ICS
A11
备案号：

JR

中 华 人 民 共 和 国 金 融 行 业 标 准

JR/T 0044—2008

银行业信息系统灾难恢复管理规范

Management specification of information system disaster recovery for banks

2008-02-04 发布　　2008-02-04 实施

中国人民银行 发布

目　　次

前　言

本标准是对银行业信息系统灾难恢复管理要求的描述。

本标准由中国人民银行提出，由全国金融标准化技术委员会归口管理。

本标准由中国人民银行批准。

本标准负责起草单位：中国人民银行。

本标准参加起草单位：万国数据服务（深圳）有限公司。

本标准主要起草人：文四立、李晓枫、杨竑、郭全明、曹旭辉、李健、袁慧萍、汪琪、于健、何政、刘东红、高勇、陈天晴、康潭云、王铮、张艳、竺毅强、周恒、王雄、刘鹏鹏。

引　　言

为规范和引导银行业信息系统灾难恢复工作，有效防范银行业信息系统风险，保护银行业客户的合法权益，特制定本规范。

银行业信息系统灾难恢复管理规范

1 范围

本规范规定了银行业信息系统灾难恢复应遵循的管理要求。

本规范适用于中国人民银行，以及在中华人民共和国境内设立的银行业金融机构（包括外资银行，以下简称“单位”）。

2 规范性引用文件

下列文件中的条款通过本规范的引用而成为本规范的条款。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规范。凡是不注日期的引用文件，其最新版本适用于本规范。

GB/T 20988-2007 信息安全技术 信息系统灾难恢复规范

3 术语和定义

3.1

信息系统 information system

由计算机系统、网络系统软硬件及其相关的设备、设施和应用软件等构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输和检索等处理的人机系统。

3.2

灾难 disaster

由于人为或自然的原因，造成信息系统严重故障、瘫痪或其数据严重受损，使信息系统支持的业务功能停顿或服务水平达到不可接受的程度，并持续特定时间的突发性事件。

3.3

灾难恢复 disaster recovery

DR

为了将信息系统从灾难造成的不可运行状态或不可接受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。

3.4

灾难恢复规划 disaster recovery planning

DRP

为了规避灾难带来的损失和保证信息系统所支持的**关键业务功能**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。

3.5

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通信、电力、交通及其它关键基础设施受到严重破坏，或大规模人口疏散的事件，导致无法维持信息系统正常运行。例如：地震、大型公共卫生事件、恐怖袭击、区域性通信网故障、区域性电网故障等。

3.6

风险分析 risk analysis

RA

确定影响信息系统正常运行的风险，评估对单位业务运营至关重要的功能，定义降低潜在危险控制手段的流程。风险分析经常会涉及到对特殊事件发生可能性的评估。

3.7

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。

3.8

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。

3.9

生产系统 production system

正常情况下支持单位生产运行的信息系统。包括主数据、主数据处理系统和主网络。

3.10

生产中心 production center

生产系统所在的数据中心。

3.11

灾难备份中心 backup center for disaster recovery

灾难发生后，接替**生产中心**进行数据处理和支持关键业务功能运作的场所，包括备用数据中心、备用工作环境、备用生活设施等。形成灾难恢复能力还需配备相关业务、技术等人员，并建立相应的运作机制。

3.12

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、业务和技术等相关人员进行备份的措施。

3.13

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网络系统等组成的信息系统。

3.14

灾难恢复预案 disaster recovery plan

定义信息系统灾难恢复所需组织、流程、资源等预先制定的行动方案（以下简称“预案”）。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。

