ICS 35.040
L 80

中华人民共和国国家标准

GB/T 20988—2007

信息安全技术
信息系统灾难恢复规范

Information security technology—
Disaster recovery specifications for information systems

2007-06-14 发布　　2007-11-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　次

前　言

本标准的附录A是规范性附录，附录B和附录C是资料性附录。

本标准由全国信息安全标准化技术委员会提出并归口。

本标准起草单位：中国信息安全产品评测认证中心。

本标准主要起草人：汪琪、熊四皓、张利、刘艳、郭全明、许强、李伟华、李建彬、谈松、刘建明、刘祖泷、江志强、徐强、冷飚、刘山泉、黄伟、于健、刘东红、上官晓丽。

引　言

本标准参照和借鉴GB/T 19716《信息技术　信息安全管理实用规则》、GB/T 20984《信息安全技术　信息安全风险评估规范》、DRI International(国际灾难恢复协会)《Professional Practices for Business Continuity Planners》和《Business Continuity Glossary》、ISACA(信息系统审计与控制协会)《COBIT Management Guidelines》、NIST(美国国家标准和技术学会)《SP 800-34 Contingency Planning Guide for Information Technology Systems》和在1992年SHARE78会议议题M028上提出的远程站点分级等的有关内容和思想，结合国家重要信息系统行业技术发展和实践经验制定而成。

信息系统灾难恢复能力等级与恢复时间目标(RTO)和恢复点目标(RPO)具有一定的对应关系，各行业可根据行业特点和信息技术的应用情况制定相应的灾难恢复能力等级要求和指标体系。

信息安全技术
信息系统灾难恢复规范

1 范围

本标准规定了信息系统灾难恢复应遵循的基本要求。

本标准适用于信息系统灾难恢复的规划、审批、实施和管理。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB/T 5271.8 信息技术 词汇 第8部分:安全

GB/T 20984 信息安全技术 信息安全风险评估规范

3 术语和定义

GB/T 5271.8 确立的以及下列术语和定义适用于本标准。

3.1

灾难备份中心 backup center for disaster recovery

备用站点 alternate site

用于灾难发生后接替主系统进行数据处理和支持**关键业务功能**(3.6)运作的场所，可提供**灾难备份系统**(3.3)、备用的基础设施和专业技术支持及运行维护管理能力，此场所内或周边可提供备用的生活设施。

3.2

灾难备份 backup for disaster recovery

为了**灾难恢复**(3.9)而对数据、数据处理系统、网络系统、基础设施、专业技术支持能力和运行管理能力进行备份的过程。

3.3

灾难备份系统 backup system for disaster recovery

用于**灾难恢复**(3.9)目的，由数据备份系统、备用数据处理系统和备用的网络系统组成的信息系统。

3.4

业务连续管理 business continuity management

BCM

为保护组织的利益、声誉、品牌和价值创造活动，找出对组织有潜在影响的威胁，提供建设组织有效反应恢复能力的框架的整体管理过程。包括组织在面临灾难时对恢复或连续性的管理，以及为保证业务连续计划或灾难恢复预案的有效性的培训、演练和检查的全部过程。

3.5

业务影响分析 business impact analysis

BIA

分析业务功能及其相关信息系统资源、评估特定灾难对各种业务功能的影响的过程。

3.6

关键业务功能 critical business functions

如果中断一定时间，将显著影响组织的正常运作，导致组织的主要职能或服务无法开展。

3.7

数据备份策略 data backup strategy

为了达到数据恢复和重建目标所确定的备份步骤和行为。通过确定备份时间、技术、介质和场外存放方式，以保证达到**恢复时间目标**(3.18)和**恢复点目标**(3.19)。

3.8

灾难 disaster

由于人为或自然的原因，造成信息系统严重故障或瘫痪，使信息系统支持的业务功能停顿或服务水平不可接受、达到特定的时间的突发性事件。通常导致信息系统需要切换到**灾难备份中心**(3.1)运行。

3.9

灾难恢复 disaster recovery

为了将信息系统从**灾难**(3.8)造成的故障或瘫痪状态恢复到可正常运行状态、并将其支持的业务功能从灾难造成的不正常状态恢复到可接受状态，而设计的活动和流程。

3.10

灾难恢复预案 disaster recovery plan

定义信息系统灾难恢复过程中所需的任务、行动、数据和资源的文件。用于指导相关人员在预定的灾难恢复目标内恢复信息系统支持的关键业务功能。

3.11

灾难恢复规划 disaster recovery planning

DRP

为了减少灾难带来的损失和保证信息系统所支持的**关键业务功能**(3.6)在灾难发生后能及时恢复和继续运作所做的事前计划和安排。

3.12

灾难恢复能力 disaster recovery capability

在灾难发生后利用灾难恢复资源和灾难恢复预案及时恢复和继续运作的能力。

3.13

演练 exercise

为训练人员和提高灾难恢复能力而根据**灾难恢复预案**(3.10)进行活动的过程。包括桌面演练、模拟演练、重点演练和完整演练等。

3.14

场外存放 offsite storage

将存储介质存放到离**主中心**(3.15)有一定安全距离的物理地点的过程。

3.15

主中心 primary center

主站点 primary site

生产中心 production center

主系统所在的数据中心。

3.16

主系统 primary system

生产系统 production system

正常情况下支持组织日常运作的信息系统。包括主数据、主数据处理系统和主网络。

中 华 人 民 共 和 国
国 家 标 准
信息安全技术
信息系统灾难恢复规范
GB/T 20988—2007
*
中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045
网址 www.spc.net.cn
电话:68523946 68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 1.5 字数 35 千字
2007年9月第一版 2007年9月第一次印刷
*
书号:155066·1-29874 定价 20.00 元

GB/T 20988-2007