ICS 35.040
L 80

中华人民共和国国家标准

GB/T 36957—2018

信息安全技术　灾难恢复服务要求

Information security technology—Requirements for disaster recovery service

2018-12-28 发布　　2019-07-01 实施

国家市场监督管理总局
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。

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这些专利的责任。

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。

本标准主要起草单位:中国网络安全审查技术与认证中心、中国信息安全测评中心、万国数据服务有限公司、北京中金云网科技有限公司、中国银行股份有限公司、上海期货交易所、中信银行卡中心、中国电子信息产业发展研究院、中国民生银行、北京市政务信息安全应急处置中心、北京邮电大学、北京时代新威信息技术有限公司、太极计算机股份有限公司、南京南瑞信息通信科技有限公司、首都信息科技发展有限公司、国网信通亿力科技有限责任公司、北京蓝快拓展信息技术有限公司、北京安码科技有限公司。

本标准主要起草人:张剑、关继铮、魏立茹、程瑜琦、张斌、赵倩倩、孙明亮、位华、王琰、杨志国、王新杰、程燕、郭涛、李东南、徐雷鸣、吴新颖、支晓繁、卫飞、张珣、刘权、高献华、王琪、魏彬、张勇、辛阳、汪琪、秦楠、熊海晋、聂庆节、张磊、刘赛、丁金富、李志超、苟晓军、徐勤。

信息安全技术　灾难恢复服务要求

1　范围

本标准规定了灾难恢复服务资源配置、灾难恢复服务过程和灾难恢复服务项目管理三个方面的灾难恢复服务要求。

本标准适用于灾难恢复服务需求方(以下简称“服务需求方”)对灾难恢复服务提供方(以下简称“服务提供方”)提出服务要求,可供相关行业和企事业单位选择灾难恢复服务时参考。

本标准也可用于规范服务提供方开展的灾难恢复服务工作。

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　信息安全技术　信息安全风险评估规范

GB/T 20985.1　信息技术　安全技术　信息安全事件管理　第1部分:事件管理原理

GB/T 20988—2007　信息安全技术　信息系统灾难恢复规范

GB/T 30285—2013　信息安全技术　灾难备份中心建设与运维管理规范

GB/T 31240—2014　信息技术　用户建筑群布缆的路径和空间

GB/T 31722—2015　信息技术　安全技术　信息安全风险管理

GB 50116—2013　火灾自动报警设计规范

GB 50370—2005　气体灭火系统设计规范

3　术语和定义

GB/T 20988—2007界定的以及下列术语和定义适用于本文件,为了便于使用,以下重复列出了GB/T 20988—2007中的一些术语和定义。

3.1

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时间。通常导致信息系统需要切换到灾难备份中心运行。

[GB/T 20988—2007,定义3.8]

3.2

灾难恢复服务　disaster and recovery services

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的状态、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进行的分析、设计、实施、运行、维护及组织管理等活动和流程。

3.3

灾难恢复服务需求方　customer of disaster recovery service

需要通过第三方专业服务和资源实现灾难恢复的组织或部门,简称服务需求方。

3.4

灾难恢复服务提供方　service provider of disaster recovery

具有专业的灾难恢复服务团队和资源，并能提供灾难恢复服务的组织或部门，简称服务提供方。

3.5

灾难恢复中心　disaster and 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。

[GB/T 30285—2013，定义 3.5]

3.6

灾难备份　backup for disaster recovery

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

[GB/T 20988—2007，定义 3.2]

3.7

灾难备份系统　backup system for disaster recovery

用于灾难恢复目的，由数据备份系统、备用数据处理系统和备用的网络系统组成的信息系统。

[GB/T 20988—2007，定义 3.3]

3.8

生产中心　production cente

主系统所在的数据中心。

[GB/T 20988—2007，定义 3.15]

3.9

主系统　primary system

生产系统　production system

正常情况下支持组织日常运作的信息系统。包括主数据、主数据处理系统和主网络。

[GB/T 20988—2007，定义 3.16]

3.10

灾难恢复规划　disaster recovery planning；DRP

为了减少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。

[GB/T 20988—2007，定义 3.11]

3.11

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。

[GB/T 20988—2007，定义 3.12]

3.12

关键业务功能　critical cusiness functions

如果中断一定时间，将显著影响组织的正常运作，导致组织的主要职能或服务无法展开。

[GB/T 20988—2007，定义 3.6]

3.13

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的过程。

[GB/T 20988—2007,定义 3.5]

3.14

恢复时间目标　recovery time objective;RTO

灾难发生后,信息系统或业务功能恢复到最低可用水平的时间段。

注:改写 GB/T 20988—2007,定义 3.18。

3.15

恢复点目标　recovery point objective;RPO

灾难发生后,系统和数据应恢复到最低可用水平的时间点。

注:改写 GB/T 20988—2007,定义 3.19。

3.16

风险评估　risk assessment;RA

风险识别、风险分析和风险评价的整个过程。

[GB/T 29246—2017,定义 2.71]

3.17

灾难恢复预案　disaster recovery plan

定义信息系统灾难恢复过程中所需的任务、行动、数据和资源的文件。用于指导相关人员在预定的灾难恢复目标内恢复信息系统支撑的关键业务功能。

[GB/T 20988—2007,定义 3.10]

3.18

演练　exercise

为训练人员和提高灾难恢复能力而根据灾难恢复预案进行活动的过程。包括桌面演练、模拟演练、重点演练和完整演练等。

[GB/T 20988—2007,定义 3.13]

3.19

桌面演练　desk exercise

采用场景模拟、分组讨论、专家点评等形式,对可能发生的灾难情景进行应急响应和处置的过程。

3.20

模拟切换演练　simulation switching exercise

根据信息系统灾难恢复预案,在确保生产正常运行的基础上建立模拟演练环境,对灾难恢复系统、业务恢复环境、灾难恢复预案、业务恢复预案及服务团队进行的能力检验的过程。

3.21

真实切换演练　actual switching exercise

在预先设定的灾难场景下,将实际的业务应用从生产中心切换至灾难恢复中心,由备份系统及资源提供业务服务,生产中心进行系统恢复后,再将业务应用从灾难恢复中心切换至生产中心,由此对恢复环境、系统、预案、流程及服务能力进行验证的过程。

4　灾难恢复服务总体要求

灾难恢复服务包括灾难恢复服务规划设计、建设实施和运行维护等环节,灾难恢复服务提供方可根据服务需求方的要求提供单个或多个环节的灾难恢复服务,服务时应满足灾难恢复服务资源配置、灾难恢复服务过程和灾难恢复服务项目组织管理的要求。

凡涉及到采用密码技术解决机密性、完整性、真实性、不可否认性需求的应遵循密码相关国家标准和行业标准。

5 灾难恢复服务资源配置要求

5.1 资源配置总体要求

灾难恢复服务资源配置包括灾难恢复中心场地资源、灾难恢复系统资源和灾难恢复服务团队，灾难恢复服务资源由服务提供方向服务需求方提供，服务提供方不得转包（合同规定除外），但可以分包，如果分包（或转包），服务提供方应确保分包（或转包）商的服务满足服务需求方的要求。

