Guidelines for Banking Financial Institutions

Information System Risk Management

CBRC [2006] No. 63

银行业金融机构信息系统风险管理指引

银监发［2006］63 号 2006 年 8 月 7 日

Chapter One General Provisions

Article 1 In order to prevent the risk created during the process of banking financial institutions that utilize information system to process business, operate management and internal controls; promote safe, continuous and healthy operation of Chinese banking industry, this guideline is formulated according to "*Banking Supervision Management Law of the People's Republic of China*", relevant requirements of national information security, and laws and regulations of information system management.

Article 2 This guidelines applies to banking financial institutions.

Banking financial institutions in this guideline refer to policy banks and financial institutions, established in People's Republic of China, that absorb public deposits, such as commercial banks, urban credit cooperation, rural cooperative banks, and rural credit cooperatives.

Financial asset management company, trust and investment corporation, finance corporation, financial lease company, auto financing company which are established in the People's Republic of China as well as other financial institutions that are approved by China Banking Regulatory Commission (Abbreviated as CBRC) or its agencies are also applicable to this guideline.

reputation risks that are caused by information system, because of technical and managerial defects, during the planning, research, construction, operation, maintenance, monitoring and quitting process.

Article 5 Goal of information system risk management is to realize the identification, measurement, evaluation, warning and control of information system risk by establishing efficient mechanism, so as to promote business innovation of banking financial institutions, improve information level, and enhance core competitiveness and sustainable development abilities.

Chapter Two Institutions' Responsibilities

Article 6 Banking financial institutions shall establish effective information system risk management framework, complete internal organizational structure and working mechanism, and prevent and control information system risks.

Article 7 Banking financial institutions shall perform the following information system management responsibilities seriously.

(1) Implementing relevant national laws, regulations and technical standards related to information system management and committing relevant supervision requirements of CBRC.

(2) Establishing effective information security system and internal control regulations; defining information system risk management post responsibility system; supervising and implementing it.

(3) Being responsible for inspection, evaluation and analysis of this institution's information system risks; submitting relevant management information to special committee of this institution AND CBRC and its agencies.

(4) Making quick responses to major information system accidents or emergencies to CBRC and its agencies according to pre-arranged planning.

(5) After annual investigation of the board or other policy-making bodies, submitting annual report of information system risk management to CBRC and its agencies.

(6) Implementing information system audit work of this institution well.

(7) Implementing information system risk supervision and inspection by coordinating CBRC and its agencies, and rectifying according to supervision advices.

(8) Organizing employees of this institution's information system for business, technical and security training about information system.

(9) Implementing other work related to information system risk management.

Article 8 The board of banking financial institutions or other policy-making bodies are responsible for strategic planning, major projects and risk supervision management of information system; Information Technological Management Committee, Risk Management Committee or other specialized committees that are responsible for risk supervision shall formulate general strategy of information system, plan information system project construction, assess and report information system risk situation of this institution regularly so as to provide suggestions to the decision-making level to adopt corresponding risk control measures.

Article 9 Legal representative or responsible-person of banking financial institutions shall be the person in charge of information system risk of this institution.

Article 10 Banking financial institutions shall set up Department of Information Technology, being responsible for planning, research, operation, maintenance and monitoring of information system in this institution and providing daily scientific service and operation technical support; establishing or defining specialized information system risk management department, setting up and perfecting information system risk management rules and regulations, assisting operation department and information science department to implement strictly; providing relevant regulation information; setting up auditing department or specialized auditing posts; establishing and perfecting information system risk auditing system, equipping appropriate qualified personnel for information system risk auditing.

Article 11 Personnel engaged in information system in banking financial institutions shall conform to the following requirements:

(1) Possessing good professional ethics; grasping and implementing professional knowledge and skills required by relevant posts of information system;

(2) People without training or unqualified trainees shall not take up their posts; employees that are unqualified during assessments shall be adjusted in time.

Article 12 Banking financial institutions shall reinforce the professional team building of information system risk management; establish incentive mechanism for talented people and adapt to development of information technology.

Article 13 Banking financial institutions shall disclose conditions of information system risks according to relevant laws and regulations timely and normatively.

Chapter Three Overall Risk Control

Article 14 Overall risks refer to the risks of information system in areas such as strategy, system, generator room, software, hardware, Internet, data and document that may influence the overall or shared risks.

Article 15 Banking financial institutions shall formulate clear and continuous risk management strategy according to the overall plan of information system; analyze and evaluate each integrated element according to sensitivity of information system; and implement effective control.

Article 16 Banking financial institutions shall adopt measures to prevent natural disasters and security threats created by operating environment changes so as to prevent various emergencies and hostile attacks.

Article 17 Banking financial institutions shall establish and perfect relevant rules and regulations, technical specifications, operating instructions of information system as well as define duties and authorities of relevant information system employees; establish restriction mechanisms and implement minimum authorization.

Article 18 Chinese banking financial institutions established overseas or overseas banking financial institutions established in China shall prevent against cross-border risks created by differences between domestic and foreign regulatory systems of information system.

Article 19 Banking financial institutions shall strictly execute relevant standards of national information security; refer to relevant international standards; propel information security standardization actively and implement classified protection of information security.

