness and accuracy for risk identification. At present, the main risk assessment method used by banks is Qualitative Risk Assessment [9], which combines the issues found by daily audit and historical risk incident, uses Delphic and flow chart, then identifies risky factors which may affect operation and maintenance.

(2) The research of compliance risk management for the commercial bank data center still exists following problems:

ⅰ. Integrity needs to be improved; the research does not cover all of the supervision requirements for the main countries and regions.

ⅱ. The research result is mainly a supervision requirement database without further research or analysis, unable to locate the difference between domestic and oversea requirements in specific control fields.

ⅲ. There are few methodology and practice which could satisfy all of the supervision requirements for different countries [10] to build a globalization maintenance system.

(3) From the whole risk control of commercial bank data center’s point of view, the operational risk and compliance risk remain as two separate branches of research, which are still not included in a unified risk management framework. So we are unable to identify and manage risk from a global perspective [11].

To solve these problems, this article establishes a risk management system for commercial bank data center, to identify operational risk and compliance risk comprehensively and effectively, achieve a specific and practical control, ensure full compliance with domestic and overseas supervision requirements and international

standards, provide strong support for overseas expansion and stable operation of commercial banks.

2. Risk Management System of Commercial Bank Data Center

Risk management is a complex process. The industry has continued in the research of risk management. The theory and practice are continuously developed. "ISO 31000: 2009, Risk Management Principles and Guidelines" (Correspondence domestic standard is GB/T24353), was released in November 2009. It is the first international universally recognized risk management standards, which provides the basic framework for risk management activities for industries. The risk management model comprises five aspects, which are “clear environmental information, risk assessment, risk response, monitoring and inspection, communication and records”. It is shown in Figure 1:

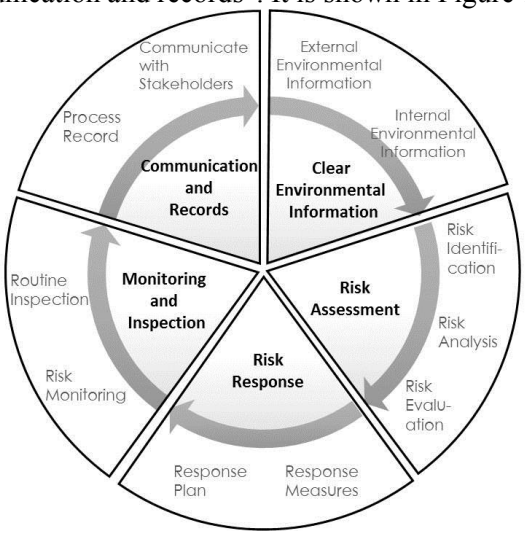

Figure 1. Risk Management Model

This international standard is intended to provide principles and guidelines for risk management. It helps industries and organizations in any range and background to manage risk with a systematic, transparent and reliable way by specifying the general approach [12]. However, different industries and organizations have different needs for all aspects of risk management. The research of risk management needs to be more specialized. To the risk management of commercial bank data center, the specific risk management objects, risk assessment and corresponding practical methods, risk management activities and daily work, continuous improvement are all needed to be researched upon the existed risk management framework and combined with operational characteristics of banking industry data center. We need to establish a risk management system which is practical and also suitable for commercial bank data center. Through the introduction of baseline management, the risk management methods and practicing results are consolidated and the operability and effectiveness of risk management are improved [13].

Considering the actual situation of commercial banks, using the risk management method, this paper presents a risk management system which is based on a comprehensive analysis and standardization refining. The system can be summarized as “One management framework, One set of risk baseline, Three control methods, Three kinds of improvement mechanism”, which makes risk management standardized and extensible. In addition, combined with shortcomings in the present risk research on commercial bank data center, this paper researches each part of the model and achieves a comprehensive and fine control on the compliance risk and operational risk.