3.15

同城备份 regional backup

生产中心与灾难备份中心处于同一地理区域，面临同一区域性灾难风险，一般距离在数十公里以内，可实现同步数据复制。

3.16

异地备份 non-regional backup

生产中心与灾难备份中心处于不同地理区域，一般不会同时面临同一区域性灾难风险，一般距离在数百公里以上。

3.17

恢复时间目标 recovery time objective

RTO

灾难发生后，信息系统从停顿到必须恢复的时间要求。

3.18

恢复点目标 recovery point objective

RPO

灾难发生后，数据必须恢复到的时间点要求。

3.19

灾难恢复外包 outsourcing for diasater recovery

选择外部资源提供灾难恢复服务，例如：承担或协助制定信息系统灾难恢复规划，提供或协助建设灾难备份设施，负责运行维护灾难备份中心，提供或协助应急响应技术支持工作等。

3.20

演练 exercise

为提高灾难恢复能力，基于**灾难恢复预案**进行的演习，形式包括桌面演练、模拟演练、实战演练。

3.21

应急响应 emergency response

为应对突发事件、最大化减少突发事件对业务运作的影响而采取的紧急行动。

3.22

重建 restoration

在灾难对单位原生产中心造成损害后，为了使业务恢复到正常运行状态而修复原生产中心或在其他地址重新建造生产中心的过程。

3.23

回退 return

生产中心重建完成并达到各项规范所要求的运营条件后，单位的信息系统由灾难备份中心迁移到已修复的或新建的生产中心并恢复运行的过程。

3.24

强制决策点 mandatory decision point

为了实现灾难恢复时间目标，在灾难事件发生后必须决定是否启动**灾难恢复预案**的时间点。

4 银行业信息系统灾难恢复综述

4.1 灾难恢复工作内容

灾难恢复工作主要包括以下内容：

- 组织机构设立和职责；
- 灾难恢复需求分析；
- 灾难恢复策略制定；
- 灾难备份系统实施；
- 灾难备份中心运行维护；
- 灾难恢复预案制订、演练和管理；
- 应急响应和灾难恢复。

4.2 灾难恢复的周期性工作

4.2.1 需求分析

灾难恢复的需求分析主要包含风险分析和业务影响分析。

灾难恢复的需求应定期进行再分析，再分析周期最长为三年。当生产中心环境、生产系统或业务流程发生重大变更时，单位应立即启动灾难恢复需求再分析工作。

4.2.2 策略制定

单位应统筹规划信息系统灾难恢复工作，制定统一的灾难恢复策略。三年及以上的灾难恢复策略规划应满足本规范7.2.2描述的最低灾难恢复能力等级要求。三年以下的临时性灾难恢复策略可降低一个灾难恢复能力等级，或部分系统降低一个灾难恢复能力等级。

单位应定期根据最新的灾难恢复需求分析重审和修订灾难恢复策略。

4.2.3 技术方案管理

单位应定期根据最新的灾难恢复策略复审和调整灾难恢复技术方案。

4.2.4 预案管理

单位应定期根据最新的灾难恢复策略复审和修订灾难恢复预案。每年应至少组织一次灾难恢复预案的审查和批准工作。

4.3 机构间合作

单位应加强与其业务密切相关的机构间的协调联系，相互合作、分享经验，共同评估面临的风险，协同制定灾难恢复策略，提高银行业整体风险防范和灾难恢复能力。

5 组织机构设立和职责

5.1 组织机构设立

单位应结合具体情况设立灾难恢复组织机构，明确工作职责。单位的灾难恢复组织机构应在灾难恢复预案中准确说明。

灾难恢复组织机构应包含灾难恢复规划建设、运行维护、应急响应和灾难恢复等各阶段工作所需的人员，有关人员可为专职，也可为兼职。关键岗位的人员应有备份。

可根据信息系统和分支机构情况设立不同级别的灾难恢复组织机构，如设立总行和分支机构的多级灾难恢复组织机构。

5.2 组织机构的组成和职责

灾难恢复组织机构应分为决策层、管理层和执行层。

a) 决策层主要由单位高层管理者组成，决策信息系统灾难恢复的重大事宜，主要职责如下：
   - —— 确定灾难恢复战略；
   - —— 审核批准灾难恢复策略；
   - —— 审核批准灾难恢复经费预算；
   - —— 审核批准灾难备份设施建设；
   - —— 审核批准灾难恢复预案；
   - —— 批准启动灾难恢复预案；
   - —— 决策应急响应与恢复重大事宜；
   - —— 审核批准对外情况通报和信息发布；
   - —— 批准生产中心的重建与回退。

b) 管理层主要由单位的业务、技术、后勤等相关部门负责人组成，在决策层领导下开展工作，负责管理和协调信息系统灾难恢复工作，主要职责如下：
   - —— 组织制定灾难恢复策略；
   - —— 编制灾难恢复经费预算；
   - —— 组织灾难备份中心建设；
   - —— 管理灾难备份中心；
   - —— 组织制定灾难恢复预案；
   - —— 组织实施灾难恢复预案的演练；
   - —— 协调内外部灾难恢复资源；
   - —— 指挥和协调应急响应与恢复工作；
   - —— 指挥和协调生产中心的重建与回退工作；
   - —— 负责内部信息通报和沟通；
   - —— 组织和管理媒体公关工作；
   - —— 监督、检查和总结灾难恢复工作。

c) 执行层主要由单位的业务、技术、后勤等相关部门工作人员和外部机构人员组成，在管理层的领导下，负责灾难恢复的具体实施工作，主要职责如下：

—— 提出灾难恢复需求和策略建议；
—— 实施灾难备份中心建设；
—— 运行维护灾难备份中心；
—— 提供灾难恢复的专业技术支持；
—— 开发、测试、培训、演练和维护灾难恢复预案；
—— 实施应急响应和恢复工作；
—— 实施生产中心的重建和回退工作；
—— 负责灾难恢复过程的记录、报告和通讯联络；
—— 承担灾难抢修、拯救和损害评估；
—— 负责资源保障和供应；
—— 负责灾难发生后的外部协作；
—— 分析和总结灾难恢复工作。

