

ICS 35.040
CCS L 80



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

GB/T 20988-2007

**Information security technology - Disaster recovery
specifications for information systems
(English Translation)**

Issued on: June 14, 2007

Implemented on: November 1, 2007

**Issued by: General Administration of Quality Supervision, Inspection and
Quarantine of PRC**

Table of Contents

Foreword...	3
Introduction...	4
1 Scope...	5
2 Normative references...	5
3 Terms and definitions...	5
4 Overview of disaster recovery...	9
4.1 Work scope for disaster recovery...	9
4.2 Organization of disaster recovery...	10
4.3 Management of disaster recovery planning...	11
4.4 External collaboration for disaster recovery...	11
4.5 Audit and filing of disaster recovery...	12
5 Determination of disaster recovery needs...	12
5.1 Risk analysis...	12
5.2 Business impact analysis...	12
5.3 Determine disaster recovery objectives...	13
6 Development of disaster recovery strategy...	13
6.1 Elements for developing disaster recovery strategy...	13
6.2 Method to obtain disaster recovery resources...	14
6.3 Requirements for disaster recovery resources...	16
7 Implementation of disaster recovery strategy...	17
7.1 Implementation of technical solution for backup system for disaster recovery...	17
7.2 Selection and construction of backup center for disaster recovery...	18
7.3 Implementation of professional technical support capabilities...	19
7.4 Implementation of operation, maintenance, management capabilities...	19
7.5 Implementation of disaster recovery plan...	20
Appendix A (Normative) Classification of disaster recovery capability grades	23
Appendix B (Informative) Framework of disaster recovery plan...	29

Foreword

Appendix A of this standard is normative. Appendix B and Appendix C are informative.

This standard was proposed by and shall be under the jurisdiction of the National Information Security Standardization Technical Committee.
Drafting organization of this standard. China Information Security Product Evaluation and Certification Center.

1 Scope

This standard specifies the basic requirements for the disaster recovery of information system.

This standard applies to the planning, approval, implementation, management of disaster recovery of information system.

2 Normative references

The provisions in following documents become the provisions of this Standard through reference in this Standard. For the dated references, the subsequent amendments (excluding corrections) or revisions do not apply to this Standard; however, parties who reach an agreement based on this Standard are encouraged to study if the latest versions of these documents are applicable. For undated references, the latest edition of the referenced document applies.

GB/T 5271.8 Information technology - Vocabulary - Part 8.security

GB/T 20984 Information security technology - Risk assessment specification for information security

3 Terms and definitions

The terms and definitions as established in GB/T 5271.8 as well as the following terms and definitions apply to this standard.

3.1

Backup center for disaster recovery

Alternate site

A site used to take over the primary system for data processing and support critical business functions (3.6) after a disaster, which can provide the

backup system for disaster recovery (3.3), backup infrastructure and technical support and operational maintenance management capabilities, or alternate living facilities in or around the site.

3.2

Backup for disaster recovery

The process of backing up data, data processing systems, network systems, infrastructure, professional technical support capabilities, operational management capabilities for disaster recovery (3.9).

3.3

Backup system for disaster recovery

For the purpose of disaster recovery (3.9), an information system which consists of a data backup system, a backup data processing system, a backup network system.

3.4

Business continuity management

BCM

An overall management process to protect the organization's interests, reputation, brand, value creation activities, identify the threats which have potential impact on the organization, provide a framework for establishing and organizing an effective reaction recovery capability. This includes an overall process of the organization's management for recovery or continuity when facing disaster as well as the training, drill, inspection to guarantee the effectiveness of the business continuity plan or disaster recovery plans.

4.1 Work scope for disaster recovery

Disaster recovery of information system includes disaster recovery planning daily operations of the backup center for disaster recovery, recovery and resumption of critical business functions in the backup center for disaster recovery, post-disaster reconstruction and return work of primary system,

emergency response after an incident occurs.

4.2.1 Establishment of an organization

The organization that uses or manages the information systems (hereinafter referred to as the "organization") shall, combining its actual conditions, establish an organization for disaster recovery, clarify its responsibilities. Some of them may undertake two or more responsibilities, other positions may be held by multiple people (it shall clarify the replacement order in the disaster recovery plan).

4.3 Management of disaster recovery planning

The organization shall assess the risks of the disaster recovery planning process, prepare the required resources, determine detailed tasks and timelines, supervise and manage planning activities, track and report on the progress of task, conduct problem management and change management.

4.4 External collaboration for disaster recovery

The organization shall liaise and collaborate with relevant management, equipment and service providers, telecommunications, power and news media, to ensure timely notification of accurate conditions and obtaining appropriate support in the event of a disaster.

4.5 Audit and filing of disaster recovery

The grading of disaster recovery and the formulation of disaster recovery plans shall be audited and filed in accordance with relevant regulations.

5.1 Risk analysis

The main contents of risk analysis include. identifying the asset value of the information system, identifying the natural and man-made threats faced by the information system, identifying the vulnerability of the information system, analyzing the possibility of various threats and quantitatively or qualitatively describing the possible losses, identifying the existing risk prevention and