5.2 场地资源配置要求

5.2.1 场地资源总体要求

服务提供方所提供的灾难恢复中心场地环境应在双方约定的服务期限内稳定运行，并能在灾难发生时接管生产系统运行。场地资源应符合安全管理要求的管理控制措施，包括物理安全、数据安全、运行安全、人员安全等安全管控措施，并进行安全审计。场地资源配置要求包括场地位置要求、布局要求、建筑结构要求、电力设施要求、消防设施要求、空调系统要求和综合布线要求。

5.2.2 场地位置要求

灾难恢复中心场地位置应满足以下要求：

a) 满足 GB/T 30285—2013 中 5.2.2 的场地选址要求；
b) 地处交通便利，周边的生活设施齐全的区域，且不能与服务需求方的生产中心场地同处于一个风险区域内；
c) 避开粉尘、油烟、有害气体源、低洼、潮湿、落雷、重盐害、强振动源、强噪音源、强电磁场，远离核辐射源等区域；
d) 不能与酒店、食堂、商店等生活设施同处一个建筑物内；
e) 与铁路及高速公路距离应大于 800 m，以保证降低化学物质溅落危险；
f) 与军事基地距离应大于 800 m，与核设施、国防设施等大于 1 600 m。

5.2.3 场地布局要求

灾难恢复中心场地应符合 GB/T 30285—2013 中 6.1 的基础设施建设管理的要求，并满足以下布局要求：

a) 灾难恢复中心场地应包括工作设施、辅助设施、生活设施和其他配套设施等。
b) 工作设施应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。
c) 辅助设施应包括日常运行辅助设施、应急与灾难恢复辅助设施、灾难恢复培训设施等。其中办公室、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、打印传真室等属于应急与灾难恢复辅助设施；培训教室、模拟演练室等属于灾难恢复培训设施。
d) 生活设施应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。

5.2.4 建筑结构要求

灾难恢复中心场地工作设施所在的建筑物应满足以下要求：

a) 抗震设防标准应达到服务需求方的灾难恢复中心当地抗震设防标准；

b) 机房楼板荷重最小不应小于 8 000 N/m²；
c) 建筑的入口至主机房的应设通道，通道净宽不应小于 1.5 m；
d) 考虑机房区楼板沉降设计，机房活动地板的高度与通道高度一致。

5.2.5 电力设施要求

灾难恢复中心场地工作设施的电力设施应满足以下要求：
a) 具备与生产中心相当的供配电系统、不间断电源系统、应急电源（发电机组）、照明系统等；
b) 满足灾难恢复系统所涉及的信息技术设备的电能使用效率要求，并采用冗余设计；
c) 选用节能环保型设备；
d) 具备高温保护系统及火灾报警系统；
e) 宜装设自动灭火系统。

5.2.6 消防设施要求

灾难恢复中心场地工作设施的消防设施应满足以下要求：
a) 火灾自动报警系统应符合 GB 50116—2013 的规定；
b) 可安装极早期火灾自动报警系统；
c) 所在建筑物已有自动灭火系统的场地、面积大于或等于 140 m² 的机房和有风险及管理需要者应安装自动灭火系统；
d) 自动灭火系统应符合 GB 50116—2013 的规定；
e) 辅助房间宜采用洁净气体灭火系统；
f) 洁净气体灭火系统应符合 GB 50370—2005 的规定。

5.2.7 空调系统要求

灾难恢复中心场地工作设施的空调系统应满足以下要求：
a) 包括制冷机（泵）、空调设备、风机、冷凝（冷却）器、管路、阀门、传感控制器等；
b) 采用冗余设计，并选用节能环保型设备；
c) 在建筑空间、结构承重、电源系统、空调冷却方式、机架结构等方面采取相应的技术措施，合理进行设计，解决局部热点；
d) 空调系统应满足与服务需求方生产中心的温湿度范围一致。

5.2.8 综合布线要求

灾难恢复中心场地工作设施的综合布线系统应满足以下要求：
a) 综合布线的组成为：配线架、主线缆、水平线缆、汇接点、管理等；
b) 布缆的路径和空间应遵循 GB/T 31240—2014 的规定。

5.3 灾难恢复系统资源配置要求

5.3.1 灾难恢复系统资源配置总体要求

服务提供方应提供专业的服务设备和设施，或能够协助服务需求方提供灾难恢复服务设备与设施，并确保服务需求方能使用服务设备和设施完成灾难恢复工作。服务的设备和设施应包括但不限于数据备份系统、备用数据处理系统、备用网络系统、灾难恢复服务工具等。

针对采用云灾备服务的服务提供方，应向服务需求方提供统一、界面友好的自服务门户，并将灾难恢复服务资源按照资源池的方式进行统一管理，并可满足应用系统在日常运行、灾难恢复、测试演练、回退等各个阶段对资源的需求。

5.3.2 数据备份系统要求

服务提供方提供的数据备份系统要求如下：

a) 按照服务需求方各应用系统的数据容量要求进行备份存储的容量配置，备份容量应满足服务需求方的应用程序、业务数据、验证数据等方面的容量要求；
b) 备份介质可采用磁盘阵列、虚拟带库、物理带库等；
c) 按照服务需求方生产系统的灾难恢复指标和等级要求提供备份软件或工具；
d) 建议采用虚拟化存储的方式提供备份存储，对于无法进行存储虚拟化的应用系统，其备用存储系统可采用传统物理存储方式提供，但应提供统一的资源管理平台对虚拟存储和物理存储进行管理。

5.3.3 备用处理系统要求

服务提供方提供的备用处理系统应满足以下要求：

a) 按照服务需求方应用系统的灾难恢复指标和等级提供备用处理资源；
b) 系统运行环境和软件版本等方面与服务需求方的生产系统完全兼容，以确保灾难恢复系统具备接管生产系统运行的能力；
c) 按照服务需求方的生产处理系统的配置要求进行对等或降配配置，其性能和容量不低于生产处理系统的 60%；
d) 建议采用虚拟机的方式进行部署，对于无法进行虚拟化的应用系统，其备用处理系统可采用传统物理机方式提供，但应提供统一的资源管理平台对虚拟机和物理机进行管理。

5.3.4 备用网络系统要求

服务提供方提供的备用网络系统应满足以下要求：

a) 按照服务需求方的生产网络架构、设备配置、安全策略进行备用网络和安全系统配置；
b) 按照服务需求方的生产网络架构进行网络区域划分和边界安全策略设计；
c) 采用光纤、专线等方式实现灾难恢复中心与服务需求方生产中心之间的高速互连，以满足数据备份、应用切换和统一监控管理要求；
d) 按照部署的应用系统外联交易要求配置灾难恢复中心的外联线路，并能实现与服务需求方生产中心外联线路进行自动切换；
e) 建议采用虚拟化的方式提供备份网络，对于无法进行虚拟化或有安全等级保护要求的应用系统，其备用网络系统可采用传统物理网络方式提供，但应提供统一的资源管理平台对虚拟网络和物理网络进行管理。

5.3.5 灾难恢复服务工具要求

服务提供方提供的灾难恢复服务工具应满足以下要求：

a) 具备对服务需求方的灾难恢复资源进行监控能力，监控范围包括对备用处理资源、存储资源和网络资源等；
b) 具备对服务需求方生产系统到灾难恢复系统的数据备份过程进行监控能力，实时反映数据备份容量、故障、性能等；
c) 具备对服务需求方灾难恢复系统的日常管理能力，包括基准管理、数据验证管理、系统切换与回切管理、预案管理、演练管理等；
d) 具备对服务需求方应急与灾难恢复管理能力，包括应急流程、诊断、处置等；
e) 对于提供云灾备的服务提供方，应提供统一的服务门户，并依据服务需求方应用系统的灾难恢复服务要求进行资源的分配、启动、调整、变更和回收。