6 灾难恢复需求分析

6.1 风险分析

6.1.1 确定风险分析目标

单位应根据长期可持续发展和信息化建设的战略目标，明确风险分析目标，全面识别信息系统灾难风险威胁和脆弱性。

6.1.2 确定风险分析范围

单位应根据信息系统的范围和特点，全面识别和分析影响信息系统正常运行的灾难风险要素。

单位应根据信息系统支持业务的区域范围，分析信息系统面临的区域性灾难风险。

单位应根据业务经营领域，分析信息系统中断造成的金融领域关联性风险。金融领域关联性风险指由于部分金融机构不能履行职责，导致其他机构无法开展特定业务，造成连锁反应，进而影响金融体系稳定的风险。

6.1.3 风险分析方法

a） 资产识别

资产是具有价值的信息或资源，是单位风险分析所要保护的对象，它以无形、有形的形式存在，主要包括：基础设施、硬件、软件、数据、文档、服务和声誉等。单位应对资产进行分类以区分资产的不同重要程度并确定重要资产的范围，应对资产进行标识以区分资产对业务正常运作的不同影响程度，据此确定资产的等级。

b） 威胁识别

威胁指对信息资产构成潜在破坏的可能性因素。灾难风险的威胁有多种分类方法，主要包括：

—— 自然或人为；
—— 无意或有意；
—— 内部、外部或内外勾结；
—— 在控制能力之内或超出控制能力之外；
—— 可先期预警或不可先期预警。

c) 脆弱性识别

脆弱性是可能被威胁利用的信息资产的弱点。脆弱性识别是风险分析中的一个主要环节。脆弱性识别可以从环境、业务、网络、系统、应用等层次进行识别。脆弱性识别的依据可以是国际或国家的安全标准，也可以是行业规范、应用流程的安全要求。对应用在不同环境中的相同弱点，其脆弱性严重程度是不同的。信息系统所采用的协议、应用流程的完备与否、与其他网络的互联

等也应考虑在内。

脆弱性识别时的数据应来自于信息系统的所有者、使用者，以及相关业务领域和软硬件方面的专业人员等。脆弱性识别所采用的方法主要有：问卷调查、工具检测、人工核查、文档查阅和渗透性测试等。

脆弱性识别主要从技术和管理两个方面进行，技术脆弱性涉及物理层、网络层、系统层、应用层等各个层面的安全问题。管理脆弱性可分为技术管理脆弱性和组织管理脆弱性两方面，前者与具体技术活动相关，后者与管理环境相关。

d) 风险计算

风险计算是采用适当的方法与工具确定威胁利用脆弱性导致信息系统灾难发生的可能性，主要包括以下内容：

1、根据威胁出现的频率及脆弱性状况，计算威胁利用脆弱性导致灾难发生的可能性；

2、根据资产重要程度及脆弱性严重程度，计算灾难发生后的损失；

3、根据计算出的灾难发生的可能性以及灾难的损失，计算风险值，并进行风险等级划分。

6.1.4 风险控制

评估现有安全策略和措施的有效性，确定信息系统仍然可能存在的风险，即残余风险。

单位应根据资产等级及残余风险发生的概率、可能造成的损失和风险防范成本，评估风险可接受的程度，确定可接受的风险。针对不可接受的风险，按照灾难恢复资源的成本与风险可能造成损失之间取得平衡的原则（以下简称“成本风险平衡原则”），确定风险防范措施，并定期评估残余风险。

