ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 20988—2025
代替 GB/T 20988—2007，GB/T 30285—2013

网络安全技术　信息系统灾难恢复规范

Cybersecurity technology—Disaster recovery specifications for information systems

2025-06-30 发布　　2026-01-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前言 …… Ⅲ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　灾难恢复概述 …… 3
4.1　灾难恢复目标 …… 3
4.2　灾难恢复生命周期和工作范围 …… 3
5　灾难恢复的组织机构设置 …… 4
5.1　组织机构的设立 …… 4
5.2　组织机构的人员组成和职责 …… 4
6　灾难恢复规划设计 …… 5
6.1　灾难恢复需求的确定 …… 5
6.2　灾难恢复策略的制定 …… 5
6.3　灾难恢复技术方案设计 …… 7
6.4　灾难恢复中心选址和等级 …… 9
6.5　灾难恢复技术方案的验证和确认 …… 9
7　灾难恢复系统和中心建设 …… 9
7.1　灾难恢复系统建设 …… 9
7.2　灾难恢复中心建设 …… 11
8　灾难恢复系统运行管理 …… 12
8.1　灾难恢复预案制定及管理 …… 12
8.2　灾难恢复系统运行维护 …… 13
8.3　应急事件响应及灾难接管 …… 15
8.4　重建和回退 …… 16
8.5　灾难恢复审计 …… 16
9　测试评价方法 …… 16
9.1　灾难恢复总体测试评价要求 …… 16
9.2　灾难恢复的组织机构设置测试评价方法 …… 16
9.3　灾难恢复规划设计测试评价方法 …… 17
9.4　灾难恢复系统和中心建设测试评价方法 …… 24
9.5　灾难恢复系统的安全建设测试评价方法 …… 28
9.6　灾难恢复系统运行管理测试评价方法 …… 36
附录 A（规范性）　灾难恢复能力等级划分 …… 42

A.1 第1级——基本支持 …… 42
A.2 第2级——备用场地支持 …… 42
A.3 第3级——电子传输和部分设备支持 …… 43
A.4 第4级——电子传输及完整设备支持 …… 43
A.5 第5级——实时数据传输及完整设备支持 …… 44
A.6 第6级——数据零丢失和远程集群支持 …… 45
A.7 灾难恢复能力等级评定原则 …… 46
A.8 灾难恢复中心的等级 …… 46
附录B（资料性） 某行业同城灾难恢复中心RTO/RPO与灾难恢复能力等级的关系示例…… 47
附录C（资料性） 某行业信息系统需求分类示例 …… 48
附录D（资料性） 云计算技术灾难恢复服务示例 …… 49
附录E（资料性） 灾难恢复系统的安全建设 …… 51
E.1 网络安全等级保护…… 51
E.2 安全管理制度…… 51
E.3 安全管理架构…… 51
E.4 安全管理人员…… 51
E.5 安全通信网络…… 51
E.6 安全计算环境…… 52
E.7 安全建设管理…… 52
E.8 安全运维管理…… 52
E.9 供应链安全…… 53
E.10 数据安全 …… 53
附录F（资料性） 灾难恢复预案框架 …… 54
F.1 目标和范围…… 54
F.2 组织和职责…… 54
F.3 联络与通信…… 54
F.4 突发事件响应流程…… 54
F.5 恢复及重续运行流程…… 55
F.6 灾后重建和回退…… 55
F.7 预案的保障条件…… 55
F.8 预案附录…… 55
参考文献 …… 56

前　言

本文件按照 GB/T 1.1—2020《标准化工作导则　第 1 部分：标准化文件的结构和起草规则》的规定起草。

本文件代替 GB/T 20988—2007《信息安全技术　信息系统灾难恢复规范》和 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》，与 GB/T 20988—2007 相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 删除了术语“灾难备份中心”“灾难备份系统”及其定义（见 2007 年版的 3.1、3.3）；
b) 增加了术语“灾难恢复系统”“灾难恢复中心”及其定义（见 3.17、3.19）；
c) 将术语“灾难恢复规划”修改为“灾难恢复计划”，术语“演练”修改为“应急演练”（见 3.15、3.11，2007 年版的 3.11、3.13）；
d) 增加了“灾难恢复生命周期概念与模型”（见第 4 章）；
e) 增加了“灾难恢复的组织机构设置”（见第 5 章）；
f) 修改了“灾难恢复规划设计”，增加了“云灾备”等方面内容（见第 6 章，2007 年版的第 6 章）；
g) 修改了“灾难恢复策略实现”，增加了“灾难恢复方案的验证和确认”“灾难恢复中心建设”等内容（见第 6 章、第 7 章，2007 年版的第 7 章）；
h) 修改了“灾难恢复策略实现”，增加了“灾难恢复生命周期中运行维护管理”（见第 8 章，2007 年版的第 7 章）；
i) 增加了“灾难恢复测试评价方法”（见第 9 章）；
j) 将“数据备份系统”修改为“数据备份容灾系统”（见附录 A，2007 年版的附录 A）；
k) 增加了“灾难恢复系统的安全建设”（见附录 E）；
l) 增加了“灾难恢复预案框架”（见附录 F）。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国网络安全标准化技术委员会（SAC/TC 260）提出并归口。

本文件起草单位：中国信息安全测评中心、北京安信天行科技有限公司、北京邮电大学、华为技术有限公司、中国电子技术标准化研究院、中科信息安全共性技术国家工程研究中心有限公司、北京金融信息化研究所有限责任公司、杭州美创科技股份有限公司、阿里巴巴（北京）软件服务有限公司、深圳市科力锐科技有限公司、教育部教育管理信息中心、国家信息中心、航天壹进制（江苏）信息科技有限公司、北京市经济和信息化局网络安全管理中心、公安部第一研究所、甘肃海丰信息科技有限公司、中国信息通信研究院、奇安信科技集团股份有限公司、深信服科技股份有限公司、广东省信息安全测评中心、民航成都电子技术有限责任公司、云南电网有限责任公司信息中心、安徽科技学院、中国互联网络信息中心、中国科学院信息工程研究所、首都信息科技发展有限公司、中国能源建设集团山西省电力勘测设计院有限公司。

本文件主要起草人：孙明亮、张晓菲、陈青民、李小勇、李晓翠、王惠莅、刘鑫、苑洁、邓娟、顾寅红、胡建勋、李海鹏、杨晓平、冯秀康、杨希、陈永刚、胡安磊、杨伟平、吴齐跃、廖运华、胡春涛、于铮、程颖博、李秋香、陆丽、郑方、赵增振、刘丰、彭海龙、马多贺、肖鹏、王文佳、马勇、李静毅、马国梁、曹京、王玉英、康楠、常新苗、曹浩、刘斌、安锦程、金铄。

本文件及其所代替文件的历次版本发布情况为：

——GB/T 20988，2007 年首次发布；GB/T 30285，2013 年首次发布；

——本次为第一次修订。

网络安全技术　信息系统灾难恢复规范

1　范围

本文件确立了信息系统灾难恢复工作原则，给出了信息系统灾难恢复生命周期，规定了信息系统灾难恢复应遵循的基本要求，描述了灾难恢复能力等级划分和测试评价方法。

本文件适用于灾难恢复的需求方、服务提供方和评估方等各类组织开展信息系统灾难恢复的规划设计、建设实施和运行管理等工作。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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—2022　信息安全技术　信息安全风险评估方法

GB/T 25069—2022　信息安全技术　术语

GB 50174—2017　数据中心设计规范

3　术语和定义

GB/T 25069—2022 界定的以及下列术语和定义适用于本文件。

3.1

场外存放　offsite storage

将存储介质存放到离主中心（3.21）有一定安全距离的物理地点的过程。

3.2

重续　resumption

灾难恢复中心（3.19）替代主中心（3.21），支持关键业务功能（3.3）重新运作的过程。

3.3

关键业务功能　critical business functions；CBF

中断一定时间将显著影响组织运作的服务或职能。

3.4

恢复点目标　recovery point objective；RPO

为使活动能够恢复操作而需将其所用信息恢复到的时间点。

［来源：GB/T 25069—2022，3.253］

3.5

恢复时间目标　recovery time objective；RTO

从事件发生到完成恢复产品或服务、活动或者资源之间的时间段。

注：对于产品、服务和活动，恢复时间目标需小于组织无法接受的导致产品、服务停止供应或活动无法执行等负面影响所需的时间。

［来源：GB/T 25069—2022，3.254］

3.6

回退　return

复原　restoration

支持业务运作的信息系统从灾难恢复中心(3.19)重新回到主中心(3.21)运行的过程。

3.7

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。

3.8

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(3.5)和恢复点目标(3.4)。

3.9

业务连续性管理　business continuity management;BCM

识别对组织的潜在威胁及其一旦发生可能对业务运行所带来影响的整套管理过程,该过程为建立具有有效响应能力的组织韧性提供框架,以保护其关键相关方利益、声誉、品牌以及价值创造活动。

[来源:GB/T 25069—2022,3.714]

3.10

业务影响分析　business impact analysis;BIA

对活动和业务中断可能带来影响的分析过程。

[来源:GB/T 25069—2022,3.715]

3.11

应急演练　emergency drill

为训练有关人员和提高应急响应能力而根据应急预案和应急响应计划所开展的活动。

[来源:GB/T 25069—2022,3.729]

3.12

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。

注:通常导致信息系统需切换到灾难恢复中心(3.19)运行。

3.13

灾难备份　backup for disaster recovery

为了灾难恢复(3.14)而对数据、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。

3.14

灾难恢复　disaster recovery

为了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。

[来源:GB/T 25069—2022,3.766]

3.15

灾难恢复计划　disaster recovery plan;DRP

信息系统灾难恢复过程中筹划所需的任务、行动、数据和资源,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所支持关键业务功能的文件。

[来源:GB/T 25069—2022,3.767]

3.16

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。

3.17

灾难恢复系统　backup system for disaster recovery

用于灾难恢复(3.14)目的,由数据备份容灾系统、备用数据处理系统和备用的网络系统组成的信息系统。

3.18

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。

注: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。

3.19

灾难恢复中心　disaster recovery center

容灾备份中心　backup center for disaster recovery

满足机构关键业务连续性的要求,承载灾难恢复系统运行的场地。

注:灾难恢复中心承载的业务和工作范畴包括灾难恢复中心、容灾数据中心等相关业务和场所。

[来源:GB/T 30285—2013,3.5,有修改]

3.20

主系统　primary system

生产系统　production system

正常情况下支持机构日常运作的信息系统。

[来源:GB/T 25069—2022,3.522,有修改]

3.21

生产中心　production center

主中心　primary center

主站点　primary site

主系统所在的数据中心。

4　灾难恢复概述

4.1　灾难恢复目标

灾难恢复目标是通过有效的技术与管理手段,确保组织在灾难发生时迅速恢复信息系统运行,最大限度地降低损失和影响,保障数据的完整性和可用性,保障业务的连续性。

4.2　灾难恢复生命周期和工作范围

灾难恢复生命周期包括规划设计、建设实施和运行管理,在全生命周期过程中应持续进行有效性分析和安全管控,以实现持续改进。见图1。

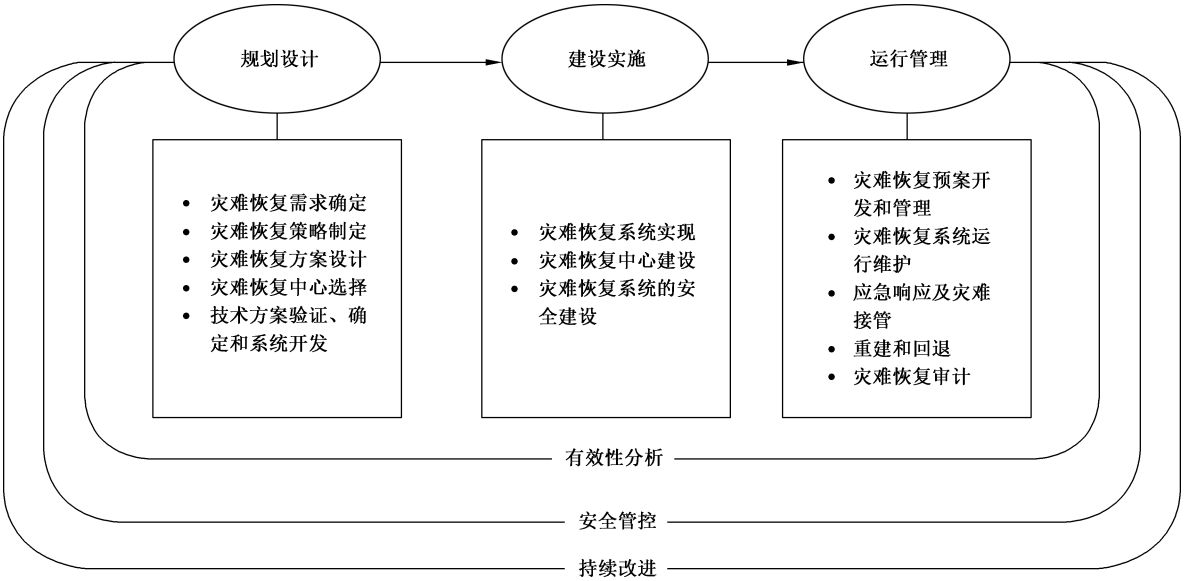


图 1　灾难恢复生命周期示意图

信息系统的灾难恢复工作，包括灾难恢复中心和灾难恢复系统的规划设计、建设实施工作，以及日常运行中的预案管理、运行维护、监控、巡检工作，还涉及应急响应及灾难接管、重建和回退、审计相关工作。组织的信息系统灾难恢复机构对整个生命周期灾难恢复过程中的资源配置、技术服务过程与过程管理等方面进行合规性、有效性分析，以确保业务的正常开展。灾难恢复工作是一个周而复始、持续改进的过程。

灾难恢复中心具备多重功能，部分灾难恢复中心发挥了数据统计、分析的作用，担当了多重角色，灾难恢复应用方可根据实际情况增加、裁剪本文件呈现的技术规范与要求。

信息系统的灾难恢复工作依据恢复能力目标划分为 6 级。

各阶段具体工作应符合第 6 章至第 8 章的要求，等级划分应符合附录 A 的要求，附录 A 确定了灾难恢复系统各等级在灾难恢复要素方面的要求，第 5 章作为组织机构要求属于基本要求，不参与到信息系统等级要求范围，第 6 到第 8 章具体内容确定了整个信息系统灾难恢复全生命周期的全面要求，具体每个等级通过附录 A 中信息系统灾难恢复等级特征进行匹配，测试评价方法应符合第 9 章要求。

5　灾难恢复的组织机构设置

5.1　组织机构的设立

信息系统的使用或管理组织（以下简称“组织”）应结合其日常组织机构建立灾难恢复的组织机构，并明确其职责。

灾难恢复的组织机构可设为以下小组：

a）　灾难恢复领导小组；

b）　灾难恢复管理小组；

c）　灾难恢复技术与执行小组；

d）　灾难恢复保障小组。

组织可聘请外部专家协助灾难恢复实施工作，也可委托具有相应资质的外部机构承担灾难恢复技术与执行小组以及灾难恢复保障小组的部分或全部工作。

5.2　组织机构的人员组成和职责

各组织机构的人员可负责两种或多种职责，一些岗位可由多人担任。各组织机构人员组成和机构

职责如下。

——灾难恢复领导小组是信息系统灾难恢复工作的组织领导机构，组长应由组织最高管理层成员担任。灾难恢复领导小组的职责是领导和决策信息系统灾难恢复的重大事宜，主要包括审核并批准灾难恢复经费预算、审核并批准灾难恢复的策略、预案，及批准灾难恢复预案的执行。

——灾难恢复管理小组主要由组织的业务、技术、后勤等相关部门负责人组成，在灾难恢复领导小组领导下开展工作，主要负责管理和协调信息系统灾难恢复工作，包括组织制定灾难恢复经费预算、组织制定灾难恢复的策略及预案、协调灾难恢复内外部资源、检查灾难恢复工作。