5.4 灾难恢复服务团队要求

5.4.1 技能要求

服务提供方的服务团队人员应具备灾难恢复服务经验和专业知识，包括：

a) 从事灾难恢复中心服务的人员，应经过应急与灾难恢复相关培训，熟悉与基础设施相关的应急与灾难恢复操作流程；

b) 从事灾难恢复咨询服务的人员应具备信息安全的基本理论，并对灾难恢复的相关政策、法规和标准有深入地了解，熟悉应用系统的运行特点；

c) 从事灾难恢复系统主机和存储服务的人员应具备主机系统、存储系统和数据备份系统的专业知识和技能，并经过应急与灾难恢复相关培训，熟悉与信息系统相关的应急与灾难恢复操作流程；

d) 从事灾难恢复网络与安全服务的人员应具备网络与安全系统的专业知识和技能，并经过应急与灾难恢复相关培训，熟悉与网络与安全相关的应急与灾难恢复操作流程；

e) 从事灾难恢复系统数据库服务的人员应具备数据库系统专业知识和技能，并经过应急与灾难恢复相关培训，熟悉与数据库系统相关的应急与灾难恢复操作流程；

f) 从事灾难恢复系统运维服务的人员应具备信息系统运维的专业知识和技能，并经过灾难恢复运维管理制度与流程培训，熟悉灾难恢复日常运维和应急管理的操作流程；

g) 从事灾难恢复系统应用软件服务的人员应具备应用软件的维护能力，并经过应急与灾难恢复相关培训，熟悉与应用软件相关的应急与灾难恢复操作流程。

5.4.2 组织架构和编制要求

服务提供方所组建的服务团队应包括服务团队负责人、基础设施服务团队、系统技术支持团队、网络与安全技术支持团队、运维管理团队和运维操作团队等专业服务团队，关键服务岗位应配备主备岗。

各专业服务团队应建立规范的服务流程和制度、良好的沟通协调机制、清晰的责任机制，确保服务的规范性、安全性、有效性。

6 灾难恢复服务过程要求

6.1 灾难恢复服务过程概述

灾难恢复的服务过程包括灾难恢复规划设计、建设实施和运行维护，灾难恢复服务提供方应满足服务需求方在上述服务过程中的灾难恢复服务要求。

6.2 灾难恢复规划设计服务过程要求

6.2.1 规划设计服务内容

灾难恢复规划设计服务包括需求分析服务、灾难恢复资源获取方式分析服务、灾难恢复中心选址分析、灾难恢复目标与策略制定服务、灾难恢复方案设计服务、灾难恢复成本效益评估服务。

6.2.2 需求分析服务过程要求

6.2.2.1 业务影响分析服务过程要求

服务提供方在业务影响分析服务过程中应提供以下服务：

a) 服务提供方应基于服务需求方的业务现状，并参照国家标准和相关行业监管要求，开展业务影

响分析服务工作；

b） 服务提供方应通过对服务需求方业务部门的调研访谈，了解和识别信息系统的业务功能、关联关系，并采用定量或定性的方法分析业务中断对服务需求方造成的财务和非财务影响，确定信息系统灾难恢复指标（恢复时间目标 RTO、恢复点目标 RPO）、灾难恢复优先级别和灾难恢复资源需求。

6.2.2.2 风险评估服务过程要求

服务提供方在风险评估服务过程中应提供以下服务：

a） 服务提供方应依据 GB/T 20984、GB/T 31722—2015 规定的风险评估要求，针对服务需求方的信息资产开展风险评估工作；

b） 服务提供方应通过对服务需求方信息技术部门的调研访谈，识别服务需求方的资产、威胁和脆弱性，并进行赋值；

c） 服务提供方应依据资产价值、威胁和脆弱性赋值，按照科学、成熟的模型计算安全（中断）事件发生的可能性和安全（中断）事件造成的损失，并据此进行风险定级；

d） 依据不同等级的制定风险控制措施和风险处置方案。

6.2.3 灾难恢复资源获取方式分析服务过程要求

服务提供方在灾难恢复资源获取方式分析服务过程中应提供以下服务：

a） 服务提供方应基于服务需求方的灾难恢复需求，并参照国家标准和相关行业监管要求，结合服务需求方的资源配置现状及灾难恢复资源投入情况，对资源获取方式进行分析；

b） 服务提供方应从财务分析、保障能力、效率分析、实践经验、人员要求、技术和资源要求等方面建立分析模型，提出资源获取方式建议；

c） 灾难恢复资源获取方式分析应包括对数据备份系统、备用数据处理系统、备用网络系统、备用基础设施、专业技术支持能力、运行维护管理能力和灾难恢复预案等资源进行分析。

6.2.4 灾难恢复中心选址分析服务过程要求

服务提供方在灾难恢复中心选址分析服务过程中应提供以下服务：

a） 服务提供方应综合分析灾难恢复中心所在城市及区域的自然环境条件、地方配套条件、区域经济环境、专业支持保障能力、政策环境和成本等各方面因素建立选址分析模型和指标体系；

b） 服务提供方应基于服务需求方的资源，本着满足需求、立足发展、绿色节能的原则进行灾难恢复中心的选址分析。

6.2.5 灾难恢复目标与策略制定服务过程要求

灾难恢复目标与策略的制定是依据国家标准，参考相关行业的成熟经验，以及风险分析和业务影响分析的结论，确定各灾难恢复范围、应用系统的灾难恢复等级，并依据应用系统的灾难恢复等级确定灾难恢复技术策略和资源配置策略，为灾难恢复技术方案提供设计依据。灾难恢复目标与策略制定的服务过程要求如下：

a） 服务提供方应从信息系统的重要性、关联性、中断后的业务替代能力等方面确定信息系统灾难恢复范围；

b） 服务提供方应按照 GB/T 20988—2007 的要求，通过与服务需求方管理层及相关业务部门进行充分沟通，结合应用系统的灾难恢复指标，确定灾难恢复范围内各应用系统的灾难恢复等级；

c） 服务提供方应按照 GB/T 20988—2007 中对不同灾难恢复等级的资源要求，确定各应用系统

的灾难恢复技术策略和资源配置策略。

6.2.6 灾难恢复方案设计服务过程要求

6.2.6.1 灾难恢复方案设计服务的内容

灾难恢复方案设计是依据灾难恢复目标和策略的要求，确定灾难恢复建设和运维过程中技术架构、资源配置及管理方案，灾难恢复方案设计服务过程包括灾难恢复技术方案、灾难恢复建设实施方案和灾难恢复运行维护方案等服务过程。

6.2.6.2 灾难恢复技术方案设计服务过程要求

服务提供方在灾难恢复技术方案设计服务过程中应提供以下服务：

a) 依据灾难恢复目标和策略要求，服务提供方应结合服务需求方生产系统的技术架构进行灾难恢复技术架构规划；

b) 服务提供方应站在第三方的立场上，对业界各类灾难恢复技术进行客观评价，并结合服务需求方的灾难恢复技术架构进行灾难恢复技术的适应性分析，为确定灾难恢复技术方案提供依据；

c) 服务提供方应按照灾难恢复技术架构和所选择的技术产品，对灾难恢复技术方案进行详细设计，其内容应包括数据复制、备份和恢复方案、网络与安全方案、服务器（虚拟机）部署方案、存储设备（存储池）配置方案、应用部署与切换方案；

d) 服务提供方应依据灾难恢复技术方案的要求，确定灾难恢复资源配置，包括备用处理资源、存储资源、网络资源、安全资源等设备的配置，各类软件的型号、配置及版本、灾难恢复中心基础设施的资源配置等。