6.2 业务影响分析

6.2.1 业务功能分析

通过业务功能分析，确定业务功能的关键程度，分析的内容主要包括：

—— 政策性：业务功能的政策要求；

—— 业务性质：核心业务或非核心业务；

—— 业务服务范围：涉及到的内外部机构、用户等范围；

—— 数据集中程度：业务数据的集中与处理的集中、地域分布；

—— 业务时间敏感性：实时与非实时业务、业务运行时段和用户使用频度；

—— 业务功能的关联性：与本单位其它业务功能及其他机构业务功能之间的关联程度。

6.2.2 评估业务中断影响

a) 以量化的方法，评估业务功能中断可能造成的直接经济损失和间接经济损失，主要包括：

—— 直接经济损失：

- 资产损失；
- 收入损失；
- 额外费用增加；
- 财务处罚。

—— 间接经济损失：

- 预期收益损失；
- 商业机会损失；
- 市场份额影响。

b) 以非量化的方法，评估业务功能中断可能造成的影响，主要包括：

—— 社会影响；

—— 法律影响；

—— 信用影响；

—— 品牌影响。

6.3 确定灾难恢复需求

6.3.1 确定需求等级

单位应根据风险分析、业务功能分析和业务中断影响分析的结论，将信息系统按时间敏感性分成三类需求等级：

a)第一类

—— 短时间中断将对国家、外部机构和社会产生重大影响的系统；

—— 短时间中断将严重影响单位关键业务功能并造成重大经济损失的系统；

—— 单位和用户对系统短时间中断不能容忍的系统。

b)第二类

—— 短时间中断将影响单位部分关键业务功能并造成较大经济损失的系统；

—— 单位和用户对系统短时间中断具有一定容忍度的系统。

c)第三类

—— 短时间中断将影响单位非关键业务功能并造成一定经济损失的系统；

—— 业务功能容许一段时间中断的系统。

6.3.2 确定最低恢复要求

根据信息系统的时间敏感性，确定信息系统灾难恢复目标的最低要求：

a) 第一类：RTO<6 小时，RPO<15 分钟；

b) 第二类：RTO<24 小时，RPO<120 分钟；

c) 第三类：RTO<7 天。

6.3.3 确定恢复优先级

根据业务功能分析、业务中断影响分析并综合考虑系统间的依赖性，确定信息系统的恢复优先级。

6.3.4 确定相关资源

单位应确定灾难恢复所需的七个方面资源要素：

—— 数据备份系统；

—— 备用数据处理系统；

—— 备用网络系统；

—— 备用基础设施；

—— 技术支持能力；

—— 运行维护管理能力；

—— 灾难恢复预案。

7 灾难恢复策略制定

7.1 成本风险分析和策略的确定

按照成本风险平衡原则，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。灾难恢复策略是单位为了达到灾难恢复目标而制定的规划、方法和措施。灾难恢复策略主要包括：

—— 灾难恢复建设计划；

—— 灾难恢复能力等级；

—— 灾难恢复建设模式；

—— 灾难备份中心布局。

7.2 灾难恢复能力等级

7.2.1 灾难恢复能力等级的确定

单位应根据信息系统的RTO和RPO要求，确定信息系统的灾难恢复能力等级，参见附录B。

7.2.2 最低的灾难恢复能力等级要求

信息系统根据灾难恢复需求等级，最低应达到以下灾难恢复能力等级：

a) 第一类：5 级；
b) 第二类：3 级；
c) 第三类：2 级。

7.3 灾难备份中心的布局

7.3.1 布局原则

a) 灾难备份中心应设置在中华人民共和国境内；
b) 灾难备份中心与生产中心之间距离合理，应避免灾难备份中心与生产中心同时遭受同类风险；
c) 灾难备份中心的选址应服从国家战略安全要求，并综合考虑生产中心与灾难备份中心交通和电讯的便利性与多样性，以及灾难备份中心当地的业务与技术支持能力、电讯资源、地理地质环境、公共资源与服务配套能力等外部支持条件。

7.3.2 布局模式

单位应根据成本风险平衡原则以及运行管理要求，可采用以下多种布局模式：

—— 一主一备：一个生产中心，一个备份中心；
—— 一主多备：一个生产中心，多个备份中心；
—— 互为备份：两个生产中心互相备份；
—— 多主一备：多个生产中心共享一个备份中心；
—— 混合方式：以上方式的混合。

7.4 资源、服务的获取和保障

7.4.1 资源的获取

a) 基础设施

灾难恢复的基础设施包括机房和其他辅助设施，其获取方式包括：

—— 自建方式：单位可自行建设灾难恢复基础设施，基础设施的功能和规格应符合相应的灾难恢复能力等级要求。在选择自建方式时应综合考虑投资效益、运营管理成本、运营管理队伍的稳定性和应急能力等因素。
—— 共享方式：单位可采用多方共建或外包方式获取灾难恢复基础设施，基础设施的功能和规格应符合相应的灾难恢复能力等级要求。在选择共享方式时应综合考虑责任界定、信息的安全保密和服务水平要求等因素。