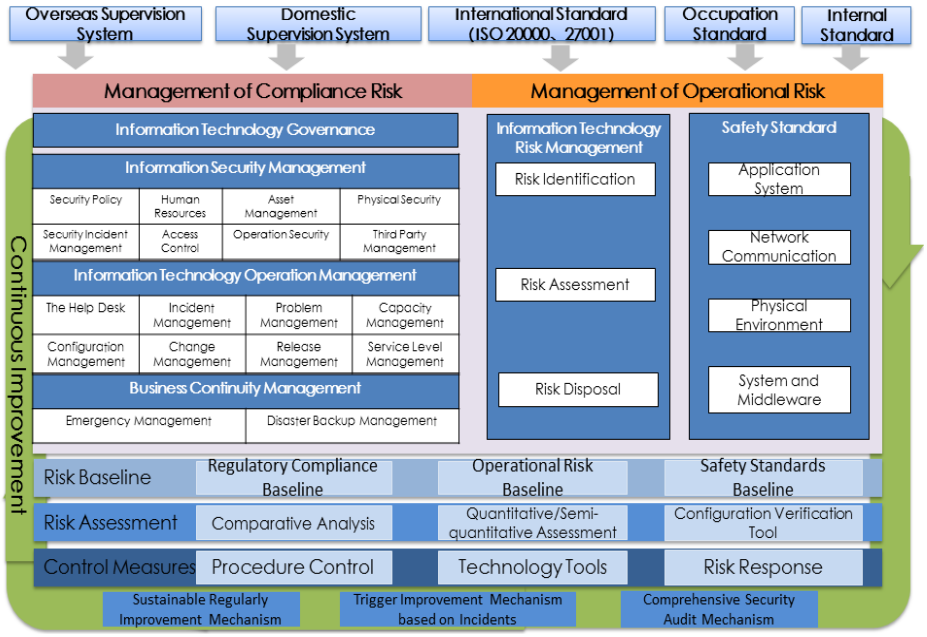

Figure 2. Risk Management System of Commercial Bank Data Center

One management framework: According to the CBRC (China Banking Regulatory Commission) "Commercial bank information technology risk management guidelines" and "Commercial bank data center regulatory guidelines", design a data center risk management framework covering 7 management areas and 26 management objects including information technology governance, information technology risk management, information security management, information technology operation management, business continuity management, security audit and technical standard, to unified control the two main risks data center faces -- compliance risk and operational risk.

One set of risk baseline: Based on the management framework, establish a risk baseline for different characteristics of compliance risk and operational risk, including regulatory compliance baseline, operational risk baseline, safety standards baseline.

Three control measures: Take three risk baselines as risk control input, centralized control the compliance risk and operational risk under the 26 management objectives with procedure control, technology tools and risk response. Ensure integrity and refinement of risk management in all areas.

Three improvement mechanisms: Risk management is a continuous improvement process, this article design a sustainable regularly improvement mechanism, the trigger improvement mechanism based on incidents, the comprehensive security audit mechanism to detect and reform the risk management issues, to ensure the continuous improvement of commercial bank data center risk management system.

3. Risk Management Framework of Commercial Bank Data Center

The design of risk management framework comes from the CBRC supervision requirements, international standards and best practices, based on COSO Enterprise Risk Management (ERM), divided into the area layer, target layer and control layer by using analytic hierarchy process, shown in Figure 3.