——灾难恢复技术与执行小组由灾难恢复中心专业技术人员、运行维护人员和服务供应商组成，主要负责灾难恢复的具体实施工作，包括灾难恢复规划设计、建设实施、运行和维护工作，以及预案的开发、测试、演练和执行。

——灾难恢复保障小组主要由组织的人力资源、后勤保障人员组成，主要负责保障灾难恢复工作所需要的资源供应、灾难抢修，及灾难发生场所的安全。

6 灾难恢复规划设计

6.1 灾难恢复需求的确定

6.1.1 风险分析

开展风险分析活动，识别信息系统的资产及其价值、面临的威胁和存在的脆弱性，识别现有的风险防范和控制措施，风险评估方法应遵循 GB/T 20984—2022。

6.1.2 业务影响分析

识别组织各信息系统与业务之间的相关性，确定支持各项业务功能的相应信息系统资源及其他资源，明确相关的保密性、完整性、可用性（包括时间敏感性）要求。

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应进行评估：

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

b) 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。

6.1.3 确定灾难恢复的需求

根据风险分析和业务影响分析的结果，应确定灾难恢复需求，包括：

a) 综合风险分析和业务影响分析的结果，确定信息系统的恢复优先级；

b) 确定灾难恢复目标，即 RTO、RPO 指标，确定信息系统可允许恢复到一个可接受的服务级别。附录 B 给出了某行业 RTO 和 RPO 与灾难恢复能力等级的关系示例。

6.2 灾难恢复策略的制定

6.2.1 灾难恢复策略要求

根据灾难恢复目标，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”）制定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。确定灾难恢复策略的要素主要应包括：

a) 根据风险分析结果确定信息系统的分类分级，分类分级具体方法按 GB/T 20984—2022，附录 C 给出了某行业信息系统需求分类划分示例；

b) 确定灾难恢复能力等级，不同的灾难恢复能力等级需要的资源要素，及对灾难恢复资源要素的

要求不尽相同；

c) 确定灾难恢复资源要素的获取方式；

d) 确定灾难恢复系统的安全要求；

e) 确定灾难恢复中的兼容性要求。

6.2.2 灾难恢复类别的规划

根据提供服务重要性、时效性要求和建设规划，灾难恢复类别分为：数据级、应用级和业务级。

a) 数据级灾难恢复：在灾难发生之后，可确保数据不受到损坏。

b) 应用级灾难恢复：是在数据级灾备的基础上，在灾难恢复中心构建与生产中心一样（或部分）的信息系统，一旦生产中心的信息系统中断时，可实现灾难恢复中心的接管，保障业务连续性。

c) 业务级灾难恢复：是在应用级灾备的基础上，不仅仅是基础设施和信息系统的部分，还要有用户和业务人员的办公场所，当发生灾难时，用户和业务人员提供现场支持。

注：数据级、应用级和业务级三种类别的恢复能力等级由其各自类别的 RTO 和 RPO 指标确定。

6.2.3 灾难恢复布局规划

组织应根据成本风险平衡原则以及管理要求，选择采用以下布局模式：

——一主一备：一个生产中心，一个灾难恢复中心；

——一主多备：一个生产中心，多个灾难恢复中心；

——互为备份：两个及两个以上生产中心互相备份；

——多主一备：多个生产中心共享一个灾难恢复中心；

——混合方式：以上方式的混合。

注：互为备份包括双活和多活方式，所有的中心均提供实时服务，互为备份，当一个生产中心服务中断，由其他的生产中心接管，提供正常的服务，确保业务连续性不受影响。

6.2.4 灾难恢复资源要素

支持灾难恢复各能力等级所需的资源要素应包括：

a) 数据备份容灾系统：一般由容灾备份的硬件、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备份容灾系统，还包括容灾备份线路和相应的通信设备；

b) 备用数据处理系统：灾难恢复所需要的系统，以实现灾难恢复系统的预期目标，指备用的计算机、外围设备和软件；

c) 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；

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

e) 专业技术支持能力：对灾难恢复系统的运转提供支撑和综合保障的能力，以实现灾难恢复系统的预期目标，包括硬件、系统软件和应用软件的问题分析和处理能力、网络系统安全运行管理能力、沟通协调能力等；

f) 运行维护管理能力：包括运行环境管理、系统管理、安全管理和变更管理等；

g) 灾难恢复预案：包括触发启动条件、实施目标、实施团队、关联的资产和切换流程等。

6.2.5 采用云计算技术的灾难恢复资源要素

在采用云计算技术的灾难恢复工作中，在满足 6.2.4 要求的基础上，宜考虑生产中心、灾难恢复中心的信息系统在使用云计算技术和不使用云计算技术的多种组合模式。在使用云计算技术时，宜考虑云上、云下、跨区、跨云场景下的适用性和兼容性需求。附录 D 给出了一个云计算技术场景下使用灾难

恢复服务的示例。

6.3 灾难恢复技术方案设计

6.3.1 灾难恢复资源的要求与获取方式

6.3.1.1 数据备份容灾系统

组织应根据灾难恢复目标，按成本风险平衡原则，应确定：

a) 灾难恢复与数据备份的范围；

b) 数据备份的时间间隔；

c) 数据备份容灾的技术和介质；

d) 数据备份容灾系统的安全要求。

数据备份容灾系统可由组织自行建设，也可通过租用其他机构的系统或由云厂商提供的灾难恢复服务而获取。

数据备份容灾系统应提供数据一致性和完整性验证，以确保灾难恢复中心与生产中心数据的一致性和完整性。

6.3.1.2 备用数据处理系统

组织应根据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，按成本风险平衡原则，应确定备用数据处理系统的：

a) 数据处理能力；

b) 与主系统的兼容性要求；

c) 平时处于就绪还是运行状态；

d) 布局规划。

组织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) 事先购买所需的设备并存放在灾难恢复中心或安全的设备仓库；

c) 租用商业化灾难恢复中心或签有协议的机构已有的兼容设备。

备用数据处理系统与生产环境的数据处理系统在系统运行环境和软件版本等方面应完全兼容。

6.3.1.3 备用网络系统

组织应根据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，按成本风险平衡原则，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。

组织可通过 6.3.1.2 所述的方式获取备用网络系统；备用数据通信线路可使用自建的数据通信线路或租用公用数据通信线路。

6.3.1.4 备用基础设施

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

a) 与主中心的距离要求；

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) 运行维护和管理要求。

组织可选用以下三种方式获取备用基础设施：

a) 由组织所有或运行；

b） 多方共建或通过协议获取；

c） 租用商业化灾难恢复中心的基础设施。

6.3.1.5 专业技术支持能力

组织应根据灾难恢复目标，按成本风险平衡原则，确定灾难恢复中心在软件、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。

组织可选用以下几种方式获取专业技术支持能力：

a） 灾难恢复中心设置专职技术支持人员；

b） 获得第三方的技术和服务支持；

c） 由主中心技术支持人员兼任；对于RTO较短的业务功能，宜关注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；

d） 灾难恢复中心宜建立灾难恢复管理技术平台，对人员、预案、系统、设备、环境等实现数字化统一管理、统一调度，灾难的快速感知、分析、评估及自动化切换等，灾难恢复流程可视、可控、可管。

6.3.1.6 运行维护管理能力

组织应根据灾难恢复目标，按成本风险平衡原则，确定灾难恢复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。

组织可选用以下对灾难恢复中心的运行维护管理模式：

a） 自行运行和维护；

b） 委托其他机构运行和维护。

6.3.1.7 灾难恢复预案

组织应根据需求分析的结果，按成本风险平衡原则，明确灾难恢复预案的：

a） 整体要求；

b） 制定过程的要求；

c） 教育、培训和演练要求；

d） 管理要求。

组织可选用以下方式，完成灾难恢复预案的制定、落实和管理：

a） 由组织独立完成；

b） 聘请外部专家指导完成；

c） 委托外部机构完成。

6.3.1.8 云灾难恢复服务

在使用云灾难恢复服务模式下，组织应根据灾难恢复目标，按成本风险平衡原则，确定对云灾难恢复服务的要求：

a） 数据级灾难恢复能力；

b） 应用级灾难恢复的接管能力；

c） 系统架构和兼容性能力要求；

d） 独立于生产云平台的场外云平台系统。

采用云灾难恢复服务，可选用以下方式获取：

a) 由组织所有或运行，实现自身云服务需要并提供灾难恢复功能；
b) 租用由外部机构提供的灾难恢复服务。

6.3.2 灾难恢复系统的安全要求

灾难恢复系统的网络安全要求不低于其承载的信息系统的最高级别，具体安全要求应遵循相关法律法规和标准，附录 E 给出了灾难恢复系统的安全建设的示例。

6.4 灾难恢复中心选址和等级

6.4.1 灾难恢复中心的选址

依据信息系统灾难恢复布局规划，选择或建设灾难恢复中心时，应根据风险分析的结果，拟建灾难恢复中心的安全等级、灾难恢复中心与生产中心的布局关系，避免灾难恢复中心与主中心同时遭受同类风险。

灾难恢复中心包括“同城”和“异地”两种类型。灾难恢复中心的选址应符合 GB 50174—2017 中 4.1 的相关要求以外，还包括：

a) 同城灾难恢复中心的选址需要关注两个中心的安全距离，应不在同一个变电所的电网内，不在同一个通信网络节点内；另外还宜关注网络延迟对生产中心的影响，同城灾难恢复中心与生产中心的直线距离宜设置在(10～100)km 之间。
b) 异地灾难恢复中心的选址应避开同一个地震带、龙卷风、台风路线等自然灾害同发地区，异地灾难恢复中心建设距离宜大于 100 km。
c) 对重要的国家战略层面的灾难恢复中心的选址宜关注防灾害、防侦测和攻击等因素。

6.4.2 灾难恢复中心基础设施的等级

根据灾难恢复中心功能和灾难恢复的目标对时效性的要求，按 GB 50174—2017 的等级要求建设灾难恢复中心基础设施。灾难恢复中心基础设施的等级宜与生产中心的等级保持一致或低一个等级。

6.5 灾难恢复技术方案的验证和确认

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。技术方案的验证包括数据完整性和一致性验证、数据备份与恢复能力验证、信息系统切换与回切能力验证、网络系统切换与回切能力验证、系统安全性验证。

7 灾难恢复系统和中心建设

7.1 灾难恢复系统建设

7.1.1 实施方案制定

根据第 6 章灾难恢复的需求和规划设计，提出灾难恢复系统实施方案，并将其规范化，并整理成文档，使得在具体实施阶段有所依据。详细实施方案应包含但不限于以下内容：

a) 建设目标和建设内容；
b) 技术实现方案；
c) 系统和组件安全功能和性能要求；
d) 系统和组件部署；

e) 安全控制策略和配置；
f) 配套的安全管理建设内容；
g) 工程实施计划；
h) 项目投资概算。

7.1.2 系统部署和配置

对灾难恢复系统进行部署和配置，应主要包含但不限于以下内容。

a) 部署准备。对实施环境进行准备，包括灾难恢复系统相关硬件设备准备、软件系统准备、环境准备。为了保证实施的质量，可制定一套可行的系统质量控制方案，以便有效地指导系统实施过程。对灾难恢复系统相关软硬件产品进行测试，符合测试要求的产品才能用于具体系统部署。
b) 系统部署。将配置好策略的灾难恢复系统相关的产品或者模块部署到实际的应用环境中，并调整相关策略。系统实施的各个环节应遵照质量控制方案的要求，部署实现质量控制目标。
c) 系统配置。对承载灾难恢复应用系统的软硬件等进行配置，使得灾难恢复系统能够工作正常，并对生产中心和灾难恢复中心的网络进行配置，使得备用网络系统工作正常。

7.1.3 系统测试

根据灾难恢复的需求和规划设计，对系统进行测试检验，测试系统是否实现了设计的功能、性能和安全性。应主要包含但不限于以下内容：

a) 对承载灾难恢复应用系统的软硬件等进行测试，保证相关功能正常，同时保证在限定的时间内，可正确恢复系统、应用软件及各类数据，可正确恢复各项关键业务功能；
b) 对生产中心和灾难恢复中心间的网络进行测试，保证客户端可与备用数据处理系统通信正常；
c) 对灾难恢复系统的安全性进行测试，如身份鉴别、访问控制、安全审计、数据保护和功能保护等内容。

同时将测试结果与规划设计进行对比，如果不满足设计要求，应对系统进行整改或者重新部署配置，再重复进行以上测试过程，直至满足要求为止。

7.1.4 验收与交付

根据灾难恢复的规划设计和实施方案，检验系统是否严格按照实施方案进行建设，是否实现了设计的功能、性能和安全性等。应主要包含但不限于以下内容。

a) 验收准备。根据设计方案中需要达到的目标，准备验收方案。验收方案立足于合同条款，需求说明书和设计方案，充分体现用户需求。
b) 组织验收。由验收工作组按照验收计划负责组织实施，组织测试人员根据已通过评审的系统验收方案进行验收测试。验收测试内容结合详细设计方案，对功能、性能和安全性等进行测试。
c) 验收报告。在测试完成后形成验收报告，验收报告需明确给出验收意见和验收结论，并根据验收意见尽快修正有关问题，重新进行验收。
d) 系统交付。系统交付包括但不限于以下内容：交付验收报告、交付清单、管理员手册、用户手册、安全概述以及系统配置说明书等，以及为了达到灾难恢复目标，建立的各种操作规程和管理制度，如：运行环境管理制度、系统管理制度、安全管理制度和变更管理制度等。
e) 培训。根据灾难恢复策略的要求，提供对灾难恢复系统的专业技术支持能力。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。

7.2 灾难恢复中心建设

7.2.1 通则

灾难恢复中心的建设过程应与7.1一致，具体灾难恢复建设按GB 50174—2017要求执行。根据灾难恢复特殊性，还应满足7.2.2～7.2.5的要求。

7.2.2 备用基础设施建设要求

灾难恢复中心基础设施建设可根据组织的建设要求组织实施，其建设内容应包含但不限于以下内容。

a) 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、信息系统设备、测试维修机房等信息系统工作设施；供配电设施、空调暖通设施、给排水设施、消防设施等保障系统工作设施。

b) 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、资料室等日常运行辅助设施；灾难恢复指挥中心、办公区、新闻发布中心（多媒体室）等灾难恢复辅助设施；培训教室、模拟演练室等灾难恢复培训设施。

c) 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。

d) 其他必要区域还包括集合区域、等候区域、人流物流通道等。

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，按基础设施规划和设计的要求进行实施。新建或选用灾难恢复中心的基础设施时，还包括：

a) 应符合有关国家标准的要求与发展规划，并遵循绿色、低碳、集约、高效的原则；

b) 应符合灾难恢复目标的要求，具备开展灾难恢复工作所需的通信、电力、地质气象等资源条件，以及方便灾难恢复人员和设备到达的交通条件；

c) 在灾难恢复中心基础设施建设中，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项目对应工程资质和数据中心建设经验的施工承包单位、造价咨询单位和施工监理单位等完成建设。

7.2.3 数据备份容灾系统的建设要求

数据备份容灾系统应本着数据的一致性以及业务持续性的原则进行建设，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，灾难恢复系统建设中还宜关注不同生产系统在灾难恢复中心备份数据的安全性。

7.2.4 备用数据处理系统的建设要求

为满足组织业务持续性运行的建设要求，灾难恢复中心的备用数据处理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，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，以确保备用系统的有效性和可操作性。

7.2.5 备用网络系统的建设要求

灾难恢复中心的备用网络系统包括灾难恢复中心内部网络、生产中心和灾难恢复中心间的备份网络、灾难恢复中心与上级机构之间的网络等。网络由通信线路和网络设备组成。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宜注意对不同生产系统的安全隔离，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。

8 灾难恢复系统运行管理

8.1 灾难恢复预案制定及管理

8.1.1 预案制定原则

灾难恢复预案(以下简称“预案”)针对不同灾难场景进行设计和制定,灾难恢复的每个等级均需制定相应预案,并进行落实和管理。预案的制定应遵循以下原则:

a) 针对性:面向数据级、应用级、业务级等不同灾难恢复类别设计相应的预案;
b) 完整性:预案包含可能发生的灾难场景;
c) 易用性:预案采用易于理解的语言、流程图等形式,适合在紧急情况下使用;
d) 明确性:预案采用清晰的结构,对资源进行清楚的描述,有具体工作内容和步骤,每项工作有明确的责任人;
e) 有效性:预案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;
f) 兼容性:预案与网络安全、数据安全等应急预案有机结合。