Article 20 Banking financial institutions shall reinforce evaluation and testing of information system; repair and update in time so as to guarantee the security and integrity of information system.

Article 21 Banking financial institutions' information system data center machine-room shall conform to national technical standards of computer site, environment, power supply and distribution and so on. National data center shall reach national A-type machine-room at least; provincial data center shall reach national B-type machine-room at least; Below-provincial data center shall reach national C-type machine-room at least. Data center machine-room shall implement strict entrance guard management measures, and no one is allowed to enter without authorization.

Article 22 Banking financial institutions shall value intellectual property protection; use copyrighted software; strengthen software version management and use software and hardware with Chinese propriety intellectual property

shall be reserved.

Article 48 After a period of information system production, banking financial institutions shall organize post evaluation to the system, and adjust and optimize the system functions according to evaluations.

Article 49 Banking financial institutions shall implement daily routine-inspection to room environment, define emergency processing procedures and plans of information system and room environment facilities when emergencies happen; data center with real-time transaction service shall implement 24-hour duty.

Article 50 Banking financial institutions shall implement event report system; when major economic or reputation losses or major influence accidents happen, they shall be reported and handled immediately; emergency processing plans shall be launched when necessary.

Chapter Six Outsourcing Risk Control

Article 51 Outsourcing risks refer to the risks formed when banking financial institutions entrust the programming, research and development, construction, operation, maintenance and monitoring to business partners or external technical suppliers.

Article 52 When banking financial institutions are outsourcing information system, they shall confirm principles and scope of outsourcing, analyze and evaluate potential risks of outsourcing, establish and complete relevant rules and regulations and formulate corresponding risk prevention measures according to risk control and real requirements.

Article 53 Banking financial institutions shall establish and complete outsourcing contractor assessment mechanism; investigate and evaluate management conditions, financial abilities, integrity history, security qualifications, technical service abilities, real risk control and responsibility undertaking abilities of the contractor; and conduct necessary due diligence. The evaluation work can be delegated to independent agencies with relevant professional experiences and whose qualifications are identified by relevant national regulatory authorities.

Article 54 Banking financial institutions shall sign written contract with contractors; define both parties' rights and obligations; and regulate contractor's rights and obligations in security, confidentiality and intellectual property.

Article 55 Banking financial institutions shall fully aware of the direct and indirect influences of outsourcing services on information system risk control; and include them into the overall security strategy and risk control.

propose evaluations and suggestions. System audit before information system production shall pay attention to security control, permission setting, validity, consistency, integrity, auditable-ness and timeliness of information system.

Key points of system audit before production:

(1) Possibility of being hedged by the outside;

(2) Design loopholes and defects in inner security control;

(3) Problems at project security development management;

(4) Efficiency and efficacy;

(5) Whether functions, design and workflow conform to laws, regulations and whether regulations of inner control have continuous compatibility.

(6) Other contents that need special audit.

Article 65 System audit documents and materials before production include:

(1) Feasibility report;

(2) Project requirement specifications;

(3) Project function specifications (including risks in business, technology and control measures);

(4) Overall technology framework;

(5) Project design specifications;

(6) Project implementation plan;

(7) Outsourcing agreement signed with the third party;

(8) Testing plan and inspection report;

(9) Production plan;

(10) Meeting minutes of project development regular meeting;

(11) Operation manual;

(12) Other documents and materials that need to be audited. As to the documents and materials with large quantities of content, data processing procedures of key transactions, transaction port and other important security matters need to be audited.

Article 66 System audit after production refers to the audit after a period that

the information system has been launched into production; the aim is to evaluate whether control of all risks of information system is appropriate; whether it can realize scheduled design goal. System audit after production shall be conducted half a year after information system is launched into production; audit report shall propose the audit suggestions, to the information systems being audited, such as increasing or changing risk control and whether production can be continued.

Article 67 Information system special risk audit refers to investigation, analysis and evaluation to the units being audited after information security accidents happen, or the audit that the previous information system has major structural adjustments, or audit department believes that certain special subject of information system needs to be audited.

Article 68 Information system risk audit of banking financial institutions can also be conducted by intermediary appraisal agencies with legal qualifications, which are entrusted and authorized by CBRC or its agencies, according to laws, regulations and rules.

Article 69 When intermediary agencies, entrusted or authorized by CBRC or its agencies, conduct the audit to banking financial institutions, they shall show the entrusting authorization; and audit according to the authorization and specified scope on the entrusting authorization.

Article 70 The audit reports issued by the intermediary agencies according to the authorization, after audited-approved by CBRC and its agencies, possess legal forces; the financial institutions being audited shall propose rectification suggestions within legal time according to the audit reports; and shall rectify in time according to suggestions in the audit reports.

Article 71 The intermediary agencies shall implement laws and regulations strictly; and protect the business secrets and risk information of the institutions being audited. Reading materials during the audit process shall have hand-over procedures; it must not be taken away from the scene or modified or copied.

Chapter Eight Supplementary Articles

Article 72 Interpretation and revision of this guideline is under the charge of China Banking Regulatory Commission.

Article 73 This guideline shall take effect from the issuing date.

END

This is an excerpt of the PDF (Some pages are marked off intentionally)

------ The End ------