ICS 35.020
L 07
备案号:

MH

# 中华人民共和国民用航空行业标准

MH/T 0026—2005

# 民用航空重要信息系统空难备份与恢复管理规范

**Management specification for important information system of civil aviation disaster backup & recovery**

2005－01－20 发布　　2005－05－01 实施

中国民用航空总局　发布

# 目　　次

# 前　言

本标准由中国民用航空总局人事科教司提出并负责解释。

本标准由中国民用航空总局航空安全技术中心归口。

本标准起草单位：中国航空结算中心。

本标准主要起草人：刘继平、钱农、江志强、杜伟军、陈鸿、祁水平、杨献峰、马艳锋。

# 民用航空重要信息系统灾难备份与恢复管理规范

## 1 范围

本标准规定了民用航空重要信息系统灾难备份与恢复的管理规范。

本标准适用于民用航空重要信息系统灾难备份与恢复的实施。

## 2 术语和定义

下列术语和定义适用于本标准。

2.1

**重要信息系统 important information system**

受到破坏后会对国家或行业安全、社会秩序、公共利益造成较大损害或带来严重经济损失的信息系统。

2.2

**灾难 disaster**

造成重要信息系统部分或全部的计算机软件、硬件设备、附属设备、数据、文档或机房环境损坏以至于严重影响业务正常运行的事件。

2.3

**灾难恢复 disaster recovery**

将重要信息系统支持的组织功能从灾难造成的停顿状态恢复到可以接受的运行状态。

2.4

**灾难备份 disaster backup**

为确保灾难恢复的顺利实施，利用技术、管理手段以及相关资源对已有的关键信息技术服务进行有效备份的过程。

2.5

**灾难备份等级 disaster backup class**

为确保灾难备份的顺利实施，按灾难备份范围、系统备份方式等将灾难备份划分为多个级别。

2.6

**灾难备份中心 disaster backup center**

灾难发生时，接替原数据处理中心运行的备份处理中心。

2.7

**灾难恢复预案 disaster recovery plan**

为确保关键信息技术服务能够持续进行，描述重要信息系统在灾难发生后业务恢复过程的预案，包括所需资源、应采取的行动、需完成的任务以及所需的数据。

2.8

**恢复时间目标 recovery time objective**

从灾难发生到关键业务功能恢复所需的时间要求。

2.9

**恢复点目标 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 机构与职责

### 3.1 机构

3.1.1 民航各单位应成立重要信息系统灾难备份与恢复领导小组（以下简称领导小组）、重要信息系统灾难备份与恢复专家小组（以下简称专家小组）、重要信息系统灾难备份与恢复建设组（以下简称建设组）、重要信息系统灾难备份与恢复运行维护组（以下简称运维组）和重要信息系统灾难恢复组（以下简称恢复组）来负责本单位的灾难备份与灾难恢复工作。

3.1.2 领导小组的成员应由高级管理层人员组成，并由单位的法人作为第一责任人。

### 3.2 职责

3.2.1 领导小组负责灾难备份与恢复项目的筹备、立项，组建专家小组、建设组、运维组和恢复组，审批灾难备份方案和灾难恢复预案。

3.2.2 专家小组负责审核灾难备份方案和灾难恢复预案，并为实施灾难备份与恢复的相关人员提供指导。

3.2.3 建设组负责灾难备份与恢复过程中的建设工作，包括对重要信息系统进行风险评估和业务影响分析，编写并维护灾难备份方案和灾难恢复预案，监督指导灾难恢复预案的测试和演练，负责灾难备份的实施、灾难备份中心的建设和对相关人员的培训。