8.1.2 预案制定过程

在灾难恢复预案制定原则的指导下,其制定过程应包括如下内容:

a) 起草:按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,结合组织其他相关的应急预案,撰写出灾难恢复预案的初稿;
b) 评审:组织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严格的评审;
c) 测试:预先制定测试计划,在计划中说明测试的案例,测试包含基本单元测试、关联测试和整体测试,测试过程有详细的记录,并形成测试报告;
d) 完善:根据评审和测试结果,纠正在初稿评审过程和测试中发现的问题和缺陷,形成预案的审批稿;
e) 审核和批准:由灾难恢复领导小组对审批稿进行审核和批准,确定为预案的执行稿;
f) 备案:向监管或主管部门提交预案信息。

8.1.3 预案内容

预案内容应包含但不限于以下内容:

a) 预案实施目标;
b) 预案实施所需资源;
c) 预案实施团队组成和职责分工;
d) 预案重要性级别;
e) 预案触发启动条件;
f) 预案关联业务清单和资产清单;
g) 预案切换资产依赖、关联和切换流程;
h) 预案关联部门、通知流程、通知内容;
i) 预案演练过程中的数据安全性防护措施;
j) 预案演练结束后的数据安全性防护措施;
k) 预案演练失败回退流程;

l) 预案技术方案和操作手册。

8.1.4 预案培训

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，应按以下要求组织灾难恢复预案培训：

a) 在灾难恢复规划初期，开展灾难恢复观念的宣传教育工作；
b) 预先对培训需求进行评估，包括培训频次和范围，开发和落实相应的培训教育课程，保证课程内容与预案要求相一致，事后保留培训的记录；
c) 组织灾难恢复预案教育培训后的监督考核，确保预案实施团队对预案内容的理解掌握。

8.1.5 预案变更

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

a) 业务变化、信息系统变更、人员变更等应在灾难恢复预案中及时变更；
b) 应对预案测试、演练和灾难发生后执行的效果进行评估，同时对预案进行相应的修订；
c) 灾难恢复预案定期评审和修订。

8.1.6 预案保存和分发

经过审核和批准的灾难恢复预案，应按以下原则进行保存和分发：

a) 预案由专人负责；
b) 预案具有多份拷贝，保存在不同的地点；
c) 预案分发给参与灾难恢复工作的所有人员；
d) 预案实施严格的版本管理，每次修订后所有拷贝统一更新；
e) 预案旧版本按有关规定销毁。

附录 F 给出了一种灾难恢复预案的框架示例。

8.2 灾难恢复系统运行维护

8.2.1 运行维护原则

灾难恢复系统运行维护宜遵循以下原则：

a) 安全性原则：灾难恢复系统的安全管理等级和要求与生产系统保持一致或低一级；
b) 关联性原则：灾难恢复系统运行维护体系与生产系统运行维护体系实现联动；
c) 制度化原则：灾难恢复系统运行维护管理制度化、流程化，提高运行维护管理质量、效率；
d) 可用性原则：灾难恢复系统运行维护管理通过全面测试和定期验证机制，确保灾难恢复资源可用性和有效性。

8.2.2 运行监控

运行监控原则上要求覆盖灾难恢复资源和过程，监控内容应包括但不限于以下内容：

a) 灾难恢复中心动力环境可用性；
b) 灾难恢复资源可用性；
c) 灾难恢复资源使用率；
d) 灾难恢复资源安全性；
e) 灾难恢复任务运行状态；
f) 业务、应用、软件、硬件间的关联关系；

g） 容灾环境关键配置、硬件资源的数据一致性；
h） 业务应用健康度。

8.2.3 系统巡检

8.2.3.1 巡检内容

要求定期开展灾难恢复系统巡检，并对巡检结果做诊断分析和改进。灾难恢复系统巡检过程应有详细记录，形成巡检报告，并对历史巡检结果进行比对分析。灾难恢复巡检内容应包含但不限于以下内容：

a） 灾难恢复中心动力环境可用性；
b） 灾难恢复资源可用性；
c） 灾难恢复资源使用率变化；
d） 灾难恢复资源变更记录；
e） 灾难恢复资源错误日志；
f） 灾难恢复资源安全性；
g） 灾难恢复任务运行状态；
h） 评估灾备系统韧性，发现薄弱点。

8.2.3.2 巡检频次

系统巡检频次可结合灾难恢复类别和等级来确定。

8.2.3.3 巡检报告

巡检报告要求应包括但不限于以下内容：

a） 巡检报告包含但不限于以下内容：巡检时间、巡检对象、巡检步骤、巡检脚本、巡检结果、巡检执行人员、巡检审核人员、巡检结论和建议等；
b） 巡检报告模板应定期评审、修订；
c） 巡检报告可采用纸质文档或电子文件方式保存。

8.2.4 灾难恢复演练

8.2.4.1 演练类型

灾难恢复演练类型应包括：

a） 桌面演练：参演人员以会议的形式，依据灾备预案对的演练情景而进行推演，确保相关人员掌握预案中所规定的职责和程序，提高指挥决策和协同配合能力；
b） 模拟演练：通过建立与生产中心相同或类似测试系统，采用测试数据，组织参演人员按照灾备预案进行演练，验证灾难恢复系统可用性；
c） 实战演练：在生产中心或灾备中心，组织参演人员按照灾备预案对真实的运行环境进行演练，验证了灾难恢复流程的合理性，灾难恢复预案和系统可用性。实战演练确保数据真实有效或回退到演练前的状态。

8.2.4.2 演练范围

灾难恢复演练范围包括：

a） 数据备份容灾系统；
b） 备用数据处理系统；

c) 备用网络系统；
d) 备用基础设施；
e) 专业技术支持能力；
f) 运行维护管理能力。

8.2.4.3 演练组织

演练组织内容应包含但不限于以下内容：
a) 确定演练类型、演练目标、演练范围、演练组织架构，制定演练计划、演练脚本等；
b) 演练前对演练人员进行灾难恢复预案和灾难恢复演练培训；
c) 组织并实施灾难恢复演练；
d) 对灾难恢复演练过程中的各项工作进行记录；
e) 总结灾难恢复演练情况，根据灾难恢复演练过程中发现的问题修订灾难恢复预案。

8.2.4.4 演练频次

每年应至少开展一次灾难恢复演练。

8.2.4.5 演练报告

演练报告应包括但不限于以下内容：演练目标、演练预案、演练组织架构、演练时间窗口、演练步骤、演练记录、演练结果、演练总结和建议。

8.2.4.6 演练培训

为了使相关人员了解灾难恢复演练目标、演练预案，熟悉灾难恢复演练步骤，应按以下要求组织灾难恢复演练培训：
a) 在灾难恢复运行维护初期，开展演练观念宣传教育工作；
b) 在灾难恢复演练前，对演练目标、演练预案等开展针对性培训；
c) 掌握灾难恢复演练步骤；
d) 组织灾难恢复演练教育培训后考核，确保演练实施相关人员对演练目标、演练预案、演练步骤理解掌握。

8.3 应急事件响应及灾难接管

8.3.1 应急事件响应

应急响应包括但不限于以下内容：
a) 采取必要控制措施，最大限度地保护运行系统和数据安全，抑制事态恶化，降低损失；
b) 评估灾难影响范围与程度，提出灾难恢复建议；
c) 结合灾难场景选择对应灾难恢复预案，确认启动灾难恢复预案；
d) 按灾难恢复预案执行应急灾难切换；
e) 应急灾难切换后验证业务和系统可用性；
f) 根据业务和系统可用性验证结果，决定结束或继续应急事件响应状态。

8.3.2 灾难恢复事件报告

灾难恢复事件报告要求应包括但不限于以下内容：
a) 针对灾难恢复事件，形成灾难恢复事件报告；

b） 灾难恢复事件报告包含但不限于以下内容：灾难类型、灾难原因，业务影响范围、业务影响时长、数据丢失时长、灾难恢复预案和整改意见；
c） 灾难恢复事件报告模板定期评审、修订；
d） 灾难恢复事件报告采用纸质文档或电子文件方式保存。

8.4 重建和回退

灾难恢复完成后，第一时间制定灾难后重建和回退方案，方案应包括但不限于以下内容：
a） 生产中心故障修复或重建，恢复生产中心运行正常；
b） 实施灾难恢复中心到生产中心的数据同步，保证生产中心和灾难恢复中心数据一致性；
c） 制定回切计划，采用真实演练方式，将业务从灾难恢复中心回切到生产中心；
d） 业务从灾难恢复中心回切到生产中心后，验证业务可用性；
e） 制定从灾难恢复中心回切到生产中心失败的应对措施。

8.5 灾难恢复审计

定期组织灾难恢复审计，应由内部审计部门或第三方审计机构组织审计，审计内容应包括但不限于以下内容：
a） 灾难恢复预案保存和分发记录；
b） 灾难恢复预案培训记录；
c） 灾难恢复预案报备记录；
d） 灾难恢复演练培训记录；
e） 灾难恢复演练报告归档记录；
f） 灾难恢复系统巡检报告归档记录；
g） 灾难恢复事件报告归档记录。
审计报告出具后，应对审计报告提出的改进意见进行及时答复。

9 测试评价方法

9.1 灾难恢复总体测试评价要求

信息系统灾难恢复工作中应按附录 A 中的要素和准则对不同灾难恢复能力等级的灾难恢复中心和灾难恢复系统的规划设计、建设实施、运行管理等各阶段进行测试评价，以确保灾难恢复目标的实现，保障数据的机密性、完整性、可用性，保障业务的连续性。

9.2 灾难恢复的组织机构设置测试评价方法

9.2.1 组织机构的设立

组织机构的设立包括：
a） 评价方法：
1） 访谈灾难恢复领导小组成员，检查是否结合其日常组织机构建立灾难恢复的组织机构，以及组织机构是否包括灾难恢复领导小组、灾难恢复管理小组、灾难恢复技术与执行小组和灾难恢复保障小组等；
2） 若聘请外部专家协助灾难恢复实施工作，则检查外部专家是否具有相关资质证明文件；若委托外部机构承担实施组以及日常运行组的部分或全部工作，则检查外部机构是否具有相关资质证明文件。

b) 预期结果：

1) 结合日常组织机构建立灾难恢复组织机构，设置灾难恢复领导小组、灾难恢复管理小组、灾难恢复技术与执行小组和灾难恢复保障小组等机构；

2) 存在聘请外部专家协助灾难恢复实施工作，或委托外部机构承担实施组以及日常运行组的部分或全部工作情况的，外部专家或外部机构具备相应的资质。

c) 结果判定：

上述预期结果均满足判定为符合，否则为不符合或部分符合。

9.2.2 组织机构的职责

组织机构的职责包括：

a) 评价方法：

1) 访谈灾难恢复领导小组成员，检查灾难恢复的各组织机构是否明确了人员组成和职责；

2) 访谈灾难恢复领导小组成员，检查灾难恢复领导小组组长是否由组织最高管理层成员担任，及其职责是否为领导和决策信息系统灾难恢复的重大事宜；

3) 访谈灾难恢复领导小组成员，检查灾难恢复管理小组是否由组织的业务、技术、后勤等相关部门负责人组成，及其职责是否为管理和协调信息系统灾难恢复工作；

4) 访谈灾难恢复领导小组成员，检查灾难恢复技术与执行小组是否由灾难恢复中心专业技术人员、运行维护人员和服务供应商组成，及其职责是否为具体实施工作；

5) 访谈灾难恢复领导小组成员，检查灾难恢复保障小组是否由组织的人力资源、后勤保障人员组成，及其职责是否为保障灾难恢复工作所需要的资源供应、灾难抢修及灾难发生场所的安全。

b) 预期结果：

1) 灾难恢复的各组织机构明确了人员组成和职责；

2) 灾难恢复领导小组组长由组织最高管理层成员担任，其职责为领导和决策信息系统灾难恢复的重大事宜；

3) 灾难恢复管理小组由组织的业务、技术、后勤等相关部门负责人组成，及其职责为管理和协调信息系统灾难恢复工作；

4) 灾难恢复技术与执行小组由灾难恢复中心专业技术人员、运行维护人员和服务供应商组成，其职责为具体实施工作；

5) 灾难恢复保障小组由组织的人力资源、后勤保障人员组成，其职责为保障灾难恢复工作所需要的资源供应、灾难抢修及灾难发生场所的安全。

c) 结果判定：

上述预期结果均满足判定为符合，否则为不符合或部分符合。

9.3 灾难恢复规划设计测试评价方法

9.3.1 灾难恢复需求的确定

9.3.1.1 风险分析

风险分析包括：

a) 评价方法：

访谈灾难恢复管理小组成员，并查看灾难恢复设计方案或风险分析报告，检查风险分析内容是否包括识别信息系统的资产及其价值、面临的威胁和存在的脆弱性，识别现有的风险防范和控制措施等，以及检查是否按 GB/T 20984—2022 开展风险评估分析活动。

b） 预期结果：

结合组织业务情况，按 GB/T 20984—2022 开展了风险分析活动，风险分析内容包括识别信息系统的资产及其价值、面临的威胁和存在的脆弱性，识别现有的风险防范和控制措施等。

c） 结果判定：

上述预期结果均满足判定为符合，否则为不符合或部分符合。

9.3.1.2 业务影响分析

业务影响分析包括：

a） 评价方法：

1） 访谈灾难恢复管理小组成员，并查看灾难恢复设计方案，检查是否识别组织各项业务功能及各项业务功能之间的相关性，是否确定支持各项业务功能的相应信息系统资源及其他资源，是否明确相关的保密性、完整性、可用性（包括时间敏感性）要求；

2） 查看灾难恢复设计方案，检查是否采用定量和/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。

b） 预期结果：

1） 充分识别了组织各项业务功能及各项业务功能之间的相关性，确定支持各项业务功能的相应信息系统资源及其他资源，明确相关的保密性、完整性、可用性（包括时间敏感性）要求；