b) 数据备份系统、备用数据处理系统

用于灾难恢复的数据备份系统和备用数据处理系统设备，其获取方式包括：

—— 自行采购；
—— 与供应商签订紧急供货协议；
—— 租赁；
—— 外包。

c) 通信网络

用于灾难恢复的通信网络包括生产中心和灾难备份中心间的备份网络和最终用户访问灾难备份中心的网络，通信线路应至少有两种以上不同的物理线路，其获取方式包括：

—— 自行建设；
—— 租用运营商线路。

7.4.2 专业服务的获取

在包括自建在内的各种灾难备份中心建设模式下，灾难备份中心的日常运行维护、应急响应和灾难恢复均可引入专业外包服务机制。

a) 灾难恢复咨询服务

咨询服务包括风险分析、业务影响分析、灾难恢复策略制定、灾难备份中心规划与建设、灾难恢复预案制订、测试、培训和演练等。咨询服务的获取方式包括：

—— 委托外部咨询机构；

—— 联合外部咨询机构。

b) 灾难恢复技术支持服务

技术支持服务对象包括数据备份系统、备用数据处理系统和通信网络等，其获取方式包括：

—— 自有技术支持队伍；

—— 专业服务提供商；

—— 设备提供商。

c) 灾难恢复运营管理服务

运营管理服务包括灾难备份中心的日常运行维护和灾难恢复预案的维护等，其获取方式包括：

—— 自主运行维护；

—— 外包。

7.4.3 外包的管理

单位应加强灾难恢复服务外包管理，与服务外包提供商签订安全保密、服务水平等协议，明确服务外包提供商的职责和应承担的法律责任，并定期验证服务外包提供商的服务水平和能力，通过采取各种管控措施，保障服务外包的安全可控和服务质量。对于涉及国家秘密信息的系统，单位应遵从国家有关政策、法规，从保障国家信息安全角度慎重选择服务外包提供商。

灾难恢复服务外包提供商应符合国家和行业的相关服务资质要求，并至少满足以下要求：

a) 应熟悉银行业信息系统架构和业务流程，具有灾难恢复外包服务的成功案例和实践经验；

b) 应具有完备的信息安全管理体系和服务质量保证体系，并通过 ISO27001、ISO9001 等认证；

c) 应独立运营管理灾难备份中心，且机房的可用性应至少达到 99.9%,其所能提供的灾难恢复能力等级应达到 5 级以上（含 5 级）。

8 灾难备份中心的建设

8.1 基础设施建设

灾难备份中心基础设施建设包括机房和辅助设施建设等。灾难备份中心的选址、规划、设计、建设和验收，应符合国家和金融行业有关标准和规范要求。机房可用性应至少达到 99.9%。

8.2 灾难备份系统建设

8.2.1 技术方案设计

根据灾难恢复策略制定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网络系统。技术方案中所涉及的系统应：

—— 获得同生产系统相当的安全防护水平；

—— 具有可扩展性。

8.2.2 技术方案验证测试

为满足灾难恢复策略的要求，应对技术方案中关键技术应用的可行性进行验证测试，并记录和保存验证测试的结果。

8.2.3 系统集成和测试

应制定灾难备份系统集成与测试计划并组织实施。通过技术和业务测试，确认灾难备份系统的功能与性能达到设计指标要求。

8.3 项目监理

单位可按需委托专业的第三方监理机构，对灾难备份中心工程实施进行有效的监督管理，保证工程进度、质量和资金管理目标的完成。

9 灾难备份中心的运行维护管理

9.1 管理制度建设

为了保证灾难备份中心的有效性，应建立完善的运行维护管理制度和操作规程，明确岗位职责。主要内容包括：

—— 灾难备份系统运维管理：问题管理、事件管理、变更管理、配置管理、安全管理、服务水平管理、介质与文档管理等规程；

—— 灾难备份中心保障管理：机房管理、环境设施管理、后勤保障管理等制度；

—— 灾难备份中心可用性管理：人员管理制度、灾难备份系统基准维护管理制度（定期对灾难备份系统面向生产系统的符合性检查维护制度）、功能性子系统验证和演练规程（针对灾难备份系统中的部分子系统进行测试验证及演练制度）、灾难恢复预案以及相关操作手册的管理制度、应急处理工作规程等。

