JR

ICS
A11
Record No.:

BANKING INDUSTRY STANDARD

OF THE PEOPLE'S REPUBLIC OF CHINA

JR/T 0044-2008

Management Specification of Information System Disaster Recovery for Banks

银行业信息系统灾难恢复管理规范

Issued on: February 4, 2008 **Implemented on: February 4, 2008**

Issued by: The People's Bank of China

Table of Contents

Foreword

This Standard is the description for the management specification of information system disaster recovery for banks.

This Standard was proposed by the People's Bank of China and is under the jurisdiction of National Technical Committee on Financial of Standardization Administration of China.

This Standard is approved by the People's Bank of China.

Drafting organization of this Standard: The People's Bank of China

Participating drafting organization of this Standard: Global Data Solutions Limited (Shenzhen).

Chief drafting staffs of this Standard: Wen Sili, Li Xiaofeng, Yang Hong, Guo Quanming, Cao Xuhui, Li Jian, Yuan Huiping, Wang Qi, Yu Jian, He Zheng, Liu Donghong, Gao Yong, Chen Tianqing, Kang Tanyun, Wang Zheng, Zhang Yan, Zhu Yiqiang, Zhou Heng, Wang Xiong and Liu Pengpeng.

Management Specification of Information System Disaster Recovery for Banks

1 Scope

This specification specifies the management requirements of information system disaster recovery for banks.

This specification is applicable to the People's Bank of China and banking financial institutions (including foreign-funded banks, hereinafter referred to as "organizations") established within the territory of the People's Republic of China.

2 Normative Reference

The following normative document contains the provisions which, through reference in this text, constitute the provisions of this Standard. For dated references, the subsequent amendments (excluding corrigendum) or revisions of these publications do not apply. However, all parties who reach an agreement according to this Standard are encouraged to study whether the latest edition of the normative document is applicable. For undated references, the latest edition of the normative document applies.

GB/T 20988-2007 Information Security Technology - Disaster Recovery Specifications for Information Systems

3 Terms and Definitions

3.1

Information system

A man-machine system that collects, processes, stores, transmits and retrieves information according to certain application objective and rule; it is consisted of computer system, network system software and hardware and their relevant equipment and facilities, application software etc.

3.2

Disaster

Emergency incidents, manually or naturally caused and last for certain time, which

cause major failure and breakdown of information system, bad data damage or stop the business functions supported by information system or make the service level reach unacceptable degree.

3.3

Disaster recovery

DR

Activity and process that are designed to recover the information system from operation failure or unacceptable state caused by disaster to normal operation state and recover the business functions it supports, from abnormal state caused by disaster to acceptable state.

3.4

Disaster recovery planning

DRP

Pre-incident plan and arrangement that are prepared to avoid loss brought about by disaster, and ensure the timely recovery and continuous operation of critical business functions supported by information system after occurrence of disaster.

3.5

Regional disaster

Incident that causes severe damage to communication, electric power, traffic and other critical infrastructure or mass evacuation in its location or closely related adjacent regions and resulting in failure of maintaining the normal operation of information system. E.g., earthquake, large public health incident, terrorist attack, regional communication network failure and grid failure, etc.

3.6

Risk analysis

RA

Process that determines the risk affecting the normal operation of information system, assessing the function vital to the business operation of organizations and defining the control measures reducing the potential hazards. Risk analysis frequently involves the assessment of special incident probability.

3.7

Business impact analysis

BIA

Analyzing business functions and their relevant information system resources and assessing the impact of specific disaster on various service functions.

3.8

Critical business functions

The service or function which will significantly affect the organization operation once it is interrupted for certain time.

3.9

Production system

Information system that supports the production operation of organizations under normal conditions, including master data, master data processing system and master network.

3.10

Production center

Data center where production system is located.

3.11

Backup center for disaster recovery

Locations where replace the production center to process data and support the operation of critical business functions in case of disaster, including backup data center, backup working environment, backup living facilities, etc. The formation of disaster recovery capability also requires to allocate relevant business and technical personnel and establish corresponding operation mechanism.

3.12

Backup for disaster recovery

Backup measures for data, data processing system, network system, infrastructure and business/technical and other relevant personnel to recover disaster.

3.13

Backup system for disaster recovery

Information system that is composed of data backup system, backup data processing system, backup network system and etc. for purpose of disaster recovery.

3.14

Disaster recovery plan

Pre-established action plan (hereinafter referred to as "plan") that defines the organization, process and resource required for information system disaster recovery. It is used to guide relevant personnel to recover critical business functions supported by information system within the disaster recovery objective.