2） 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了评估。

c） 结果判定：

上述预期结果均满足判定为符合，否则为不符合或部分符合。

9.3.1.3 确定灾难恢复的需求

确定灾难恢复的需求包括：

a） 评价方法：

访谈灾难恢复管理小组成员，并查看灾难恢复设计方案，检查是否综合风险分析和业务影响分析的结果确定信息系统的恢复优先级，是否确定灾难恢复目标。

b） 预期结果：

综合风险分析和业务影响分析的结果，确定信息系统的恢复优先级和灾难恢复目标（包括 RTO、RPO 指标）。

c） 结果判定：

上述预期结果均满足判定为符合，否则为不符合或部分符合。

9.3.2 灾难恢复策略制定

9.3.2.1 灾难恢复策略要求

灾难恢复策略要求包括：

a） 评价方法：

访谈灾难恢复管理小组成员，并查看灾难恢复设计方案，检查组织是否按照成本风险平衡原则制定业务功能的灾难恢复策略，能否实现不同的业务功能采用不同的灾难恢复策略。检查灾难恢复策略的要素是否包括 GB/T 20984—2022 方法和附录 C 中进行信息系统的分类分级、确定灾难恢复能力等级、确定灾难恢复资源要素的获取方式、确定灾难恢复系统的安全要求、确定灾难恢复中的兼容性要求等。

b) 预期结果：

结合组织灾难恢复目标，按照成本风险平衡原则制定业务功能的灾难恢复策略，能够实现不同的业务功能采用不同的灾难恢复策略。灾难恢复策略要素包括 GB/T 20984—2022 方法和附录 C 中进行信息系统的分类分级、确定灾难恢复能力等级、确定灾难恢复资源要素的获取方式、确定灾难恢复系统的安全要求、确定灾难恢复中的兼容性要求等。

c) 结果判定：

上述预期结果均满足判定为符合，否则为不符合或部分符合。

9.3.2.2 灾难恢复类别的规划

灾难恢复类别的规划包括：

a) 评价方法：

访谈灾难恢复管理小组成员，并查看灾难恢复设计方案，检查是否根据提供服务重要性、时效性要求和建设规划确定灾难恢复的类别，检查服务类别是否为数据级、应用级或业务级中的一项或多项。

b) 预期结果：

结合组织灾难恢复目标，根据提供服务重要性、时效性要求和建设规划明确了灾难恢复的类别，且类别为数据级、应用级或业务级中的一项或多项。

c) 结果判定：

上述预期结果均满足判定为符合，否则为不符合或部分符合。

9.3.2.3 灾难恢复布局规划

灾难恢复布局规划包括：

a) 评价方法：

访谈灾难恢复管理小组成员，并查看灾难恢复设计方案，检查组织是否根据成本风险平衡原则以及管理要求明确灾难恢复布局模式，以及模式是否为一主一备、一主多备、互为备份、多主一备和混合方式中的一种或多种。

b) 预期结果：

结合组织灾难恢复目标，根据成本风险平衡原则以及管理要求明确了灾难恢复布局模式，且布局模式为一主一备、一主多备、互为备份、多主一备和混合方式中的一种或多种。

c) 结果判定：

上述预期结果均满足判定为符合，否则为不符合或部分符合。

9.3.2.4 灾难恢复资源要素

灾难恢复资源要素包括：

a) 评价方法：

访谈灾难恢复管理小组成员，查看灾难恢复设计方案或灾难恢复预案，并核查灾难恢复相关资源要素，检查灾难恢复各能力等级所需的资源要素是否全面。

b) 预期结果：

灾难恢复各能力等级所需的资源要素全面，包括数据备份容灾系统、备用数据处理系统、备用网络系统、备用基础设施、专业技术支持能力、运行维护管理能力、灾难恢复预案等。

c) 结果判定：

上述预期结果均满足判定为符合，否则为不符合或部分符合。

9.3.2.5 采用云计算技术的灾难恢复资源要素

采用云计算技术的灾难恢复资源要素包括：

a) 评价方法：
   1) 访谈灾难恢复管理小组成员，了解是否采用了云计算技术；
   2) 访谈灾难恢复管理小组成员，查看灾难恢复设计方案，并核查灾难恢复相关资源要素，检查采用云计算技术中灾难恢复各能力等级所需的资源要素是否全面，以及是否考虑了云上、云下、跨区、跨云场景下的适用性和兼容性需求。
b) 预期结果：
   1) 组织使用了云灾备服务模式；
   2) 在满足灾难恢复资源要素基础上，充分考虑了云上、云下、跨区、跨云场景下的适用性和兼容性需求。
c) 结果判定：
   上述预期结果均满足判定为符合，1)项不满足判定为不适用，否则为不符合或部分符合。

9.3.3 灾难恢复技术方案设计

9.3.3.1 灾难恢复资源的要求与获取方式

9.3.3.1.1 数据备份容灾系统

数据备份容灾系统包括：

a) 评价方法：
   1) 访谈灾难恢复技术与执行小组成员，查看灾难恢复技术方案，检查数据备份容灾系统是否确定灾难恢复与数据备份的范围、数据备份的时间间隔、数据备份容灾的技术和介质、数据备份容灾系统的安全要求等内容，检查灾难恢复技术方案中是否包含数据一致性和完整性验证相关说明；
   2) 若数据备份容灾系统是租用其他机构的系统或云厂商提供的服务获取，访谈灾难恢复技术与执行小组成员，查看其他机构提供的灾难恢复技术方案和合同，检查数据备份容灾系统确定内容是否全面。
b) 预期结果：
   1) 组织按照成本风险平衡原则，明确了数据备份容灾系统的灾难恢复与数据备份范围、数据备份时间间隔、数据备份容灾技术和介质、数据备份容灾系统安全要求等。
   2) 若数据备份容灾系统是租用其他机构的系统或云厂商提供的服务获取，数据备份容灾系统满足了灾难恢复目标。数据备份容灾系统租赁或服务合同处于有效性，合同中明确了灾难恢复与数据备份的范围、数据备份的时间间隔、数据备份容灾的技术和介质、数据备份容灾系统的安全要求等。
   3) 灾难恢复技术方案中数据备份容灾系统相关文档内容完整，包括了数据容灾系统要求和获取方式，阐述了数据一致性和完整性验证要求和方法。
c) 结果判定：
   上述预期结果均满足判定为符合，否则为不符合或部分符合。

9.3.3.1.2 备用数据处理系统

备用数据处理系统包括：

a) 评价方法：

1） 访谈灾难恢复技术与执行小组成员，查看灾难恢复技术方案，检查备用数据处理系统是否按照成本风险平衡原则，确定了数据处理能力、与主系统的兼容性要求、平时处于就绪还是运行状态、布局规划等内容；

2） 访谈灾难恢复技术与执行小组成员，查看灾难恢复技术方案，检查备用数据处理系统采用何种获取方式，检查技术方案中是否包含系统运行环境和软件版本兼容性相关说明。

b） 预期结果：

1） 组织明确了备用数据处理系统的数据处理能力、与主系统的兼容性要求、平时处于就绪还是运行状态、布局规划等内容；

2） 组织采用事先与厂商签订紧急供货协议、事先购买所需的设备并存放在灾难恢复中心或安全的设备仓库、租用商业化灾难恢复中心或签有协议的机构已有的兼容设备三种方法之一获取备用数据处理系统；

3） 灾难恢复技术方案中备用数据处理系统相关文档内容完整，包括了资源要求和获取方式，且内容符合相关要求，阐述了备用数据处理系统与生产环境的数据处理系统应在系统运行环境和软件版本等兼容性相关要求和方法。

c） 结果判定：

上述预期结果均满足判定为符合，否则为不符合或部分符合。

9.3.3.1.3 备用网络系统

备用网络系统包括：

a） 评价方法：

1） 访谈灾难恢复技术与执行小组成员，查看灾难恢复技术方案文档，检查灾难恢复资源需求确定过程中是否根据灾难恢复目标确定备用网络系统要求，以及备用网络系统要求是否满足备用网络系统的建设要求；

2） 查看灾难恢复技术方案文档，检查是否通过提前签订紧急供货协议或购买所需的设备等方式获取备用网络系统；

3） 查看灾难恢复技术方案文档，检查备用网络系统是否使用自建的数据通信线路或租用公用数据通信线路。

b） 预期结果：

1） 组织根据灾难恢复资源需求，明确了备用网络系统资源要求和获取方式；

2） 灾难恢复技术方案中备用网络系统相关文档内容完整，包括了备用网络系统资源要求和获取方式，且内容符合相关要求。

c） 结果判定：

上述预期结果均满足判定为符合，否则为不符合或部分符合。

9.3.3.1.4 备用基础设施

备用基础设施包括：

a） 评价方法：

1） 访谈灾难恢复技术与执行小组成员，查看灾难恢复技术方案文档，检查灾难恢复资源需求确定过程中是否根据灾难恢复目标确定备用基础设施，检查备用基础设施要求是否包括与主中心的距离、场地、环境、运行维护和管理要求等；

2） 访谈灾难恢复技术与执行小组成员，查看灾难恢复技术方案文档，检查是否通过由自有、共建或租用等方式获取备用基础设施。

b） 预期结果：

1） 组织根据灾难恢复资源需求明确了备用基础设施资源要求和获取方式，且备用基础设施要求，包括与主中心的距离、场地、环境、运行维护和管理要求等；
2） 灾难恢复技术方案中备用网络系统相关文档内容完整，包括了备用基础设施要求和获取方式，且内容符合相关要求。

c） 结果判定：
上述预期结果均满足判定为符合，否则为不符合或部分符合。

9.3.3.1.5 专业技术支持能力

专业技术支持能力包括：

a） 评价方法：
1） 访谈灾难恢复技术与执行小组成员，查看灾难恢复技术方案文档，检查灾难恢复资源需求确定过程中是否根据灾难恢复目标确定灾难恢复中心在软件、硬件和网络等方面的技术支持能力要求和获取方式；
2） 访谈灾难恢复技术与执行小组成员，查看灾难恢复技术方案文档，检查是否制定专业技术支持的组织架构、各类技术人员的数量和素质、管理制度等要求。

b） 预期结果：
1） 组织根据灾难恢复资源需求，明确了专业技术支持要求和获取方式；
2） 灾难恢复技术方案中专业技术支持要求包括组织架构、各类技术人员的数量和素质、管理制度等内容。

c） 结果判定：
上述预期结果均满足判定为符合，否则为不符合或部分符合。

9.3.3.1.6 运行维护管理能力

运行维护管理能力包括：

a） 评价方法：
1） 访谈灾难恢复技术与执行小组成员，查看灾难恢复技术方案文档，检查灾难恢复资源需求确定过程中是否根据灾难恢复目标确定运行维护管理能力要求和获取方式；
2） 访谈灾难恢复技术与执行小组成员，查看灾难恢复技术方案文档，检查是否制定运行维护管理的组织架构、各类技术人员的数量和素质、管理制度等。

b） 预期结果：
1） 组织根据灾难恢复资源需求，明确了运行维护管理能力要求和获取方式；
2） 灾难恢复技术方案中运行维护管理能力要求包括组织架构、各类技术人员的数量和素质、管理制度等内容。

c） 结果判定：
上述预期结果均满足判定为符合，否则为不符合或部分符合。

9.3.3.1.7 灾难恢复预案

灾难恢复预案包括：

a） 评价方法：
1） 访谈灾难恢复技术与执行小组成员，检查是否制定了灾难恢复预案；
2） 查看灾难恢复技术方案文档，检查是否明确了灾难恢复预案的整体、制定过程、教育、培训、演练和管理要求，及预案的编制是否符合灾难恢复原制定的要求。

b） 预期结果：

组织制定了灾难恢复预案，预案内容完整，包括整体、制定过程、教育、培训和演练、管理要求等内容。

c) 结果判定：

上述预期结果均满足判定为符合，否则为不符合或部分符合。

9.3.3.1.8 云灾难恢复服务

云灾难恢复服务包括：

a) 评价方法：

1) 访谈灾难恢复技术与执行小组成员，了解是否使用云灾备服务模式；

2) 访谈灾难恢复技术与执行小组成员，查看灾难恢复技术方案文档，检查组织是否根据灾难恢复目标，确认服务要求。检查服务要求是否包括数据级灾难恢复能力、应用级灾难恢复的接管能力、系统架构和兼容性能力要求、独立于生产云平台的场外云平台系统等；

3) 访谈灾难恢复技术与执行小组成员，查看灾难恢复技术方案文档，检查是否规定了采用组织所有或运行、租用由外部机构提供的灾难恢复服务中的方法获取服务。

b) 预期结果：

1) 组织使用了云灾备服务模式；

2) 组织制定了云灾难恢复服务要求，内容包括：数据级灾难恢复能力、应用级灾难恢复的接管能力、系统架构和兼容性能力要求、独立于生产云平台的场外云平台系统；

3) 规定了云灾难恢复服务获取方式，采用由组织所有或运行、租用由外部机构提供的灾难恢复服务。

c) 结果判定：

上述预期结果均满足判定为符合，1)项不满足判定为不适用，否则为不符合或部分符合。

9.3.3.2 灾难恢复系统的安全要求

灾难恢复系统的安全要求包括：

a) 评价方法：

访谈灾难恢复管理小组成员，查看灾难恢复技术方案文档，检查灾难恢复系统的网络安全要求是否不低于其承载的信息系统的最高级别。

b) 预期结果：

灾难恢复系统的网络安全要求不低于其承载的信息系统的最高级别。

c) 结果判定：

上述预期结果均满足判定为符合，否则为不符合或部分符合。

9.3.4 灾难恢复中心选址和等级

9.3.4.1 灾难恢复中心的选址

灾难恢复中心的选址包括：

a) 评价方法：

1) 访谈灾难恢复管理小组成员，查看灾难恢复技术方案文档，检查灾难恢复中心的选址是否符合 GB 50174—2017 中 4.1 的规定，及是否充分考虑同城灾难恢复中心、异地灾难恢复中心的与生产中心间安全距离、地址条件差异等要求，重要的国家战略层面的灾难恢复中心的选址是否考虑防侦测和攻击等因素的要求；

2) 访谈灾难恢复管理小组成员，查看灾难恢复技术方案文档，检查组织是否遵守 GB 50174—

2017 附录 A 规定的各等级技术要求建设灾难恢复中心基础设施。

b） 预期结果：

1） 灾难恢复中心的选址符合相关国标及相关技术要求；

2） 灾难恢复中心基础设施符合 GB 50174—2017 附录 A 规定的各等级技术建设规定。

c） 结果判定：

上述预期结果均满足判定为符合，否则为不符合或部分符合。

9.3.4.2 灾难恢复中心基础设施的等级

灾难恢复中心基础设施的等级包括：

a） 评价方法：

1） 访谈灾难恢复管理小组成员，查看灾难恢复技术方案文档，检查组织是否遵守 GB 50174—2017 附录 A 规定的各等级技术要求建设灾难恢复中心基础设施；

2） 访谈灾难恢复管理小组成员，查看灾难恢复技术方案文档，检查灾难恢复中心基础设施的等级是否与生产中心的等级保持一致或低一等级。

b） 预期结果：

1） 灾难恢复中心基础设施符合 GB 50174—2017 附录 A 规定的各等级技术建设规定；

2） 灾难恢复中心基础设施的等级与生产中心的等级保持一致或低一等级。

c） 结果判定：

上述预期结果均满足判定为符合，否则为不符合或部分符合。

9.3.5 灾难恢复技术方案的验证和确认

灾难恢复技术方案的验证和确认包括：

a） 评价方法：

1） 访谈灾难恢复管理小组成员，检查组织相关部门是否对技术方案进行确认和验证；

2） 查看灾难恢复技术方案文档评审和验证证明材料，确认认证证明材料中是否包含数据完整性和一致性验证、数据备份与恢复能力验证、信息系统切换与回切能力验证、网络系统切换与回切能力验证、系统安全性验证等内容。

b） 预期结果：

1） 灾难恢复技术方案经组织评审并开展了验证工作；

2） 灾难恢复技术方案验证包括：数据完整性和一致性验证、数据备份与恢复能力验证、信息系统切换与回切能力验证、网络系统切换与回切能力验证、系统安全性验证，且相关记录文档齐全。

c） 结果判定：

上述预期结果均满足判定为符合，否则为不符合或部分符合。

9.4 灾难恢复系统和中心建设测试评价方法

9.4.1 灾难恢复系统建设

9.4.1.1 实施方案制定

实施方案制定包括：

a） 评价方法：

1） 访谈灾难恢复技术与执行小组，检查是否根据灾难恢复的需求和规划设计，制定灾难恢复系统实施方案，并形成规范化文档；

2） 查看灾难恢复系统实施方案，检查实施方案中是否涵盖建设目标和建设内容、技术实现方案、系统和组件安全功能和性能要求、系统和组件部署、安全控制策略和配置、配套的安全管理建设内容、工程实施计划、项目投资概算等内容。

b） 预期结果：

1） 根据灾难恢复的需求和规划设计，制定灾难恢复系统实施方案，并形成规范化文档；

2） 灾难恢复系统实施方案中包括建设目标和建设内容、技术实现方案、系统和组件安全功能和性能要求、系统和组件部署、安全控制策略和配置、配套的安全管理建设内容、工程实施计划、项目投资概算等内容。

c） 结果判定：

上述预期结果均满足判定为符合，否则为不符合或部分符合。

9.4.1.2 系统部署和配置

系统部署和配置包括：

a） 评价方法：

1） 访谈灾难恢复技术与执行小组人员，查看灾难恢复系统实施方案，检查灾难恢复系统建设过程中是否进行部署准备、系统部署和系统配置工作；

2） 检查是否制定质量控制方案，并评价其是否具有指导意义；

3） 检查灾难恢复系统相关软硬件产品是否具备测试报告，并评估报告的真实性、有效性；

4） 现场勘察灾难恢复系统，检查是否按照灾难恢复系统实施方案正确地将相关产品或者模块部署到实际的应用环境中，以及检查系统实施的各个环节是否遵照质量控制方案的要求，实现质量控制目标；