6.2.6.3 灾难恢复建设实施方案设计服务过程要求

服务提供方在灾难恢复建设实施方案设计服务过程中应提供以下服务：

a) 按照服务需求方项目的整体实施规划，服务提供方应制定详细的实施计划，实施计划需明确项目实施的各项工作目标、内容、起始时间、各阶段交付物、实施的人员及需要服务需求方提供的资源；

b) 服务提供方应依据灾难恢复技术方案的要求，组织相关产品的厂商和服务商编写详细的实施方案，实施方案应列出每项实施的内容、步骤和方法；

c) 服务提供方应按照项目实施的要求，起草项目实施文档模板，以确保实施的标准化与规范化。

6.2.6.4 灾难恢复运行维护方案设计服务过程要求

服务提供方在灾难恢复运行维护方案设计服务过程中应提供以下服务：

a) 服务提供方应按照服务需求方灾难恢复系统的特点，进行运行维护方案的设计；

b) 运行维护方案的内容应包括运维组织管理架构设计、运维管理制度和流程体系设计、运维管理文档模板设计等；

c) 为确保运行维护方案具备可操作性，服务提供方应在设计过程中与服务需求方的相关部门进行充分地沟通，了解服务需求方的运维要求，并在文档开发的每个关键环节都应征求服务需求方的意见。

6.2.7 灾难恢复成本效益评估服务过程要求

灾难恢复成本效益评估服务是通过灾难恢复的成本和效益进行科学、客观评估分析，为服务需求方在灾难恢复预算、资源配置及资源获取方式等方面提供依据，灾难恢复成本效益评估服务过程要求

如下：

a) 服务提供方应识别灾难恢复的各类成本，并对灾难恢复的经济效益和社会效益进行综合评估，确定成本效益最佳的资源配置方案和资源获取方式；
b) 服务提供方应明确成本效益评估的目标、范围、数据采集和分析方法、成本效益管理方法；
c) 服务提供方应全面识别灾难恢复的规划成本、设计成本、实施成本、运维成本、废弃成本等多项成本，并按照生命周期方法进行成本计算；
d) 服务提供方应通过科学的经济效益来源分类方法获取可量化的直接经济效益和间接经济效益数据；
e) 服务提供方应通过科学的社会效益分类方法进行社会经济效益、政治效益和社会满足度评价；
f) 服务提供方应依据成本效益评估的结果，确定服务需求方对灾难恢复系统管理的策略，包括投资计划、资源配置方式和资源获取方式等。

6.3 灾难恢复系统建设实施服务过程要求

6.3.1 灾难恢复系统建设实施服务内容

灾难恢复建设实施服务包括灾难恢复系统部署实施、系统验证、灾难恢复预案开发、灾难恢复演练等。

6.3.2 灾难恢复系统部署实施服务过程要求

灾难恢复系统的部署实施应依据灾难恢复系统实施和运维方案的要求，结合产品和解决方案的特点进行实施工作，其工作内容包括生产系统的改造实施、灾难恢复系统的安装调试、设备的网络连接、软件的安装部署、实施前后的系统测试、实施文档开发等，灾难恢复系统部署实施服务过程要求：

a) 服务提供方应在确保服务需求方生产系统和数据安全的情况下进行实施工作，避免对生产系统运行造成影响；
b) 服务提供方应严格按照实施方案的要求进行实施操作和实施文档编写，确保实施的规范性；
c) 服务提供方应做好灾备实施的准备工作，包括场地环境的确认、设备上架安装、关键技术测试、数据备份、系统上电自检等；
d) 服务提供方应在实施过程中避免造成服务需求方系统中断和数据丢失、损坏；
e) 服务提供方应制定实施过程中的应急处置和回退计划；
f) 服务提供方应加强在实施过程中的项目培训和知识转移。

6.3.3 系统验证服务过程要求

灾难恢复系统的验证是对灾难恢复系统部署实施的结果进行验证，验证服务的内容包括生产中心与灾难恢复中心的数据一致性和完整性验证、灾难恢复系统的数据可用性验证、灾难恢复系统的可用性验证、灾难恢复系统的切换与回切验证、外部服务需求方端对灾难恢复系统的访问性能等，灾难恢复系统验证服务过程要求如下：

a) 服务提供方应制定详细的验证测试方案，明确测试验证的目标、范围、工作内容、验证环境要求、验证人员、验证方法和步骤等；
b) 服务提供方应建立独立的系统测试环境，并与生产运行环境及开发环境相隔离，以避免系统验证对服务需求方生产系统正常运行的影响；
c) 服务提供方应按照应用系统运行的特点提供多种测试方式，包括单系统测试、应用组测试、集成测试；
d) 服务提供方应组织相关设备与产品厂商进行系统验证，并详细、如实记录和统计测试过程和结

果数据；

e) 服务提供方应在系统验证测试中出现的问题应协调相关厂商及时解决，对于未达到预期的测试结果，应组织相关厂商找出问题的根源并及时解决，同时对于已解决的问题应再次进行测试验证，直至验证结果达到预期。

6.3.4 灾难恢复预案开发服务过程要求

灾难恢复预案体系应包括两部分，一是总体预案，即服务需求方最高层需要协调执行的预案；二是专项预案，专项预案包括两部分，一是基于场景的专项预案，二是信息系统专项预案。灾难恢复预案开发服务过程要求如下：

a) 服务提供方应建立预案的开发与管理规范，确保预案的开发及运维过程中预案管理的规范性；

b) 所有预案应包括但不限于应急与灾难恢复的组织管理、工作流程（包括灾难切换、回退和重续运行）、处置方法、审核与问责等，同时应将组织架构中各方人员的联系方式作为附件包含在预案文档中；

c) 服务提供方应与服务需求方的最高管理层沟通并确定总体预案的内容，总体预案应得到服务需求方最高管理层的认可后方可颁布实施；

d) 基于灾难场景的专项预案应依据场景的类型与服务需求方相关部门进行沟通确定内容，信息系统专项预案应与服务需求方信息系统主管部门进行沟通确定内容，每套专项预案都应包括配套的切换和维护手册，因此服务提供方应提供手册模板，并协调相关厂商完成手册的开发。

6.3.5 灾难恢复演练服务过程要求

服务提供方在完成灾难恢复系统部署和预案开发后，应进行灾难恢复首次演练，以避免灾难恢复系统的技术缺陷，并验证预案的有效性和可操作性，灾难恢复演练服务过程要求如下：

a) 服务提供方应依据灾难恢复预案的内容，制定详细的演练方案，包括演练场景、范围、内容、计划、流程、方法、演练控制表、演练结果验证标准、文档模板系统等；

b) 服务提供方应对参与演练的人员进行演练培训，明确演练内容、时间要求及各方的职责；

c) 服务提供方应在演练过程中担任主持人，并控制整个演练的过程；

d) 服务提供方应对演练过程进行详细记录；

e) 演练结束后，服务提供方应依据演练过程记录，对演练过程进行回顾，并对结果进行评估；如通过演练发现预案存在问题，应向服务需求方提交预案修订申请，得到服务需求方认可后，依据演练结果对预案进行修订和完善，并更新预案版本。