9.2 运行维护工作内容

9.2.1 基础设施

应定期维护基础设施，保证灾难备份中心工作设施（电力、通讯、机房环境、安防监控设施等）、辅助设施和生活设施等的可用性。

9.2.2 数据备份系统

应定期检测维护数据备份系统，保证数据备份系统软硬件可用性，并确保数据备份系统的备份数据与生产系统相一致。

生产系统的各种补丁、更新以及变化应及时更新到数据备份系统中。

9.2.3 备用数据处理系统

应定期检测维护备用数据处理系统，包括硬件系统、系统软件和应用软件检测。

生产系统的各种补丁、更新以及变化应及时更新到备用数据处理系统中。

9.2.4 备用网络系统

应定期检测维护备用网络系统，包括数据网络、存储网络和语音通信系统等。

生产系统的各种补丁、更新以及变化应及时更新到备用网络系统中。

9.3 运行维护的资源保障

灾难备份中心应配备一定数量具有灾难恢复专业素质的人员，必要的工作与生活等设施，保障足够的运维资金投入，确保灾难备份中心的正常运作。

10 灾难恢复预案的制订、演练与管理

10.1 灾难恢复预案的制订

10.1.1 制订内容

单位应结合自身实际开发灾难恢复预案（以下简称预案）。灾难恢复预案包括应急预案和信息系统灾难恢复预案。

应急预案至少应包含以下内容：

a) 灾难场景定义、目标和范围；
b) 应急管理组织机构；
c) 应急恢复决策及授权，包括应急恢复条件、权限、处置策略以及强制决策点等；
d) 应急响应工作规程，包括紧急事件初始响应、损害评估、指挥中心成立和人员召集、灾难预警、灾难宣告、启动灾难切换流程等；
e) 应急管理工作中使用的各项文档，包括通讯录、工作文档、应急工具等。

信息系统灾难恢复预案至少应包含以下内容：

a) 灾难恢复范围和目标；
b) 灾难切换规程；
c) 灾后重续运行操作指引；
d) 各系统灾难切换操作手册。

10.1.2 制订原则

a) 完整性：预案应涵盖灾难恢复工作的各个环节，以及灾难恢复所需的尽可能全面的数据和资料；
b) 易用性：预案应采用易于理解的语言和图表，适合在紧急情况下使用；
c) 明确性：预案应采用清晰的结构，对资源及工作内容和步骤进行明确的描述，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：预案应与其它应急预案体系有机结合。

10.1.3 制订过程

a) 初稿的制订：按照风险分析和业务影响分析所确定的灾难恢复内容，根据灾难恢复能力等级的要求，结合单位其它相关的应急预案，撰写灾难恢复预案的初稿；
b) 初稿的评审：应对灾难恢复预案初稿的完整性、易用性、明确性、有效性和兼容性进行评审；
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) 预案的测试和验证：制定测试用例，进行基本单元测试、关联测试和整体测试，验证预案的合理性和有效性。测试的整个过程应有详细的记录，并形成测试报告；
e) 预案的审查和批准：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，并由单位决策层对经过测试和验证的灾难恢复预案进行审查和批准，确定为预案的执行稿。

10.2 灾难恢复预案的演练

10.2.1 演练的目的

演练是为了验证灾难恢复预案的完整性、易用性、明确性、有效性和兼容性，提高单位的预案执行能力。

10.2.2 演练的形式

演练包括事前通告相关参加演练人员和非事前通告两种方式。演练的主要形式包括：

a) 桌面演练：组织相关的灾难恢复组织机构人员，以会议形式模拟各种灾难场景，集中讨论应急响应和恢复流程中的管理与指挥协调，验证灾难恢复预案的决策和指挥能力；
b) 模拟演练：模拟灾难场景，利用灾难备份系统和灾难恢复预案模拟系统切换和业务恢复，通常不涉及真实的业务操作；
c) 实战演练：模拟灾难场景，利用灾难备份系统和灾难恢复预案完成系统切换和业务恢复，涉及真实的业务操作，在演练完成后需进行数据和环境的回导。

10.2.3 演练的层次

单位根据演练工作涉及的范围，开展多层次的演练工作，主要包括：

a) 以指挥协调为主的指挥演练；
b) 以技术操作为主的技术演练；
c) 以业务恢复为主的业务演练。

10.2.4 演练的组织实施

单位每年应至少组织一次实战演练，可根据单位实际情况不定期地组织各种形式、层次与范围的演练，逐年提高演练的难度和复杂性。

在演练前，应制订演练方案，明确演练目标、涉及的形式、层次和范围，设定灾难情景、演练流程、操作内容、业务验证测试、应急资源、演练的风险及其应对措施。演练应尽量减少对正常业务和生产的影响。

10.2.5 演练的评估

演练完成后，应对演练的组织、过程、效果进行评估，主要包括以下内容：

a) 灾难恢复预案的有效性和可用性；

b) 演练结果与演练目标的差距；
c) 演练过程中发现的生产系统和灾难备份系统存在的问题；
d) 演练工作的组织；
e) 参演人员的应急能力；
f) 应急资源的协调、保障能力。

