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

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》[redacted]

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。

3.17

区域性灾难　regional disaster

造成所在地区或有紧密联系的邻近地区的交通、通信、能源及其他关键基础设施受到严重破坏，或大规模人口疏散的事件。

3.18

恢复时间目标　recovery time objective

RTO

灾难发生后，信息系统或业务功能从停顿到必须恢复的时间要求。

3.19

恢复点目标　recovery point objective

RPO

灾难发生后，系统和数据必须恢复到的时间点要求。

3.20

重续　resumption

[redacted]

3.21

回退　return

复原　restoration

支持业务运作的信息系统从灾难备份中心(3.1)重新回到主中心(3.15)运行的过程。

[redacted]

——审核并批准灾难恢复策略；

——审核并批准灾难恢复预案；

——批准灾难恢复预案的执行。

4.2.2.2 灾难恢复规划实施组

灾难恢复规划实施组的主要职责是负责：

——灾难恢复的需求分析；

——提出灾难恢复策略和等级；

——灾难恢复策略的实现；

——制定灾难恢复预案；

——组织灾难恢复预案的测试和演练。

4.2.2.3 灾难恢复日常运行组

灾难恢复日常运行组的主要职责是负责：

——协助灾难恢复系统实施；

——灾难备份中心日常管理；

——灾难备份系统的运行和维护；

——灾难恢复的专业技术支持；

——参与和协助灾难恢复预案的教育、培训和演练；

——维护和管理灾难恢复预案；

——突发事件发生时的损失控制和损害评估；

——灾难发生后信息系统和业务功能的恢复；

——灾难发生后的外部协作。

4.3 灾难恢复规划的管理

组织应评估灾难恢复规划过程的风险、筹备所需资源、确定详细任务及时间表、监督和管理规划活动、跟踪和报告任务进展以及进行问题管理和变更管理。

4.4 灾难恢复的外部协作

组织应与相关管理部门、设备及服务提供商、电信、电力和新闻媒体等保持联络和协作，以确保在灾

[redacted]

难发生时能及时通报准确情况和获得适当支持。

4.5 灾难恢复的审计和备案

[redacted]

——定量分析：以量化方法，评估业务功能的中断可能给组织带来的直接经济损失和间接经济损失；

——定性分析：运用归纳与演绎、分析与综合以及抽象与概括等方法，评估业务功能的中断可能给组织带来的非经济损失，包括组织的声誉、顾客的忠诚度、员工的信心、社会和政治影响等。

5.3 确定灾难恢复目标

根据风险分析和业务影响分析的结果，确定灾难恢复目标，包括：

——关键业务功能及恢复的优先顺序；

——灾难恢复时间范围，即 RTO 和 RPO 的范围。

6 灾难恢复策略的制定

6.1 灾难恢复策略制定的要素

6.1.1 灾难恢复资源要素

——数据备份系统：一般由数据备份的硬件、软件和数据备份介质（以下简称“介质”）组成，如果是依靠电子传输的数据备份系统，还包括数据备份线路和相应的通信设备；

——备用数据处理系统：指备用的计算机、外围设备和软件；

——备用网络系统：最终用户用来访问备用数据处理系统的网络，包含备用网络通信设备和备用数据通信线路；

6.2.3 备用网络系统

备用网络通信设备可通过 6.2.2 所述的方式获取；备用数据通信线路可使用自有数据通信线路或租用公用数据通信线路。

6.2.4 备用基础设施

可选用以下三种方式获取备用基础设施：

——由组织所有或运行；

——多方共建或通过互惠协议获取；

——租用商业化灾难备份中心的基础设施。

6.2.5 专业技术支持能力

可选用以下几种方式获取专业技术支持能力：

——灾难备份中心设置专职技术支持人员；

——与厂商签订技术支持或服务合同；

——由主中心技术支持人员兼任；但对于 RTO 较短的关键业务功能，应考虑到灾难发生时交通和通信的不正常，造成技术支持人员无法提供有效支持的情况。

6.2.6 运行维护管理能力

可选用以下对灾难备份中心的运行维护管理模式：

——自行运行和维护；

——委托其他机构运行和维护。

6.2.7 灾难恢复预案

可选用以下方式，完成灾难恢复预案的制定、落实和管理：

——聘请具有相应资质的外部专家指导完成；

——委托具有相应资质的外部机构完成。

6.3 灾难恢复资源的要求

6.3.1 数据备份系统

组织应根据灾难恢复目标，按照成本风险平衡原则，确定：

——数据备份的范围；

——数据备份的时间间隔；

——数据备份的技术及介质；

——数据备份线路的速率及相关通信设备的规格和要求。

——场地和环境(如面积、温度、湿度、防火、电力和工作时间等)要求;

