ICS 35.040
L 80

中华人民共和国国家标准

GB/T 30285—2013

信息安全技术
灾难恢复中心建设与运维管理规范

Information security technology—
Construction and sustain management specifications of disaster recovery center

2013-12-31 发布　　2014-07-15 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

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:北京万国长安容灾备份服务有限公司。

本标准主要起草人:汪琪、王娜、熊四皓、李爱东、吴晓军、李丹、何瑜、周云峰、刘书明、刘建明、王军、黄伟、刘东红、关继铮、高勇、杨海涛、刘洋、上官晓丽。

信息安全技术
灾难恢复中心建设与运维管理规范

1 范围

本标准规定了灾难恢复中心建设与运维的管理过程。

本标准适用于开展信息系统灾难恢复及业务连续性活动的机构或提供信息系统灾难恢复及业务连续性服务的服务机构(以下简称“机构”)。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 20984—2007 信息安全技术 信息安全风险评估规范

GB/T 20988—2007 信息安全技术 信息系统灾难恢复规范

GB 50174—2008 电子信息系统机房设计规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

生产系统 production system

正常情况下支持机构日常运作的信息系统。

3.2

灾难备份系统 disaster recovery system

用于灾难恢复目的,当灾难发生导致生产系统不可用时用于接替生产运行的信息系统,以满足机构业务运营的连续性要求。

3.3

数据中心 data center

用于支撑信息系统运行的场地和环境,一般由电力保障系统、空气调节系统、安全保障系统、监控系统、消防系统、机柜及桥架、办公及生活保障设施等构成。

3.4

生产中心 production center

利用数据中心场地和环境支撑机构生产系统运行,对机构的重要信息进行集中管理和处理的场所和组织。

3.5

灾难恢复中心 disaster recovery center

满足机构关键业务运营连续性的要求,利用数据中心场地和环境支撑机构灾难备份系统运行,抵御导致生产系统全部或部分不可用的灾难,用以接替生产中心部分或全部职能,对机构重要信息进行集中管理和处理的场所和组织。

注:灾难恢复中心也称为灾备中心或容灾中心。灾难恢复中心按照其风险防范职能及与生产中心的距离,可分为

同城灾难恢复中心和异地灾难恢复中心。

3.6

同城灾难恢复中心　city disaster recovery center

与生产中心一般处于同一城市，但与生产中心处于不同的风险区域内，能够抵御同一城市内的小范围停电、建筑物火灾、基础设施设备故障、通信线路故障、软硬件故障以及其他突发事件可能造成的局部交通封锁或中断等小范围灾难的灾难恢复中心。

注：同城灾难恢复中心具有通讯成本较低，可实现同步“零数据丢失”复制，可抵御较小范围风险等特点。

3.7

异地灾难恢复中心　remote disaster recovery center

与生产中心一般处于不同城市，能够抵御大范围停电、地震、战争、洪水、海啸、滑坡、泥石流、台风、洪水、较大范围的公共卫生事件、社会动乱等较大规模的区域性灾难的灾难恢复中心。

注：异地灾难恢复中心可实现异步复制或定时备份方式，可抵御较大范围的风险等特点。

3.8

灾难恢复演练　disaster recovery exercises

为验证灾难备份系统的有效性，确保灾难备份系统能够顺利接替生产系统运行，机构需要通过演练的方式验证灾难备份系统与生产系统数据的一致性和完整性，验证灾难备份系统接替生产系统的能力。

注：灾难恢复演练的形式可分为桌面演练、模拟切换演练和实际切换演练。

3.9

灾难备份系统切换　disaster recovery system failover

将生产系统切换到灾难备份系统运行，利用灾难恢复中心接管部分或全部生产中心职能的活动。

3.10

灾难备份系统回切　disaster recovery system failback

将灾难备份系统切换回生产系统，并恢复生产中心职能的活动。

4　建设与运维管理概述

4.1　建设与运维管理原则

灾难恢复中心建设与运维管理原则如下：

a）　预防为主原则

充分认识生产中心在使用和管理过程中所面临的风险，及时提出风险处置策略，明确在灾难恢复中心需要解决或处置的灾难事件风险场景，根据成本效益原则采取必要的措施降低风险发生的可能性，最大限度地减少可能造成的损害。在灾难恢复中心选址时，应避免与生产中心同处一个风险区域和环境，以达到风险分散的目的。

b）　资源共享原则

灾难恢复中心是在灾难发生时为机构从事灾难恢复活动所提供的专用资源，一般处于闲置或就绪状态，为最大限度地降低灾难恢复中心的总体拥有成本，提高灾难恢复资源建设的投入费效比，应在保证机构业务、数据安全的前提下利用灾难恢复中心的闲置资源或利用第三方机构的资源实现机构之间和机构内部功能区之间的资源共享。

c）　持续保障原则

充分考虑与生产中心的业务和数据处理能力的一致性，保证灾难恢复中心具有接管生产中心关键信息系统运行的能力。机构应建立一整套长效保障机制以确保灾难恢复中心资源的完整性和长期有效性。

d） 安全保障原则

应加强灾难恢复中心的安全保障工作，使灾难恢复中心与生产中心具备同等的安全保障机制，以确保灾难恢复中心的信息安全和信息系统的运行安全，实现灾难发生时灾难恢复中心对生产中心的平稳接替。

4.2 建设与运维管理的生命周期模型

根据灾难恢复体系建设最佳实践，灾难恢复中心的建设与运维管理过程一般可分为分析、规划、建设、交付和运维五个阶段，见图 1，为保证灾难恢复中心的功能和水平能够跟随业务发展和灾难恢复需求的变化，应定期对灾难恢复需求进行重新评估，并根据需求评估的结果重复进行规划、建设、交付和运维等管理活动的开展。

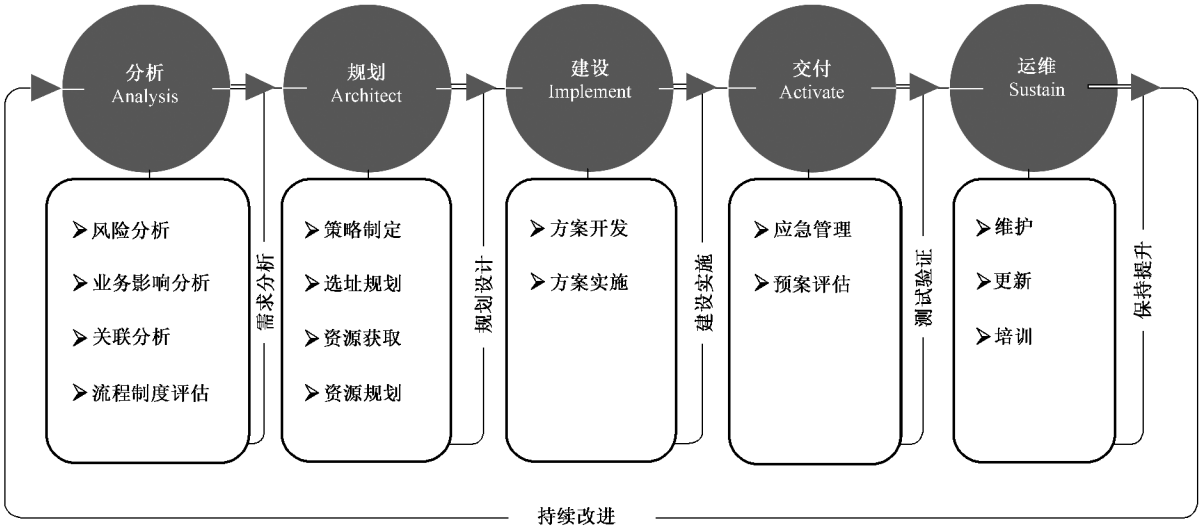

图 1 灾难恢复中心建设与运维管理生命周期模型

a） 分析阶段

通过风险分析、业务影响分析、应用系统关联分析、流程与制度评估等需求分析方法获取灾难恢复中心建设需求，确定建设目标、范围及路线等。

b） 规划阶段

根据需求分析结论，制定灾难恢复策略，进行灾难恢复中心选址规划、资源获取方式规划、资源获取方式规划、基础设施资源规划、信息系统规划、运维管理体系规划和灾难备份技术方案设计。