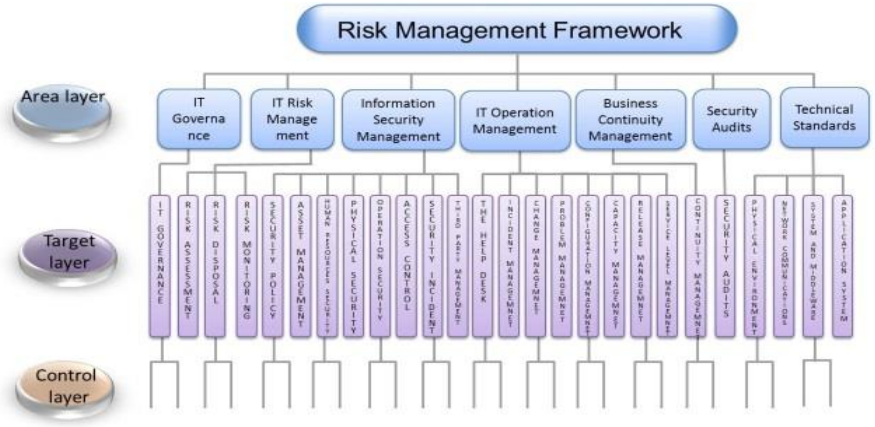

Figure 3. Risk Management Framework of Commercial Bank Data Center

(1) The Area layer: Reflects the concerned areas that the operational risk of bank with control objects. According to the guidelines of the CBRC, it is divided into 7 risk management areas: IT governance, IT risk management, information security management, IT operation management, business continuity management, security audits, and technical standards. Every area takes the corresponding international standard and best practice as a reference for further risk management (Figure 4): the IT governance area introduces ISO38500 for IT governance framework design; the IT risk management area introduces national standard GB/T 20984 (information security risk assessment specification); the information security management area introduced ISO27001; the IT operation management area introduces methods in IT service management standard ISO 20000; the business continuity management area introduces ISO22031; the security audits area introduces the audit idea of controlling headed in COBIT; the technical standards area introduces kinds of technical standards in several industries such as the national technical standards of "facility universal norms", "computer room design specifications" and the information security industry best practice of IBM GSD331.

Figure 4. Area Layer of Risk Management Framework

(2) Target layer: Figure 5 shows the specific control objects in each area which are divided into 26 control targets.

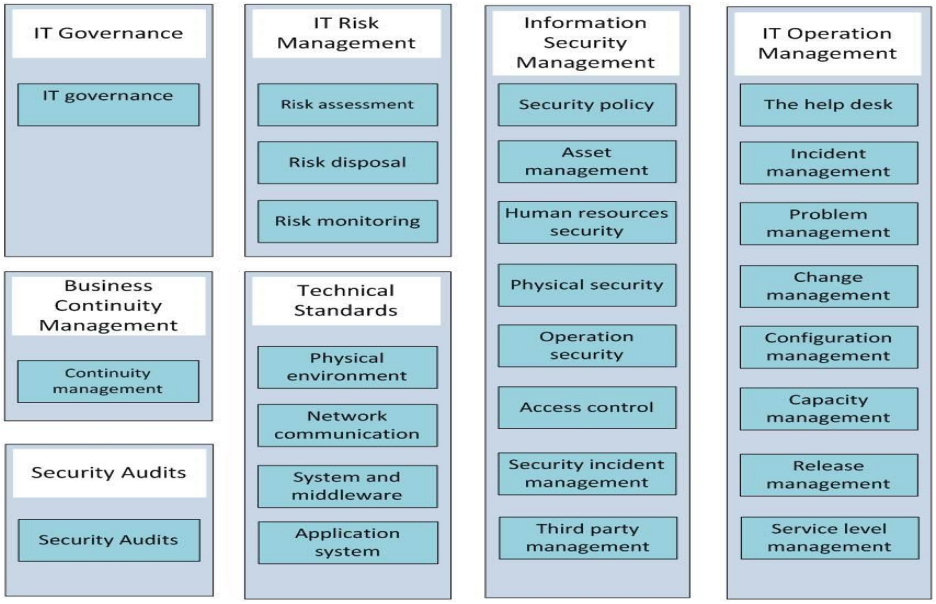

Figure 5. Target Layer of Risk Management Framework

(3) Control layer: Specific risk control requirements, divided into 69 sub-objects, as shown in figure 6. Design corresponding management and technical methods to achieve the control of compliance risk and operational risk which commercial banks faced to according to domestic and oversea regulations, industry standards, specific articles of best practices, kinds of security technical standards and the operational risks in commercial banks.