——运行维护和管理要求。

6.3.5 专业技术支持能力

组织应根据灾难恢复目标,按照成本风险平衡原则,确定灾难备份中心在软件、硬件和网络等方面的技术支持要求,包括技术支持的组织架构、各类技术支持人员的数量和素质等要求。

6.3.6 运行维护管理能力

组织应根据灾难恢复目标,按照成本风险平衡原则,确定灾难备份中心运行维护管理要求,包括运行维护管理组织架构、人员的数量和素质、运行维护管理制度等要求。

6.3.7 灾难恢复预案

组织应根据需求分析的结果,按照成本风险平衡原则,明确灾难恢复预案的:

——整体要求;

——制定过程的要求;

——教育、培训和演练要求;

——管理要求。

7 灾难恢复策略的实现

7.1 灾难备份系统技术方案的实现

7.1.1 技术方案的设计

根据灾难恢复策略制定相应的灾难备份系统技术方案,包含数据备份系统、备用数据处理系统和备用的网络系统。技术方案中所设计的系统,应:

——获得同主系统相当的安全保护;

——具有可扩展性;

——考虑其对主系统可用性和性能的影响。

7.1.2 技术方案的验证、确认和系统开发

为确保技术方案满足灾难恢复策略的要求,应由组织的相关部门对技术方案进行确认和验证,并记录和保存验证及确认的结果。

按照确认的灾难备份系统技术方案进行开发,实现所要求的数据备份系统、备用数据处理系统和备用网络系统。

7.1.3 系统安装和测试

按照经过确认的技术方案,灾难恢复规划实施组应制定各阶段的系统安装及测试计划,以及支持不

7.2.2 基础设施的要求

新建或选用灾难备份中心的基础设施时：

——计算机机房应符合有关国家标准的要求；

——工作辅助设施和生活设施应符合灾难恢复目标的要求。

7.3 专业技术支持能力的实现

组织应根据灾难恢复策略的要求，获取对灾难备份系统的专业技术支持能力。

灾难备份中心应建立相应的技术支持组织，定期对技术支持人员进行技能培训。

7.4 运行维护管理能力的实现

为了达到灾难恢复目标，灾难备份中心应建立各种操作规程和管理制度，用以保证

[redacted]

——数据备份的及时性和有效性；

——备用数据处理系统和备用网络系统处于正常状态，并与主系统的参数保持一致；

——有效的应急响应、处理能力。

7.5 灾难恢复预案的实现

7.5.1 灾难恢复预案的制定

灾难恢复预案的制定应遵循以下原则：

——完整性：灾难恢复预案（以下称预案）应包含灾难恢复的整个过程，以及灾难恢复所需的尽可能全面的数据和资料；

——易用性：预案应运用易于理解的语言和图表，并适合在紧急情况下使用；

[redacted]

——明确性：预案应采用清晰的结构，对资源进行清楚的描述，工作内容和步骤应具体，每项工作应有明确的责任人；

——有效性：预案应尽可能满足灾难发生时进行恢复的实际需要，并保持与实际系统和人员组织的同步更新；

7.5.3 灾难恢复预案的管理

经过审核和批准的灾难恢复预案，应按照以下原则进行保存和分发：

——由专人负责；

——具有多份拷贝在不同的地点保存；

——分发给参与灾难恢复工作的所有人员；

——在每次修订后所有拷贝统一更新，并保留一套，以备查阅；

——旧版本应按有关规定销毁。

为了保证灾难恢复预案的有效性，应从以下方面对灾难恢复预案进行严格的维护和变更管理：

——业务流程的变化、信息系统的变更、人员的变更都应在灾难恢复预案中及时反映；

——预案在测试、演练和灾难发生后实际执行时，其过程均应有详细的记录，并应对测试、演练和执行的效果进行评估，同时对预案进行相应的修订；

——灾难恢复预案应定期评审和修订，至少每年一次。

附 录 A
（规范性附录）
灾难恢复能力等级划分

A.1 第1级 基本支持

第1级灾难恢复能力应具有技术和管理支持，如表A.1所示。

表A.1 第1级——基本支持

要 素	要 求
数据备份系统	a) 完全数据备份至少每周一次； b) 备份介质场外存放。
备用数据处理系统	—
备用网络系统	—
备用基础设施	有符合介质存放条件的场地。
专业技术支持能力	—
运行维护管理能力	a) 有介质存取、验证和转储管理制度； b) 按介质特性对备份数据进行定期的有效性验证。
灾难恢复预案	有相应的经过完整测试和演练的灾难恢复预案。
注：“—”表示不作要求。	