5） 查看灾难恢复应用系统的软硬件配置，以及生产中心和灾难恢复中心的网络配置，检查相关配置是否正确，以及检查灾难恢复系统和备用网络系统工作是否正常。

b） 预期结果：

1） 灾难恢复系统建设过程进行了部署准备、系统部署和系统配置等工作；

2） 制定了质量控制方案，并具有指导意义；

3） 灾难恢复系统相关软硬件产品具备测试报告，并真实、有效；

4） 灾难恢复系统按照实施方案正确地将相关产品或者模块部署到实际的应用环境中，并且检查系统实施的各个环节遵照质量控制方案的要求，实现了质量控制目标；

5） 灾难恢复应用系统的软硬件配置，以及生产中心和灾难恢复中心的网络配置正确，以及灾难恢复系统和备用网络系统工作正常。

c） 结果判定：

上述预期结果均满足判定为符合，否则为不符合或部分符合。

9.4.1.3 系统测试

系统测试包括：

a） 评价方法：

1） 结合灾难恢复的需求和规划设计文档，查看系统测试文档，检查是否对规划设计的功能、性能和安全性进行测试；

2） 查看系统测试文档，检查是否对承载灾难恢复应用系统的软硬件、生产中心和灾难恢复中心间的网络、灾难恢复系统的安全性等方面的测试。

b） 预期结果：

1） 依照灾难恢复的需求和规划设计文档，对灾难恢复系统规划设计的功能、性能和安全性进

行测试；

2） 测试内容包括承载灾难恢复应用系统的软硬件、生产中心和灾难恢复中心间的网络、灾难恢复系统的安全性等。

c） 结果判定：

上述预期结果均满足判定为符合，否则为不符合或部分符合。

9.4.1.4 验收与交付

验收与交付包括：

a） 评价方法：

1） 访谈灾难恢复技术与执行小组成员，查看验收方案、验收报告等文档，检查是否开展了验收准备、组织验收、系统交付、培训等工作；

2） 访谈灾难恢复技术与执行小组成员是否设计验收方案，并查看其是否满足设计方案要求；

3） 访谈灾难恢复技术与执行小组成员是否依照验收方案进行验收测试，并查看验收测试文档，检查其是否结合详细设计方案，对功能、性能和安全性等进行测试；

4） 访谈灾难恢复技术与执行小组成员是否在测试完成后形成验收报告，并查看验收报告，检查其是否明确给出验收意见和验收结论，对于提出修改建议的，检查整改和重新收情况；

5） 访谈灾难恢复技术与执行小组成员是否进行系统交付，并查看交付记录，检查是否交付验收报告、交付清单、管理员手册、用户手册、安全概述以及系统配置说明书、各种操作规程和管理制度等；

6） 访谈灾难恢复技术与执行小组成员是否建立技术支持组织和是否进行培训，查看技术支持记录和培训记录，检查是否建立技术支持组织及其能力，以及是否开展培训及其频次等。

b） 预期结果：

1） 验收与交付过程开展了验收准备、组织验收、系统交付、培训等工作；

2） 设计验收方案，并满足设计方案要求；

3） 依照验收方案进行验收测试，验收测试文档包括详细设计方案，并对功能、性能和安全性等进行测试；

4） 测试完成后形成验收报告，报告明确给出验收意见和验收结论，对于提出修改建议的，进行整改，并重新验收；

5） 系统交付了验收报告、交付清单、管理员手册、用户手册、安全概述以及系统配置说明书、各种操作规程和管理制度等；

6） 建立技术支持组织，并定期开展培训。

c） 结果判定：

上述预期结果均满足判定为符合，否则为不符合或部分符合。

9.4.2 灾难恢复中心建设

9.4.2.1 备用基础设施建设

备用基础设置建设包括：

a） 评价方法：

1） 查看建设实施文档，现场查看备用基础设施建设情况，检查是否包含工作设施（包括信息系统工作设施和保障系统工作设施）、辅助设施、生活配套设施，以及其他必要的区域，及其建设情况是否符合 GB 50174—2017 中 4.2 的规定；

2） 对于新建或选用灾难恢复中心的基础设施的，查看建设实施文档，现场查看备用基础设施建设情况，检查是否按照符合有关国家标准的要求与发展规划建设，检查是否具备开展灾难恢复工作所需的通信、电力、地质气象等资源条件，以及是否方便灾难恢复人员和设备到达的交通条件；

3） 对于新建或选用灾难恢复中心的基础设施的，查看建设实施文档，现场查看备用基础设施建设情况，检查是否成立建设管理团队，查看施工承包、造价咨询和施工监理等单位的工程资质，以及相关项目经验案例，检查其是否具有项目对应的工程资质和数据中心建设经验。

b） 预期结果：

1） 备用基础设施建设内容包含工作设施（包括信息系统工作设施和保障系统工作设施）、辅助设施、生活配套设施，以及其他必要的区域，相关设施建设情况符合 GB 50174—2017 中 4.2 的规定；

2） 新建或选用灾难恢复中心的基础设施的，按照符合有关国家标准的要求与发展规划建设，并具备开展灾难恢复工作所需的通信、电力、地质气象等资源条件，以及方便灾难恢复人员和设备到达的交通条件；

3） 新建或选用灾难恢复中心的基础设施的，成立建设管理团队，施工承包、造价咨询和施工监理等单位的具有工程资质，以及相关项目经验。

c） 结果判定：

上述预期结果均满足判定为符合，否则为不符合或部分符合。

9.4.2.2 数据备份容灾系统建设

数据备份容灾系统建设包括：

a） 评价方法：

1） 查看灾难恢复中心与生产中心数据一致性和完整性验证文档，分别查看恢复中心与生产中心数据，检查其一致性和完整性是否有效；

2） 对于多个生产中心共享的灾难恢复中心的，查看建设实施文档，现场查看数据备份容灾系统建设情况，检查对不同生产系统在灾难恢复中心的备份数据是否进行安全性设计和实现，并测试验证其安全性是否有效。

b） 预期结果：

1） 灾难恢复中心与生产中心的数据具备一致性和完整性，在系统实施过程中，进行了必要的数据一致性和完整性验证；

2） 对于多个生产中心共享的灾难恢复中心的，不同生产系统在灾难恢复中心的备份数据充分考虑了安全性，并且安全性有效。

c） 结果判定：

上述预期结果均满足判定为符合，否则为不符合或部分符合。

9.4.2.3 备用数据处理系统建设

备用数据处理系统建设包括：

a） 评价方法：

1） 现场查看备用数据处理系统，检查其系统运行环境和软件版本等方面是否与生产系统完全兼容；

2） 查看备用数据处理系统运行能力的测试验证文档，检查是否开展测试验证，及其有效性。

b） 预期结果：

1） 备用数据处理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；
2） 备用数据处理系统建设时，进行了运行能力的测试验证，且测试验证有效。

c） 结果判定：
上述预期结果均满足判定为符合，否则为不符合或部分符合。

9.4.2.4 备用网络系统建设

备用网络系统建设包括：

a） 评价方法：
对于多个生产中心共享的灾难恢复中心，查看备用网络系统和网络设备的安全隔离策略和配置，并测试验证其有效性，检查是否对不同生产系统进行安全隔离，以及安全隔离措施是否有效。

b） 预期结果：
对于多个生产中心共享的灾难恢复中心，备用网络系统对不同生产系统进行安全隔离，能够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。

c） 结果判定：
上述预期结果均满足判定为符合，否则为不符合或部分符合。

9.5 灾难恢复系统的安全建设测试评价方法

9.5.1 网络安全等级保护

网络安全等级保护包括：

a） 评价方法：
访谈灾难恢复领导小组负责人，查看定级、备案、测评、商用密码应用安全性评估报告等证明材料，检查灾难恢复系统是否按 GB/T 22239—2019 和 GB/T 39786—2021 描述的网络安全等级保护级别要求进行安全建设。

b） 预期结果：
灾难恢复系统按 GB/T 22239—2019 描述的网络安全等级保护级别要求进行安全建设。

c） 结果判定：
上述预期结果均满足判定为符合，否则为不符合或部分符合。

9.5.2 安全管理制度

安全管理制度包括：

a） 评价方法：
1） 访谈灾难恢复管理小组负责编制和灾难恢复技术与执行小组的专业技术人员，了解计划制定的过程、目标设定以及实施策略。查看灾难恢复安全保护计划文档，检查计划是否包含管理体系、技术体系、运行维护体系和保障体系的详细规划。此外，检查计划文档是否经过审批并已发送至相关人员。
2） 访谈灾难恢复保障小组人力资源及后勤保障负责人，了解资源保障的策略和执行情况。并查看相关的预算分配记录、人员培训记录、装备采购和维护记录等，以检查机构、人员、经费和装备等资源的保障情况。
3） 访谈灾难恢复管理小组负责人，询问修订和更新过程中考虑的因素和实施的改进。通过查看灾难恢复系统安全策略文档的修订记录，包括修订日期、修订内容和审批过程，检查安全策略是否至少每年修订一次，或在发生重大变化时是否进行更新。

4） 访谈灾难恢复技术与执行小组的团队成员，了解如何识别和应对新的安全风险和威胁。通过审查风险评估报告和策略调整记录，验证管理制度和安全策略是否根据安全风险和威胁的变化进行了相应的调整。

b） 预期结果：

1） 组织拥有一套全面的灾难恢复安全保护计划，该计划详细规划了管理体系、技术体系、运行维护体系和保障体系。计划文档应经过适当审批并已向相关人员分发，确保所有相关方都了解灾难恢复的目标和策略。

2） 组织能够提供充分的资源保障，包括但不限于机构、人员、经费和装备，以支持灾难恢复的安全保护工作。预算分配、人员培训、装备采购和维护等方面的记录完整，反映出组织已经采取了适当的措施来确保资源的充分性。

3） 灾难恢复系统的安全策略文档至少每年进行一次修订，或在系统或环境发生重大变化时进行及时更新。修订记录包括修订日期、修订内容和审批过程，显示出组织对于维护当前和有效的安全策略的承诺。

4） 组织能够有效地识别和应对新的安全风险和威胁。风险评估报告和策略调整记录表明，管理制度和安全策略根据安全风险和威胁的变化进行了相应的调整，确保灾难恢复措施的效果与时俱进。

c） 结果判定：

上述预期结果均满足判定为符合，否则为不符合或部分符合。

9.5.3 安全管理架构

安全管理架构包括：

a） 评价方法：

1） 访谈灾难恢复管理小组的负责人，查看组织结构图和相关职责描述文档，检查是否在灾难恢复组织机构中明确指定了负责灾难恢复系统安全保护工作的专职管理人员；

2） 访谈灾难恢复保障小组人力资源的人员，查看考核政策、监督流程文档及问责制度实施记录，检查是否建立了针对灾难恢复系统安全保护工作的考核及监督问责机制；

3） 访谈灾难恢复安全管理机构人员，查看决策体系的文档，检查灾难恢复安全管理机构人员是否被纳入灾难恢复的组织机构决策体系中。

b） 预期结果：

1） 组织已明确指定了专职管理灾难恢复系统安全保护工作的负责人，并在组织结构中给予了明确的职责和权力。存在针对灾难恢复系统安全保护工作的考核及监督问责机制，且有记录证明该机制被有效实施。

2） 灾难恢复安全管理机构人员被有效纳入组织的决策体系中，能够在决策过程中发挥作用，确保灾难恢复计划的安全性得到充分考虑和实施。

c） 结果判定：

上述预期结果均满足判定为符合，否则为不符合或部分符合。

9.5.4 安全管理人员

安全管理人员包括：

a） 评价方法：

1） 访谈灾难恢复保障小组负责人力资源考核人员，检查是否对灾难恢复系统关键岗位的人员进行了安全技能考核；

2） 访谈灾难恢复保障小组负责人力资源考核人员及参加培训的人员，查看灾难恢复系统系

统安全教育培训制度、培训记录等文件，检查是否建立了灾难恢复系统的安全教育培训制度，并定期开展安全教育培训和技能考核；

3） 访谈灾难恢复保障小组负责人力资源考核相关人员，查看人员变动记录等文件，检查当灾难恢复系统安全管理机构的负责人和关键岗位人员的身份、安全背景等发生变化时，组织是否按照相关要求进行了重新核查；

4） 访谈灾难恢复保障小组和相关从业人员，查看安全保密协议的副本，检查是否明确了从业人员的安全保密职责和义务，以及相关人员是否签订了安全保密协议。

b） 预期结果：

1） 灾难恢复系统关键岗位的人员均通过了安全技能考核，且考核记录完整；

2） 组织已建立并有效执行灾难恢复系统的安全教育培训制度，定期开展培训和考核，提升人员的安全意识和技能水平；

3） 针对安全管理机构负责人和关键岗位人员变动，组织及时进行了身份和安全背景的核查，确保所有人员均符合安全要求；

4） 所有从业人员都清楚自己的安全保密职责和义务，并签订了安全保密协议，加强了安全意识和保密意识。

c） 结果判定：

上述预期结果均满足判定为符合，否则为不符合或部分符合。

9.5.5 安全通信网络

9.5.5.1 网络架构

网络架构包括：

a） 评价方法：

访谈灾难恢复技术与执行小组的技术人员，查看网络架构设计相关文档，检查灾难恢复系统的通信线路是否实现了“一主多备”，以及是否为多网络运营商多路由保护。查看网络关键节点和重要设施的配置和网络拓扑图，检查网络关键节点和重要设施是否为“双节点”冗余备份。

b） 预期结果：

灾难恢复系统的通信线路应具备“一主多备”的配置，且涵盖多个运营商，确保在主线路发生故障时能够无缝切换至备用线路，保障通信不中断。网络的关键节点和重要设施采用了“双节点”冗余备份策略，以提高系统的可靠性和容错能力。

c） 结果判定：

上述预期结果均满足判定为符合，否则为不符合或部分符合。

9.5.5.2 互联安全

互联安全包括：

a） 评价方法：

1） 访谈灾难恢复管理小组负责人，查看互联安全相关文档，检查是否建立或完善了灾难恢复系统与不同业务系统之间、不同区域的系统之间、不同运营者运营的系统之间的安全互联策略。

2） 访谈灾难恢复管理小组负责人，查看用户管理系统和访问控制策略相关文档和配置，检查同一用户在本地及异地灾难恢复系统中的用户身份和访问权限是否保持一致性。这可通过审查用户账户信息、权限分配记录和同步机制来完成。

3） 访谈灾难恢复管理小组技术人员，查看远程通信安全防护相关文档和配置，检查是否对不

同局域网远程通信的灾难恢复系统之间采取安全防护措施。

b) 预期结果：

1) 组织已建立或完善了灾难恢复系统与不同业务系统、不同区域系统、不同运营者系统之间的安全互联策略，确保所有连接都符合安全要求；

2) 同一用户在本地和异地灾难恢复系统中的用户身份和访问权限一致；

3) 针对不同局域网远程通信的灾难恢复系统之间实施了有效的安全防护措施，包括但不限于防火墙、加密设备、VPN 和网络入侵保护等。

c) 结果判定：

上述预期结果均满足判定为符合，否则为不符合或部分符合。

9.5.5.3 边界防护

边界防护包括：

a) 评价方法：

1) 访谈灾难恢复技术与执行小组技术人员，查看网络架构和安全边界防护相关文档和配置，检查灾难恢复系统在不同业务系统、区域系统和运营者系统之间的互操作、数据交换和信息流向是否进行了严格控制；