Area Layer	Target Layer	Control Layer	Area Layer	Target Layer	Control Layer
IT Govermance	IT Govermance	Organization Management	Information Security Management	Security Policy	Security Management
		System Management		Asset Management	Asset Liability System
		Resource Management			Daily Asset Management
IT Risk Management	Risk Assessment	Assessment Strategy		Human Resources Security	Entry
		Assessment Process			Illegal Accountability
		Risk Tolerance			Training Education
	Risk Disposal	Disposal Activities			Dimission
	Risk Monitoring	Audit Evaluation		Physical Security	Computer Room Construction
		Detection System			Computer Room Security
IT Operation Management	Help Desk Management	Service Implementation			Computer Room Power Supply
		Service Tracking			Computer Room Environment
	Service Level Management	Service Level Agreement			Office Environment
		Service Level Assessment		Operation Security	Backup Management
	Incident Management	Incident Process Management			Operation Guidance
	Problem Management	Problem Process Management			Log Management
	Capacity Management	Availability Management			Attack Prevention
		Capacity Management			Operation Monitoring
	Change Management	Change Process Management			Terminal Management
		Change Plan			Network Management
		Change Preparation			System Management
		Change Approval			Application Management
		Change Implementation			Data Management
	Release Management	Release Process Management		Access Control	Access Control Policy
	Configuration Management	Configuration Management Process			Access Authorization
		Configuration Library Management			Access Subject
Business Continuity Management	IT Continuity Management	Emergency Process			Access Object
		Emergency Plan			Access Monitoring
		Emergency Drill		Security Incident	Security Incident Management
		Disaster Backup Construction		Third Party Management	Third Party Management Policy
		Emergency Response and Disaster Recovery			Service Provider Management
Technical Standard	Physical Environment	Physical Environment Standard			Third Party Personnel Management
	Network Communication	Network Communication Standard	Security Audit	Security Audit	Internal Control
	System and Middleware	System and Middleware Standard			External Regulatory Compliance
	Application System	Application System Standard			Internal Audit
					External Audit

Figure 6. Control Layer of Risk Management Framework

4. Risk Baseline of Commercial Banks Data Center

The risk baseline of commercial banks data center includes regulatory compliance baseline, operational risk baseline, and security standards baseline. The detailed content are three information bank and the corresponding risk assessment methods which covers

kinds of risks, ensures the integrity of the risk recognition, consolidates risk assessment methods and experience and standardizes the risk assessment. The integration of the recognition risks are input of subsequent risk controls.