6.4 灾难恢复运行维护服务过程要求

6.4.1 灾难恢复运行维护服务内容

灾难恢复运行维护服务包括日常运行维护服务和应急与灾难恢复运行维护服务。

6.4.2 日常运行维护服务过程要求

6.4.2.1 日常运行维护服务内容

日常运行维护服务包括灾难恢复系统的物理巡检服务、健康检查服务、监控服务、灾难恢复信息系统资产管理服务、基准管理服务、数据验证服务、系统验证服务、桌面演练服务、模拟切换演练服务、真实切换演练服务和预案维护服务。

6.4.2.2 灾难恢复系统的物理巡检服务过程要求

物理巡检服务是检查承载灾难恢复系统运行的物理设备状态，包括各类指示灯、告警灯等，发现设

备异常立即通知服务需求方，并协调设备厂商及时解决。物理巡检服务过程要求如下：

a) 服务提供方应按照既定的巡检频率，在明确巡检范围和工作内容的前提下对物理设备进行巡检；
b) 服务提供方应建立巡检排班制度，确保各时段均有巡检人员；
c) 巡检人员应按标准的巡检表做好巡检记录；
d) 针对巡检中发现的问题，服务提供方应及时如实通知服务需求方。

6.4.2.3 灾难恢复系统健康检查服务过程要求

为及时发现灾难恢复系统的系统错误，应定期对灾难恢复系统进行健康检查，确保系统的性能和容量满足灾难恢复系统的运行要求。系统健康检查的服务过程要求如下：

a) 服务提供方应按照既定的频率定期对系统进行健康检查；
b) 在服务需求方的授权下，服务提供方应按照服务需求方分配的系统管理员账号登录系统进行健康检查；
c) 服务提供方应针对不同的系统制定标准的系统检查表，并在检查过程中应做好记录，检查结束后应向服务需求方提交系统检查报告；
d) 对于检查过程中发现的系统潜在问题，针对不同的系统及时通知服务需求方，并协助厂商解决问题，避免故障的发生和扩散。

6.4.2.4 系统监控服务过程要求

通过系统监控平台对灾难恢复系统的运行状态进行监控，及时发现灾难恢复系统运行过程中存在的性能和容量问题，系统监控服务过程要求如下：

a) 服务提供方应使用监控工具发现系统的安全性事件，收集并处理来自不同系统的事件和报警信息；
b) 服务提供方应通过对灾难恢复系统资源的监控，尽早发现系统资源的容量瓶颈或者潜在问题；
c) 服务提供方应依据监控平台的功能对灾难恢复中心的信息系统的性能进行实时监控，及时发现潜在的系统性能问题；
d) 服务提供方应通过监控平台的功能对数据复制/备份线路及状态进行实时监控，确保生产中心与灾难恢复中心的数据一致性和完整性。

6.4.2.5 信息系统资产管理服务过程要求

建立生产中心与灾难恢复中心统一的资产配置库，确保资产标识的规范性和唯一性、资产维护的有效性和资产变更的及时性，信息技术资产管理服务过程要求如下：

a) 服务提供方应协助服务需求方梳理灾难恢复中心的信息技术资产，建立资产配置库；
b) 服务提供方应及时响应生产中的资产变更，同步更新灾难恢复中心的资产配置；
c) 服务提供方应协助服务需求方进行资产登记和资产整理。

6.4.2.6 基准管理服务过程要求

为确保灾难恢复系统能够在灾难发生时接管生产系统运行，应建立生产中心与灾难恢复中心的资源配置基准，并进行维护，确保两端基准的一致性和完整性。基准管理服务过程要求如下：

a) 服务提供方应依据信息系统的类型和用途，配合用户梳理各类信息系统的软硬件配置信息，并建立标准规范的基准文件；
b) 服务提供方应协助服务需求方建立基准维护策略，定期进行基准核对，保证灾难恢复系统与生产系统的基准的一致性；
c) 服务提供方应如实、准确、完整地基准变更记录，详细记录变更内容；
d) 服务提供方应定期向服务需求方提交基准信息核对文档，并进行版本控制。

6.4.2.7 数据验证服务过程要求

为确保生产系统与灾难恢复系统业务数据的一致性、完整性和可用性，应定期进行数据验证工作。数据验证服务过程要求如下：

a) 服务提供方应依据数据复制/备份技术要求，制定数据验证方案，包括数据验证策略、验证工具、验证周期和验证标准；
b) 服务提供方应协助服务需求方搭建数据验证环境，并检查数据备份环境和链路。

6.4.2.8 系统验证服务过程要求

为确保灾难恢复系统能接管生产系统运行，应定期进行系统验证工作。系统验证服务过程要求如下：

a) 服务提供方应制定详细的系统验证方案，明确验证范围、验证计划、验证环境、验证方法和验证标准等；
b) 服务提供方应协助服务需求方搭建系统验证环境，并检查灾难恢复系统运行的软硬件环境和系统切换链路。

6.4.2.9 桌面演练服务过程要求

为确保服务需求方的相关人员了解灾难恢复预案的内容和职责，应通过桌面推演的方式对预案中的灾难恢复流程进行培训和演练。桌面演练服务过程要求如下：

a) 服务提供方应基于灾难恢复预案，编写桌面演练文档，包括：桌面演练方案、演练培训材料、演练流程控制表、演练流程及责任机制、演练职责说明等；
b) 服务提供方应委派灾难恢复方面的专家作为桌面推演的主持人，控制演练的流程，指导演练工作开展；
c) 服务提供方应委派专人对桌面演练过程进行全程记录，并进行分析和评估；
d) 服务提供方应结合演练过程中存在的问题，形成桌面演练总结报告及预案修订意见。

6.4.2.10 模拟切换演练服务过程要求

为确保信息系统切换技术满足灾难恢复预案要求和应用系统的灾难恢复指标，应通过模拟切换演练的方式对预案中的灾难恢复技术进行验证。模拟切换演练服务过程要求如下：

a) 服务提供方应基于灾难恢复预案，制定详细的模拟切换演练方案，包括切换步骤、系统切换技术、数据复制技术、业务验证方式等；
b) 服务提供方应协助服务需求方准备演练数据，并在演练结束后删除演练数据；
c) 服务提供方应依据服务需求方业务部门的业务验证案例及相关要求，进行业务验证；
d) 服务提供方应委派专人主持演练，并对切换演练过程中进行详细记录，对演练结果进行分析和评估。

6.4.2.11 真实切换演练服务过程要求

在桌面演练和模拟切换演练的基础上，基于特定的灾难场景，按照场景预案中的流程要求，进行真实切换演练，真实切换演练时将服务需求方的部分或全部应用系统切换到灾难恢复中心运行一段时间，验证灾难恢复系统是否可以接替生产系统运行，然后再将灾难恢复系统回切到生产系统，并退回到切换前的状态。真实切换演练服务过程要求如下：

a) 服务提供方应基于灾难恢复预案，编制真实切换演练文档，包括演练的场景分析、灾备环境分析、演练计划、演练流程、演练组织管理、演练技术方案、演练操作手册等；
b) 服务提供方应在真实切换演练前对参演人员进行动员和培训，确保演练人员明确各自职责和整个演练流程；

c) 服务提供方应协助服务需求方对灾难恢复系统的运行状态和资源进行确认，保证灾难恢复系统能继续支撑业务系统运行；
d) 服务提供方应委派专人主持演练，并对切换演练过程中进行详细记录，对演练结果进行分析和评估。