3.15

Regional backup

The production center and backup center for disaster recovery where are located in the same geographic region and are threatened by the same regional disaster risk. Generally, they are within tens of kilometers from each other and can realize synchronous data replication.

3.16

Non-regional backup

The production center and backup center for disaster recovery where are located in different geographic regions and generally will not be threatened by the same regional disaster risk simultaneously. Generally, the distance between them is more than hundreds of kilometers.

3.17

Recovery time objective

RTO

The time from breakdown to required recovery of information system, after the occurrence of disaster.

3.18

Recovery point objective

RPO

The time point requirements for data recovery after the occurrence of disaster.

3.19

Outsourcing for disaster recovery

Select external resources to provide disaster recovery services, such as undertaking

4 Overview of Information System Disaster Recovery for Banks

4.1 Disaster Recovery Contents

Disaster recovery mainly includes the following contents:

- Establishment and responsibilities of organizational institution;
- Analysis of disaster recovery demand;
- Development of disaster recovery strategy;
- Implementation of backup system for disaster recovery;
- Operating maintenance of backup center for disaster recovery;
- Establishment, exercise and management of disaster recovery plan;
- Emergency response and disaster recovery.

4.2 Periodic Duty for Disaster Recovery

4.2.1 Demand analysis

Demand analysis for disaster recover mainly includes risk analysis and business impact analysis.

The disaster recover demand shall be periodically reanalyzed with the maximum reanalysis period of three years. Where the production center environment, production system or business process is significantly changed, the organization shall immediately start the reanalysis of disaster recovery.

4.2.2 Strategy preparation

The organization shall comprehensively plan the information system disaster recovery and prepare the uniform disaster recovery strategy. Disaster recovery strategic planning of three or more years shall meet the requirements of the minimum disaster recovery capability grade as described in 7.2.2 of this specification. The temporary disaster recovery strategy within three years may be reduced by one disaster recovery capability grade, or partial system may be reduced by one disaster recovery capability grade.

The organization shall periodically re-examine and revise the disaster recovery strategy according to the latest disaster recovery demand analysis.

4.2.3 Technical scheme management

The organization shall periodically re-examine and adjust the disaster recovery technical scheme according to the latest disaster recovery strategy.

4.2.4 Plan management

The organization shall periodically re-examine and revise the disaster recovery plan according to the latest disaster recovery strategy. The disaster recovery plan shall be examined and approved at least once annually.

4.3 Inter-organization Cooperation

The organization shall strengthen the coordination, contact, mutual cooperation and experience sharing with other organizations with business closely related to it to jointly assess the risk confronted and collaboratively prepare disaster recovery strategy to improve the overall risk prevention and disaster recovery capability of banks.

5 Establishment and Responsibilities of Organizational Institution

5.1 Establishment of Organizational Institution

The organization shall establish organizational institution of disaster recovery in combination with specific conditions and define job responsibilities. The organizational institution of disaster recovery of organization shall be exactly described in disaster recovery plan.

Organizational institution of disaster recovery shall include personnel required for the works in each stage of construction, operating maintenance, emergency response, disaster recovery and etc. Personnel concerned may be either full-time or part-time. Personnel on key posts shall be backed up.

Organizational institutions of disaster recovery of different grades may be established according to the information system and branches; e.g. multi-grade organizational institution of disaster recovery for head office and branches may be established.

5.2 Composition and Responsibilities of Organizational institution

Organizational institution of disaster recovery shall be classified into decision layer, management layer and execution layer.

a) Decision layer is mainly composed of high-level managers of the organization, deciding the significant matters concerned with information system disaster recovery; its major responsibilities are as follows:

   - Determine the disaster recovery strategy;

- Verify and approve the disaster recovery strategy;

- Verify and approve the disaster recovery budget;

- Verify and approve the construction of backup facility for disaster recovery;

- Verify and approve the disaster recovery plan;

- Approve and start the disaster recovery plan;

- Decide significant matters concerned with emergency response and recovery;

- Verify and approve external condition announcement and information release;

- Approve the restoration and return of production center.

b) Management layer is mainly composed of principals of relevant departments like business, technology and logistics in the organization. It works under the leading of decision layer and is in charge of managing and coordinating the information system disaster recovery. Its major responsibilities are as follows:

- Organize the preparation the disaster recovery strategy;

- Prepare disaster recovery budget;

- Organize the construction of backup center for disaster recovery;

- Manage the backup center for disaster recovery;

- Organize the preparation of disaster recovery plan;

- Organize the exercise of disaster recovery plan;

- Coordinate the internal and external disaster recovery resources;

- Command and coordinate emergency response and recovery;

- Command and coordinate the restoration and return of production center;

- Be responsible for announcement and communication of internal information;

- Organize and manage the media public relations;

- Supervise, inspect and summarize the disaster recovery.

c) Execution layer is mainly composed of working personnel of relevant departments like business, technology and logistics and personnel of external institutions. It is responsible for specific implementation of disaster recovery

business field and software and hardware aspects. The methods adopted for vulnerability identification mainly include: questionnaire survey, tool detection, manual checking, document review, permeability test, etc.

