

重要信息系统灾难恢复指南

国务院信息化工作办公室
2005 年 4 月

目 次

前 言	IV
引 言	V
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 灾难恢复规划的管理	2
4.1 灾难恢复规划的过程	2
4.2 灾难恢复规划的组织机构及其职责	3
4.2.1 组织机构的设立	3
4.2.2 组织机构的职责	3
4.3 灾难恢复规划的管理	3
4.4 灾难恢复规划的外部协作	4
4.5 灾难恢复规划的审计和监理	4
5 灾难恢复需求的分析	4
5.1 风险分析	4
5.2 业务影响分析	4
5.2.1 分析业务功能和相关资源配置	4
5.2.2 评估中断影响	4
5.3 确定灾难恢复目标	4
6 灾难恢复策略的制定	4
6.1 灾难恢复策略制定的过程	4
6.1.1 要素分析	4
6.1.2 成本风险分析和策略的确定	4
6.2 确定灾难恢复资源的获取方式	5
6.2.1 数据备份系统	5
6.2.2 备用基础设施	5
6.2.3 备用数据处理系统	5
6.2.4 备用网络系统	5
6.2.5 技术支持能力	5
6.2.6 运行维护管理能力	5
6.2.7 灾难恢复预案	5
6.3 确定灾难恢复等级各要素的要求	6
6.3.1 数据备份系统	6
6.3.2 备用基础设施	6
6.3.3 备用数据处理系统	6

6.3.4	备用网络系统	6
6.3.5	技术支持能力	6
6.3.6	运行维护管理能力	6
6.3.7	灾难恢复预案	6
7	灾难恢复策略的实现	6
7.1	灾难备份中心的选择和建设	6
7.1.1	选址原则	6
7.1.2	基础设施的要求	7
7.2	灾难备份系统技术方案的实现	7
7.2.1	技术方案的设计	7
7.2.2	技术方案的验证、确认和系统开发	7
7.2.3	系统安装和测试	7
7.3	技术支持能力的实现	7
7.4	运行维护管理能力的实现	7
7.5	灾难恢复预案的实现	7
8	灾难恢复预案的制订、落实和管理	7
8.1	灾难恢复预案的制订	7
8.1.1	制订原则	7
8.1.2	制订过程	8
8.2	灾难恢复预案的教育、培训和演练	8
8.3	灾难恢复预案的管理	8
8.3.1	保存与分发	8
8.3.2	维护和变更管理	9
附录 A (规范性附录)	灾难恢复的等级划分	10
A.1	第 1 级 基本支持	10
A.2	第 2 级 备用场地支持	10
A.3	第 3 级 电子传输和部分设备支持	10
A.4	第 4 级 电子传输及完整设备支持	11
A.5	第 5 级 实时数据传输及完整设备支持	11
A.6	第 6 级 数据零丢失和远程集群支持	12
A.7	灾难恢复等级评定原则	12
A.8	灾难备份中心的等级	12
附录 B (资料性附录)	灾难恢复预案框架	13
B.1	目标和范围	13
B.2	组织和职责	13
B.3	联络与通讯	13
B.4	紧急响应流程	13
B.4.1	灾难预警	13
B.4.2	人员疏散	13

B.4.3 损害评估	13
B.4.4 研判和灾难宣告	13
B.5 恢复及重续运行流程	13
B.5.1 恢复	13
B.5.2 重续运行	13
B.6 灾后重建和回退	14
B.7 预案的保障条件	14
B.8 预案附录	14
参考文献	15
表 A.1 第 1 级灾难恢复的技术和管理支持	10
表 A.2 第 2 级灾难恢复的技术和管理支持	10
表 A.3 第 3 级灾难恢复的技术和管理支持	10
表 A.4 第 4 级灾难恢复的技术和管理支持	11
表 A.5 第 5 级灾难恢复的技术和管理支持	11
表 A.6 第 6 级灾难恢复的技术和管理支持	12