3.2.4 运维组负责灾难备份与恢复实施过程中的日常运行和维护。

3.2.5 恢复组负责定期测试、演练灾难恢复预案和灾难发生时实施灾难恢复。

## 4 风险评估与业务影响分析

### 4.1 确定重要信息系统相关资源

4.1.1 确定需要进行风险评估的信息系统，收集相关信息，包括系统架构、软件、硬件、数据信息、用户信息、系统功能、系统的重要程度和安全策略等。

4.1.2 收集重要信息系统相关资料可采用问卷、座谈、查看文档和工具收集等方式。

### 4.2 风险评估

4.2.1 应对所确定的重要信息系统相关资源现状进行分析，得出分析报告，报告应形成电子和打印文档并妥善保存。

4.2.2 评估的风险类型应包括：

a） 自然风险，包括地震、水灾、火灾、台风等；

b） 人为风险，包括战争、恐怖袭击、人为破坏、电脑病毒等；

c） 其他风险，包括设备故障、电力中断等。

4.2.3 评估的内容应包括：

a） 风险类型：自然风险、人为风险和其他风险；

b） 风险发生的概率及风险可能造成的损失；

c） 业务运作中的漏洞；

d） 各种风险发生的因果关系；

e） 风险的集中程度。

4.2.4 评估完成后，应形成风险评估报告，报告应形成电子和打印文档并妥善保存。

4.2.5 应根据风险评估报告进行风险管理，部署防范相关风险的安全控制措施，以防止或减少损害。

### 4.3 业务影响分析

4.3.1 应对关键业务进行业务影响分析，分析要点包括：

a） 各项业务停顿可能造成的损失，应考虑流失客户、损失营业额、企业形象、社会安定因素等，并将其量化；

b) 各项业务停顿的最大容忍时间；

c) 各项业务的相关性；

d) 各项业务的恢复优先级；

e) 可接受的数据损失程度；

f) 保障各项业务运作的其他最低要求。

4.3.2 应根据相关系统的拥有者、最终用户和合作伙伴所提供的信息进行业务影响分析。

4.3.3 应定期进行业务影响分析；当业务发生重大变化时，应立即进行业务影响分析。

4.3.4 业务影响分析完成后，应形成业务影响分析报告，报告应形成电子和打印文档并妥善保存。

### 4.4 成本效益分析

#### 4.4.1 成本构成

灾难备份与恢复的成本应包括重要信息系统灾难备份的建设或租用成本，运行管理成本，培训成本，灾难恢复预案制定、测试、演练与维护管理的成本以及为实现灾难恢复而获取其他相关服务的费用等。

#### 4.4.2 成本效益平衡原则

对不同的灾难恢复目标和策略，灾难备份与恢复的成本也不同。应在实施灾难备份与恢复过程中平衡所需成本与风险可能造成的损失。

### 4.5 确定灾难备份目标和灾难备份等级

4.5.1 应根据风险评估报告和业务影响分析报告，确定重要信息系统的灾难备份目标。

4.5.2 应根据风险评估报告、业务影响分析报告和成本效益平衡原则，并按 5.1 确定重要信息系统的灾难备份等级。

### 4.6 确定灾难恢复目标和优先顺序

4.6.1 应根据风险评估报告、业务影响分析报告和成本效益平衡原则，确定重要信息系统灾难恢复的目标，包括恢复时间目标、恢复点目标和灾难恢复范围。

4.6.2 应根据风险评估报告和业务影响分析报告，确定重要信息系统业务恢复的优先顺序。

## 5 灾难备份

### 5.1 灾难备份等级

#### 5.1.1 等级零：无异地备份

该等级没有在异地保存备份介质。

#### 5.1.2 等级一：备份介质异地存放

该等级需要将备份介质采用物理手段运至异地进行保存，同时可建立机房等基础设施用于日后放置信息系统处理设备。一旦灾难发生，需要在机房重新建立整套信息系统及网络并恢复数据。该等级所需的灾难恢复时间最长。

#### 5.1.3 等级二：备份介质异地存放和灾难备份中心

该等级在等级一的基础上，需要在异地设置灾难备份中心，配备充足的硬件和网络资源来支持重要信息系统的恢复。当灾难发生时利用已配置的硬件及网络资源，安装操作系统，从备份介质上恢复应用系统和数据，切换网络，支持重要业务处理。恢复速度比等级一有较大提高。