c） 建设阶段

根据灾难备份技术方案的要求进行灾难备份系统建设，包括基础设施建设、信息系统建设和预案体系建设，通过灾难恢复中心建设，获取机构灾难恢复所必需的环境、场地、系统、人员等灾难恢复资源。

d） 交付阶段

交付阶段是建设阶段向运维阶段过渡的重要阶段，在此阶段，通过预案和手册的培训、测试、演练等方式，是灾难恢复中心的运行管理团队逐渐熟悉并接管灾难恢复中心。确保灾难恢复资源满足机构灾难恢复能力要求。

e） 运维阶段

通过持续维护、培训、验证、演练等方式保持灾难恢复能力在整个生命周期内的有效性，逐步改善并提升运行维护管理水平和管理效率。

当机构的业务模式、管理目标、外围环境、技术架构发生重大变化且对机构灾难恢复需求产生重大

影响时，应重新进行灾难恢复需求分析，并根据新的需求进行重新规划、建设、交付和运维，因此灾难恢复中心建设与运维管理是一个循环往复、不断改进、不断完善的过程。

4.3 建设与运维管理的内容

灾难恢复中心建设与运维管理的内容见图 2，包括以下几个方面：

a） 灾难恢复中心的组织体系建设和管理

机构应建立一个构架合理、岗位清晰、职责明确、管理有序、执行高效的灾难恢复管理、实施和运维团队，确保灾难发生后的恢复过程能够得到有效组织和管理。

b） 预案体系的建设和管理

预案体系应包括应急响应预案和灾难恢复预案，通过事先的定义和文档化，明确在应急响应和灾难恢复过程中的分工职责、决策依据、行动流程、具体操作步骤和行动建议等，清晰明确的预案能够避免应急和恢复过程的无序和混乱，减少人为差错和时间的浪费。

c） 灾难恢复资源的获取和维护

灾难恢复资源包括灾难恢复中心基础设施环境、灾难备份系统、备用数据、技术支持等，灾难恢复资源的获取和维护是衡量机构灾难恢复能力的重要因素，灾难恢复中心则是完成灾难恢复工作的重要载体。

d） 灾难恢复管理工具

为了在灾难恢复中心日常维护和灾难恢复过程中对人员、预案、系统、设备、环境等实现统一管理、统一调度，灾难恢复中心还可以通过建立灾难恢复管理技术平台，利用信息技术和管理手段提高灾难恢复中心维护管理的效率和规范性。

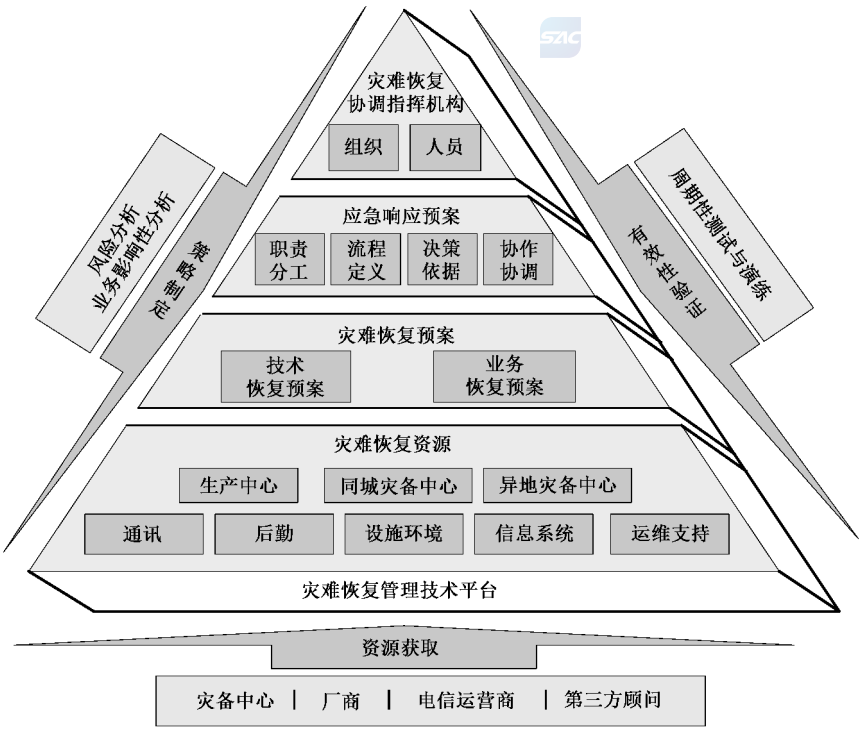

图 2 灾难恢复中心建设与运维管理内容

为了获取灾难恢复能力并保证其能够持续有效的发挥作用，不但应关注灾难恢复中心的建设过程，还应关注灾难恢复中心的管理和维护，特别是灾难恢复中心的规划、资源获取和运行维护。

明确灾难恢复中心的建设策略，通过风险分析、业务影响分析等方法明确灾难恢复中心的组织体系、职责分工、恢复目标、恢复范围、恢复水平、恢复次序和优先级，建立灾难恢复中心场地、线路、设备、系统、数据等资源获取的渠道和方法；

根据灾难恢复中心的建设需求和策略，组织规划、建设或通过其他渠道购买、租赁，以获得机构的灾难恢复能力；

已经获取的灾难恢复能力（包括组织、预案、设施、设备等）进行周期性的验证、检查和演练以确保灾难恢复中心能够适应机构管理体系和业务需求的变化，保证机构灾难恢复能力的持续性和稳定性。

4.4 灾难恢复中心组织机构及岗位的设立

机构应根据自身的发展战略，结合机构业务特点和信息系统运行平台的特点，本着“合理布局、有效利用、平战结合、持续保障”的原则对灾难恢复中心进行职能定位。灾难恢复中心除应具备灾难恢复及业务持续运营的基本职能外，还可以根据自身的具体情况，赋予灾难恢复中心以其他辅助职能，如测试开发、统一监控、教育培训等。

灾难恢复中心作为机构业务持续管理的重要组成部分，应建立由机构高层管理人员领导，各相关部门参与的灾难恢复中心组织机构。

灾难恢复中心组织机构应由灾难恢复中心建设管理机构、灾难恢复中心运维管理机构组成。

灾难恢复中心建设管理机构负责灾难恢复中心的规划、设计、施工、测试、试运行、交付的管理等工作；灾难恢复中心运维管理机构负责灾难恢复中心的日常运行维护、应急响应管理、灾难恢复的管理等工作。

灾难恢复中心建设管理机构应设立规划设计、协调管理、建设实施等岗位，灾难恢复中心运维管理机构应设立组织管理、运行维护、操作执行等岗位，在灾难发生时，应设立应急指挥、应急管理岗位。每个岗位都应有专人负责，关键岗位至少应设立两个互为备份的角色，以避免由于岗位缺失导致实施和运维质量的下降。