Vulnerability identification is mainly carried out from technical and management aspects; technical vulnerability involves the security problems of physical layer, network layer, system layer, application layer, etc. Management vulnerability may be classified into technical management vulnerability and organization management vulnerability; the former is related to specific technical activity and the latter is related to management environment.

d) Risk calculation

Risk calculation is to determine the possibility of occurrence of information system disaster caused by vulnerability exploited by threat with appropriate method and tool, mainly including the following contents:

1. Calculate the possibility of occurrence of disaster caused by vulnerability exploited by threat according to the frequency of threat occurrence and vulnerability condition;

2. Calculate the loss after disaster occurrence according to the importance degree of asset and the severity of vulnerability;

3. Calculate the risk value according to the calculated possibility of disaster occurrence and the loss of disaster and divide the risk grade.

6.1.4 Risk control

The effectiveness of existing security strategy and measure is accessed to determine the possible risk of information system, namely residual risk.

The organization shall assess the acceptable level of risk and determine the acceptable risk according to the asset class, occurrence probability of residual risk, likely loss and risk prevention cost. It shall also determine the risk prevention measure against unacceptable risk according to the balance principle between the cost of disaster recovery resources and the likely loss caused by the risk (hereinafter referred to as “Cost Risk Balance Principle”), and regularly assess the residual risk.

6.2 Business Impact Analysis

6.2.1 Business function analysis

The criticality of business function is determined through business function analysis; the analysis contents mainly include:

- Policy: policy requirements of business function;

- Business nature: core business or non-core business;

- Business service scope: involved internal and external institution, user, etc.;

- Data concentration degree: concentration of business data and processing, and geographical distribution;

- Business time sensitivity: real-time and non-real time businesses, business operation period and use frequency of user;

- Business function relevance: the relevance degree with other business functions of this organization and the business functions of other institution.

6.2.2 Assessment of business interruption impact

a) Direct and indirect economic losses which may be caused by business function interruption are assessed with quantization method, mainly including:

- Direct economic loss:

  - Asset loss;
  - Income loss;
  - Extra expense increase;
  - Financial penalties.

- Indirect economic loss:

  - Loss of prospective earnings;
  - Business opportunity loss;
  - Market share impact.

b) The impacts which may be caused by business function interruption are assessed with non-quantization method, mainly including:

- Social impact;

- Legal impact;

- Credit impact;

- Brand impact.

6.3 Determination of Disaster Recovery Demand

6.3.1 Determination of demand grade

The information system shall reach the following disaster recovery capability grade at minimum according to the disaster recovery demand grade:

a) Class I: Grade 5;

b) Class II: Grade 3;

c) Class III: Grade 2.

7.3 Layout of Backup Center for Disaster Recovery

7.3.1 Layout principle

a) The backup center for disaster recovery shall be arranged within the territory of the People's Republic of China;

b) The distance between the backup center for disaster recovery and the production center shall be reasonable, and they shall be avoided to suffer similar risks at the same time;

c) The site selection of backup center for disaster recovery shall comply with the security requirements of national strategy, and the convenience and diversity of traffic and telecommunication of production center and backup center for disaster recovery as well as external support conditions such as local business and technical support capability of backup center for disaster recovery, telecommunication resource, geographical and geological environment, public resources and service matching capability shall be taken into comprehensive consideration.

7.3.2 Layout mode

The organization shall adopt the following multiple layout modes according to the Cost Risk Balance Principle and operation management requirements:

- One master plus one backup: one production center and one backup center;

- One master plus multiple backups: one production center and multiple backup centers;

- Mutual backup: mutual backup of two production centers;

- Multiple masters plus one backup: multiple production centers share one backup center;

- Mixed mode: mix of above modes.

7.4 Acquisition and Guarantee of Resource and Service

7.4.1 Resource acquisition

outsourcing provider from the angle of guaranteeing national information security.