#### 5.1.4 等级三：数据通过网络传输定期备份

该等级在等级二的基础上将备份方式由物理运送介质变成网络传输，数据处理中心的部分数据通过网络定期传送到灾难备份中心进行保存，灾难备份中心保持日常运行状态。采用网络传输手段加快了灾难恢复的速度。

#### 5.1.5 等级四：活动状态的灾难备份中心

该等级在等级三的基础上，灾难备份中心与数据处理中心信息系统处理设备同时保持运行状态，具有双向恢复能力。等级四的数据及时性高于等级三，从而加快了灾难恢复速度。

5.1.6 **等级五：镜像灾难备份中心**

该等级在等级四的基础上，数据处理中心重要信息系统与灾难备份中心保持远程两阶段提交同步镜像状态。该等级还要求在灾难备份中心安装用于灾难备份的部分或全部信息系统处理设备，并具备网络切换能力。该等级对重要信息系统采用远程两阶段提交同步备份，数据丢失量进一步减少，加快灾难恢复的速度。

5.1.7 **等级六：零数据丢失**

该等级无任何数据丢失，灾难发生时数据处理能立即自动切换到灾难备份中心。

5.2 **灾难备份方案**

5.2.1 **编制灾难备份方案**

5.2.1.1 应对所有重要信息系统编制灾难备份方案。灾难备份方案的编制应做到切实有效、力求全面、责任落实到人、便于检查。灾难备份方案应形成电子和打印文档并妥善保存。

5.2.1.2 领导小组应组织建设组人员编制灾难备份方案草案；编制完成后，应由专家小组对灾难备份方案草案进行审核；审核通过，领导小组批准灾难备份方案草案后，灾难备份方案草案成为正式的灾难备份方案。

5.2.1.3 应根据风险评估和业务影响分析得出的灾难备份目标和灾难备份等级编制灾难备份方案，其中可能涉及多个级别的业务应用，并且应考虑技术手段、投资和管理等多方面的因素。

5.2.1.4 灾难备份方案应包括以下内容：

a) 灾难备份方案的名称、编号；
b) 灾难备份方案所适用的范围；
c) 灾难备份等级；
d) 灾难备份人员联络图及人员的职责；
e) 灾难备份内容列表；
f) 灾难备份的频度；
g) 灾难备份所采取的技术手段；
h) 灾难备份所需资源列表；
i) 灾难备份方案的基准。