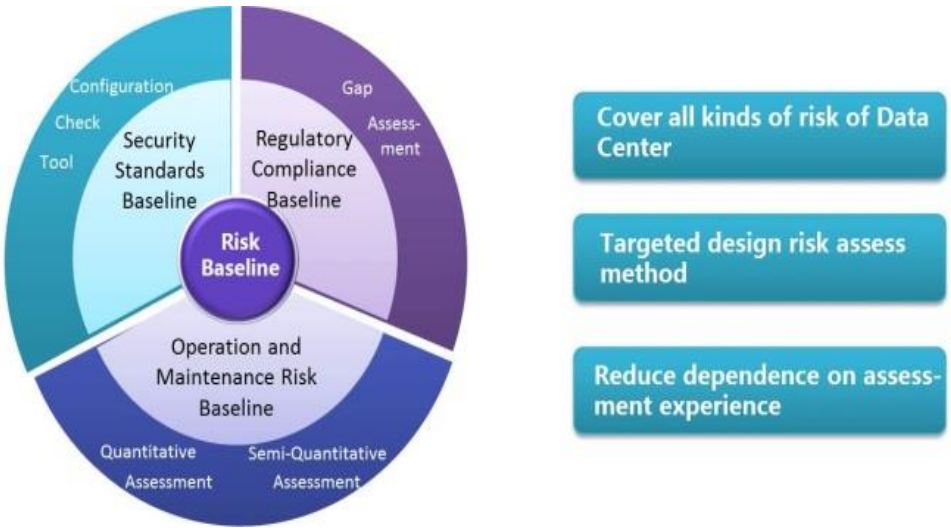

Figure 7.Risk Baseline of Commercial Banks Data Center

4.1 Regulatory Compliance Risk Baseline

By choosing domestic and overseas' supervision requirements, combining with ISO27001 (information security management standards), ISO20000 (IT service management standards) and other international standards, this article generates a supervision requirements database based on classifying, integrating, mapping risk management framework. The database covers nearly all of the supervision requirements of domestic and oversea, is considered as the baseline of compliance risk management.

First, collecting and analyzing the supervision requirements of each country, mapping the requirements to target layer, then generating the original supervision requirements database. Taking the CBRC supervision requirements as baseline; identifying the related supervision requirements of overseas, and mapping to the requirements of CBRC; reporting the difference of each country's supervision requirements in different risk control areas. Finally, doing a multi-dimensional mapping between industry standards and internal specification of data center, it can help to find the gaps quickly in supervision requirements and improve it complying with international standards and best practice.

Figure 8 is a sample of supervision requirement database. With this database, we can clearly and intuitively understand the focus and difference of each supervision requirements in specific area. It is also helpful to check the implementation of each supervision requirements for the commercial bank data center.

Domain Layer	Target layer	Domestic Regulatory	Regulatory Requirement	Overseas Regulatory Requirement	Country/Region	ISO 27001	ISO 20000	ISO 22301	Internal Rules
IT Risk Management	Risk Monitoring	CBRC Guidelines on the Risk Management of Commercial Banks' Information Technology	Article 18. (1) Pre and post-implementation review of IT projects.	Issues of concern in policies and procedures of development and acquisition are, amongst others: a. Minimum including the following items: 1) identification and analysis of user requirements; 2) definition of requirements (user requirement); 3) System planning; 4) programming; 5) testing; 6) implementation; 7) post implementation review; 8) Maintenance.	Indonisia	A.10.3.2 System acceptance	NA	NA	Post Peview Regulation of the Data Center
			(2) Benchmarks for periodic review of system performance.	Bank should review their existing systems to determine whether they satisfy current and projected bank needs.	Pilipinas	A.10.3.1 Capacity management	6.3 Service continuity and availability management	NA	Capacity Regulation of the Data Center
				Bank should monitor and supply the network capacity which can satisfy the demand.	Japan				
			(3) Reports of incidents and complaints about IT services.	The help desk should record and track incoming problem reports.	USA	A.13.2 Management of information security incidents and improvements	7.2 Business relationship management	NA	Business Relationship Regulation of the Data Center
				Consider monitoring of the following areas: . Volume and type of customer complaints, including time to successful resolution.	USA				
			(4) Reports of internal audit, external audit, and issues indentified by CBRC.	The board should approve written information security policies and the written report on the effectiveness of the information security program at least annually. The annual approval should consider the results of management assessments and reviews, internal and external audit activity related to information security,	USA	A.15.3 Information systems audit considerations	4.4 Continual improvement (Act)	NA	Security Audit Regulation of the Data Center
				Internal audit function.	Hong Kong				

Figure 8. Example of Regulatory Compliance Information Base

4.2 Operational Risk Baseline

The paper introduces a quantitative risk assessment method based on assets and researches specific embodiments in the large-scale data center. It sets up the operational risk baseline from the perspective of assets, threats and vulnerabilities, summaries and consolidates risk identifying experience, which promotes the standardization of risk identification.

Regarding the risk assessment method, according to the operational risk baseline, we introduce a quantitative risk assessment method based on assets, through which we could comprehensively identify and quantitatively calculate the risks of assets facing.

On the other hand, we create a semi-quantitative risk assessment method by combining current qualitative assessment method with assets-based quantitative assessment method.