2) 访谈灾难恢复技术与执行小组技术人员，查看边界设备访问控制策略配置，检查灾难恢复系统跨边界的访问和数据流是否通过边界设备的受控接口进行通信。

b) 预期结果：

1) 灾难恢复系统在不同业务系统之间、不同区域的系统之间、不同运营者运营的系统之间的互操作、数据交换和信息流向进行了严格控制；

2) 灾难恢复系统跨边界的访问和数据流通过边界设备的受控接口进行通信。

c) 结果判定：

上述预期结果均满足判定为符合，否则为不符合或部分符合。

9.5.5.4 安全审计

安全审计包括：

a) 评价方法：

1) 访谈灾难恢复技术与执行小组负责审计管理的人员，查看审计策略相关文档和配置、审计日志记录等，检查是否对灾难恢复系统中数据备份、恢复、删除、迁移和系统配置变更等操作进行审计；

2) 访谈灾难恢复技术与执行小组人员，查看审计管理系统相关访问控制策略，检查是否只有相应权限的用户能够读取审计数据；

3) 访谈灾难恢复技术与执行小组负责审计日志管理的技术人员，查看审计管理系统配置和审计记录，检查相关日志数据的留存期是否不少于 6 个月。

b) 预期结果：

1) 灾难恢复系统的数据备份、恢复、删除、迁移和系统配置变更等操作均进行审计；

2) 审计数据通过有效的管理功能进行保护，且访问控制得当，确保只有授权用户能够访问审计数据；

3) 审计日志数据留存不少于 6 个月。

c) 结果判定：

上述预期结果均满足判定为符合，否则为不符合或部分符合。

9.5.6 安全计算环境

9.5.6.1 鉴别与授权

鉴别与授权包括：

a) 评价方法：

1) 访谈灾难恢复管理小组负责人，查看鉴别与授权相关文档和身份管理系统配置，检查是否对用户身份进行标识和鉴别，是否配置合适的口令复杂度策略，以及测试验证其有效性；

2) 访谈灾难恢复技术与执行小组技术人员，查看鉴别与授权相关文档、操作清单文档等，检查是否明确了灾难恢复系统中重要业务操作、重要用户操作或异常用户操作行为，以及是否形成了清单；

3) 访谈灾难恢复技术与执行小组技术人员，查看鉴别与授权相关文档和身份管理系统配置，检查是否对灾难恢复系统设备、用户、服务或应用、数据进行安全管控，是否对重要业务操作、重要用户操作或异常用户操作行为采用动态的身份鉴别，或者采用多因子身份鉴别等方式；

4) 访谈灾难恢复技术与执行小组技术人员，查看鉴别与授权相关文档和配置，检查是否对灾难恢复系统中的日志访问、策略管理、备份数据访问等安全相关的所有操作设置访问控制策略，检查操作权限是否不超过预定义的范围，以及是否满足了最小特权原则；

5) 访谈灾难恢复技术与执行小组技术人员，查看鉴别与授权相关文档和配置，或查看商用密码安全性评估报告，检查商用密码应用是否符合 GB/T 39786—2021 要求。

b) 预期结果：

1) 灾难恢复系统实现了有效的用户身份标识和鉴别机制，口令复杂度策略得到合理配置和执行；

2) 明确了灾难恢复系统重要业务操作、重要用户操作或异常用户操作行为，并形成清单；

3) 对灾难恢复系统设备、用户、服务、应用和数据实施了严格的安全管控，对关键操作采用动态身份鉴别或多因子鉴别；

4) 对灾难恢复系统中安全相关的所有操作设置访问控制策略，对资源进行访问的内容，操作权限不超过预定义的范围，满足最小特权原则。

c) 结果判定：

上述预期结果均满足判定为符合，否则为不符合或部分符合。

9.5.6.2 入侵防范

入侵防范包括：

a) 评价方法：

1) 访谈灾难恢复技术与执行小组技术人员，了解他们如何监测、识别和响应高级可持续威胁和其他网络攻击，以及相关工具和技术的选择和实施情况。检查是否采用入侵检测系统、入侵防御系统、威胁情报防御系统等技术手段，提高对高级可持续威胁等网络攻击行为的入侵防范能力；

2) 访谈灾难恢复技术与执行小组技术人员，了解灾难恢复系统安全性提升措施的选择、配置和管理过程。检查是否采用后台加密、动态口令等安全措施提升灾难恢复系统的安全性。

b) 预期结果：

1) 灾难恢复系统采取了有效的技术手段，提高对高级可持续威胁等网络攻击行为的入侵防范能力；

2） 通过实施后台加密、动态口令等安全措施，提升了灾难恢复系统的安全性。

c） 结果判定：

上述预期结果均满足判定为符合，否则为不符合或部分符合。

9.5.6.3 自动化工具

自动化工具包括：

a） 评价方法：

1） 访谈灾难恢复技术与执行小组技术人员，了解自动化工具的选型、部署和使用情况，以及如何通过这些工具来提升管理效率和安全性。检查是否部署了自动化工具来管理系统账户和配置，包括账户创建、修改、禁用和删除的流程是否自动化。

2） 访谈灾难恢复技术与执行小组技术人员，询问如何利用自动化工具进行漏洞管理和补丁应用，包括如何确保补丁在应用前经过充分验证。检查是否采用自动化工具进行漏洞扫描和补丁管理，包括漏洞的自动识别、评估和补丁的自动部署。

3） 访谈灾难恢复技术与执行小组技术人员，询问病毒库自动更新的实施情况，了解更新机制的选择、监控和维护策略，检查病毒防护软件和其他安全工具是否配置了病毒库的自动更新机制，以确保对最新威胁的有效防护。

b） 预期结果：

1） 通过自动化工具实现系统账户和配置的高效管理，减少人为错误，提高系统的安全性和稳定性；

2） 自动化工具支持对漏洞的及时识别和评估，以及补丁的自动下载和应用，确保系统针对已知漏洞保持最新的防护状态；

3） 病毒防护软件和安全工具配置了病毒库的自动更新机制，能够及时响应新的安全威胁，保障系统安全。

c） 结果判定：

上述预期结果均满足判定为符合，否则为不符合或部分符合。

9.5.7 安全建设管理

安全建设管理包括：

a） 评价方法：

1） 访谈灾难恢复管理小组及灾难恢复技术与执行小组管理人员，查看安全建设相关文件，检查在灾难恢复系统建设、改造、升级等环节，是否实现安全措施同步规划、同步建设、同步使用；

2） 访谈灾难恢复技术与执行小组负责测试和评审的技术人员，查看测试和评审记录，包括安全测试（如渗透测试、漏洞扫描）和安全评审（如代码审查、架构评审）的实施情况和结果，检查安全建设过程是否采用测试、评审等方式进行验证；

3） 访谈灾难恢复管理小组、灾难恢复技术与执行小组、灾难恢复保障小组等参与攻防演练的人员，查看攻防演练的计划、执行记录和改进措施记录，包括演练场景、参与人员、发现的安全问题和后续的整改措施，检查是否采用攻防演练的方式进行安全性验证。

b） 预期结果：

1） 在灾难恢复系统建设、改造、升级等环节，实现灾了难恢复系统的安全措施同步规划、同步建设、同步使用；

2） 通过开展安全测试和评审验证了灾难恢复系统的安全性，并有效识别和解决了安全问题；

3） 通过攻防演练验证了灾难恢复系统的安全性。

c） 结果判定：

上述预期结果均满足判定为符合，否则为不符合或部分符合。

9.5.8 安全运维管理

安全运维管理包括：

a） 评价方法：

1） 访谈灾难恢复管理小组负责运维管理的人员，了解运维地点的选择依据、境外运维的合规措施及相关法律法规的遵循情况，查看灾难恢复系统运维地点的相关记录和合同，检查运维活动是否全部或主要在中国境内进行。若涉及境外运维，需检查相关活动是否符合中国的相关法律法规要求。

2） 访谈灾难恢复保障小组人力资源部门或灾难恢复管理小组负责运维团队的管理人员，了解安全保密协议的签署流程、内容和执行监督机制。查看与维护人员签订的安全保密协议文档，检查在运维前是否所有维护人员均已签署安全保密协议。

3） 访谈灾难恢复技术与执行小组运维团队，了解运维工具的选择标准、备案流程及未备案工具的测试和审批流程，查看运维工具的登记备案记录，检查是否优先使用已备案的运维工具。对于需使用未登记备案的工具，检查是否在使用前通过恶意代码检测等测试。

b） 预期结果：

1） 确保灾难恢复系统的运维活动主要在中国境内进行，符合国家相关法律法规。对于必要的境外运维活动，有明确的合规性证明文件和管理措施；

2） 所有维护人员在运维前签署安全保密协议；

3） 优先使用已在本组织登记备案的运维工具，确保工具的安全性和适用性。对于未备案的工具，通过严格的测试流程，确保其在使用前不含恶意代码，保障运维过程的安全。

c） 结果判定：

上述预期结果均满足判定为符合，否则为不符合或部分符合。

9.5.9 供应链安全

供应链安全包括：

a） 评价方法：

1） 访谈灾难恢复领导小组负责人及灾难恢复保障小组供应链管理的后勤保障人员，查看供应链安全管理策略、供应链安全管理制度等文件，检查是否建立供应链安全管理策略，以及管理策略是否包括风险管理、供应方选择和管理、产品开发采购、安全维护等策略，检查是否制定供应链安全管理制度文件。

2） 访谈负责灾难恢复保障小组供应链管理的后勤保障人员，查看灾难恢复产品和服务符合相关国家标准要求的证明材料，检查采购的灾难恢复产品和服务是否符合相关国家标准要求。对可能影响国家安全的产品和服务，查看审查记录，检查是否通过国家网络安全审查。

3） 访谈负责灾难恢复保障小组供应链管理的采购和供应链管理人员，查看合格供应方目录，及建立和维护记录，检查是否建立和维护合格供应方目录，以及是否选择有保障的供应方。

4） 访谈负责灾难恢复保障小组或灾难恢复管理小组负责供应链管理人员，了解采购渠道的选择、管理和风险控制方法，查看采购渠道管理策略，检查是否强化采购渠道管理，能否保持采购的灾难恢复产品和服务来源的稳定或多样性。

5） 访谈负责灾难恢复保障小组或灾难恢复管理小组负责法律部门和合同管理人员，了解安

全保密协议的制定、谈判和执行监督过程，查看与供应商签订的采购协议，检查是否明确提供者的安全责任和义务等。

6） 访谈负责灾难恢复保障小组或灾难恢复管理小组人员，了解是否与灾难恢复产品和服务的提供者签订安全保密协议，查看保密协议，并检查其内容是否包括安全职责、保密内容、奖惩机制、有效期等。

7） 访谈负责灾难恢复保障小组或灾难恢复管理小组负责采购部门，查看供应商提供的知识产权授权证明文件，检查相关知识产权是否获得10年以上授权，或在灾难恢复产品和服务使用期内是否获得持续授权。

8） 访谈灾难恢复技术与执行小组相关人员和供应商，查看采购协议和供应商提供的技术资料等，检查供应商是否提供中文版运行维护、二次开发等技术资料。

9） 访谈灾难恢复技术与执行小组相关人员和供应商，查看采购协议和相关检测报告，检查自行或委托第三方服务机构定制开发的软件是否进行源代码安全检测，或供应方是否提供第三方机构出具的代码安全检测报告。

10） 访谈灾难恢复技术与执行小组相关人员，了解安全缺陷和漏洞的识别、评估和处理流程，查看发现安全缺陷和漏洞时的响应记录，检查当使用的灾难恢复产品和服务存在安全缺陷、漏洞等风险时，是否及时采取措施消除风险隐患，涉及重大风险的是否按规定向相关部门报告。

b） 预期结果：

1） 组织已建立包含风险管理、供应方选择、产品开发采购、安全维护等全方位的供应链安全管理策略。具体预期包括有文档记录的策略制定和定期更新流程，策略中明确了风险评估方法、供应方评价标准、采购流程的安全要求和安全维护措施。制定供应链安全管理制度，提供用于供应链安全管理的资金、人员和权限等可用资源。

2） 所有采购的灾难恢复产品和服务都符合国家相关标准和安全要求，特别是涉及国家安全的产品和服务已经通过国家网络安全审查。

3） 成功建立和维护了一个包含经过严格评估和符合安全要求的合格供应方目录。

4） 确保了采购渠道的稳定性和多样性，有效降低了单一供应来源的风险。

5） 采购灾难恢复产品和服务时，明确了提供者的安全责任和义务。

6） 与所有供应商签订的安全保密协议中明确了供应商的安全责任和义务，包括对灾难恢复产品和服务的安全管理要求，以及非法获取用户数据、控制和操纵用户系统设备的禁止声明。

7） 要求供应商对其提供的产品和服务中涉及的所有知识产权有超过10年的授权或在使用期内持续授权。具体预期包括授权证明文件、授权期限记录以及定期的授权验证报告。

8） 灾难恢复产品和服务的提供者提供中文版运行维护、二次开发等技术资料。

9） 对定制开发的软件进行源代码安全检测，并具有安全检测报告。

10） 针对使用的产品和服务发现的安全缺陷和漏洞，组织能够及时采取措施进行修复，并对涉及重大风险的情况按规定向相关部门报告。

c） 结果判定：

上述预期结果均满足判定为符合，否则为不符合或部分符合。

9.5.10 数据安全

数据安全包括：

a） 评价方法：

1） 访谈灾难恢复技术与执行小组技术人员，了解备份和恢复过程中实施的数据完整性校验

方法及其效果，查看备份和恢复操作的文档和相关操作的审计日志，检查是否对灾难恢复系统在备份、恢复过程中的数据完整性进行校验，并验证其有效性；

2） 访谈灾难恢复技术与执行小组技术人员，查看防病毒软件的部署策略和配置，检查是否支持防病毒软件扫描，以及能否防止文件被病毒感染；

3） 访谈灾难恢复技术与执行小组技术人员，查看数据防泄露相关产品配置，检查是否采用数据防泄露功能，数据是否使用合规的商用密码算法进行加密存储，并测试验证其能否防止数据被非法访问和泄露；