灾难恢复中心的部分职能可以由外包服务机构承担，外包服务机构应视外包职能的范围设立内部组织机构履行相应的灾难恢复中心建设职能和灾难恢复中心运维职能，并与服务对象的灾难恢复组织机构对接。同时，服务对象机构应指定或设立相应组织负责对外包服务机构进行管理并担负起相应的管理责任。

5 灾难恢复中心规划

5.1 灾难恢复中心需求分析

5.1.1 生产系统风险分析

应依据 GB/T 20984—2007 的要求，识别生产中心信息系统的资产价值、潜在的威胁和脆弱性，并对资产价值、威胁和脆弱性进行等级评估，从而确立信息系统风险级别。根据不同的风险级别制定可行的风险管控措施，并对分析实施风险管控措施后的残余风险，提出灾难备份系统建设的必要性，风险分析应根据业务和环境变换的情况至少每三年进行一次。

5.1.2 基础设施风险分析

为了加强风险防范和管控能力，机构应对其生产中心基础设施进行风险分析，通过对机构生产中心基础设施资产的威胁和脆弱性识别，按照脆弱点被威胁利用时对生产中心所造成的影响范围和影响程度划分风险级别，并针对不同级别的风险制定相应的风险管控措施，以及实施风险管控措施后的残余风险分析。基础设施风险分析的范围应至少涵盖生产中心可能面临的供电中断、地质灾害、气象灾害、交

通、通信中断以及生产中心基础设施本身的缺陷和弱点。

5.1.3 业务影响分析

应按照 GB/T 20988—2007 的要求，分析机构各业务系统中断后对机构所造成的财务影响和非财务影响，确立业务系统的灾难恢复指标(RTO 和 RPO)。通过对业务系统和信息系统的关联分析，进而确定信息系统的灾难恢复指标、灾难恢复的优先级别和灾难恢复资源需求。

5.1.4 应用关联分析

应通过对业务应用逻辑架构和业务功能的分析，明确各应用系统的关联关系，包括数据流向、信息交互方式、交互时段和交互路径等，通过应用系统关联分析，确立机构灾难备份的范围和灾难恢复中心信息系统的部署方式。

5.1.5 应急流程与运维制度评估

应通过对机构生产中心现有的应急流程和运维管理制度的调研分析，按照相关标准和规范的要求制定评估基线，对机构现有的应急流程和运维管理制度进行差异分析，提出整改建议和措施。

5.2 灾难恢复中心的规划

5.2.1 灾难恢复策略制定

灾难备份策略制定包括如下的灾难恢复技术策略制定、业务恢复策略制定、灾难恢复范围确定、灾难备份系统实施策略制定、灾难恢复预案开发策略制定和灾难恢复中心运维管理策略制定等方面：

a) 业务恢复策略制定

业务恢复策略的制定应包括业务恢复的手段和恢复流程，数据追补手段和流程，确保发生灾难时业务的持续运行。

b) 灾难恢复范围的确定

应根据机构的业务特点，按照国家和行业相关规范的要求，依据应用系统关联分析，确定信息系统灾难恢复的范围。

c) 灾难恢复技术策略制定

应根据应用系统灾难恢复指标的要求，制定信息系统灾难恢复等级，按照 GB/T 20988—2007 中针对不同灾难恢复等级所确定的灾难恢复资源需求，制定灾难恢复的技术策略。

d) 灾难备份系统实施策略制定

按照灾难备份系统技术策略的要求，结合灾难恢复的范围，制定灾难备份系统的实施策略，包括实施原则、实施范围、实施方法、实施流程等。

e) 灾难恢复预案开发策略制定

按照灾难恢复的实施策略，结合企业自身的特点，制定灾难恢复预案开发策略。

f) 灾难恢复中心运维管理策略制定

针对灾难备份系统运维的要求，确定灾难备份系统运维模式、运维制度、运维团队和运维流程。

5.2.2 场地选址规划

考虑场地建设的合规性，机构业务的持续发展和机构现有资源配置状况等多方面因素等，提出场地选址要求。

所在城市的自然条件、政策环境、区域经济环境、配套设施条件、专业支持保障能力、建设成本等多方面的综合评估。

所在城市环境资源、技术资源、人力资源、配套生活资源等方面的整体布局。

考虑灾难恢复中心的场地条件和风险状况，避免灾难恢复中心与生产中心处于同类风险区域，或发生与生产中心类似的风险状况。

灾难恢复中心场地选址还应综合考虑以下因素：

a） 自然威胁

灾难恢复中心应避免建立在环境灾害高发或高危地区，例如，地震带、气象灾害高发区、低洼易涝地区等。

b） 临近威胁

灾难恢复中心的选址应该避开一些临近的工业和商业风险。这些风险可能包括：制造危险化学品或爆炸物品的工厂、飞机航线直接经过的地区、工业废气（粉尘、酸雾）影响地区、高速和高架桥临近区域等。

c） 交通条件

灾难恢复中心的选址应考虑交通便利的地区，保证人员和装备能够顺利地进入目标恢复区域而不会遭遇计划外的延迟。

d） 连带威胁

灾难恢复中心应尽量避免临近公共设施，尽量避免受到公共设施动荡、冲突或被破坏所造成的影响。

e） 网络接入

灾难恢复中心的选址应便于不同网络运营商的线路接入，以方便分支机构和合作伙伴的网络接入。

5.2.3 资源获取规划

通过对灾难恢复中心建设的可行性分析，包括财务分析、技术及运维能力分析，确定灾难恢复中心的场地资源的获取方式。

灾难恢复中心基础设施资源获取方式，可根据机构的具体情况可采取以下方式获得：

a） 自建

机构所有并运行。

b） 购买

购买现有第三方基础设施。

c） 共建

多个机构共同所有并运行。

d） 外包

由具有信息系统灾难恢复能力的第三方商业机构提供并负责运行。

5.2.4 基础设施资源规划

灾难恢复中心基础设施资源规划是按照机构灾难恢复中心建设的总体要求和基础设施风险分析的结论，对灾难恢复中心的场地、电力、制冷、网络、消防等基础设施资源配置进行规划。规划的主要内容包括：

a） 按照灾难恢复中心全生命周期，制定基础设施总体需求；

b） 按照机构管理要求和外部监管要求和信息系统灾难恢复策略要求，提出灾难恢复中心基础设施建设指标体系；

c） 按照灾难恢复中心基础设施建设指标要求，进行灾难恢复中心的功能区划分和容量分析，并进行电力资源、制冷量、安全资源、运维监控、后勤保障等方面的资源规划。

在灾难恢复中心基础设施资源规划时应重点考虑以下因素：

a） 机构业务活动对于信息系统活动依赖程度；

b） 防范的灾难场景；

c） 机构信息系统运行的特点；

d） 机构归属行业的监管要求；

e） 灾难恢复中心的生命周期。

资源规划应根据灾难恢复中心基础设施资源需求，结合灾难恢复中心基础设施的地理环境和资源状况进行灾难恢复中心机房环境规划和配套设施规划。

5.2.5 信息系统规划

灾难恢复中心的信息系统规划应根据灾难恢复需求评估结论，结合机构生产中心信息系统的具体情况进行灾难备份技术策略的制定、信息系统资源规划和信息系统资源部署规划。

灾难备份技术策略的制定应根据灾难恢复需求评估的结论，结合机构生产中心信息系统的配置情况，通过对业界主流灾难备份技术的分析，结合 GB/T 20988—2007 中关于不同灾难恢复等级的各要素要求，制定适合机构灾难恢复需求的技术策略，包括数据备份策略、数据复制策略、系统切换策略和网络切换策略。