前 言

本指南是对重要信息系统灾难恢复的规划和准备工作基本要求的描述。

本指南的附录 A 灾难恢复的等级划分是规范性附录，附录 B 灾难恢复预案框架是资料性附录。

本指南由 xxxxx 提出；

本指南由 xxxxx 批准；

本指南由 xxxxx 归口；

本指南起草单位：

本指南主要起草人：

引 言

灾难恢复是确保信息和信息系统安全的一项重要措施。遵从重要信息系统灾难恢复指南的要求，是做好重要信息系统灾难恢复工作的基础。

本指南用于规范和指导重要信息系统的使用和管理单位对信息系统灾难恢复的规划和准备工作。本指南主要从灾难恢复规划的管理、灾难恢复的需求分析、灾难恢复等级的确定、灾难恢复等级的实现、灾难恢复预案的制订、落实和管理等方面，对灾难恢复的规划和准备活动的规范化要求进行全面描述。本指南还以规范性附录的形式对灾难恢复的等级划分进行了描述，并以资料性附录的形式对灾难恢复预案的框架进行了说明。

重要信息系统灾难恢复指南

1 范围

本指南规定了对重要信息系统的灾难恢复应遵循的基本要求。

本指南适用于指导重要信息系统的使用和管理单位(以下简称“单位”)进行灾难恢复的规划和准备工作,对重要信息系统灾难恢复规划项目的审批和监督管理也可参照使用。

2 规范性引用文件

下列文件中的条款通过本指南的引用而成为本指南的条款。凡是注日期的引用文件,其随后所有的修改单(不包含勘误的内容)或修订版均不适用于本指南,然而,鼓励根据本指南达成协议的各方研究是否可适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指南。

GB/T 5271.1—2000 信息技术 词汇 第1部分:基本术语

GB/T 5271.9—2000 信息技术 词汇 第9部分 数据通信

GB/T 5271.12—2000 信息技术 词汇 第12部分 外围设备

GB/T 5271.20—94 信息技术 词汇 20部分 系统开发

GB/T 2887-2000 电子计算机场地通用规范

3 术语和定义

GB/T 5271.1—2000 第1部分、GB/T 5271.9—2000 第9部分、GB/T 5271.12—2000 第12部分和GB/T 5271.20—94 第20部分确立的术语和定义,以及下列术语和定义适用于本指南。

3.1

灾难 disaster

由于人为或自然的原因,造成信息系统运行严重故障或瘫痪,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备用场地运行。

3.2

灾难恢复 disaster recovery

将信息系统从灾难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。

3.3

灾难恢复规划(DRP) disaster recover planning

为了减少灾难带来的损失和实现灾难恢复所做的事前计划和安排。

3.4

业务影响分析(BIA) business impact analysis

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。

3.5

恢复时间目标(RTO) recovery time objective

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。

3.6

恢复点目标 (RPO) recovery point objective
灾难发生后,系统和数据必须恢复到的时间点要求。

3.7

关键业务功能 critical business functions
如果中断一定时间,将显著影响单位运作的服务或职能。

3.8

生产系统 production system
正常情况下支持单位日常业务运作的信息系统,包括生产数据、生产数据处理系统和生产网络。

3.9

灾难备份中心;备用场所 alternate site
用于灾难发生时接替生产系统运行进行数据处理和支持关键业务功能运作的场所,包括备用数据处理中心、备用的工作环境、备用生活设施和技术支持及运行管理人员。

3.10

灾难备份 backup for disaster recovery
为了灾难恢复而对数据、数据处理系统、网络系统、基础设施、技术支持能力和运行管理能力进行备份的过程。

3.11

灾难备份系统 backup system for disaster recovery
用于灾难恢复目的,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。

3.12

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 RPO 和 RT0。

3.13

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。

3.14

演练 exercise
用于训练人员和提高灾难恢复能力的活动,包括桌面演练、模拟演练、操作演练和演习等。

3.15

[灾难恢复]演习 mock drill
按设定的灾难场景,参与人员根据灾难恢复预案进行活动的过程。

4 灾难恢复规划的管理

4.1 灾难恢复规划的过程

灾难恢复规划是一个周而复始、持续改进的过程,包含以下几个阶段:

- a) 灾难恢复需求的确定;
- b) 灾难恢复策略的制订;

- c) 灾难恢复策略的实现；
- d) 灾难恢复预案的制订、落实和管理。

4.2 灾难恢复规划的组织机构及其职责

4.2.1 组织机构的设立

单位应结合其日常组织机构的具体情况建立灾难恢复规划组织机构，并明确其职责。其中一些人可负责两种或多种职责，一些职位可由多人担任（灾难恢复预案中应明确他们的替代顺序）。

灾难恢复规划的组织机构由管理、业务、技术和行政后勤等人员组成，分为灾难恢复规划领导小组、灾难恢复规划实施组和灾难恢复规划日常运行组。其中，实施组的人员在实施任务完成后可成为日常运行组的成员。

单位可聘请外部专家协助灾难恢复规划工作，也可委托外部机构承担实施组和运行组的部分或全部工作。

4.2.2 组织机构的职责

a) 灾难恢复规划领导小组

灾难恢复规划领导小组是实施灾难恢复规划工作的组织领导机构，组长应由单位高层领导担任，领导和决策灾难恢复规划重大事宜，其主要职责如下：

- 审核并批准经费预算；
- 审核并批准灾难恢复策略；
- 审核并批准灾难恢复预案；
- 组织灾难恢复预案的测试和演练；
- 批准灾难恢复预案的执行。

b) 灾难恢复规划实施组

灾难恢复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；
- 制订灾难恢复预案；

c) 灾难恢复规划日常运行组

灾难恢复日常运行组的主要职责是负责：

- 灾难备份中心日常管理；
- 灾难备份系统的运行和维护；
- 灾难恢复的技术支持；
- 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

单位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 灾难恢复规划的外部协作

单位应与相关管理部门、新闻媒体、设备及服务提供商、电信和电力部门等保持联络和协作，以确保在灾难发生时能及时通报准确情况和获得适当支持。

4.5 灾难恢复规划的审计和监理

灾难恢复的等级评定、灾难恢复预案的制订，应按有关规定进行审计、监理和备案。

5 灾难恢复需求的分析

5.1 风险分析

标识信息系统的资产价值，识别信息系统面临的自然的和人为的威胁，识别信息系统的脆弱性，分析各种威胁发生的可能性，并定量或定性描述可能造成的损失。通过技术或管理手段，防范或控制信息系统的风险。依据防范或控制风险的可行性和残余风险的可接受程度，确定对风险的防范和控制措施。

5.2 业务影响分析

5.2.1 分析业务功能和相关资源配置

分析单位的各项业务功能及各项业务之间的相关性，确定支持各种业务功能的相应信息系统资源及其它资源，明确相关信息的保密性、完整性和可用性要求。

5.2.2 评估中断影响

应采用定量和/或定性的方法，对各种业务功能的中断造成的影响进行评估：

- a) 定量分析：以量化方法，评估业务功能的中断可能给单位带来的直接经济损失和间接经济损失；
- b) 定性分析：以非量化方法，评估业务功能的中断可能对国家的政治、社会、法律及单位内部事务等造成的影响。

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：

- a) 关键业务功能及恢复的优先顺序；
- b) 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过程

6.1.1 要素分析

按照附录 A 的灾难恢复等级划分标准，将支持灾难恢复各个等级所需的资源（以下简称“灾难恢复资源”）分为 7 个要素：

- a) 数据备份系统
- b) 备用数据处理系统
- c) 备用网络系统
- d) 备用基础设施
- e) 技术支持能力
- f) 运行维护管理能力
- g) 灾难恢复预案

6.1.2 成本风险分析和策略的确定

按照灾难恢复资源的成本与风险可能造成的损失之间取得平衡的原则（以下简称“成本风险平衡

原则”)确定每项关键业务功能的灾难恢复策略,不同的业务功能可采用不同的灾难恢复策略。

灾难恢复策略包括:

- a) 灾难恢复资源的获取方式;
- b) 灾难恢复等级各要素的具体要求。

6.2 确定灾难恢复资源的获取方式

6.2.1 数据备份系统

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。

数据备份系统可由单位自行建设,也可通过租用其它机构的系统而获取。

6.2.2 备用基础设施

备用基础设施是灾难恢复所需的、支持灾难备份系统运行的建筑、设备和组织,包括介质的场外存放场所、备用的机房及工作辅助设施,以及容许灾难恢复人员连续停留的生活设施。

可采用以下三种方式获取备用基础设施:

- a) 由单位所有或运行;
- b) 多方共建或通过互惠协议获取;
- c) 租用商业化灾难备份中心的基础设施。

6.2.3 备用数据处理系统

可选用以下三种方式之一来获取备用数据处理系统:

- a) 事先与厂商签订紧急供货协议;
- b) 事先购买所需的数据处理设备并存放在灾难备份中心或安全的设备仓库;
- c) 利用商业化灾难备份中心或签有互惠协议的机构已有的兼容设备。

6.2.4 备用网络系统

备用网络系统包含备用网络通信设备和备用数据通信线路,备用网络通信设备可通过本指南 6.2.3 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。

6.2.5 技术支持能力

可选用以下几种方式获取技术支持能力:

- a) 灾难备份中心设置专职技术支持人员;
- b) 与厂商签订技术支持或服务合同;
- c) 由生产系统技术支持人员兼任;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:

- a) 自行运行和维护;
- b) 委托其它机构运行和维护。

6.2.7 灾难恢复预案

可采用以下方式,完成灾难恢复预案的制订、落实和管理:

- a) 由单位独立完成;
- b) 聘请外部专家指导完成;
- c) 委托外部机构完成。

6.3 确定灾难恢复等级各要素的要求

6.3.1 数据备份系统

单位应根据灾难恢复目标，按照成本风险平衡原则，确定：

- a) 数据备份的范围；
- b) 数据备份的时间间隔；
- c) 数据备份的技术及介质；
- d) 数据备份线路的速率及相关通信设备的规格和要求。

6.3.2 备用基础设施

单位应根据灾难恢复目标，按照成本风险平衡原则，确定对备用基础设施的要求，包括：

- a) 与生产系统所在的数据处理中心（以下简称“生产中心”）的距离要求；
- b) 场地和环境（如面积、温度、湿度、防火、电力和工作时间等）要求；
- c) 运行和管理要求。

6.3.3 备用数据处理系统

单位应根据关键业务功能的灾难恢复对备用数据处理系统的要求和未来发展的需要，确定备用数据处理系统的：

- a) 数据处理能力；
- b) 与生产系统的兼容性要求；
- c) 平时处于就绪还是运行状态。

6.3.4 备用网络系统

单位应根据关键业务功能的灾难恢复对网络容量及切换时间的要求和未来发展的需要，选择备用数据通信的技术和线路带宽，确定网络通信设备的功能和容量，保证灾难恢复时，最终用户能以一定速率连接到备用数据处理系统。

6.3.5 技术支持能力

单位应根据灾难恢复目标，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

单位应根据灾难恢复目标，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

单位应根据需求分析的结果，明确灾难恢复预案的：

- a) 整体要求；
- b) 制订过程的要求；
- c) 教育、培训和演练要求；
- d) 管理要求。

7 灾难恢复策略的实现

7.1 灾难备份中心的选择和建设

7.1.1 选址原则

选择或建设灾难备份中心时，应根据风险评估的结果，避免灾难备份中心与生产中心同时遭受同类风险。灾难备份中心还应具有方便灾难恢复人员或设备到达的交通条件，以及数据备份和灾难恢复