10.2.6 演练后预案的修订

应根据演练评估结论对灾难恢复预案进行维护和更新。在下次演练中应加强对更新部分的演练，验证更新部分的有效性。

10.3 灾难恢复预案的管理

10.3.1 保管、更新和分发

单位应安排专人负责灾难恢复预案的日常维护管理，主要包括以下工作内容：

—— 灾难恢复预案应作为单位保密文件保管；
—— 灾难恢复组织机构的所有工作人员应保留最新版本的灾难恢复预案；
—— 预案以多种形式的介质拷贝保存在不同的安全地点，应保证在生产中心以外的安全地点存放有灾难恢复预案，并保障预案的可获取性；
—— 应加强灾难恢复预案版本管理、分发和回收。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。

10.3.2 更新维护

灾难恢复预案的更新维护，主要包括以下工作要求：

—— 灾难恢复预案涉及的内容发生变更后应立即更新灾难恢复预案；
—— 灾难恢复预案涉及的机构、人员有义务向预案管理人员提供变更信息；
—— 演练后应根据演练评估结论立即更新灾难恢复预案；
—— 灾难恢复预案若发生重大变更，应由管理层进行必要的审查。

10.3.3 教育和培训

应定期组织灾难恢复预案的教育和培训，确保相关人员熟知预案。培训后保留培训的记录。

11 应急响应和灾难恢复

11.1 应急响应

信息系统发生紧急事件后，单位应根据应急预案，注意以下紧急措施：

a) 启动应急机制，响应紧急事件；
b) 接收和报告紧急事件信息，调度应急资源；
c) 评估分析紧急事件影响范围、程度，初步诊断紧急事件原因，判断恢复业务功能所需时间；
d) 采取必要的控制措施，最大限度保护运行数据安全、抑制事态恶化、降低损失；
e) 根据有关制度规定，通报相关主管部门，并做好社会公告和客户服务工作；

应急响应的具体工作要点可参见附录 A.1。

单位根据对紧急事件的处置和评估结果，判断紧急事件是否为灾难事件，决策后，分别进入应急处置流程和灾难恢复流程。

11.2 灾难恢复

信息系统发生灾难事件后，单位应根据灾难恢复预案有序实施应对，注意以下环节的工作：

a) 采用最快、最有效的联络方式，通知和召集灾难恢复预案中各组织机构人员，进入操作流程；
b) 遵循一人指挥原则，服从决策层或其授权的统一指挥，业务、技术、后勤等部门相关人员密切协作，加强沟通；
c) 快速调动和有效配置灾难恢复资源；
d) 根据有关制度规定，通报相关主管部门，并做好社会公告和客户服务工作；