6.4.2.12 预案维护服务过程要求

针对演练发现预案中的问题以及系统变更对预案修订的要求，需要对预案进行及时修订和完善，采用生命周期管理方法进行预案维护工作，预案维护服务过程要求如下：

a) 服务提供方应协助服务需求方建立灾难恢复预案管理制度和流程，对预案的开发、版本控制、修订、审批、颁发、归档、废止、销毁进行全过程规范化管理；
b) 服务提供方应建立预案标识规范，对所有预案文档进行分类管理。

6.4.3 应急与灾难恢复服务过程要求

6.4.3.1 应急与灾难恢复服务内容

应急与灾难恢复服务是在灾难发生时，服务提供方按照预定的应急流程，并在接到服务需求方的切换指令后接管启用灾难恢复系统，并接管生产系统运行，并当生产系统修复后，进行灾难回切，恢复到灾难发生前的状态的全部服务活动。

应急与灾难恢复服务包括突发事件的发现与初始响应、灾难恢复启动、灾难恢复切换实施服务、灾难恢复系统回切与生产系统重续运行服务、灾难恢复工作总结等服务活动。

6.4.3.2 突发事件的发现与初始响应服务过程要求

服务提供方应依据 GB/T 20985.1 规定的事件管理要求对突发事件进行管理，事件发现和初始响应的主要目标是及时发现危害信息系统正常运行的突发事件，及时评估、判断和确定突发事件性质和级别，并根据预定策略启动日常事件处理流程或应急响应预案，及时进行抢修和抢救工作，使事件影响降到最低。突发事件的发现与初始响应服务过程要求如下：

a) 服务提供方应协助服务需求方根据突发事件的影响范围、持续时间和事件性质等因素判断灾难事件的等级，并按照不同等级的通知流程及时上报；
b) 服务提供方应按照场景预案的要求，对灾难事件进行初始响应；
c) 服务提供方应检查灾难恢复系统的运行状态，确保灾难恢复系统具备接管生产运行的条件。

6.4.3.3 灾难恢复启动服务过程要求

服务提供方在灾难恢复启动服务过程中应提供以下服务：

a) 服务提供方应提供灾难恢复中心数据验证和系统验证服务；
b) 服务提供方应通知服务需求方协调相关业务部门进行业务数据备份，避免操作过程中造成业务数据丢失或损坏；
c) 服务提供方应对各类灾备技术等进行验证，避免灾难恢复过程出现技术缺陷；
d) 服务提供方应检查灾难恢复中心的广域网线路连通性和端口流量；
e) 对于检查和验证过程中发现的问题应及时上报；
f) 启动灾难恢复程序。

6.4.3.4 灾难恢复切换实施服务过程要求

服务提供方在灾难恢复系统切换实施服务过程中应提供以下服务：

a) 服务提供方应按照恢复预案或实施方案中的流程和步骤实施灾难恢复操作；
b) 服务提供方应委派专人实施灾难恢复，确保实施过程中的故障得到及时解决；

c) 当灾难恢复启动失败，并需要回退流程时，服务提供方应先组织业务部门进行回退的业务验证，确保业务已回退到系统实施前的状态，再进行系统回退操作，回退操作完成后编写系统回退实施总结报告，详细描述系统回退手段和回退结果；

d) 灾难恢复完成后，服务提供方应编写灾难恢复实施报告，详细记录实施的过程、处理手段和操作结果。

6.4.3.5 灾难恢复系统回切与生产系统重续运行服务过程要求

服务提供方在灾难恢复系统回切与生产系统重续运行服务过程中应提供以下服务：

a) 服务提供方应在灾难恢复数据与生产数据一致的前提下，组织相关厂商完成系统回切工作；

b) 服务提供方应验证系统回切后的数据一致性和完整性；

c) 服务提供方应启动生产系统，并重新建立数据复制/备份环境；

d) 在验证生产中心运行正常后，服务提供方应按照灾难恢复实施预案及策略要求，将系统回切至生产中心。

6.4.3.6 灾难恢复工作总结服务过程要求

服务提供方在灾难恢复工作总结服务过程中应提供以下服务：

a) 服务提供方应整理并归档灾难恢复过程记录，客观、务实地编写灾难恢复总结报告；

b) 服务提供方应提出预案修订意见，完善预案的内容，并进行预案版本更新。

6.4.4 灾难恢复能力持续改进服务过程要求

为确保服务需求方的灾难恢复能力得到不断提升，服务提供方应在运行维护服务过程中为服务需求方提供灾难恢复服务能力评估，并能依据服务需求方的信息系统和信息技术架构变化进行定期评估，以确保服务需求方的灾难恢复系统得以持续改进，灾难恢复能力持续改进服务过程要求如下：

a) 服务提供方应每年对服务需求方的灾难恢复系统进行能力评估，找出技术和管理的脆弱点，并提出改进建议；

b) 服务提供方应按照生命周期法对灾难恢复系统规划设计、建设实施和运行维护各个阶段进行评估，发现问题，并提出解决方案；

c) 服务提供方应建立规范标准的评估模型和指标体系，并依据信息系统的灾难恢复需求建立评估基线，对现有灾难恢复系统进行差距评估；

d) 服务提供方应针对灾难恢复系统存在的问题，并依据问题发生时对服务需求方信息系统造成的潜在影响（影响范围和影响程度），确定解决问题的紧迫性和时效性。

7 灾难恢复服务项目组织管理要求

7.1 项目组织管理内容

灾难恢复服务项目组织管理包括质量管理、管理配置、风险管理、项目规划、项目监控、系统工程支持环境管理、技能与知识提升服务、保密要求、与供应商协调等。

7.2 项目质量管理要求

7.2.1 项目质量管理内容

为确保灾难恢复服务满足服务需求方信息系统的灾难恢复需求，服务提供方应加强对服务各阶段的质量审核和控制，项目质量管理的内容包括服务交付物的质量审核、服务过程的质量监督和质量问题的分析与纠正。

7.2.2 服务交付物的质量审核

服务提供方的质量审核人员应对服务过程中向服务需求方提供的所有交付物进行质量审核，使其满足服务需求方的服务要求，服务交付物质量审核要求如下：

a) 审核规划设计阶段的系统调研及需求分析文档，以确保文档能真实反映服务需求方的系统现状和灾难恢复要求；
b) 审核规划设计阶段的系统规划和设计方案，避免方案存在技术缺陷，确保方案满足服务需求方的信息系统灾难恢复指标，并具备可实施性和可操作性；
c) 审核规划设计阶段的实施和运维方案，避免方案存在技术和管理缺陷，确保实施和运维方案符合系统规划设计要求；
d) 审核建设实施阶段的各类文档，检查建设实施管理的规范性和实施目标的可达性；
e) 审核运行维护阶段的各类文档，检查运行维护管理的规范性和运维目标的可达性。