As to qualitative assessment results, we analyze it again from aspects of assets, threats and vulnerabilities in combination with operational risk baseline in accordance with assets-based quantitative risk assessment process, so as to clarify the qualitative risk involved assets and to evaluate risk level. By using and combining the two assessment methods, we can identify operational risk in a more comprehensive, complete and accurate manner.

(1) Quantitative Risk Assessment Model Based on Assets

As the species and quantity of information assets of commercial bank data center are numerous, the threat has its particularity, and integrity requirements for risk identification is high, therefore, in the process of applying the model, the asset identification, vulnerability and threat identification, risk identification three aspects are the most critical.

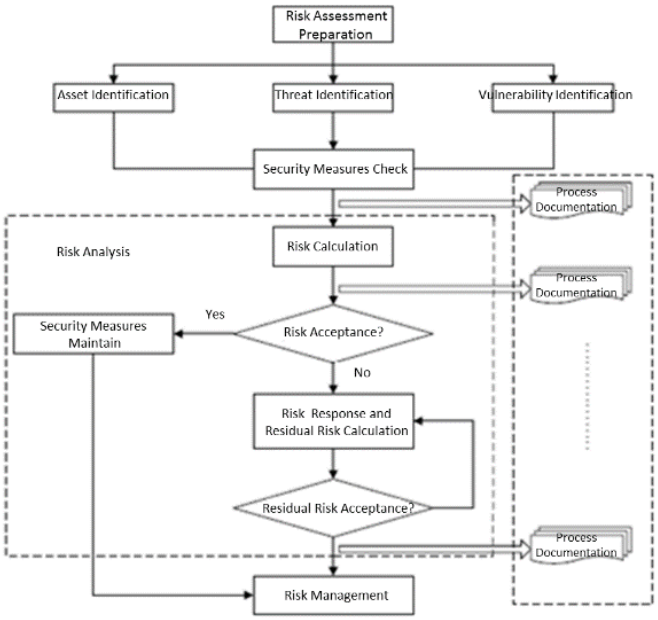

Figure 9. Quantitative Risk Assessment Model Based on Assets

(2) Semi-quantitative Risk Assessment

To ensure the integrity of the results of the operation and maintenance risk identification, this paper take advantage of the information systems potential risks inspected by the first-line maintenance personnel themselves according to their actual production experience, the risk inspected in this way with high accuracy, high dangerous characteristics, which is another source of operation and maintenance risk. But the self-assessment (qualitative assessment) result has the following problems:

ⅰ. Because the risk proposed by operation and maintenance personnel is not limited to their own section line operation and maintenance areas, such as the application line staff may propose system-level issues, therefore we need to integrate risk. Meanwhile, as the risks description of self-assessment (qualitative assessment) is not corresponding to assets, it is difficult to ensure that the integration work without omission or inaccuracy.

ⅱ. Although the risk actually exists, but some disposal costs of the risk may far outweigh the impact of it, whether the risk is within the scope of the Bank's risk tolerance can't be determined only by qualitative description.

ⅲ. Because there is no corresponding asset, the risk needed disposal cannot be accurately determined what threats, vulnerabilities it may face and what level it should be set. Accordingly, it is impossible to determine whether the disposal should be taken, what the priority is, how to compare with the qualitative risk characterization.

To solve the above problems, quantitative risk assessment methodology and existing asset-based qualitative assessment methods are combined to form a semi-quantitative assessment method, as shown in picture 10. Each result of the qualitative assessment, will be re-quantified from the angles of asset, threat and vulnerability, determine the scope of the qualitative risk's impact, quantify the impact level, and improve the accuracy of risk identification clearly.