所需的通信、电力等资源。

7.1.2 基础设施的要求

新建或选用灾备份中心的基础设施时：

- a) 计算机机房应符合 GB/T 2887-2000 的要求；
- b) 工作辅助设施和生活设施应符合灾难恢复目标的要求。

7.2 灾难备份系统技术方案的实现

7.2.1 技术方案的设计

根据灾难恢复策略制订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：

- a) 获得同生产系统相当的安全保护；
- b) 具有可扩展性。

7.2.2 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，应由单位的相关部门组织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。

7.2.3 系统安装和测试

按照经过确认的技术方案，实施组应制定各阶段的系统安装及测试计划，以及支持不同关键业务功能的系统安装及测试计划，并组织最终用户共同进行测试。确认以下各项功能可正确实现：

- a) 数据备份及数据恢复功能；
- b) 在限定的时间内，利用备份数据正确恢复系统、应用软件及各类数据，并可正确恢复各项关键业务功能；
- c) 客户端可与备用数据处理系统通信正常。

7.3 技术支持能力的实现

单位应根据灾难恢复策略的要求，获取对灾难备份系统的技术支持能力。

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的教育和培训。

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和管理制度，用以保证：

- a) 数据备份的及时性和有效性；
- b) 备用数据处理系统和备用网络系统处于正常状态，并与生产系统的参数保持一致；
- c) 有效的应急响应、处理能力。

7.5 灾难恢复预案的实现

灾难恢复的每个等级均应按第 8 章的具体要求制订相应的灾难恢复预案，并进行落实和管理。

8 灾难恢复预案的制订、落实和管理

8.1 灾难恢复预案的制订

8.1.1 制订原则

- a) 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；
- b) 易用性：预案应运用易于理解语言和图表，并适合在紧急情况下使用；

- c) 明确性：预案应采用清晰的结构，对资源进行清楚描述，工作内容和步骤应具体，每项工作应有明确的责任人；
- d) 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；
- e) 兼容性：灾难恢复预案应与其它应急预案体系有机结合。

8.1.2 制订过程

灾难恢复预案制订的过程如下：

- a) 初稿的制订：参照附录 B 灾难恢复预案框架，按照风险分析和业务影响分析所确定的灾难恢复内容，根据灾难恢复等级的要求，结合单位其它相关的应急预案，撰写出灾难恢复预案的初稿。
- b) 初稿的评审：单位应对灾难恢复预案初稿的全面性、易用性、明确性、有效性和兼容性进行严格的评审。评审应有相应的流程保证。
- c) 初稿的修订：根据评审结果，对预案进行修订，纠正在初稿评审过程中发现的问题和缺陷，形成预案的修订稿。
- d) 预案的测试：应预先制订测试计划，在计划中说明测试的案例。测试应包含基本单元测试、关联测试和整体测试。测试的整个过程应有详细的记录，并形成测试报告。
- e) 预案的审核和批准：根据测试的记录和报告，对预案的修订稿进一步完善，形成预案的报批稿，并由灾难恢复领导小组审核和批准，确定为预案的执行稿。

8.2 灾难恢复预案的教育、培训和演练

为了使相关人员了解信息系统灾难恢复的目标和流程，熟悉灾难恢复的操作规程，单位应按以下要求，组织灾难恢复预案的教育、培训和演练：

- a) 在灾难恢复规划的初期就应开始灾难恢复观念的宣传教育工作；
- b) 应预先对培训需求进行评估，开发和落实相应的培训/教育课程，保证课程内容与预案的要求相一致；
- c) 应事先确定培训的频次和范围，事后保留培训的记录；
- d) 预先制订演练计划，在计划中说明演练的场景。演练的整个过程应有详细的记录，并形成报告。
- e) 灾难恢复演习应保证至少每年一次。

8.3 灾难恢复预案的管理

8.3.1 保存与分发

经过审核和批准的灾难恢复预案，应：

- a) 由专人负责保存与分发；
- b) 具有多份拷贝在不同的地点保存；
- c) 分发给参与灾难恢复工作的所有人员；
- d) 在每次修订后所有拷贝统一更新，并保留一套，以备查阅，原分发的旧版本应予销毁。