信息系统资源规划是根据灾难备份技术策略的要求，进行灾难恢复中心信息系统资源规划，包括备用数据处理资源规划、数据存储与备份资源规划和备用网络资源规划。

信息系统资源部署规划应按照信息系统资源规划中不同信息系统资源的类型和配置的要求，进行信息系统资源部署规划；多个生产中心共享的灾难恢复中心，在信息系统资源部署规划时应考虑各机构在灾难恢复中心信息系统资源的安全和可用。信息系统资源部署规划应包括数据备份与复制平台的部署规划、备用数据处理资源部署规划、备用数据存储资源部署规划、备用网络资源部署规划和灾难恢复中心应用系统部署规划。

灾难备份系统需考虑信息安全等级保护要求，灾难备份系统的使用单位需按照信息安全等级保护管理规范和技术标准，对灾难备份系统分等级实行安全保护。

5.2.6 运维管理规划

灾难恢复中心运维管理规划应充分考虑灾难恢复中心的职能定位，按照灾难恢复中心运维管理策略的要求，进行运维管理组织架构和岗位职责规划、运维管理制度体系规划、运维管理流程规划，运维管理体系规划应突出灾难恢复中心专业运维的特点，从组织管理、岗位职责、管理制度、流程设计等方面体现灾难恢复中心的运维专业性。

运维管理体系规划不仅应考虑未发生灾难时灾难恢复中心的工作内容和运维流程，还要考虑发生灾难时的应急响应和灾难恢复的工作内容和流程。

5.2.7 方案设计

根据灾难恢复策略，进行灾难恢复中心方案设计。包括灾难恢复中心基础设施方案、灾难恢复技术方案和灾难恢复中心实施方案。详细规定如下：

a） 灾难恢复中心基础设施方案设计

根据灾难恢复中心基础设施资源规划，进行灾难恢复中心的基础环境设计和机房设计。其中基础环境设计包括园区、建筑物设计；机房设计包括场地、供配电、空调、安防、网络等方面的设计。

所有设计的结论应记入灾难恢复策略文档，并获得机构高层管理的批准。设计方案应以文档方式留存，以便于复查和更新。

b） 灾难恢复技术方案设计

根据灾难恢复中心信息系统规划，进行灾难恢复中心技术方案设计，包括备用数据处理系统、备用

数据存储系统、备用网络和安全系统方案的设计，灾难恢复中心系统资源配置建议；

灾难恢复技术方案设计应按照灾难恢复的技术策略，制定灾难备份系统的技术架构，包括数据备份与恢复技术架构、数据复制技术架构、网络技术架构、系统切换与回切技术架构等。

c） 灾难恢复中心实施方案设计

按照灾难恢复技术方案的要求，制定灾难恢复中心实施方案，包括实施计划、实施流程、实施管理方案和实施的风险控制等。

6 灾难恢复中心的建设管理

6.1 基础设施建设管理

6.1.1 建设内容

灾难恢复中心基础设施建设可根据机构的建设要求组织实施，其建设内容包括工作设施、辅助设施、生活设施和其他必要区域等。

工作设施包括信息系统工作设施和保障系统工作设施等。例如，计算机机房、主操作室、通讯机房、介质机房、信息系统设备测试维修机房等属信息系统工作设施；供配电设施、空调暖通设施、给排水设施、消防设施、监控设施、货运设施等属于保障系统工作设施。

辅助设施包括日常运行辅助设施、灾难恢复辅助设施、灾难恢复培训设施等。例如，灾难恢复中心办公室、会议室、资料室、值班室、仓库、接待室、休息室、访问活动区域、停车场、货物装卸区等属于日常运行辅助设施；灾难恢复指挥中心、灾难恢复坐席区、办公区、新闻发布中心（多媒体室）、会议室、打印传真室等属于灾难恢复辅助设施；培训教室、模拟演练室等属于灾难恢复培训设施。

生活配套设施包括日常保障人员生活设施和灾难恢复人员生活设施等。例如，宿舍、食堂、活动室等。

其他必要区域还包括集合区域、等候区域、人流物流通道等。

在灾难恢复中心基础设施建设中，机构应组织成立建设管理团队，并根据国家相关标准的要求选择具有数据中心建设经验的施工承包单位，施工监理单位等完成建设。

机构还应组织专家或第三方评估单位对数据中心建设和验收的过程及重要节点给予专业监督，确保灾难恢复中心的建设满足设计和运行要求。

6.1.2 建设管理要求

基础设施建设应遵循“统一协调、分工协作、精心组织、严格审核”的原则，按照基础设施规划和设计的要求进行实施。在建设实施的各个阶段应严格按照施工安全标准和项目管理标准组织实施，并且在实施过程中对质量、安全和进度进行持续的监控和审查，确保施工与设计目标的一致性。同时灾难恢复中心的建设还应尽可能规避施工的风险，坚持成本效益平衡原则，最大限度地提高资源利用率，并综合考虑技术可行性、技术先进性、可扩展性、可管理性、可持续性，以及环保、节能和社会效益等多个方面。

6.1.3 建设实施要求

灾难恢复中心基础设施的实施要求如下：

a） 机构应组建专门的基础设施建设工程项目管理机构，负责对建设工程的全过程进行管理，项目管理机构中应至少包括建设单位代表、监理机构代表和承建单位代表；

b） 项目管理机构可聘请或委托第三方专业机构提供指导或协助；

c） 工程项目管理机构应充分理解需求规划和设计要求，建设过程中发生的重大调整和变更都应被记录并提交灾难恢复中心建设管理机构进行评审，避免出现与需求和设计目标的偏离；

d) 建设过程中工程项目管理机构应对工程进度、工程质量、工程成本等情况进行持续的记录和监控，及时发现问题并推动问题解决；

e) 工程项目管理机构应关注施工现场安全管理，制定施工现场安全管理办法，避免出现施工安全事故；

f) 灾难恢复中心基础设施的施工应遵循相关领域的建筑施工标准组织实施。

6.2 灾难备份系统的建设管理

6.2.1 管理要求

灾难恢复中心基础设施的实施要求如下：

a) 数据备份系统建设管理要求

数据备份系统应本着数据的一致性原则进行建设，确保灾难恢复中心与生产中心数据的一致性和完整性，在系统实施过程中，应进行必要的数据一致性和完整性验证。对于多个生产中心共享的灾难恢复中心，在数据备份系统建设过程中还应考虑不同生产系统在灾难恢复中心备份数据的安全性。

b) 备用处理系统建设管理要求

为满足机构业务持续性运行的要求，灾难备份应用系统应在系统运行环境和软件版本等方面与生产系统完全兼容，在备用数据处理系统建设时，应进行灾难恢复中心子系统运行能力的测试验证和灾难备份系统切换与恢复验证，以确保灾难备份系统平台的有效性和可操作性，以及灾难备份系统接管生产系统运行的能力。

c) 备用网络系统建设管理要求

备用网络系统的建设与实施应按照灾难备份系统规划方案的要求，对灾难恢复中心内部网络、生产中心与灾难恢复中心之间的互联网络、灾难恢复中心与上级机构之间的网络、灾难恢复中心与分支机构之间的网络平台进行实施，搭建灾难备份系统切换和恢复所需要的网络支撑环境。对于多个生产中心共享的灾难恢复中心，备用网络系统建设时应注意对不同生产系统网络的安全隔离，避免由于多个生产系统在灾难恢复中心内部的网络互通导致的安全隐患。

d) 灾难恢复指挥和管理系统建设管理要求

灾难恢复中心往往与生产中心相距较远，需要相对独立的运行管理团队和运行管理的流程制度，为保证灾难恢复中心的可靠运行，建议在灾难恢复中心建立独立的运行维护管理团队和运行管理系统，对灾难恢复中心的事件、问题、变更、发布、配置等关键管理活动和流程进行标准化、规范化管理；

