

**INDUSTRY STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

JR/T 0044-2008

**Management specification of information system disaster
recovery for banks
(English Translation)**

Issued on: February 4, 2008

Implemented on: February 4, 2008

Issued by: The People's Bank of China

Table of Contents

Foreword...	4
Introduction...	5
1 Scope...	6
2 Normative Reference...	6
3 Terms and Definitions...	6
4 Overview of Information System Disaster Recovery for Banks...	11
5 Establishment and Responsibilities of Organizational Institution...	12
6 Demand Analysis of Disaster Recovery...	14
7 Establishment of Disaster Recovery Strategy...	19
8 Construction of Backup Center for Disaster Recovery...	23
9 Operating Maintenance Management of Backup Center for Disaster Recovery...	24
10 Establishment, Exercise and Management of Disaster Recovery Plan...	25
11 Emergency Response and Disaster Recovery...	30
12 Supervision and Management...	32

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.

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.

4.1 Disaster Recovery Contents

Disaster recovery mainly includes the following contents.

4.2.1 Demand analysis

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

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.

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.

5.1 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.

6.1.1 Determination of risk analysis objective

The organization shall make clear the risk analysis objective and comprehensively identify the disaster risk threat and vulnerability of information system according to the strategic objective of long-term sustainable development and information construction.

6.2.1 Business function analysis

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