8.3.2 维护和变更管理

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变更管理：

- a) 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；
- b) 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、演练和执行的评估，同时对预案进行相应的修订；
- c) 灾难恢复预案还应定期评审和修订，至少每年一次。

附录 A (规范性附录) 灾难恢复的等级划分

A.1 第 1 级 基本支持

第 1 级灾难恢复应具有技术和管理支持如表 A.1 所示。

表 A.1 第 1 级灾难恢复的技术和管理支持

	要素	要求
A.1.1	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。
A.1.2	备用数据处理系统	—
A.1.3	备用网络系统	—
A.1.4	备用基础设施	a) 有符合介质存放条件的场地。
A.1.5	技术支持	—
A.1.6	运行维护支持	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。
A.1.7	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.2 第 2 级 备用场地支持

第 2 级灾难恢复应具有技术和管理支持如表 A.2 所示。

表 A.2 第 2 级灾难恢复的技术和管理支持

	要素	要求
A.2.1	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。
A.2.2	备用数据处理系统	a) 灾难发生时能在预定时间内调配所需的数据处理设备到场。
A.2.3	备用网络系统	a) 灾难发生时能在预定时间内调配所需的通信线路和网络设备到位。
A.2.4	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备用场地。
A.2.5	技术支持	—
A.2.6	运行维护支持	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) 有备用场地管理制度； 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。
A.2.7	灾难恢复预案	a) 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 级灾难恢复应具有技术和管理支持如表 A.3 所示。

表 A.3 第 3 级灾难恢复的技术和管理支持

	要素	要求
A.3.1	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) 每天多次利用通信网络将关键数据定时批量传送至备用场地。
A.3.2	备用数据处理系统	a) 配备灾难恢复所需的部分数据处理设备。
A.3.3	备用网络系统	a) 配备部分通信线路和相应的网络设备。
A.3.4	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。
A.3.5	技术支持	a) 在备用场地有专职的计算机机房运行管理人员。
A.3.6	运行维护支持	a) 按介质特性对备份数据进行定期的有效性验证；

		b) 有介质存取、验证和转储管理制度； c) 有备用计算机机房管理制度； d) 有备用数据处理设备硬件维护管理制度； e) 有电子传输数据备份系统运行管理制度。
A.3.7	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.4 第4级 电子传输及完整设备支持

第4级灾难恢复应具有技术和管理支持如表A.4所示。

表 A.4 第4级灾难恢复的技术和管理支持

	要素	要求
A.4.1	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) 每天多次利用通信网络将关键数据定时批量传送至备用场地。
A.4.2	备用数据处理系统	a) 配备灾难恢复所需的全部数据处理设备，并处于就绪状态或运行状态。
A.4.3	备用网络系统	a) 配备灾难恢复所需的通信线路； b) 配备灾难恢复所需的网络设备，并处于就绪状态。
A.4.4	备用基础设施	a) 有符合介质存放条件的备用场地； 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 x 24运作。
A.4.5	技术支持	在备用场地有： a) 7 x 24 专职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。
A.4.6	运行维护支持	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。
A.4.7	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

第五级灾难恢复应具有技术和管理支持如表A.5所示。

表 A.5 第5级灾难恢复的技术和管理支持

	要素	要求
A.5.1	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) 采用远程数据复制技术，并利用通信网络将关键数据实时复制到备份场地。
A.5.2	备用数据处理系统	a) 配备灾难恢复所需的全部数据处理设备，并处于就绪或运行状态。
A.5.3	备用网络系统	a) 配备灾难恢复所需的通信线路； b) 配备灾难恢复所需的网络设备，并处于就绪状态； c) 具备通信网络自动或集中切换能力。
A.5.4	备用基础设施	a) 有符合介质存放条件的备用场地； 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； a) 以上场地应保持7 x 24运作。
A.5.5	技术支持	在备用场地有： a) 7 x 24 专职计算机机房管理人员； b) 7 x 24 专职数据备份技术支持人员； c) 7 x 24 专职硬件、网络技术支持人员。
A.5.6	运行维护支持	a) 有介质存取、验证和转储管理制度；