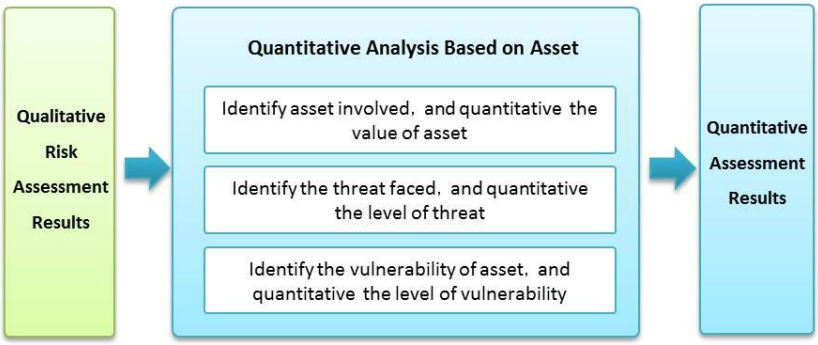

Figure 10. Semi Quantitative Risk Assessment Method

4.3 Security Technology Standard Baseline

As for the security technology standard, we establish security technology standard baseline for mainframe and open platforms, by taking reference of international standards ISO27001, the CBRC "commercial bank information technology risk management guidelines", PBoC "Guiding Opinions on Further Strengthening the banking organization's information security work", information security control standards GSD331 of the IBM methodology "IBM ISeC information security controls system". The baseline covers 402 security configuration requirements from 26 realms, including 224 requirements of mainframe, 119 requirements of open platforms, and 59 requirements of network. Configuration items and examples of the security standard relating to user ID and authentication is shown in figure 11.

User ID

Index	System Parameter	Description	Configuration Requirement	Environment I	Environment II
1	UID	The unique identification (UID) of all system users.	The UID of all system users must be unique.	√	√

Password

Index	System Parameter	Description	Configuration Requirement	Environment I	Environment II
1	maxage	The longest period of validity (week)	4	√	
2	minage	The shortest period of validity (week)	0	√	
3	minlen	The shortest length	8	√	√
4	minalpha	Contain at least a specified number of letters	1	√	√

Figure 11. Example of Commercial Bank Data Center Security Standards Baseline

5. Control Measures of Commercial Bank Data Center

This article takes the following control measures to process the operational risks and compliance risks that identified by 26 control targets. For the risks solvable, we set improvement tasks to eliminate potential risks in management and technical two levels through system specification and technology tools. For the risks unresolvable temporarily, we take risk responses to reduce the risk pressure.

Take compliance risk as an example. A large domestic commercial bank is gradually concentrating oversea information systems to achieve centralized operation. It establishes regulatory compliance baseline by analyzing individual countries' regulatory requirements, and conduct a comprehensive assessment by using the regulatory compliance baseline. Nonconformities are found and disposed with these following manners:

(1) By taking measures to make-up and modify the policy to improve the non-conformance term. For example, about the frequency of emergency drills, domestic regulatory requires all information systems should be covered every three years, and

overseas regulatory requires, such as Japan, Malaysia only require periodic drills and qualitative assessment, Singapore, Hong Kong, Panama, Australia only require drills should be tested once a year, British requires a higher frequency that for banks, drills should cover 75% of business functions in the past two years. By taking the rule of "on high not low", the existing emergency management policy was revised, different frequency of emergency drills are set for the systems of different countries separately. Annual emergency exercise plan should be set with the requirement that at least 50% of overseas business and all information relating to that should be covered, and 75% of business should be implemented emergency drills within two years to ensure that international regulatory requirements are met.

(2) As to the non-conformities which cannot be improved by management, we deploy technology tools to complete the rectification. For example, American regulators clearly request “There should be available tools to analysis log and provide specific activity monitoring”, Singapore regulators request “It should be to identify unauthorized modification of critical IT resources (such as database, system program or database file) by using the security monitoring tools”. This requires commercial banks to deploy professional security log management system, which will realize log statistics, analyzing and monitoring, and complete monitoring of critical IT resources.