The service outsourcing provider for disaster recovery shall comply with the relevant service qualification requirements of the state and industry, and shall at least meet the following requirements:

a) Shall be familiar with information system architecture and business process of banking industry and have successful case and practical experience of outsourcing service for disaster recovery;

b) Shall be provided with complete information security management system and service quality guarantee system and pass through the certification of ISO 27001, ISO 9001, etc.;

c) Shall independently operate and manage the backup center for disaster recovery, the availability of computer room shall at least reach 99.9% and the disaster recovery capability grade that can be provided by it shall reach Grade 5 or above (including Grade 5).

8 Construction of Backup Center for Disaster Recovery

8.1 Infrastructure Construction

The infrastructure construction of backup center for disaster recovery includes the construction of computer room and auxiliary facilities. The site selection, planning, design, construction and acceptance of backup center for disaster recovery shall comply with the requirements of relevant standards and specifications of the state and financial industry. The availability of computer room shall at least reach 99.9%.

8.2 Construction of Backup System for Disaster Recovery

8.2.1 Technical scheme design

The technical scheme of backup system for disaster recovery is established according to the disaster recovery strategy, including data backup system, backup data processing system and backup network system. The system involved in the technical scheme shall:

- Obtain the security protection level equivalent to that of production system;

- Be provided with expandability.

8.2.2 Verification test of technical scheme

For meeting the requirements of disaster recovery strategy, verification test shall be carried out on the feasibility of critical technology application in the technical scheme, and the result of verification test shall be recorded and preserved.

The infrastructure shall be maintained regularly to ensure the availability of work facilities (electricity, communication, computer room environment, security monitoring facilities, etc.), auxiliary facilities and living facilities of backup center for disaster recovery.

9.2.2 Data backup system

The data backup system shall be detected and maintained regularly to ensure the availability of software and hardware of data backup system, and the backup data of data backup system shall be ensured to be consistent with that of production system.

Various patches, updates and changes of production system shall be timely updated to the data backup system.

9.2.3 Backup data processing system

The backup data processing system shall be detected and maintained regularly, including the detection of hardware system, system software and application software.

Various patches, updates and changes of production system shall be timely updated to the backup data processing system.

9.2.4 Backup network system

Backup network system shall be detected and maintained regularly, including data network, storage network, voice communication system, etc..

Various patches, updates and changes of production system shall be timely updated to the backup network system.

9.3 Resource Assurance of Operating Maintenance

The backup center for disaster recovery shall be provided with a certain quantity of personnel with professional quality of disaster recovery and necessary work and living facilities; sufficient operation and maintenance fund input shall be guaranteed to ensure the normal operation of backup center for disaster recovery.

10 Establishment, Exercise and Management of Disaster Recovery Plan

10.1 Establishment of Disaster Recovery Plan

10.1.1 Established contents

The organization shall combine its actually developed disaster recovery plan

organically.

10.1.3 Establishing process

a) Establishment of first draft: write the first draft of disaster recovery plan according to the disaster recovery content defined by risk analysis and business impact analysis and the requirements of disaster recovery capability grade in combination with other correlated emergency plans of the organization;

b) Evaluation of first draft: evaluate the integrity, usability, definiteness, effectiveness and compatibility of first draft of disaster recovery plan;

c) Revision of first draft: revise the plan according to the evaluation result, correct the problems and defects found during the first draft evaluation process, thus forming the revised draft of plan;

d) Test and verification of plan: establish test case and carry out basic unit test, associated test and integrity test to verify the rationality and effectiveness of plan. The entire test process shall be provided with detailed record and test report shall be formed;

e) Examination and approval of plan: further improve the revised draft of plan according to the test record and report to form the draft plan for approval; the decision layer of the organization examines and approves the tested and verified disaster recovery plan and determines it as the implementing draft of plan.

10.2 Exercise of Disaster Recovery Plan

10.2.1 Exercise purpose

The exercise aims at verifying the integrity, usability, definiteness, effectiveness and compatibility of the disaster recovery plan and improving the plan executive capacity of the organization.

10.2.2 Exercise form

The exercise includes prior-notice and non-prior-notice exercise of correlated personnel. Main forms of exercise include:

a) Table-top exercise: organize correlated disaster recovery personnel of organizational institution to simulate various disaster scenes in conference form, focus on discussing the management, command and coordination of emergency response and recovery process, and verify the decision-making and command capability of disaster recovery plan;

b) Simulating exercise: simulate the disaster scene and utilize the backup system

strengthen the communication;

c) Rapidly mobilize and effectively allocate disaster recovery resource;

d) Announce correlated competent departments according to the requirements of related system and complete social announcement and client service work;

e) Dispose the disaster incident reasonably and closely trace the situation change and recovery progress;

f) Switch the decision into backup center for disaster recovery to substitute the operation based on the principle of minimum impact and loss.