5.2.2 **实施灾难备份方案**

5.2.2.1 应制定明确的灾难备份方案实施计划。

5.2.2.2 应由建设组负责完成灾难备份方案的实施。

5.2.2.3 如灾难备份方案实施过程中出现不合理因素，应根据实际情况，按 5.2.3 及时更新灾难备份方案。

5.2.3 **维护灾难备份方案**

5.2.3.1 应由专人定期检查维护灾难备份方案。

5.2.3.2 灾难备份方案的更新及重新编制应遵循变更管理流程，由专家小组审核，领导小组批准。

5.2.3.3 出现人员、设备等变更时，应及时更新灾难备份方案。

5.2.3.4 出现业务流程改变、信息系统改变、客户改变等情况时，应重新编制灾难备份方案。

5.3 **灾难备份管理**

5.3.1 **备份介质的管理**

5.3.1.1 应采取防磁、防潮、防火、防静电、防盗等措施妥善保存备份介质。

5.3.1.2 应记录备份介质中所保存的内容，形成电子和打印文档，并在本地和异地妥善保存。

5.3.2 **灾难备份中心的建设**

5.3.2.1 灾难备份中心的建设可采用自行建设、联合建设和租用商业化灾难备份中心三种模式。

5.3.2.2 自行建设灾难备份中心应根据灾难备份需求，按 4.4.2 的要求，充分利用资源进行建设。

5.3.2.3 联合建设灾难备份中心应由各单位协商形成统一的管理机制，明确各自职责，统筹安排灾难备份中心的技术手段，以保证各单位数据的保密性、安全性和独立性。

5.3.2.4 自行建设和联合建设灾难备份中心应考虑以下因素：

a) 地理区域：灾难备份中心离数据处理中心的距离以及灾难备份中心与数据处理中心受到相同灾难影响的可能性；

b) 可访问性：访问灾难备份中心数据所需时间和灾难备份中心工作时间；

c) 安全：灾难备份中心的安全性和保密性应满足数据的敏感级别和安全需求；

d) 环境：灾难备份中心的环境条件；

e) 费用：灾难备份中心的建设费用、运行费用等。

5.3.2.5 灾难备份中心的建设与运行应符合数据处理中心的一般管理规范，并建立与灾难备份工作相应的管理制度，如灾难备份变更管理制度、灾难备份中心安全管理制度等。

5.3.2.6 租用商业化灾难备份中心应全面考察服务提供商的综合管理水平，并应签订具有法律效力的文件来保障服务质量。

**5.3.3 灾难备份有效性检查**

5.3.3.1 灾难备份有效性检查的内容应包括：灾难备份方案的实施情况和灾难备份中心的运行情况。

5.3.3.2 灾难备份有效性检查的方式应采用全面检查与抽查相结合的方式。

5.3.3.3 建设组应组织相关人员对灾难备份的情况每年至少进行一次有效性检查，并应完成相应的文档记录。专家小组应对检查结果进行评估，提出改进建议。领导小组批准改进建议后，组织实施改进建议。

## 6 灾难恢复

### 6.1 灾难恢复预案的制定

**6.1.1 制定灾难恢复预案的原则**

根据风险评估和业务影响分析得出的灾难恢复目标和灾难恢复优先顺序制定灾难恢复预案。灾难恢复预案应明确、简洁，容易被理解、使用和维护，也易于在紧急情况下迅速启动和执行。灾难恢复预案应完整，涉及灾难恢复的整个过程。

**6.1.2 灾难恢复预案的内容**

灾难恢复预案应包括：

a) 目标：见4.6.1；

b) 优先顺序：根据4.6.2确定的优先顺序，按照逐步和顺序的格式书写；

c) 人员组成；

d) 联络清单：数据处理中心联络清单、灾难备份中心联络清单、单位各部门联络清单和供应商联络清单等；

e) 启动条件；

f) 灾难恢复的步骤和内容：见6.4；

g) 灾难恢复操作手册：灾难恢复过程中进行重要信息系统恢复的方法和步骤，包括关键业务替代作业方式及业务运行流程。

**6.1.3 灾难恢复预案的定稿**

6.1.3.1 建设组人员应按照灾难恢复预案的编制原则和灾难恢复预案的内容要求对灾难恢复预案进行编制和可行性测试。

6.1.3.2 编制完成后应由专家小组对灾难恢复预案进行审核。

6.1.3.3 审核完成后应向领导小组提交灾难恢复预案，获得批准后将灾难恢复预案形成电子和打印文档，在本地和异地由专人负责妥善保存，并分发给参与灾难恢复工作的人员。