灾难恢复的过程对恢复时间要求严格，涉及的部门组织较多、系统结构复杂，恢复任务数量多、关联复杂，在不同的故障情况下需要启动的预案也各不相同，为了方便日常的培训和演练，更有效的组织灾难恢复的指挥协调工作，建议灾难恢复中心应建立专门的灾难恢复指挥系统，通过对灾难恢复流程和方案的预先定义，通过对日常演练培训的便捷组织，提高灾难恢复的指挥效率和操作能力水平。

6.3 预案体系建设管理

机构应建立有效的预案管理体系，建立有效的开发、维护机制和流程，确保预案符合机构的应急和灾难恢复管理要求。预案体系包括应急预案体系和灾难恢复预案体系。

应急体系描述在紧急状况下机构的应急响应和处置过程，包括应急组织管理、紧急事件的发现、报告和处置，损害评估、恢复、重续运行、重建与回退处理流程和审核与问责制度等内容。应急预案应包括基础设施应急预案、网络系统应急预案和应用系统专项应急预案。

灾难恢复预案则描述在紧急状况下机构如何进行抢救和恢复的过程，包括：灾难恢复组织管理、紧急事件的发现、报告和处置，损害评估、灾难宣告、恢复、重续运行、重建和回退处理流程和处理步骤等内容。灾难恢复预案是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。灾难恢复中心的启用和恢复工作必须在灾难恢复预案的指导下进行。灾难恢复预案应包括灾难恢复中心基础设施恢复预案、灾难备份网络切换恢复预案、信息系统切换恢复预案和业务恢复预案等。

预案体系应按以下要求进行建设和管理：

a) 在预案开发阶段，机构内应设立专门的团队负责预案的开发和验证工作。

b) 开发团队应了解应急和灾难恢复的管理流程、管理原则和业务、技术恢复方法，能够协调和获取管理层和业务、技术部门的支持，具备相关文档的开发写作能力。

c) 预案开发团队人员应由本机构业务、技术等各方面的专业人员以专职或兼职的方式参与，也可聘用或委托其他灾难恢复专业服务机构人员提供辅导和帮助。

d) 预案的制定应遵循“完整性、易用性、明确性、有效性、兼容性”原则，并明确灾难恢复中心启用的限制和前提、灾难恢复的组织和分工、决策机制和流程、决策依据和标准、通讯手段和联络方式、业务与技术的恢复方法和流程、恢复资源的获取方式、持续运行的周期，以及重建和回退策略等方面。

e) 开发完成的预案应交各专业团队进行验证，并组织人员进行验证，灾难恢复预案确认有效后应交由机构领导层进行审批和发布。

f) 机构应建立有效的预案维护体系，并有专人负责预案的维护，包括预案的版本控制、预案的生命周期管理、预案的更新机制等。

7 灾难恢复中心交付管理

7.1 基础设施的验收和移交

7.1.1 基础设施的验收

灾难恢复中心基础设施的验收应严格依照设计规划和施工标准的要求进行，在正式验收开始前应组织包括基础设施运行维护团队参与测试运行，建立基础设施运行管理规范并核对、验证建设方提交的运行维护规程和操作手册的完整性和正确性；

a) 灾难恢复中心基础设施的验收组织应遵循“验评分离、强化验收、完善手段、过程控制”原则；

b) 灾难恢复中心综合验收应根据验收范围和验收类别，分别组织制定验收工作计划和验收方案；

c) 灾难恢复中心的综合验收应在完成国家规范规定的建筑规范验收后进行；

d) 灾难恢复中心综合验收的参与人员应至少包括：灾难恢复中心的灾难恢复管理人员，灾难恢复中心的规划人员，灾难恢复中心的设计人员及跨行业的灾难恢复领域的专家；

e) 验收范围不但应该包含相关设备、设施的数量和施工质量，还应包括相关的图纸、使用说明和操作手册等资料性文档；

f) 灾难恢复中心综合验收后，相关单位应根据验收的结论，对相应工作完成材料补充或整改工作。

7.1.2 基础设施的移交

灾难恢复中心基础设施的移交应建立对基础设施验收合格基础上进行，在基础设施移交前，建设管理机构应组织相关人员准备移交的所有文档，包括建设实施文档、测试文档、验收文档、技术文档，在正式移交时，建设管理机构应与运维管理机构召开移交会议，讨论移交工作内容和工作流程，并使运维管理人员了解和掌握基础设施的建设情况和设备的运行情况，确保灾难恢复中心的基础设施能顺利进入运行维护阶段。

7.2 灾难备份系统的有效性验证

7.2.1 数据的完整性验证

采用技术和业务手段两种手段对灾难恢复中心数据的有效性和完整性进行验证，确保灾难发生时灾难恢复中心的接管能力。

7.2.2 数据的一致性验证

采用技术和业务手段两种手段对生产中心与灾难恢复中心业务数据的一致性进行验证，防止一旦灾难发生，数据丢失量超过灾难恢复指标要求和业务系统容忍度。

7.2.3 数据备份与恢复能力验证

采用技术和业务两种手段对灾难恢复中心数据备份能力进行验证，防止数据备份中断，或是数据备份周期超出设计的时间范围；同时通过技术和业务手段验证灾难恢复中心备份数据的可恢复性，防止一旦灾难发生时备份数据失效，导致系统恢复失败。

7.2.4 信息系统切换与回切能力验证

a） 主机操作系统切换与回切能力验证

通过技术手段进行主机操作系统的切换与回切的验证和测试，保证灾难发生时应用系统主机能顺利切换到灾难恢复中心，以及灾后回退时，主机也能顺利回切至生产中心。防止生产中心与灾难恢复中心主机操作系统环境不一致，导致主机接管失败。

b） 存储系统能力验证

通过技术手段验证灾难恢复中心存储系统能力，保证灾难发生时，灾难恢复中心存储系统的可访问和数据的可用性。

c） 数据库系统切换与回切能力验证

通过技术手段进行数据库系统的切换与回切的验证和测试，保证灾难发生时，数据库系统能够顺利切换到灾难恢复中心，以及灾后回退时，数据库系统也能回切至生产中心。

7.2.5 网络系统切换与回切能力验证

a） 网络设备的切换与回切能力验证

通过技术手段进行网络设备的切换与回切的验证和测试，确保灾难发生时，灾难恢复中心的网络能对外提供服务，以及灾后回退时生产中心的网络能提供对外服务。

b） 网络线路的切换与回切能力验证

通过技术手段进行网络线路的切换与回切的验证和测试，确保灾难发生时，灾难恢复线路畅通，各分支机构、外联单位、监管部门能够顺利连接到灾难恢复中心进行交易，以及灾后回退时各分支机构、外联单位、监管部门能够顺利连接到生产中心进行交易。