Refer to Appendix A.2 for specific working focus for disaster recovery.

11.3 Restoration and Return

11.3.1 Restoration of production system

The organization shall assess the loss caused by the disaster after its occurrence, the assessment contents mainly include:

a) Disaster damage condition;

b) Business impact degree;

c) Probability of in-situ restoration or new site selection;

d) Saved equipment list and test conditions.

The organization shall, according to loss assessment condition in combination with maximum continuous operation time of backup system for disaster recovery, determine the repair or restoration scheme of production system and implement restoration and function recovery of production system.

11.3.2 Return of production system

Main return contents of production system include:

- Test of restored system;

- Network return switching;

- System return switching;

- Data return switching to inspect backup data in the system;

- Business function switching;

- Secure disposal of related data to avoid leakage of important information;

- Backup system for disaster recovery under backup state;

- Evacuation of personnel and important equipment.

12 Supervision and Management

12.1 Audit

The audit of disaster recovery is divided into internal audit and external audit. Internal audit is organized and implemented by internal personnel in the organization, while external audit is organized and implemented by the intermediary possessing the qualification confirmed by corresponding national supervision department.

Audit work mainly includes the following contents:

- Risk assessment and control;

- Organization cooperation and authorization mechanism;

- Disaster recovery strategy;

- Construction of system for disaster recovery

- Management and maintenance of disaster recovery plan;

- Exercise organization and assessment;

- Availability and effectiveness of backup center for disaster recovery.

The organization shall determine the audit frequency according to the condition of disaster recovery of information system. The organization shall organize internal audit for disaster recovery at least annually.

Conclusion for disaster recovery audit work shall be formed into audit report which shall be filed as the achievement of internal risk control measures and may be incorporated into annual audit of IT system.

Data retrieval involved during the audit process shall be provided with handover procedure, the preservation and distribution of secret data in the audit process shall be controlled strictly, the intermediary shall keep the business secret and risk information of the audited company.

12.2 Recording

The disaster recovery condition of the organization shall be reported to the People's Bank of China by the end of each year, and the main contents include:

- Construction of backup center for disaster recovery of the organization and

Appendix A

(Informative)

Working Focuses of Emergency Response and Disaster Recovery

A.1 Working focuses of emergency response

A.1.1 Incident report and inspection

a) Emergency incident is reported immediately according to emergency incident reporting process of the organization.

b) Emergency response personnel shall record the incident information and carry out the following main works:

- Judge the incident type: e.g. network system failure, infrastructure failure, server hardware failure, application software failure, artificial damage, natural disaster, etc.;

- Analyze incident impacting area as well as business scope and degree to determine incident severity;

- Preliminarily diagnose the cause of incident;

- Assess incident impact and loss;

- Analyze the expected recovery time of business function.

c) Organize on-site inspection and assessment, form emergency incident report, report to the decision layer or management layer and propose the next working suggestion;

A.1.2 Pre-warning and rescue

a) Pre-warning release

- Announce emergency incident conditions to relevant department of the organization;

- Send warning information to external business affiliates;

- Inform relevant personnel for emergency response to gather at designated place and start the rescue;

A.2.3 Personnel contact and gathering

Complete personnel contact and gathering according to personnel notification mode in disaster recovery plan.

A.2.4 Resource dispatching

Uniformly dispatch and purchase all resources for disaster recovery and complete the resource management and dispatching.

A.2.5 Disaster recovery command

The disaster recovery team shall carry out the command, coordination and management according to the requirements plan disaster recovery plan.

Personnel at executive layer shall carry out the recovery work according to the system and business priority orders specified in the plan and report the work schedule at any time.

A.2.6 Information system recovery

Recover the information system according to recovery priority order.

A.2.7 Successful recovery announcement

After the backup system for disaster recovery is put into operation, ensure to provide various technical supports and security works and timely announce correlated management and business departments to cooperate and complete the business function recovery.

A.2.8 Process record and data filing

Strictly record all information and disposal process related to the incident for future reference.

Appendix B

(Informative)

Relationship between RTO/RPO and Disaster Recovery Capability Grade

B.1 Relationship between RTO/RPO and disaster recovery capability grade

The organization may refer to Table.1 to determine the disaster recovery capability grade of information system according to RTO and RPO:

Table B.1 Relationship between RTO/RPO and Disaster Recovery Capability Grade

Disaster recovery capability grade	RTO	RPO
1	2d above	1-7d
2	24h above	1-7d
3	12h above	Several hours to 1d
4	Several hours to 2d	Several hours to 1d
5	Several minutes to 2d	0-30min
6	Several minutes	0

_____ END _____