		<ul style="list-style-type: none"> 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。
A.5.7	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.6 第6级 数据零丢失和远程集群支持

第六级灾难恢复应具有技术和管理支持如表 A.6 所示。

表 A.6 第6级灾难恢复的技术和管理支持

	要素	要求
A.6.1	数据备份系统	<ul style="list-style-type: none"> 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。
A.6.2	备用数据处理系统	<ul style="list-style-type: none"> 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。
A.6.3	备用网络系统	<ul style="list-style-type: none"> a) 配备与生产系统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。
A.6.4	备用基础设施	<ul style="list-style-type: none"> a) 有符合介质存放条件的备用场地； 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 x 24 运作。
A.6.5	技术支持	在备用场地有： <ul style="list-style-type: none"> a) 7 x 24 专职计算机机房管理人员； b) 7 x 24 专职数据备份技术支持人员； c) 7 x 24 专职硬件、网络技术支持人员； d) 7 x 24 专职操作系统、数据库和应用软件技术支持人员。
A.6.6	运行维护支持	<ul style="list-style-type: none"> 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。
A.6.7	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 灾难恢复等级评定原则

如要达到某个灾难恢复等级，应同时满足该等级中 7 个要素的要求。

A.8 灾备份中心的等级

灾备份中心的等级等于其可以支持的灾难恢复最高等级。

示例：可支持 1 至 5 级的灾备份中心的级别为 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

定义灾难恢复预案中的相关术语和方法论，并说明灾难恢复的目标，如恢复时间目标（RTO）和恢复点目标（RPO）。说明预案的作用范围，解决哪些问题，不解决哪些问题。

B.2 组织和职责

描述灾难恢复组织的组成、各个岗位的职责和人员名单。灾难恢复组织应包括应急响应组、灾难恢复组等。

B.3 联络与通讯

列出灾难恢复相关人员和组织的联络表。包含灾难恢复团队、运营商、厂商、主管部门、媒体、员工家属等。联络方式包括固定电话、移动电话、对讲机、电子邮件和住址等。

B.4 紧急响应流程

B.4.1 灾难预警

任何人员在发现灾难即将发生时，应立即报告灾难预警值班人员，由值班人员确认后及时报告有关领导，并通知相关技术人员，为其正常关闭系统，减少损失赢得时间。

B.4.2 人员疏散

提供指定的集合地点和替代的集合地点，还包括通知人员撤离的办法，撤离的组织和步骤等。

B.4.3 损害评估

在灾难发生后，应由应急响应组的损害评估人员，确定事态的严重程度。由灾难恢复责任人召集相应的专业人员对灾难事件进行慎重评估，确认灾难事件对信息系统造成的影响程度，确定下一步将要采取的行动。一旦系统的影响被确定，应将最新信息按照预定的通告流程通知给相应的团队。

B.4.4 研判和灾难宣告

应预先制定灾难恢复预案启动的条件。当损害评估的结果达到一项或多项启动条件时，单位将正式发出灾难宣告，宣布启动灾难恢复预案，并根据宣告流程通知各有关部门。

B.5 恢复及重续运行流程

B.5.1 恢复

按照业务影响分析中确定的优先顺序，在灾难备份中心恢复支持关键业务功能的数据、数据处理系统和网络系统。描述时间、地点、人员、设备和每一步的详细操作步骤，同时还包括特定情况发生时各团队之间进行协调的指令。

B.5.2 重续运行

灾难备份中心的系统替代生产系统，支持关键业务功能的提供。这一阶段包含生产系统运行管理所涉及的主要工作，包含重续运行的所有操作流程和规章制度。

XXX1—XXXX

B.6 灾后重建和回退

最后阶段是生产系统的重建工作，中止灾难备份系统的运行，将系统回退到单位的生产系统。

B.7 预案的保障条件

- 专业技术保障
- 通信保障
- 后勤保障

B.8 预案附录

- 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

参 考 文 献

1. GB 17859-1999 计算机信息系统安全保护等级划分准则
-