7.2.3 服务过程的质量监督

服务提供方的质量审核人员应依据服务内容和服务计划的要求，通过内部评审的方式在服务各阶段里程碑交付前对该阶段的服务过程进行回顾和审核，服务过程的质量监督要求如下：

a) 对服务计划的合理性进行评估，及时调整影响服务计划和服务资源，确保服务能按计划完成；
b) 对服务流程的可操作性进行审核，及时调整和优化服务流程，确保服务的交付能做到规范管理、责任到人；
c) 对服务各阶段的技术实施方法进行审核，及时调整和优化实施方案，提高服务交付质量。

7.2.4 质量问题分析与纠正

服务提供方的质量审核人员对审核过程中发现的问题，应及时上报项目经理，重大质量问题应上报服务需求方的主管人员，共同对质量问题进行分析评估，并提出纠正和改进措施，避免问题的扩散。服务质量问题的分析与纠正要求如下：

a) 对质量问题进行分析，找出导出质量问题的根源和责任人；
b) 制定质量问题纠正和改进方案，并进行内部评审，以降低改进方案实施的风险；
c) 制定质量改进实施计划，明确实施的时间、所需的资源和实施目标。

7.3 项目的管理配置要求

7.3.1 项目管理配置内容

为确保灾难恢复服务资源满足服务需求方信息系统灾难恢复的资源需求，服务提供方应加强对服务资源配置的管理，项目管理配置的内容包括建立服务资源配置基线、服务资源配置基线维护和服务配置管控。

7.3.2 服务资源配置基线要求

服务提供方的项目经理应依据灾难恢复服务的内容确定服务资源的配置基线，配置基线应明确满足服务质量和服务水平要求的资源配置，包括灾难恢复中心场地、灾难恢复系统、服务团队和服务工具等。服务资源配置基线要求如下：

a) 服务资源配置基线应为满足灾难恢复服务质量和服务水平要求的量化配置单元的组合，配置单元应为满足某项服务要求的完整、独立的资源配置；
b) 每个配置单元应依据该项服务需求进行合理配置，既要满足服务要求，也要避免资源浪费；
c) 配置单元应包括确保服务质量和服务水平要求的场地资源、系统资源和人力资源。

7.3.3 服务资源配置基线维护要求

服务提供方的项目经理应制定专人维护服务资源配置基线，依据服务需求的变化，对基线内的配置单元进行增加或删除，以保证配置基线不断适应服务需求的变化。服务资源配置基线维护要求如下：

a) 服务提供方应与服务需求方共同协商确定服务资源配置基线，明确基线中各配置单元的配置项；
b) 服务提供方应依据服务需求的变化通过增加或删除基线内的配置单元进行配置基线的修改和完善，使其适应服务需求的变化；
c) 服务提供方应定期跟踪和监视配置基线对服务需求的满足程度，并及时调整配置基线；
d) 服务提供方应根据配置基线的调整方案及时对服务资源进行调整，确保其满足服务需求。

7.3.4 服务资源配置管控要求

服务提供方的项目经理应定期组织评估配置基线修改方案实施的可行性和风险，缩小服务配置修改对服务质量和服务水平造成的影响。服务资源配置管控要求如下：

a) 服务提供方应依据服务需求的变化向服务需求方提供配置基线修改建议，明确基线修改方案和服务资源配置调整的可行性和风险，得到服务需求方认可后方可进行配置调整；
b) 配置调整实施过程中应严格控制调整实施对现有服务质量、进度和服务水平的影响；
c) 配置调整实施后需经过服务需求方确认后方可确定新的配置基线。

7.4 项目风险管理要求

7.4.1 项目风险管理内容

为控制灾难恢复服务项目风险，服务提供方应对持续 6 个月以上的服务项目进行风险评估，并提出管控建议，以降低服务项目风险，项目风险管理的内容包括风险识别与评估、制定和实施风险管控计划和跟踪风险管控实施效果。

7.4.2 风险识别与评估要求

服务提供方应充分识别项目服务风险，并对风险发生对服务需求方造成的影响进行充分评估，以便制定有效的风险防范措施。风险识别与评估要求如下：

a) 服务提供方应从技术风险和管理风险两个角度识别服务项目风险，其中技术风险包括所采用的技术和工具对原有环境的影响、技术可行性和成熟性、技术实施的难度、技术实施对现有系统造成的潜在影响等；管理风险包括其他参与方的协调配合、服务团队的技能、服务团队的稳定性对项目计划和服务质量的影响等；
b) 服务提供方应对项目风险造成的影响范围和程度进行充分评估，并进行风险等级划分，以便制定差异化的风险管控措施；
c) 服务提供方应依据技术脆弱性和管理脆弱性发生的频率，结合脆弱性发生对项目影响的范围和程度确定风险等级。

7.4.3 风险管控计划要求

服务提供方应依据风险等级要求，制定差异化的管控计划，确保风险处置按计划执行。风险管控计划要求如下：

a) 风险管控计划应明确各类风险处置的及时性和紧迫性，以控制风险影响程度和范围，风险处置的紧迫程度从高到低应包括立即处置、在不影响系统正常运行的情况下处置、密切观察暂不处置等；
b) 风险管控计划应明确各类风险的处置策略和技术方案，并对技术方案的可行性进行评估；

c) 风险管控计划应明确各类风险处置所需的资源，包括场地资源、设备资源、软件资源和人力资源；
d) 风险管控计划应得到服务需求方认可后方可实施。

7.4.4 风险管控跟踪要求

服务提供方应实时跟踪风险处置策略执行的效果，并定期评估风险处置方案实施后的残余风险，及时采取有效措施控制风险的蔓延。风险管控跟踪要求如下：

a) 服务提供方应在风险处置方案实施后评估风险处置是否达到预期效果，对于未到达预期效果的处置方案应及时修改和调整；
b) 服务提供方应对风险处置方案实施后的残余风险进行评估，及时采取有效措施控制风险蔓延，包括风险规避和风险转移；
c) 上述风险评估方案和风险管控措施应及时服务需求方进行沟通汇报。

7.5 项目规划要求

7.5.1 项目规划内容

项目规划是服务提供方制定的项目服务计划和技术规划，内容包括项目计划、技术规划、资源投入与费用预算，以及项目跟踪与监控计划等。项目规划要求包括项目计划管理要求和项目计划规划要求。

7.5.2 项目计划管理要求

服务提供方应按照服务需求方的服务要求和工作内容制定项目计划，落实项目计划、任务分配、所需的关键资源及费用等。项目计划管理要求如下：

a) 服务提供方应为服务需求方制定详细的项目计划管理方案，明确服务目标和范围、项目计划、关键资源、质量标准、测试验收及费用预算等；
b) 项目计划应明确项目的阶段划分，并制定各阶段的时间计划和里程碑；
c) 服务提供方应明确项目各阶段的服务目标、范围、工作任务、责任机制和交付物，并与时间计划相对应；
d) 服务提供方应按照项目的时间计划要求，明确服务所需的资源的到位时间、期限和组织管理方式；
e) 服务提供方应依据项目各时间点的资源投入计划，提出项目所需的费用。

7.5.3 项目技术规划要求

服务提供方应按照项目计划管理方案的要求制定项目技术规划方案，明确项目各阶段的关键技术、实施方法和流程。项目技术规划要求如下：

a) 服务提供方应为服务需求方制定详细的项目技术规划方案，明确项目各阶段的技术架构、产品与解决方案，以及实施方法和步骤等；
b) 项目技术规划方案应通过服务需求方组织的专家评审后方可实施；
c) 针对技术规划方案中的关键技术，服务提供方应组织产品和解决方案厂商进行技术测试，确保实施过程中无技术缺陷；
d) 服务提供方应对服务需求方进行技术实施方案培训，包括技术指标、实施与测试的方法和步骤等。