4） 访谈灾难恢复保障小组人员，了解数据删除、销毁和存储介质重用的实施细节和监督措施，查看退役和废弃设施处理流程，检查灾难恢复系统设施退役废弃时，是否按照数据安全保护策略对数据删除、销毁和存储介质的重用提出相应要求。

b） 预期结果：

1） 所有备份和恢复操作均通过数据完整性校验，且审计日志显示所有备份和恢复活动均遵循了既定的数据完整性校验流程；

2） 防病毒软件全面覆盖灾难恢复系统中的所有关键组件，定期更新和扫描，无病毒感染报告；

3） 支持数据防泄露功能，能够防止数据被非法访问和泄露；

4） 退役和废弃的数据存储介质按照数据安全保护策略进行了安全删除和销毁，无未经处理的敏感数据残留。

c） 结果判定：

上述预期结果均满足判定为符合，否则为不符合或部分符合。

9.6 灾难恢复系统运行管理测试评价方法

9.6.1 灾难恢复预案制定及管理

9.6.1.1 预案制定原则

预案制定原则包括：

a） 评价方法：

访谈灾难恢复领导小组人员，结合灾难恢复需求和灾难恢复技术方案，查看灾难恢复预案，检查是否按照相应灾难恢复等类别设计，检查是否包含可能发生的灾难场景，检查是否易于理解，适合在紧急情况下使用，检查是否明确资源、步骤、责任人等，检查是否及时更新，检查是否与其他预案兼容。

b） 预期结果：

灾难恢复预案按照相应灾难恢复类别进行了设计，针对不同灾难场景进行了设计和制定，易于理解，适合在紧急情况下使用，明确了资源、步骤、责任人，更新及时且有更新记录；明确了兼容灾备相关其他预案。

c） 结果判定：

上述预期结果均满足判定为符合，否则判定为不符合或部分符合。

9.6.1.2 预案制定过程

预案制定过程包括：

a） 评价方法：

查看灾难恢复预案制定过程记录，检查是否包括起草、评审、测试、完善、审核和批准、备案等过程，检查对应过程记录、签字、评审意见报告等文档是否完整。

b） 预期结果：

1） 预案制定过程完整，包括了起草、评审、测试、完善、审核和批准、备案等过程；

2） 预案制定过程具有完整的过程记录、签字、评审意见、报告等文档。

c） 结果判定：

上述预期结果均满足判定为符合，否则判定为不符合或部分符合。

9.6.1.3 预案内容

预案内容包括：

a） 评价方法：

访谈灾难恢复技术与执行小组人员，结合灾难恢复需求和灾难恢复技术方案，查看灾难恢复预案，检查预案内容是否全面，以及是否与灾难恢复需求和灾难恢复技术方案相符。

b） 预期结果：

灾难恢复预案内容完整，包含了预案实施目标、预案实施所需资源、预案实施团队组成和职责分工、预案重要性级别、预案触发启动条件、预案关联业务清单和资产清单、预案切换资产依赖、关联和切换流程、预案关联部门、通知流程、通知内容、预案演练过程中的数据安全性防护措施、预案演练结束后的数据安全性防护措施、预案演练失败回退流程、预案技术方案和操作手册等内容，且预案内容与灾难恢复需求和灾难恢复技术方案相符。

c） 结果判定：

上述预期结果均满足判定为符合，否则判定为不符合或部分符合。

9.6.1.4 预案培训

预案培训包括：

a） 评价方法：

1） 访谈灾难恢复技术与执行小组成员，查看预案培训相关材料和过程记录，检查培训教育时机、频次、范围、课程、培训记录等是否满足培训需求；

2） 查看预案实施团队成员的考核记录，并质询相关人员，检查其是否掌握预案内容等。

b） 预期结果：

1） 灾难恢复规划初期，开始灾难恢复观念的宣传教育工作；

2） 培训频次和范围、课程内容等满足培训需求，且具有培训记录；

3） 预案实施团队具有考核记录，并掌握预案内容和流程。

c） 结果判定：

上述预期结果均满足判定为符合，否则判定为不符合或部分符合。

9.6.1.5 预案变更

预案变更包括：

a） 评价方法：

1） 查看预案变更过程记录，检查当业务、信息系统、人员等发生变更时，灾难恢复预案是否及时变更；

2） 查看预案变更过程记录，检查是否对预案测试、演练和灾难发生后执行的效果进行评估，以及是否及时修订预案；

3） 查看预案变更过程记录，检查是否对预案进行定期评审和修订，以及评审和修订的频次等是否符合要求。

b） 预期结果：

1） 业务变化、信息系统变更、人员变更等对灾难恢复预案及时进行变更；
2） 已对预案测试、演练和灾难发生后执行的效果进行了评估，并修订预案；
3） 定期对灾难恢复预案进行评审和修订。

c） 结果判定：
上述预期结果均满足判定为符合，否则判定为不符合或部分符合。

9.6.1.6 预案保存和分发

预案保存和分发包括：

a） 评价方法：
1） 访谈灾难恢复技术与执行小组人员和灾难恢复保障小组人员，确认是否指定专人负责预案的保存和分发；
2） 查看预案保存和分发记录，检查是否有多份保存了副本并保存在不同地点，检查是否分发给相关人员，检查是否有明确的版本管理，检查是否销毁预案旧版本。

b） 预期结果：
1） 指定了专人负责预案的保存，具有分发记录；
2） 预案保存和分发记录完整，具有多份保存副本并保存在不同地点，分发给相关人员，具有明确的版本管理，具有预案旧版本销毁记录。

c） 结果判定：
上述预期结果均满足判定为符合，否则判定为不符合或部分符合。

9.6.2 灾难恢复系统运行维护

9.6.2.1 运行维护原则

运行维护原则包括：

a） 评价方法：
访谈灾难恢复技术与执行小组人员和灾难恢复保障小组人员，查看灾难恢复系统运行维护制度，检查灾难恢复系统的安全管理等级和要求是否与生产系统保持一致或低一级，检查灾难恢复系统运行维护体系与生产系统运行维护体系是否实现联动，检查灾难恢复系统运行维护管理是否制度化、流程化，能提高运行维护管理质量、效率，检查灾难恢复系统运行维护管理是否通过全面测试和定期验证机制，能确保灾难恢复资源可用性和有效性。

b） 预期结果：
灾难恢复系统的安全管理等级和要求与生产系统保持一致或低一级，灾难恢复系统运行维护体系与生产系统运行维护体系实现了联动，灾难恢复系统运行维护管理进行了制度化、流程化，能提高运行维护管理质量、效率，灾难恢复系统运行维护管理通过了全面测试和定期验证机制，能确保灾难恢复资源可用性和有效性。

c） 结果判定：
上述预期结果均满足判定为符合，否则判定为不符合或部分符合。

9.6.2.2 运行监控

运行监控包括：

a） 评价方法：
查看监控平台和运行监控记录，检查是否覆盖灾难恢复资源和过程，检查是否包含灾难恢复中心动力环境可用性、灾难恢复资源可用性、灾难恢复资源使用率、灾难恢复资源安全性、灾难恢

复任务运行状态。

b) 预期结果：

运行监控覆盖了灾难恢复资源和过程，包含了灾难恢复中心动力环境可用性、灾难恢复资源可用性、灾难恢复资源使用率、灾难恢复资源安全性、灾难恢复任务运行状态。

c) 结果判定：

上述预期结果均满足判定为符合，否则判定为不符合或部分符合。

9.6.2.3 系统巡检

系统巡检包括：

a) 评价方法：

1) 查看监控运维平台和巡检过程记录，检查是否定期开展灾难恢复系统巡检，并对巡检结果做诊断分析，检查巡检内容是否全面；

2) 查看巡检过程记录，确认巡检频次是否与灾难恢复类别和等级的要求一致；

3) 查看巡检报告，检查是否包含巡检时间、巡检对象、巡检步骤、巡检脚本、巡检结果、巡检执行人员、巡检审核人员、巡检结论和建议等内容；查看巡检报告模板，检查是否定期评审、修订。

b) 预期结果：

1) 巡检内容全面，包含了灾难恢复中心动力环境可用性、灾难恢复资源可用性、灾难恢复资源使用率变化、灾难恢复资源变更记录、灾难恢复资源错误日志、灾难恢复资源安全性、灾难恢复任务运行状态等，巡检有详细记录和巡检报告，并对历史巡检结果进行比对分析；

2) 巡检频次与灾难恢复类别和等级一致；

3) 巡检报告包含了巡检时间、巡检对象、巡检步骤、巡检脚本、巡检结果、巡检执行人员、巡检审核人员、巡检结论和建议等内容；有巡检报告模板和对应的定期评审、修订的记录。

c) 结果判定：

上述预期结果均满足判定为符合，否则判定为不符合或部分符合。

9.6.2.4 灾难恢复演练

灾难恢复演练包括：

a) 评价方法：

1) 访谈灾难恢复技术与执行小组人员和灾难恢复保障小组人员，检查是否开展相应灾难恢复演练，确认演练类型是否满足业务需求；

2) 查看演练过程记录，检查演练频次巡是否与灾难恢复类别和等级的要求一致；

3) 查看演练报告，检查是否包含演练目标、演练预案、演练指挥组、演练执行组、演练时间窗口、演练步骤、演练记录、演练结果、演练总结和建议等内容；

4) 查看演练报告模板，检查是否定期评审、修订；

5) 查看培训材料和记录，检查是否在灾难恢复运行维护初期组织开展演练观念宣传教育工作，检查是否在灾难恢复演练前，对演练目标、演练预案等开展针对性培训，检查是否掌握灾难恢复演练步骤，检查是否组织了灾难恢复演练教育培训后考核，确保演练实施相关人员对演练目标、演练预案、演练步骤理解掌握，检查是否具有培训签到表、考核记录等文档。

b) 预期结果：

1) 开展了相应灾难恢复演练，演练类型满足业务需求；

2) 演练频次应与灾难恢复类别和等级的要求一致；

3） 演练报告内容包含了演练目标、演练预案、演练指挥组、演练执行组、演练时间窗口、演练步骤、演练记录、演练结果、演练总结和建议；

4） 演练报告模板定期进行了评审、修订；

5） 在灾难恢复运行维护初期组织开展演练了观念宣传教育工作，在灾难恢复演练前，对演练目标、演练预案等开展了针对性培训，掌握了灾难恢复演练步骤；组织了灾难恢复演练教育培训后考核，确保了演练实施相关人员对演练目标、演练预案、演练步骤理解掌握；具有培训签到表、考核记录等文档。

c） 结果判定：

上述预期结果均满足判定为符合，否则判定为不符合或部分符合。

9.6.3 应急事件响应及灾难接管

9.6.3.1 应急事件响应

应急事件响应包括：

a） 评价方法：

查看应急事件响应相关材料，检查应急事件响应是否采取必要控制措施，最大限度地保护运行系统和数据安全，抑制事态恶化，降低损失，检查是否结合灾难场景选择对应灾难恢复预案，确认启动灾难恢复预案，检查是否按灾难恢复预案执行应急灾难切换；检查应急灾难切换后是否验证业务和系统可用性，检查是否根据业务和系统可用性验证结果，决定结束或继续应急事件响应状态；检查是否有应急事件完整的过程记录文档。

b） 预期结果：

应急事件响应采取了必要控制措施，最大限度地保护运行系统和数据安全，抑制事态恶化，降低损失，结合了灾难场景选择对应灾难恢复预案，确认启动灾难恢复预案，按灾难恢复预案执行应急灾难进行了切换，应急灾难切换后验证了业务和系统可用性，根据业务和系统可用性进行了验证结果，决定结束或继续应急事件响应状态；具有应急事件完整的过程记录文档。

c） 结果判定：

上述预期结果均满足判定为符合，否则判定为不符合或部分符合。

9.6.3.2 灾难恢复事件报告

灾难恢复事件报告包括：

a） 评价方法：

1） 查看灾难恢复事件报告，检查是否包含灾难类型、灾难原因，业务影响范围、业务影响时长、数据丢失时长、灾难恢复预案和整改意见等内容；

2） 查看灾难恢复事件报告模板，检查是否定期评审、修订及对应的记录。

b） 预期结果：

1） 灾难恢复事件报告包含了灾难类型、灾难原因，业务影响范围、业务影响时长、数据丢失时长、灾难恢复预案和整改意见；

2） 灾难恢复事件报告模板有定期评审、修订及对应的记录。

c） 结果判定：

上述预期结果均满足判定为符合，否则判定为不符合或部分符合。

9.6.4 重建和回退

重建和回退包括：

a） 评价方法：

1） 访谈灾难恢复技术与执行小组人员和灾难恢复保障小组人员，确认在灾难恢复完成后，是否第一时间制定灾难后重建和回退方案；

2） 查看重建和回退方案，检查方案内容是否全面。

b） 预期结果：

1） 灾难恢复完成后，第一时间制定了灾难后重建和回退方案；

2） 重建和回退方案内容完整，方案包含生产中心故障修复或重建、实施灾难恢复中心到生产中心的数据同步、实施灾难恢复中心到生产中心的数据同步、验证从灾难恢复中心回切到生产中心后的业务可用性、制定从灾难恢复中心回切到生产中心失败的应对措施等内容。

c） 结果判定：

上述预期结果均满足判定为符合，否则判定为不符合或部分符合。

9.6.5 灾难恢复审计

灾难恢复审计包括：

a） 评价方法：

1） 查看审计报告等相关材料，检查是否定期组织内部或第三方审计机构审计并出具审计报告，以及审计内容是否全面；

2） 访谈灾难恢复技术与执行小组人员，查看审计报告提出的改进意见和改进方案，检查是否对改进意见进行及时答复，以及答复情况。

b） 预期结果：

1） 定期组织了内部或第三方审计机构审计并出具了审计报告，审计内容包含了灾难恢复预案保存和分发记录、灾难恢复预案培训记录、灾难恢复预案报备记录、灾难恢复演练培训记录、灾难恢复演练报告归档记录、灾难恢复系统巡检报告归档记录等内容；

2） 对审计报告提出的改进意见进行及时答复。

c） 结果判定：

上述预期结果均满足判定为符合，否则判定为不符合或部分符合。

附 录 A
（规范性）
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	能力要求
数据备份容灾系统	a） 完全数据备份至少每周一次，至少保留 1 个月冗余数据； b） 备份存储场外存放或者本地存放。异地备份或者本地备份要使用专属的备份存储； c） 生产中心和灾难恢复中心，重要系统数据周期性同步，实现天级 RPO； d） 当生产中心发生灾难，灾难恢复中心能够在 72 h 内拉起应用，接管业务 注：借助数据备份系统提供一定程度的容灾保护。
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	能力要求
数据备份容灾系统	a） 完全数据备份至少每周一次，至少保留 1 个月冗余数据； b） 备份存储场外存放或者本地存放，异地备份或者本地备份要使用专属的备份存储； c） 生产中心和灾难恢复中心，重要系统数据周期性同步，实现天级 RPO； d） 当生产中心发生灾难，灾难恢复中心能够在 48 h 内拉起应用，接管业务 注：借助数据备份系统提供一定程度的容灾保护。
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，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； b） 备用数据处理系统独立于生产系统运行

表 A.2　第 2 级——备用场地支持（续）

要素	能力要求
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	在灾难恢复中心有专职的计算机机房运行管理人员
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	能力要求
数据备份容灾系统	a)　完全数据备份至少每天一次，至少保留 1 个月冗余数据； b)　备份存储场外存放或者本地存放，异地备份或者本地备份要使用专属的备份存储； c)　生产中心和灾难恢复中心，重要系统数据周期性同步，实现小时级到天级 RPO； d)　副本数据不可修改和防泄漏机制，保护备份数据加密和不被非法篡改，保障数据完整性； e)　支持防勒索功能，建立安全的隔离区用于数据存储，防止备份数据被非法访问； f)　当生产中心发生灾难，灾难恢复中心能够在 24 h 内拉起应用，接管业务 **注**：借助数据备份系统提供一定程度的容灾保护。
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； b)　备用数据处理系统独立于生产系统运行
备用网络系统	配备部分通信线路和相应的网络设备
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	在灾难恢复中心有专职的计算机机房运行管理人员
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 级灾难恢复能力应具有技术和管理支持如表 A.4 所示。

表 A.4　第 4 级——电子传输及完整设备支持

要素	能力要求
数据备份容灾系统	a)　完全数据备份至少每天一次，至少保留 1 个月冗余数据； b)　备份存储场外存放或者本地存放，异地备份或者本地备份要使用专属的备份存储； c)　生产中心和灾难恢复中心，重要系统数据周期性同步，实现小时级 RPO； d)　副本数据不可修改和防泄漏机制，保护备份数据加密和不被非法篡改，保障数据完整性； e)　支持防勒索功能，建立安全的隔离区用于数据存储，防止备份数据被非法访问； f)　当生产中心发生灾难，灾难恢复中心能够在小时级拉起应用，接管业务
备用数据处理系统	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
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
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	在灾难恢复中心有： a)　7×24 h 专职计算机机房管理人员； b)　数据灾难恢复系统、数据备份系统技术支持人员； c)　专职硬件、网络技术支持人员
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	能力要求
数据备份容灾系统	a)　完全数据备份至少每天一次，至少保留 1 个月冗余数据； b)　备份存储场外存放或者本地存放，异地备份或者本地备份要使用专属的备份存储； c)　生产中心和灾难恢复中心，重要系统数据周期性同步，实现小时级 RPO、数据零丢失； d)　副本数据不可修改和防泄漏机制，保护备份数据加密和不被非法篡改，保障数据完整性； e)　支持防勒索功能，建立安全的隔离区用于数据存储，防止备份数据被非法访问； f)　备份中心支持以生产中心相同数据格式进行备份，并在备份中心实现数据秒级实时挂载恢复； g)　数据中心之间网络抖动、闪断等亚健康场景，具备良好的网存联动措施，保障业务高可靠； h)　当生产中心发生灾难，灾难恢复中心能够在分钟级到小时级快速拉起应用，接管业务

表 A.5　第 5 级——实时数据传输及完整设备支持（续）

要素	能力要求
备用数据处理系统	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
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
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	在灾难恢复中心 7×24 h 有专职的： a）　计算机机房管理人员； b）　数据灾难恢复系统、数据备份系统技术支持人员； c）　硬件、网络技术支持人员
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）　有实时数据容灾和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.6　第 6 级——数据零丢失和远程集群支持