### 6.2 灾难恢复预案的测试和演练

6.2.1 **测试和演练的管理要求**

6.2.1.1 应对灾难恢复预案进行测试。应首先对每一个部分进行单独测试，然后再整体测试灾难恢复预案的正确性、有效性和各部分之间的关联性。

6.2.1.2 应模拟灾难发生的现实场景，对灾难恢复预案每年至少进行一次演练。

6.2.1.3 当重要信息系统、所支持的业务处理或灾难恢复预案有重大变动时应进行测试。

6.2.1.4 应根据实际情况确定测试作用于生产环境还是备用环境。如作用于生产环境，应制定生产环境与测试环境切换的预案。

6.2.1.5 因演练的规模较大，对生产环境产生的影响会较大，因此演练应在备份系统或备份数据中心进行。

6.2.2 **测试和演练的步骤**

测试和演练应包括以下步骤：

a) 明确测试和演练的目标；

b) 制定测试和演练的计划；

c) 建立测试和演练的评估标准；

d) 执行测试和演练并监控情况；

e) 完成测试和演练报告；

f) 评估测试和演练的结果，完成评估报告。

6.3 **灾难恢复预案的维护**

6.3.1 **灾难恢复预案的变更**

6.3.1.1 当单位的业务、环境、信息系统、联系人名单等发生变化时应更新灾难恢复预案。

6.3.1.2 在每次测试和演练完成后，应根据测试和演练的评估报告更新灾难恢复预案。

6.3.1.3 所有的变更应遵循变更管理流程。

6.3.1.4 应评估所有变更对灾难恢复预案的影响。

6.3.1.5 灾难恢复预案的变更应向领导小组汇报并征得同意。

6.3.1.6 所有的变更应及时通知相关部门及人员，并具体落实到每一次的培训和测试过程中去。

6.3.2 **灾难恢复预案的检查**

6.3.2.1 应对灾难恢复预案的完整性和有效性每年至少进行一次检查。

6.3.2.2 应定期检查灾难恢复预案中经常变动的部分，如联络清单等。

6.3.3 **灾难恢复预案的审核**

6.3.3.1 领导小组应组织专家小组或外部有资质的专家定期对灾难恢复预案进行审核，以保证其正确性。测试和演练的结果应作为审核的重点。

6.3.3.2 审核的结果应上报领导小组，得到批准后对灾难恢复预案进行更新。

6.4 **灾难恢复的执行**

6.4.1 **启动阶段**

6.4.1.1 灾难发生时，应由相关负责人向数据处理中心发出灾难警报，并通知相关业务机构。

6.4.1.2 恢复组应对灾难进行损害评估。

6.4.1.3 当损害评估的结果显示启动条件被满足时，由恢复组提出启动灾难恢复预案申请，得到领导小组批准后发出灾难宣告，启动灾难恢复预案。

6.4.2 **处理阶段**

处理阶段应完成以下工作：

a) 将基本经营活动或者配套服务转移到临时替代地点；

b) 与相关部门取得联系；

c) 向上级机关报告灾难事件情况。

6.4.3 **恢复阶段**

6.4.3.1 启用灾难备份中心。

6.4.3.2 如没有建立灾难备份中心，应准备恢复所需要的资源，包括办公用品、工作空间、硬件、软件和备份介质等。

6.4.3.3 应根据灾难恢复目标，按照业务恢复优先顺序和灾难恢复操作手册进行恢复。

6.4.3.4 恢复所用的时间如果超过了恢复时间目标，应立即上报领导小组。

6.4.4 **重建阶段**

6.4.4.1 当原数据处理中心严重损坏而无法使用时，应重建数据处理中心。

6.4.4.2 在完成原数据处理中心或重建的数据处理中心的恢复和测试之前，备份中心应继续运行。

6.4.4.3 当原数据处理中心或重建的数据处理中心可以支持业务正常处理时，应将重要信息系统转回，终止恢复活动。

6.4.5 **评估阶段**

6.4.5.1 在灾难事件处理完成后，应对灾难备份与恢复的组织机构、灾难备份方案和灾难恢复预案等进行评估，并形成评估报告。

6.4.5.2 应根据评估报告对相关内容进行修改和完善。

## 7 培训

### 7.1 培训对象

培训对象应包括领导小组、建设组、运维组、恢复组及其他相关人员。

### 7.2 培训内容

培训内容应包括：

a) 意识培养；

b) 基本知识和专业知识培训；

c) 操作技能培训。

### 7.3 培训实施

7.3.1 应定期对相关人员进行培训。

7.3.2 灾难备份方案和灾难恢复预案变更后，应在变更后的一周内对变化部分涉及的相关人员进行培训。