(3) For these requirements which are too picky to achieve or cannot be achieved in a short time, according to risk tolerance we need take the necessary measures to reduce risk, then accept the risk and prepare for the supervision. For example, The US supervision requires, when banks do a BCP drill, the mimetic process status of IT system should be at the peak of average daily volume, and detecting the capacity of system to ensure RTO and RPO of system and business can be reached. However, there is a resource gap between disaster environment and production environment, and we need to think about the input and output, so it is difficult to provide such a condition in a short time which can support the transaction peak. We need take action to deal with risk. On the basis of normal service, by researching the relationship between transactions of drill and daily trading volume peak, the coverage of the daily transaction type in the drill, the relationship between transactions of drill and system capacity, designs the more scientific scheme of disaster drill, ensures the rationality of verification of drill, and satisfies overseas' supervision requirements.

6. The Continuous Improvement Measures of Commercial Bank Data Center Risk Management System

Risk management is a continuous improvement process, we design the sustainable regularly improvement mechanism, the trigger improvement mechanism based on incidents, the comprehensive security audit mechanism (shown in figure 12) to detect and reform the risk management issues, to ensure the continuous improvement of commercial bank data center risk management system.

Figure 12. The Continuous Improvement Measures of Commercial Bank Data Center Risk Management System

(1) The sustainable regularly improvement mechanism: Promote the continuous improvement of risk management system through full safety awareness through education, the linkage with the first team, regular assessment and review three methods.

(2) The trigger improvement mechanism based on incidents: Focus on the related incidents of risk management, establish trigger improvement mechanism for internal and external events, to improve the baseline of existing risk management and the effectiveness of control measures.

(3) The comprehensive security audit mechanism: Supervise the effective implementation of risk control measures covering all aspects of production and operation and maintenance activities by means of continuous self-examination by the team, the audit team regularly sampling and key areas of operation and maintenance of the special inspection.

7. Summary

This article establishes a set of risk management system for commercial bank data center based on the standard risk management method. The system takes risk baseline as core, covers management framework, risk baseline, control methods, continuous improvement, consolidates risk assessment experience, reduce the dependency on auditor's skills, improve the standardization level of risk assessment. With a unified management framework, comprehensively identify the compliance risk and operational risk of commercial bank datacenter. This could make a definite object in view for risk control and keep the baseline up to date with continuous improvement.

Reference

[1] Q. Yan, C. Xie and X. Luo, "Research on Banking Industry Financial Institutions IT Risk Supervision", Beijing: China Finance Publishing House, **(2013)**.
[2] COSO, Enterprise Risk Management – Integrated Framework.
[3] Z. Huang, J. Hu and X. Yu, "Information System Audit", Liaoning: Dongbei University of Finance And Economics Press, **(2012)**.
[4] S. Qiu, "Internal Control and Operational Risk Management—Operational Practical Guide", Beijing: Enterprise Management Publishing House, **(2013)**.
[5] G. Wang and S. Xian, "Global Information System Audit Guide", Beijing: China Times economy Publishing House, **(2010)**.

[6] S. Ping, "Commercial Banks Compliance Risk Management", Beijing: China Finance Publishing House, **(2010)**.
[7] H. Men, "Information Security Risk Assessment", Beijing: China Standard Press, **(2004)**.
[8] Z. Zhang and D. Zhao, "Information Security Management and Risk Assessment", Beijing: Publishing House of Electronics Industry, **(2013)**.
[9] J. Li, "A Study on Internal Control Evaluation of Commercial Banks from View of Internal Audit", Beijing: Economic Science Press, **(2011)**.
[10] T. Wulgaert, "Security Awareness: Best Practices to Secure Your Enterprise", USA: ISACA, **(2005)**.
[11] G. Hamel, "The Future of Management", USA: Harvard Business Review Press, **(2007)**.
[12] D. W. Karolak, "Software Engineering Risk Management", USA: IEEE Computer Society Press, **(1995)**.
[13] G. Hamel, "What Matters Now: How to Win in A World of Relentless Change, Ferocious Competition, and Unstoppable Innovation", USA: Jossey-Bass, **(2012)**.