7.2.6 应用系统切换与回切能力验证

a） 灾难恢复中心应用系统运行能力验证

通过技术手段和业务手段对灾难恢复中心应用系统进行验证，验证应用系统能否正常对外服务，验证应用系统数据访问能力，验证应用系统变更后的业务处理有效性。

b） 应用系统切换与回切能力验证

通过技术手段和业务手段对灾难恢复中心应用系统进行切换与回切的验证和演练，保证灾难发生

时应用系统能够顺利切换到灾难恢复中心，以及灾后回退时应用系统能回切至生产中心运行。

7.3 灾难恢复预案的验证

灾难恢复预案至少应包含灾难恢复的组织体系、恢复流程、技术操作等内容，灾难恢复预案开发完成后应通过桌面演练和操作演练（模拟切换演练和实际切换演练）的方式对预案设定的组织、流程和操作的可行性、正确性、有效性进行验证，并针对验证过程中反应的问题进行修正和调整。灾难恢复中心正式启用前应至少进行一次灾难恢复演练。

a） 灾难恢复预案应明确灾难发生时进行灾难恢复的组织体系，至少应包括灾难恢复的指挥体系、灾难恢复执行体系和灾难恢复的后勤保障体系。

b） 灾难恢复预案应明确灾难恢复的管理和响应流程，至少应包括灾难预警、灾难宣告、人员的通知和集结、评估和决策、灾难恢复技术操作、灾难恢复成功标志、灾难恢复中心持续运行管理、重建及回退等。

c） 灾难恢复预案应包括明确的技术操作说明，包括执行权限、操作步骤、操作指令、返回结果、异常处置等，技术操作说明中应明确操作步骤、执行的顺序和依赖关系。

d） 灾难恢复预案应在明显处标明最后更新日期和版本号，明确灾难恢复预案的更新、发放管理办法和负责人；新版本灾难恢复预案发布后老版本的灾难恢复预案应集中收回并销毁。

7.4 灾难恢复中心与生产中心的协作管理

在灾难恢复中心交付期间应明确在日常维护期和灾难恢复期间与生产中心间的分工界面与工作流程，并对相关机制进行检验和测试，保证正式运营后双方工作协调一致。

a） 灾难恢复中心与生产中心间应建立备份数据传输校验机制，保证双方收发数据的完整性一致性；

b） 灾难恢复中心与生产中心间应建立统一变更流程，生产中心发生的变更和调整应事先评估可能对灾难恢复中心产生的影响，并同时规划灾难恢复中心的变更方案和计划；

c） 灾难恢复中心与生产中心间应建立比对基准和基准核对流程，生产中心和灾难恢复中心应定期检查核对相关应用、设备的状态和参数是否保持在正确状态，并对发生的差错进行及时的纠正；

d） 灾难恢复中心与生产中心间应协调演练和测试计划，保证对双方的正常工作内容和周期不产生重大影响。

8 灾难恢复中心运行维护管理

8.1 运行维护管理原则

灾难恢复中心运行维护管理应遵循以下原则：

a） 安全性原则

灾难恢复中心的安全管理的等级和要求应与生产中心保持一致，灾难恢复中心存储的网络、数据、应用等安全等级不可因使用模式和状态的不同降低安全要求。

b） 关联性原则

灾难恢复中心运维管理体系应与生产中心运维管理体系相关联，在人员岗位构成、日常管理流程和应急恢复期管理流程的衔接、应用和数据的备份恢复操作、数据有效性测试、演练组织、数据安全管理要求等方面都应与生产中心相关联。

c） 流程化与制度化原则

机构应按照灾难恢复中心运维管理要求，建立具有完善的、可行的运维管理流程和制度，以规范运

维人员的工作行为，提高运维管理的质量、效率和水平。

d） 可用性与有效性原则

灾难恢复中心运维管理应通过全面测试和定期的验证机制，确保资源的可用性和有效性。

8.2 运行维护管理的组织

8.2.1 组织形式

a） 灾难恢复中心与生产中心采用统一领导、集中管理、协同配合的方式进行组织和管理，这种形式适合于灾难恢复中心等级较高、规模较大、日常运行维护管理工作量较大且独立性强等情形；

b） 灾难恢复中心的组织从属于生产中心，并接受生产中心的管理，这种形式适合于中等规模灾难恢复中心；

c） 灾难恢复中心与生产中心共享运行维护管理团队，运维团队为灾难恢复中心设置特定的岗位和角色，日常的运行维护以远程监控和第三方团队代为现场操作为主。适合于现场维护和操作量较小，不需驻场人员或只需要少数驻场人员等情形；

d） 不论何种模式下灾难恢复中心都应设定专门团队或人员负责灾难恢复中心的安全管理，并与生产中心的安全管理要求保持同步建设和更新。

8.2.2 管理职责

灾难恢复中心的管理职责应包括下列内容：

a） 基础设施运维管理

——负责灾难恢复中心基础设施监控；

——负责灾难恢复中心基础设施相关设备的维护；

——负责灾难恢复中心安防管理；

——负责灾难恢复中心卫生管理；

——负责灾难恢复中心生活设施管理；

——负责灾难恢复中心电力、通讯设施管理；

——负责灾难恢复交通工具管理；

——负责灾难恢复临时人员生活设施管理。

b） 信息系统运维管理

——负责灾难备份系统的监控及日常操作；

——负责灾难备份系统的专业技术支持；

——负责运行事件的管理；

——负责运行问题的管理；

——负责灾难恢复中心 IT 设备变更管理；

——负责灾难备份系统及数据有效性验证；

——负责灾难恢复预案的维护和管理；

——负责灾难恢复演练。

8.2.2.1 应急及灾难恢复支持

应急及灾难恢复支持的职责如下：

a） 负责接受处理突发事件及其预警信息；

b） 负责突发事件处置工作程序和工作机制的相关事务；

c) 接受灾难恢复应急处置的各项指挥；
d) 负责安排和获取灾难恢复所需的资源；
e) 负责跟踪恢复处置态势，协调各恢复团队的处置工作；
f) 负责收集和整理灾难恢复全面信息，为决策层提供支持；
g) 负责协助灾难备份系统实施；
h) 负责灾难恢复的技术操作；
i) 协助其他部门开展业务功能的恢复。

8.2.2.2 接替生产运行

接替生产运行的职责如下：
a) 负责接替运行期间的灾难备份系统的维护；
b) 负责协助安排接替运行期间业务部门和其他机构现场工作场所和环境的保持；
c) 负责生产系统和灾难备份系统的切换和回退检查；
d) 负责协调切换和回退过程中相关人员和重要设备的转移；
e) 负责灾难备份系统的切换和回退后的环境清理和复原。

8.2.2.3 安全管理

安全管理的职责如下：
a) 安全策略的规划与确定；
b) 安全管理制度的制定和落实；
c) 安全管理方案的设计和实施；
d) 安全事件的管理和追踪；
e) 安全记录的检查和审计。