第 6 级灾难恢复能力应具有技术和管理支持如表 A.6 所示。

表 A.6　第 6 级——数据零丢失和远程集群支持

要素	能力要求
数据备份容灾系统	a）　完全数据备份至少每天一次，至少保留 1 个月冗余数据； b）　备份存储场外存放或者本地存放，异地备份或者本地备份要使用专属的备份存储； c）　生产中心和灾难恢复中心，重要系统数据周期性同步，实现小时级 RPO、数据零丢失； d）　副本数据不可修改和防泄漏机制，保护备份数据加密和不被非法篡改，保障数据完整性； e）　支持防勒索功能，建立安全的隔离区用于数据存储，防止备份数据被非法访问； f）　备份中心支持以生产中心相同数据格式进行备份，并在备份中心实现数据秒级实时挂载恢复； g）　数据中心之间网络抖动、闪断等亚健康场景，具备良好的网存联动措施，保障业务高可靠； h）　当生产中心发生灾难，灾难恢复中心能够在分钟级快速拉起应用，接管业务
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

表 A.6　第 6 级——数据零丢失和远程集群支持（续）

要素	能力要求
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	在灾难恢复中心 7×24 h 有专职的： a）　计算机机房管理人员； b）　专职数据灾难恢复系统、数据备份系统技术支持人员； 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各要素的相应要求。

A.8　灾难恢复中心的等级

灾难恢复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 级灾难恢复中心的级别为 5 级灾难恢复能力。

附 录 B
（资料性）
某行业同城灾难恢复中心 RTO/RPO 与灾难恢复能力等级的关系示例

表 B.1 说明信息系统灾难恢复各等级对应的 RTO/RPO 范围。

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 d 以上	1 d 至 7 d
2	24 h 以上	1 d 至 7 d
3	12 h 以上	数小时至 1 d
4	数小时至 1 d	数小时至 1 d
5	数分钟至数小时	0
6	数分钟	0

附 录 C
（资料性）
某行业信息系统需求分类示例

表 C.1 给出了信息系统灾难恢复需求分类示例。

表 C.1 信息系统灾难恢复需求分类和灾备建设示例

需求分类	需求分类划分依据	恢复次序	RTO	RPO	灾备建设等级
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	首先	＜6 h	＜15 min	≥5 级
	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				
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	其次	＜24 h	＜120 min	≥3 级
	单位和用户对系统短时间中断具有一定容忍度的系统				
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	最后	＜7 d	＜24 h	≥2 级
	业务功能容许一段时间中断的系统				

附 录 D
（资料性）
云计算技术灾难恢复服务示例

表 D.1 给出了基于云计算技术的信息系统灾难恢复服务的示例。

表 D.1 云计算技术灾难恢复服务示例

服务类型	应用场景	资源要素要求	RPO	RTO
云端数据备份服务	在云端部署数据备份系统，定期将生产环境的数据在云端进行备份	云端数据备份系统： ——提供弹性的数据备份服务； ——其他要求同 6.3.1.1	小时级	—
		网络要求： ——具备生产环境和云端的数据通信线路		
		安全要求： ——云端存储数据需要隔离机制，从而防止数据泄露； ——其他安全需求同 6.3.1.1		
冷容灾备份服务	在云端部署的备份业务系统，在灾难发生时，启动云端备份业务系统，提供服务	云端数据存储系统： ——提供弹性伸缩的数据存储服务； ——其他要求同 6.3.1.1	分钟级	小时级
		云端备份业务系统要求： ——在云端提供跟生产环境相同的业务系统功能以及性能； ——云端备份业务系统在系统运行环境和软件版本等方面完全兼容	—	—
		网络要求： ——具备生产环境和云端的单向实时数据通信线路； ——生产环境和云端分别独立的业务通信线路； ——生产环境和云端之间的业务通信线路	—	—
		安全要求： ——云端存储数据需要隔离机制，从而防止数据泄露； ——云端的备份业务系统需要隔离机制，从而防止业务系统被恶意篡改； ——其他安全需求同 6.3.1.1	—	—
多活容灾服务	云端部署两套或者多套业务系统，并且同时提供服务	云端数据存储系统： ——提供弹性伸缩的数据存储服务； ——其他要求同 6.3.1.1	分钟级	0～分钟级

表 D.1　云计算技术灾难恢复服务示例（续）

服务类型	应用场景	资源要素要求	RPO	RTO
多活容灾服务	云端部署两套或者多套业务系统，并且同时提供服务	云端业务系统要求： ——在云端部署多套功能以及性能相同的业务系统，并且同时提供服务； ——云端的业务系统具备弹性； ——云端业务系统在系统运行环境和软件版本等方面完全兼容	分钟级	0～分钟级
		网络要求： ——具备多套数据存储系统的之间的双向实时数据通信线路； ——各套业务系统具备独立的业务通信线路； ——各套业务系统之间具备业务通信路线		
		安全要求： ——云端存储数据需要隔离机制，从而防止数据泄露； ——云端的业务系统需要隔离机制，从而防止业务系统被恶意篡改； ——其他安全需求同 6.3.1.1		
注：“—”表示不作要求。				

附 录 E
（资料性）
灾难恢复系统的安全建设

E.1 网络安全等级保护

灾难恢复系统可根据其网络安全等级保护级别要求，安全建设见 GB/T 22239—2019 和 GB/T 39786—2021。

E.2 安全管理制度

灾难恢复系统安全管理制度包括：

a） 制定适合本组织的灾难恢复安全保护计划，明确灾难恢复安全保护工作的目标，从管理体系、技术体系、运行维护体系、保障体系等方面进行规划，加强机构、人员、经费、装备等资源保障，支撑灾难恢复安全保障工作。灾难恢复过程的安全保护计划形成文档并经审批后发送至相关人员，宜根据内容的敏感程度和重要程度，确定分发范围，做好保密性和安全性管理。灾难恢复系统安全策略应每年至少修订一次，或发生重大变化时进行修订。

b） 建立灾难恢复系统的管理制度和安全策略，并根据灾难恢复系统面临的安全风险和威胁的变化进行相应调整。

E.3 安全管理架构

灾难恢复安全管理机构设置见第 6 章，从灾难恢复系统安全性角度还包含以下：

a） 在灾难恢复的组织机构中明确负责人专职管理灾难恢复系统安全保护工作，建立并实施考核及监督问责机制；

b） 将灾难恢复安全管理机构人员纳入灾难恢复的组织机构决策体系。

E.4 安全管理人员

灾难恢复系统安全管理人员包括：

a） 对灾难恢复系统关键岗位的人员进行安全技能考核，符合要求的人员方能上岗；

b） 建立灾难恢复系统系统安全教育培训制度，定期开展安全教育培训和技能考核；

c） 当灾难恢复系统安全管理机构的负责人和关键岗位人员的身份、安全背景等发生变化或必要时，可根据情况重新按照相关要求进行核查；

d） 明确从业人员安全保密职责和义务，并签订安全保密协议。

E.5 安全通信网络

E.5.1 网络架构

宜实现灾难恢复系统的通信线路“一主多备”的多电信运营商多路由保护，宜对网络关键节点和重要设施实施“双节点”冗余备份。

E.5.2 互联安全

互联安全包括：

a） 建立或完善灾难恢复系统与不同业务系统之间、不同区域的系统之间、不同运营者运营的系统

之间的安全互联策略；

b） 保持同一用户其用户身份和访问权限等在本地和异地灾难恢复系统中的一致性；

c） 对不同局域网远程通信的灾难恢复系统之间采取安全防护措施。

E.5.3 边界防护

边界防护包括：

a） 对灾难恢复系统在不同业务系统之间、不同区域的系统之间、不同运营者运营的系统之间的互操作、数据交换和信息流向进行严格控制；

b） 保证灾难恢复系统跨边界的访问和数据流通过边界设备的受控接口进行通信。

E.5.4 安全审计

安全审计包括：

a） 对灾难恢复系统的数据备份、恢复、删除、迁移、系统配置的变更等操作进行审计；

b） 提供对审计数据的管理功能，且只有相应权限的用户才能读取对应的审计数据；

c） 相关日志数据留存不少于 6 个月。

E.6 安全计算环境

E.6.1 鉴别与授权

鉴别与授权包括：

a） 对用户身份进行标识和鉴别，并配置合适的口令复杂度策略。

b） 明确灾难恢复系统重要业务操作、重要用户操作或异常用户操作行为，并形成清单。

c） 对灾难恢复系统设备、用户、服务或应用、数据进行安全管控，对于重要业务操作、重要用户操作或异常用户操作行为，建立动态的身份鉴别方式，或者采用多因子身份鉴别等方式。

d） 对灾难恢复系统中安全相关的所有操作设置访问控制策略，应包括但不限于日志访问、策略管理、备份数据访问等。对资源进行访问的内容，操作权限不超过预定义的范围，满足最小特权原则。

e） 身份标识和鉴别技术应符合商用密码应用要求。

E.6.2 入侵防范

入侵防范包括：

a） 采取技术手段，提高对高级可持续威胁等网络攻击行为的入侵防范能力；

b） 采取技术手段，提升灾难恢复系统的安全性，通过灾难恢复系统后台加密、动态口令等设置。

E.6.3 自动化工具

使用自动化工具来支持系统账户、配置、漏洞、补丁、病毒库等的管理。对于漏洞、补丁，在经过验证后及时修补。

E.7 安全建设管理

在灾难恢复系统建设、改造、升级等环节，实现灾难恢复系统的安全措施同步规划、同步建设、同步使用，并采取测试、评审、攻防演练等多种形式验证。

E.8 安全运维管理

安全运维管理包括：

a) 保证灾难恢复系统的运维地点位于中国境内，如确需境外运维，需符合我国相关规定；
b) 在运维前与维护人员签订安全保密协议；
c) 确保优先使用已在本组织登记备案的运维工具，如确需使用未登记备案的运维工具，在使用前需通过恶意代码检测等测试。

E.9 供应链安全

供应链安全保护包括：

a) 建立供应链安全管理策略，包括：风险管理策略、供应方选择和管理策略、产品开发采购策略、安全维护策略等。建立供应链安全管理制度，提供用于供应链安全管理的资金、人员和权限等可用资源。
b) 应采购、使用符合相关国家标准要求的灾难恢复产品和服务。可能影响国家安全的，需应通过国家网络安全审查。
c) 需建立和维护合格供应方目录。选择有保障的供应方，防范出现因政治、外交、贸易等非技术因素导致产品和服务供应中断的风险。
d) 强化采购渠道管理，保持采购的灾难恢复产品和服务来源的稳定或多样性。
e) 采购灾难恢复产品和服务时，需明确提供者的安全责任和义务，要求提供者对灾难恢复产品和服务的设计、研发、生产、交付等关键环节加强安全管理。要求提供者声明不非法获取用户数据、控制和操纵用户系统和设备，或利用用户对产品的依赖性谋取不正当利益或者迫使用户更新换代。
f) 需与灾难恢复产品和服务的提供者签订安全保密协议，协议内容包括安全职责、保密内容、奖惩机制、有效期等。
g) 要求灾难恢复产品和服务的提供者对灾难恢复产品和服务研发、制造过程中涉及的实体拥有或控制的已知技术专利等知识产权获得 10 年以上授权，或在灾难恢复产品和服务使用期内获得持续授权。
h) 灾难恢复产品和服务的提供者提供中文版运行维护、二次开发等技术资料。
i) 需自行或委托第三方服务机构对定制开发的软件进行源代码安全检测，或由供应方提供第三方机构出具的代码安全检测报告。
j) 使用的灾难恢复产品和服务存在安全缺陷、漏洞等风险时，需及时采取措施消除风险隐患，涉及重大风险的需按规定向相关部门报告。

E.10 数据安全

灾难恢复系统数据安全包括：

a) 对灾难恢复系统在备份、恢复过程中的数据完整性进行校验；
b) 支持防病毒软件扫描，防止文件被病毒感染；
c) 支持数据防泄露功能，数据存储使用符合商用密码算法要求的算法进行加密存储，防止数据被非法访问和泄露；
d) 在灾难恢复系统设施退役废弃时，按照数据安全保护策略对数据删除、销毁和存储介质的重用提出相应要求。

附 录 F
（资料性）
灾难恢复预案框架

F.1 目标和范围

首先定义灾难恢复预案的目标、术语和方法论，包括但不限于恢复时间目标、恢复点目标和最大可容忍停工时间。明确预案的作用范围，包括以下内容：

a) 预案的适用范围：该预案适用于哪些组织、部门或业务单位；
b) 问题解决范围：指明预案的主要目标，即在发生灾难或突发事件时，确保组织信息系统的连续性和数据完整性；
c) 问题不解决范围：明确指出预案不覆盖的问题，以及在某些情况下可能需要其他预案或应对措施。

F.2 组织和职责

详细描述灾难恢复组织的组成、各个岗位的职责和人员名单。灾难恢复组织包括但不限于应急响应团队、灾难恢复团队等，并明确他们的职责和责任。

F.3 联络与通信

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、员工等。联络方式包括固定电话、移动电话、对讲机、电子邮件、住址及紧急联络应用等。

提供灾难恢复相关人员和组织的详细联络信息，包括但不限于灾难恢复团队、运营商、供应商、主管部门、媒体、员工等。明确各人员的联络方式，包括电话号码、电子邮件、地址、紧急联络应用等。

F.4 突发事件响应流程

F.4.1 事件通告

任何人员在发现信息系统相关突发事件发生或即将发生时，需按预定的流程报告相关人员，并由相关人员进行初步判断、通知和处置。

F.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。

F.4.3 损害评估

在突发事件发生后，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突发事件进行慎重评估，确定突发事件对信息系统及关联业务流程造成的影响程度，确定下一步将要采取的行动。一旦系统的影响被确定，将最新信息按照预定的通告流程通知给相应的团队。

F.4.4 灾难宣告

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，组织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。

F.5 恢复及重续运行流程

F.5.1 恢复

按业务影响分析和风险评估中确定的优先顺序，在灾难恢复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，以及异常处理流程。

F.5.2 重续运行

这一阶段包含主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。灾难恢复中心的系统替代主系统，支持关键业务功能的提供。这一阶段应提供详细的业务影响分析结果，并根据优先级顺序描述灾难恢复中心中的数据、数据处理系统和网络系统的恢复过程。明确操作步骤、时间表、所需设备和人员，同时包括特定情况下的团队协调指南和异常处理流程。

F.6 灾后重建和回退

最后阶段是主中心的重建工作，中止灾难恢复系统的运行，平稳地迁移并回退到组织的主系统。在此阶段，提供灾后重建的详细计划，包括主中心的重建工作、切换回组织的主系统的程序和步骤。

F.7 预案的保障条件

预案的保障条件如下：

a） 专业技术支持：确保有足够的技术专家、安全专家和资源可供调用；

b） 通信支持：保障通信系统的可用性，包括备用通信渠道；

c） 后勤支持：确保应急设施和设备的供应和维护。

F.8 预案附录

在预案的附录部分，包括但不限于以下内容：

a） 人员疏散计划；

b） 预案的培训、测试和演练计划；

c） 产品说明书；

d） 信息系统标准操作流程；

e） 服务级别协议和备忘录；

f） 资源清单；

g） 业务影响分析报告；

h） 预案的版本控制、保存、分发程序及办法，并明确预案的定期审查和更新周期。

参 考 文 献

[1] GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
[2] GB/T 22240—2020 信息安全技术 网络安全等级保护定级指南
[3] GB/T 24353—2022 风险管理 指南
[4] GB/T 28453—2012 信息安全技术 信息系统安全管理评估要求
[5] GB/T 29246—2023 信息安全技术 信息安全管理体系 概述和词汇
[6] GB/T 30279—2020 信息安全技术 网络安全漏洞分类分级指南
[7] GB/T 31509—2015 信息安全技术 信息安全风险评估实施指南
[8] GB/T 31722—2015 信息技术 安全技术 信息安全风险管理
[9] GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求
[10] NIST Special Publication 800-26 Security self-assessment guide for information technology systems
[11] NIST Special Publication 800-30 Risk management guide for information technology systems