e) 合理处置灾难事件，密切跟踪事态变化和恢复进程；

f) 本着最小影响、最小损失的原则，合理时间内决策切换至灾难备份中心接替运行。

灾难恢复的具体工作要点可参考附录A.2。

11.3 重建与回退

11.3.1 生产系统的重建

灾难发生后，单位应评估灾难造成的损失，评估内容主要包括：

a) 灾难破坏情况；

b) 业务影响程度；

c) 原址重建的可能性或新址选择；

d) 挽救的设备清单和测试情况。

单位应根据损失评估情况，结合灾难备份系统可持续运行的最长时间，确定生产系统的修复或者重新建设方案，实施生产系统的重新建设和功能恢复。

11.3.2 生产系统的回退

生产系统的回退主要内容包括：

—— 重建系统的测试；

—— 网络的回退切换；

—— 系统的回退切换；

—— 数据的回退切换，检查系统中的备份数据；

—— 业务功能的切换；

—— 相关数据安全处理，防止重要信息的泄漏；

—— 灾难备份系统恢复为备用状态；

—— 人员和重要设备撤离。

12 监督管理

12.1 审计

灾难恢复工作的审计分为内部审计和外部审计。内部审计由单位内部人员组织实施。外部审计由具有国家相应监管部门认定资质的中介机构组织实施。

审计工作主要包括以下内容：

—— 风险评估和管控；

—— 组织协作和授权机制；

—— 灾难恢复策略；

—— 灾难恢复工作的制度建设

—— 灾难恢复预案的管理和维护；

—— 演练组织和演练评估；

—— 灾难备份中心的可用性和有效性。

单位应根据信息系统的灾难恢复工作情况，确定审计频率。单位应每年至少组织一次内部灾难恢复工作审计。

灾难恢复审计工作结论应形成审计报告，审计报告应作为风险内控措施的成果进行存档，可纳入IT系统年度审计。

审计过程所涉及的资料调阅应有交接手续，严格控制审计过程中涉密资料的保管和发放，中介机构应保守被审计公司的商业秘密和风险信息。

12.2 备案

单位灾难恢复工作情况应在每年年底前向中国人民银行报备，主要内容包括：

——　单位的灾难备份中心建设及重大变更情况；

——　单位的年度灾难恢复重大演练情况。

附录 A
（资料性附录）
应急响应和灾难恢复工作要点

A.1 应急响应工作要点

A.1.1 事件报告与检测

a) 紧急事件报告，按照单位的紧急事件报告流程立即报告。

b) 应急响应人员应记录事件信息，并开展以下主要工作：

—— 判断事件的类型：例如：网络系统故障、基础设施故障、服务器硬件故障、应用软件故障、人为破坏、自然灾害等；

—— 分析事件影响地域和业务的范围、程度等，确定事件的严重程度；

—— 初步诊断事件发生的原因；

—— 评估事件的影响和损失；

—— 分析业务功能的预计恢复时间。

c) 组织现场检查和评估，形成紧急事件报告，上报决策层或管理层，并提出下一步工作建议。

A.1.2 预警与抢救

a) 预警发布

—— 向单位有关部门通报紧急事件情况；

—— 向外部业务关联机构发出预警信息；

—— 通知应急响应相关人员到指定地点集合，并开始抢救工作；

—— 通知灾难备份中心进入预警状态；

—— 如果紧急事件涉及外部服务供应商，根据服务供应商的服务协议进行联系，要求参与前期的损失评估和抢救等工作。

b) 挽救和减少损失

—— 在保证安全的前提下，积极调动本单位和社会救援机构的力量，抢救人员、资产设备和数据等资源，减少损失；

—— 安排抢救物资，运输到事先准备的场地；

A.1.3 分析评估

a) 对事件的原因和事态发展进行判断；

b) 对损失进行评估和记录；

c) 分析和决策应急处置策略；

d) 在接到报告后和强制决策点之前，评估是否启动灾难备份中心和灾难恢复预案。灾难宣告的强制决策点有多种确定方式，常用方法之一是：若紧急事件评估为灾难，从事件发生起计算，信息系统恢复要求RTO减去预计恢复操作时间这个时刻为灾难宣告的强制决策点。

A.1.4 应急处置

a) 应急处置工作在强制决策点之前完成。如果紧急事件在规定的时间内解决，通知人员取消预警；

b) 若需要，安排人员安全疏散，安排人员救助；

c) 若需要，立刻通知厂商维护人员按照合同约定的时间到现场进行本地抢修；

d) 将目前抢救进程情况汇报决策层；

e) 根据决策意见或强行启动灾难恢复预案的条件，启动灾难恢复预案，进入灾难恢复流程；

f) 根据事态发展，决策层按照有关规定负责向人民银行和有关监管机构报告突发事件情况；

g） 应严格记录所有事件相关的处理过程。

必要时，借助社会救援力量。

A.2 灾难恢复工作要点

A.2.1 灾难宣告

a） 灾难宣告授权

—— 灾难宣告由单位的授权人员进行。灾难宣告的决策通常由单位的决策层人员担任。应事先安排备份授权人员；

—— 授权人员名单和联系方式应在灾难恢复预案中记录,并保存在每个灾难备份中心。

b） 灾难宣告方式

—— 灾难宣告可采用多种方式，包括电话通知、传真和其它事先准备的紧急通信方式等；

—— 公关和媒体关系部门负责对外通报相关信息，通报信息的内容和范围应符合相关规定，并经决策层领导批准。

c） 灾难宣告可包括以下主要内容：

—— 灾难的类型、时间和地点；

—— 灾难影响范围；

—— 目前的恢复状态；

—— 灾难恢复预案的启动；

—— 灾难恢复目标和工作要求。

A.2.2 启动灾难恢复预案

启动经过审批的指定版本的灾难恢复预案。

A.2.3 人员联络和集合

按照灾难恢复预案中人员通知方式，完成人员联络和集合。

A.2.4 资源调度

统一调度和采购灾难恢复的各项资源，做好资源管理和调度工作。

A.2.5 灾难恢复指挥

灾难恢复小组应按照在灾难恢复预案中的要求开展指挥、协调和管理工作。

执行层人员按照预案规定的系统和业务优先级顺序进行恢复工作，并随时报告工作进度。

A.2.6 信息系统恢复

按照恢复优先级顺序恢复信息系统。

A.2.7 恢复成功通报

在灾难备份系统投入运行后,确保提供各项技术支持和保障工作,并及时通报相关管理和业务部门,配合完成业务功能恢复。

A.2.8 过程记录和资料存档

严格记录所有事件相关的信息和处理过程，以备事后检查。

附录 B
（资料性附录）
RTO/RPO 与灾难恢复能力等级的关系

B.1 RTO/RPO与灾难恢复能力等级的关系

单位可参照表B.1，依据RTO和RPO确定信息系统的灾难恢复能力等级：

表 B.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