8.3 灾难恢复中心运行维护管理内容和要求

8.3.1 安全管理

安全管理内容和要求如下：
a) 人员健康和安全应该优先于所有的设施和 IT 设备的保护策略和程序；
b) 灾难恢复中心的安全管理水平要求原则上应与生产中心保持一致，灾难恢复中心应特别注意数据保管、测试和废弃过程中的处理，避免发生遗失和泄漏；
c) 应为灾难恢复中心定义明确的安全管理制度，明确操作和管理权限，包括物理区域安全等级、访问授权办法，应用、数据访问途径和权限等，保证事前的控制审批和事后的审计追查；
d) 应由主要领导人对灾难恢复中心信息安全负责，并有专人承担灾难恢复中心的安全管理职能；
e) 应定期对灾难恢复中心人员进行适当的安全知识及相应技能的培训，在其上岗前进行必要的资格认证并明确安全责任；对在工作中涉及组织秘密的人员（含第三方人员），应签署保密协议；
f) 应加强灾难恢复中心信息资产管理，识别信息资产并建立责任制，根据信息资产重要性实施分类控制和分级保护，防范信息资产生成、使用和处置过程中的风险；
g) 应建立网络通信与访问安全策略，隔离不同网络功能区域，采取与其安全级别对应的预防、监测等控制措施，防范对网络的未授权访问，保证网络通信安全；
h) 应建立数据安全管理制度，规范数据的产生、获取、存储、传输、分发、备份、恢复和清理的管理，以及存储介质的台账、转储、抽检、报废和销毁的管理，保证数据的保密、真实、完整和可用；

i) 应建立基础设施和重要信息的授权访问机制，制定访问控制流程，保留访问记录，防止未授权访问；

j) 应建立和落实物理环境安全管理制度，明确安全区域、规范区域访问管理，减少未授权访问所造成的风险；

k) 应采用适当的技术手段，包括监控、门禁、入侵检测、网络安全设备和相关信息管理平台来保证可接受的安全和效率的一致；

l) 应制定紧急访问流程以保证在紧急状况发生时（如发生灾难性事件）获得效率和最基本的安全保证；

m) 应按照安全策略、标准、规范对灾难恢复中心的安全体系进行全面的审查和核实；对安全事故进行审查和监控。检查策略的有效性及其对业务效率的影响，确保在最初风险评估的基础有变化时，根据明确规定的审查程序对安全体系进行审查和维护。

8.3.2 基础设施运维管理

基础设施运维管理内容和要求如下：

a) 机构应设专人负责灾难恢复中心园区、建筑、机房的安全防护和卫生管理，建立、落实安全防护管理制度和标准，并定期进行检查；

b) 应对灾难恢复中心基础设施进行定期维护，确保其满足设计和建设指标要求，能够完全承担相应的职能；

c) 应对灾难恢复中心的基础设施运行使用情况进行监控，对基础设施发生异常情况要及时响应处理并依据流程升级和上报。对异常情况产生的原因进行分析，找出根本原因并从源头上防范和避免问题的再次发生；

d) 应对电力设施、通信设施、交通设施和生活设施等进行定期功能和性能检查，确保其能满足灾难发生时电力供应、通信联络、交通联系和生活保障功能；

e) 应对基础设施的性能和容量进行定期检查评估，如需进行升级改造，之前需要按照建设的流程和标准进行评估、审核，保证能够按照预期提升能力。需保留过程相关文档备查。

8.3.3 灾难备份系统运维管理

灾难备份系统运维管理内容和要求如下：

a) 应建立灾难恢复中心信息系统的运行监控平台，及时发现灾难备份系统运行的故障。灾难恢复中心应保留所有监控记录，以满足故障定位、诊断及事后审计的要求；

b) 应建立有效的事件跟踪机制、问题排查机制、变更管理机制，确保灾难恢复中心的事件和问题能得到及时解决，避免重大隐患的发生；

c) 应建立灾难备份系统资产清单和配置项清单，确保资产和配置项可审核、可追溯；

d) 应建立灾难备份系统的定期审核与验证机制，确保灾难备份系统能够在灾难发生时接替生产系统运行。监控和操作管理：应采用适当的监控手段，能够及时发现灾难恢复中心基础设施和设备运行的故障和问题；应保留所有监控记录，以满足故障定位、诊断及事后审计要求；

e) 存储介质和数据管理：应建立规范的流程和记录确保数据的传输和复制过程有章可依，有据可查，保证存储介质和数据的安全，不遗失、不泄露；同时应对存储介质和数据进行定期的检查和验证，保证存储介质和数据的正确、完整、可用；

f) 事件管理：应制定规范的事件处置流程，规定所有事件的记录、优先排序、业务影响、分类、更新、调整、解决和正式关闭，并在系统中记录事件处理的全过程；应能够记录并跟踪、统计事件处置的过程和结果，以保证服务能力和服务承诺的实现和改善；

g) 问题管理：应建立问题管理流程，落实问题分析及解决机制，有效约束和控制重复性故障，主动

排除重大隐患；

h) 变更管理：应制定变更管理流程，以应对常规和紧急状态下的硬件、软件、通信、服务要求和文档流程等方面的变更，减少或避免因为疏忽、缺少资源、准备不充分等缘故导致变更失败或产生其他的问题；

i) 配置管理：应建立资产清单和配置项清单，确保资产和配置项可审核、可追溯。

8.3.4 服务商管理

应对灾难恢复服务商的管理内容及要求如下：

a) 评估紧急采购流程风险对恢复能力和恢复水平的影响，对关键设备和服务应事先签订紧急供货或紧急服务协议；

b) 明确约定服务范围、服务内容、服务水平、定价机制、保密条款和违约责任；

c) 定期对服务商的支持能力和服务水平进行测试，包括响应时间、保障能力、人员稳定性和服务技能等。如果可能还应指明可能的替换资源和途径；

d) 应制定服务商管理制度、流程，建立全面的服务质量控制和风险控制措施；

e) 结合业务恢复需求，科学合理定义服务范围和服务水平要求；

f) 签订书面合同，在合同中明确重要事项，包括双方的权利和义务、服务水平、服务的可靠性、服务的可用性、信息安全控制、服务持续性计划、审计、合规性要求、违约赔偿等；

g) 通过服务水平协议(SLA)明确可检核的服务质量水平目标，作为检验服务的质量标准，根据服务内容约定服务的质量和时间要求；

h) 应禁止服务提供方转包并严格控制分包，保证服务水平；

i) 加强服务安全管理，通过技术和流程手段控制服务人员接触系统的权限和内容，执行信息安全管理的标准和规范，保障业务、管理和客户敏感数据信息安全；

j) 应建立服务商考核、评价机制，定期对服务活动和服务提供方的服务能力进行审核和评估，确保获得持续、稳定的外包服务；

k) 定期对服务提供方进行非现场审计；

l) 定期对服务提供方进行现场考察；

m) 定期对报告服务结果进行抽查、抽测；

n) 定期的执行联合测试及演练考察服务商的实际响应能力。

8.3.5 基准核对管理

基准核对管理内容和要求如下：

a) 组织应根据灾难备份系统的范围和特点，建立灾难备份系统的基准，并形成相应的基准文档；

b) 基准文档应包括灾难备份信息系统资源的配置信息，包括主机、存储、网络、安全等硬件设备及操作系统、数据库、中间件等软件的配置信息；

c) 在灾难备份系统投入运营后，应根据变更情况，及时修改和更新基准文档；

d) 应定期对生产中心和灾难恢复中心的基准进行统计核对工作，发现差异及时处理。

8.3.6 子系统验证管理

子系统验证管理内容和要求如下：

a) 定期对各子系统进行能力和状态的测试工作，以保证灾难备份各子系统的有效性和运行的可靠性；

b) 关键测试应通过机构管理者的批准和授权，机构管理者和客户也应参与关键测试，使其了解测试过程和结果；

c) 所有的测试的目标、计划和结果都应记录在案用于复审或审核的跟踪；在测试中发现的缺陷应尽可能及时改正；没有改正的缺陷将通过与机构管理者沟通来评价，每次疏忽的潜在后果应展示出来；