A.2 第2级 备用场地支持

第2级灾难恢复能力应具有技术和管理支持，如表A.2所示。

表A.2 第2级——备用场地支持

要 素	要 求
数据备份系统	a) 完全数据备份至少每周一次； b) 备份介质场外存放。
备用数据处理系统	配备灾难恢复所需的部分数据处理设备，或灾难发生后能在预定时间内调配所需的数据处理设备到备用场地。
备用网络系统	配备部分通信线路和相应的网络设备，或灾难发生后能在预定时间内调配所需的通信线路和网络设备到备用场地。
备用基础设施	a) 有符合介质存放条件的场地； b) 有满足信息系统和关键业务功能恢复运作要求的场地。
专业技术支持能力	—
运行维护管理能力	a) 有介质存取、验证和转储管理制度； b) 按介质特性对备份数据进行定期的有效性验证； c) 有备用站点管理制度； d) 与相关厂商有符合灾难恢复时间要求的紧急供货协议； e) 与相关运营商有符合灾难恢复时间要求的备用通信线路协议。
灾难恢复预案	有相应的经过完整测试和演练的灾难恢复预案。

A.3 第3级 电子传输和部分设备支持

第3级灾难恢复能力应具有技术和管理支持，如表A.3所示。

表A.3 第3级——电子传输和部分设备支持

要 素	要 求
数据备份系统	a) 完全数据备份至少每天一次； b) 备份介质场外存放；

表 A.4（续）

要　　素	要　　求
运行维护管理能力	a）　有介质存取、验证和转储管理制度； b）　按介质特性对备份数据进行定期的有效性验证； c）　有备用计算机机房运行管理制度； d）　有硬件和网络运行管理制度； e）　有电子传输数据备份系统运行管理制度。
灾难恢复预案	有相应的经过完整测试和演练的灾难恢复预案。

A.5　第 5 级　实时数据传输及完整设备支持

第 5 级灾难恢复能力应具有技术和管理支持，如表 A.5 所示。

表 A.5　第 5 级——实时数据传输及完整设备支持

要　　素	要　　求

表 A.6 第 6 级——数据零丢失和远程集群支持

要　　素	要　　求
数据备份系统	a) 完全数据备份至少每天一次； b) 备份介质场外存放； c) 远程实时备份，实现数据零丢失。
备用数据处理系统	a) 备用数据处理系统具备与生产数据处理系统一致的处理能力并完全兼容； b) 应用软件是“集群的”，可实时无缝切换； c) 具备远程集群系统的实时监控和自动切换能力。
备用网络系统	a) 配备与主系统相同等级的通信线路和网络设备； b) 备用网络处于运行状态； c) 最终用户可通过网络同时接入主、备中心。
备用基础设施	a) 有符合介质存放条件的场地； b) 有符合备用数据处理系统和备用网络设备运行要求的场地； c) 有满足关键业务功能恢复运作要求的场地； d) 以上场地应保持 7×24 h 运作。
专业技术支持能力	在灾难备份中心 7×24 h 有专职的： a) 计算机机房管理人员； b) 专职数据备份技术支持人员； c) 专职硬件、网络技术支持人员； d) 专职操作系统、数据库和应用软件技术支持人员。
运行维护管理能力	a) 有介质存取、验证和转储管理制度； b) 按介质特性对备份数据进行定期的有效性验证； c) 有备用计算机机房运行管理制度； d) 有硬件和网络运行管理制度； e) 有实时数据备份系统运行管理制度； f) 有操作系统、数据库和应用软件运行管理制度。
灾难恢复预案	有相应的经过完整测试和演练的灾难恢复预案。

A.7 灾难恢复能力等级评定原则

如要达到某个灾难恢复能力等级，应同时满足该等级中 7 个要素的相应要求。

A.8 灾难备份中心的等级

灾难备份中心的等级等于其可支持的灾难恢复最高等级。

示例：可支持 1 至 5 级的灾难备份中心的级别为 5 级。

附 录 B
（资料性附录）
灾难恢复预案框架

B.1 目标和范围

B.7 预案的保障条件

预案的保障条件如下：

——专业技术保障；

——通信保障；

——后勤保障。

B.8 预案附录

预案的附录如下：

——人员疏散计划；

——产品说明书；

——信息系统标准操作流程；

——服务级别协议和备忘录；

——资源清单；

——业务影响分析报告；

——预案的保存和分发办法。

附 录 C
（资料性附录）
某行业 RTO/RPO 与灾难恢复能力等级的关系示例

C.1 RTO/RPO 与灾难恢复能力等级的关系

表 C.1 说明信息系统灾难恢复各等级对应的 RTO/RPO 范围。

表 C.1 RTO/RPO 与灾难恢复能力等级的关系

灾难恢复能力等级	RTO	RPO
1	2 天以上	1 天至 7 天
2	24 小时以上	1 天至 7 天
3	12 小时以上	数小时至 1 天
4	数小时至 2 天	数小时至 1 天
5	数分钟至 2 天	0 至 30 分钟
6	数分钟	0

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