d) 每次测试应选取不同的形式，保证测试所覆盖的完整性。

8.3.7 灾难恢复演练

灾难恢复演练内容和要求如下：

a) 灾难恢复中心建设完成后应组织全面的演练，验证灾难恢复中心基础设施、灾难备份系统和灾难恢复预案的正确性和有效性，进一步改进和提升灾难恢复中心的恢复能力和管理水平。灾难恢复演练实施应包括演练策略的制定、演练计划的落实、演练方案设计、演练的组织、演练的实施、演练过程的过程记录和应急处置、演练结果的评估与总结。灾难恢复演练的形式包括：桌面演练、模拟切换演练和实际切换演练。

b) 灾难恢复演练应充分考虑系统验证的实际需要，应灵活选择桌面演练、模拟切换演练和实际切换演练等不同形式定期开展灾难恢复演练。在条件成熟的情况下应定期开展实际切换演练，验证灾难恢复中心的实际切换和真实生产任务的接管能力。但在组织实际切换演练时应在人员培训、系统测试、预案验证等方面做好充足的准备，充分注意对实际业务可能产生的风险和影响，避免由于演练组织不当对生产业务造成重大影响。

c) 灾难恢复演练应做到“目标明确、全员参与、组织有序、结果真实”，机构的高层管理人员应充分认识灾难恢复演练的重要性，组织机构内部的各部门落实演练策略、制定演练计划、指挥演练实施、评估演练结果，确保演练的顺利实施。灾难恢复切换演练应按照以下要求进行组织实施：

   1) 演练实施管理团队应根据机构的业务特点和灾难备份系统操作熟练程度规划演练目标、演练范围和演练方式，并组织机构的业务、技术和管理人员对演练方案进行评审；应仔细评估演练失败或操作失误可能造成的影响，并事前采取相应防范措施，避免对生产系统的正常运行造成重大影响；

   2) 演练方案应通过演练实施管理团队的审批，如果涉及生产中心或业务部门还应获得机构管理层的批准后方可执行；

   3) 灾难恢复演练前应对演练场所、演练设备、配置要求等进行仔细的核对和检查，并组织相关参演人员进行培训，使其熟悉和了解相关的操作过程和操作结果；

   4) 演练过程中应尽量模拟真实场景、真实环境和真实问题，并对演练中发生的突发事件制定有效的应对措施；

   5) 演练结果应形成正式的书面演练报告，演练报告应包含：演练的目标、演练范围、演练实施的组织架构和岗位职责、演练过程记录，演练过程中的应急处置方案、演练结果的评价等。

8.3.8 预案维护

预案的维护的内容和要求如下：

a) 在演练实施后，应及时组织相关人员进行总结，对预案进行必要的更新；

b) 应定期检查和核对灾难恢复预案中的变更情况（如成员及联络方式的变更、信息系统的日常变更等），对预案进行及时的文档更新及分发，确保预案的切实有效；

c) 应预先制定灾难恢复预案启动的条件，确定灾难宣告的决策和授权机制。并明确对内和对外宣告的范围和内容。

8.3.9 应急和切换

应急和切换的内容和要求如下：

a) 应建立灾难预警和预告机制，明确责任，加强与公共专业服务机构的沟通与联系，如气象、地震、消防、防疫、公安、供电等，做到灾难的早发现、早报告，提前进行灾难预防和灾难切换准备；
b) 应明确灾难恢复环境必需的资源和配置，并定期进行测试演练，以保证灾难恢复所需资源和配置的有效性。灾难恢复环境一般应包括灾难备份系统的监控平台、灾难恢复指挥中心、业务恢复操作终端环境、业务连续性恢复配套资源、技术支持平台、后勤保障平台等；
c) 在灾难切换过程期间，灾难恢复中心应在场地环境、设备操作等方面提供支持，配合将生产系统从生产中心切换到灾难恢复中心，切换过程主要工作包括：网络切换、存储切换、主机切换、数据校验、系统校验、数据追补、业务验证等；
d) 在接替生产运营服务期间，灾难恢复中心应加强技术支持与设施保障的资源和人力，以接替生产中心的日常工作。

8.3.10 教育与培训

教育与培训的内容和要求如下：

a) 机构应为所有员工提供业务连续性或灾难恢复的专业培训。培训形式可根据机构的自身条件选择内部培训或聘请外部机构培训；
b) 应按照灾难恢复运维管理要求为关键岗位和关键角色提供特殊的岗位培训；
c) 应对每次培训的结果进行记录和评估。

8.3.11 文档和知识管理

机构应建立一个知识管理体系来获得并保持其在业务连续性或灾难恢复管理的过程和结果文档。该体系包括：

a) 关键人员的联系方式和业务连续性计划文档；
b) 内部知识和最佳实践共享；
c) 历史项目的文档和恢复成果。

8.4 灾难恢复中心管理的审核与验证

为确保机构灾难恢复中心的有效性和合规性，机构应定期组织内部和外部专家对灾难恢复中心进行定期审验，以保证各方面工作得到落实。

a) 应组建独立于灾难恢复中心组织机构的内部或外部审计团队，对灾难恢复运行维护有效性进行审计，审计内容至少应包括灾难恢复技术有效性，灾难恢复预案正确性、恢复组织管理流程的合理性和熟练度等；
b) 内部审计团队可由机构内的业务部门、技术专家和运维管理专家构成；
c) 外部审计团队可由灾难恢复管理领域的专业机构或专家构成；
d) 内部及外部审计应定期开展。

8.4.1 外包管理

对于通过外包方式获取灾难恢复中心资源的机构，应对外包服务机构进行严格地考核，并制定有效的外包服务管理机制，以确保外包服务质量。外包服务机构选择应注重：

a) 专业性

考察服务提供机构是否专业从事灾难恢复服务领域；

b) 服务质量

是否具有完善的服务质量管理体系，以及服务体系和安全体系的认证；

c) 机构规模

考察服务提供机构是否具有一定规模，是否能长期稳定地提供服务；

d） 服务经验

从事灾难恢复服务的历史，服务案例，提供恢复测试、演练的服务经历；

e） 服务范围

考察服务体系是否完整，是否能够提供机构所需的所有服务；

f） 地理区域

考察服务是否有地理区域限定，机构的需求会不会受到限制；

g） 服务人员

考察服务提供机构能否维持一个专业的灾难恢复服务团队；

h） 应急管理

在服务提供机构发生意外时是否有合适的响应体系和计划。

外包服务机构持续管理应注重：

a） 合约保障

签订书面合同，在合同中明确重要事项，包括双方的权利和义务、外包服务水平、服务的可靠性、服务的可用性、信息安全控制、服务持续性计划、审计、合规性要求、违约赔偿等；

b） 服务水平

通过服务水平协议（SLA）明确可检核的灾难恢复中心外包服务质量水平目标，作为检验灾难恢复外包服务的质量标准，根据服务内容约定服务的质量和时间要求；

c） 服务控制

服务提供机构不应转包并严格控制分包，保证外包服务水平；

d） 服务安全

通过技术和流程手段控制服务人员接触系统的权限和内容，执行信息安全管理的标准和规范，保障业务、管理和客户敏感数据信息安全；

e） 考核机制

应建立外包服务考核、评价机制，定期对外包服务活动和服务提供方的服务能力进行审核和评估，确保获得持续、稳定的外包服务。

中 华 人 民 共 和 国
国 家 标 准
信息安全技术
灾难恢复中心建设与运维管理规范
GB/T 30285—2013
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲 2 号(100029)
北京市西城区三里河北街 16 号(100045)
网址:www.gb168.cn
服务热线:400-168-0010
010-68522006
2014 年 5 月第一版
*
书号:155066·1-49209

GB/T 30285-2013