7.6 项目监控要求

7.6.1 项目监控概述

项目监控是服务提供方按照灾难恢复的服务需求，通过检查、监督的方式，确保项目执行过程满足

项目规划的要求，并对服务过程中发生的严重偏差进行及时修正。项目监控要求包括项目的监督要求、问题分析与修正要求。

7.6.2 项目监督要求

服务提供方应在项目实施过程中进行跟踪监督，发现不符合进度要求的问题应及时查明原因，提出解决方案，并向服务需求方汇报，项目监督要求包括：

a) 服务提供方的项目经理应定期组织内部项目评审会，审核项目服务偏差、存在的问题，并提出改进计划和建议；

b) 服务提供方应定期监督项目实施进度，检查项目完成情况与项目计划的偏差，如发现任务完成滞后于项目计划，应及时查明原因，并提出解决方案，减少整体实施进度的偏差；

c) 服务提供方应定期检查项目实施质量，分析项目实施质量与项目质量计划的偏差，提出改进建议并实施，避免后期项目存在质量问题。

7.6.3 问题分析与修正要求

服务提供方应针对项目监督检查结果中的问题，提出修正、调整和优化建议，如需要变更服务计划，则应及时通报服务需求方。问题分析与修正要求包括：

a) 针对项目进度拖延问题，服务提供方应分析项目滞后的原因，提出解决方案。如因产品质量和服务问题导致的项目滞后，服务提供方应及时与产品厂商协商解决；如因服务资源问题导致的项目滞后，服务提供方应及时补充相关资源；如因服务需求方的原因导致的项目滞后，服务提供方应与服务需求方协商调整项目服务计划。

b) 针对项目质量问题，服务提供方应分析产生质量问题的原因，提出技术优化建议。如因产品质量和服务问题导致的项目质量问题，服务提供方应及时与产品厂商协商更换产品；如因服务资源问题导致的项目滞后，服务提供方应及时调整相关资源；如需调整服务计划，则应与服务需求方协商解决。

7.7 系统工程支持环境管理要求

7.7.1 系统工程支持环境管理内容

作为灾难恢复服务的辅助手段，服务提供方可在服务过程中改进系统工程支持环境，以提升服务效率和质量，系统工程支持环境包括计算机、通信、测试工具、软件工具等，加强对系统工程支持环境的管理有助于提升服务提供方的管理能力、技术水平、工作效率和服务安全性。系统工程支持环境管理要求包括系统工程支持环境的确认和系统工程支持环境的获取与维护。

7.7.2 系统工程支持环境的确认

为确保服务的安全性，服务提供方所使用的支持环境应得到服务需求方的确认后方可使用，服务提供方应对其提供的系统工程支持环境做出如下承诺：

a) 系统工程支持环境能满足或促进服务的交付进度和质量；

b) 系统工程支持环境不会导致服务需求方的数据丢失、损坏，不会造成信息安全问题；

c) 系统工程支持环境不会对服务需求方的信息系统运行造成影响；

d) 系统工程支持环境不会导致服务需求方的信息系统性能突降；

e) 系统工程支持环境的使用不会改变服务需求方的灾备系统技术架构。

7.7.3 系统工程支持环境的获取与维护

系统工程支持环境得到确认后，服务提供方应对其提供如下维护服务：

a) 首次用于灾难恢复服务或系统工程支持环境版本升级时，应通过服务需求方组织的测试；

b） 服务提供方有责任对服务需求方提供系统工程支持环境的使用培训；
c） 当系统工程支持环境出现问题时，服务提供方应及时更换或对其进行优化和改进。

7.8 技能与知识提升服务要求

7.8.1 技能与知识提升服务内容

为确保服务需求方能够全面、系统地了解和掌握灾难恢复相关知识，应在灾难恢复项目的规划、实施和运维阶段对服务需求方的管理人员、业务人员和信息技术人员进行有针对性的培训，培训的内容应包括但不限于灾难恢复基础知识培训、灾难恢复技术培训、灾难恢复实施培训、灾难恢复预案管理培训、灾难恢复运维管理制度培训和灾难恢复演练培训，从事灾难恢复培训的服务提供方应准备全面的培训课程和教材，并安排资深的培训讲师为服务需求方提供培训。技能与知识提升服务要求包括培训讲师要求和培训内容要求两部分。

7.8.2 培训讲师要求

服务提供方的培训讲师应具备以下条件：
a） 对灾难恢复国家标准和相关行业监管要求有深入地理解；
b） 具备灾难恢复相关知识和技术；
c） 具备至少 5 年的灾难恢复服务过程管理工作经历；
d） 参与过至少 3 个大型服务需求方（如金融、政府、企业）灾难恢复服务项目（如咨询、实施、运维）。

7.8.3 培训内容要求

7.8.3.1 灾难恢复培训内容

服务提供方提供的课程应系统全面地反映服务需求方的灾难恢复服务内容，涵盖灾难恢复的规划设计、建设实施和运维管理各个方面，内容涉及灾难恢复基础知识、灾难恢复技术、灾难恢复实施、灾难恢复预案管理、灾难恢复运维管理、灾难恢复演练等。

7.8.3.2 灾难恢复基础知识培训要求

服务提供方的灾难恢复基础知识培训应包括以下内容：
a） 信息技术基础架构风险评估培训；
b） 业务影响分析培训；
c） 灾难恢复目标与策略的制定培训；
d） 灾难恢复技术架构和实施方法培训；
e） 灾难恢复运维管理体系架构培训。

7.8.3.3 灾难恢复技术培训要求

服务提供方的灾难恢复技术培训应包括以下内容：
a） 灾难恢复技术架构分析；
b） 灾难恢复技术产品与解决方案培训；
c） 灾难恢复技术与产品选型培训；
d） 灾难恢复关键技术测试方法培训；
e） 灾难恢复资源配置方法培训。

7.8.3.4 灾难恢复实施培训要求

服务提供方的灾难恢复实施培训应包括以下内容：

a) 灾难恢复实施方案内容培训；
b) 灾难恢复实施文档规范培训；
c) 灾难恢复实施流程和方法培训；
d) 灾难恢复实施管理方法培训；
e) 首次灾难恢复演练培训。

7.8.3.5 灾难恢复预案管理培训

服务提供方的灾难恢复预案管理培训应包括以下内容：

a) 灾难恢复预案体系框架培训；
b) 灾难恢复预案开发与维护规范培训；
c) 灾难恢复预案内容培训；
d) 灾难恢复切换手册模板培训。

7.8.3.6 灾难恢复运维管理制度培训

服务提供方的灾难恢复运维管理制度培训应包括以下内容：

a) 灾难恢复运维管理制度框架培训；
b) 灾难恢复运维管理制度内容培训；
c) 灾难恢复运维组织管理培训；
d) 灾难恢复运维文档开发培训。

7.8.3.7 灾难恢复演练培训

服务提供方的灾难恢复演练培训应包括以下内容：

a) 灾难恢复演练基础培训；
b) 灾难恢复演练流程培训；
c) 灾难恢复演练组织管理培训；
d) 灾难恢复演练文档开发培训。

7.9 灾难恢复服务保密要求

服务提供方应履行灾难恢复服务保密职责，并满足服务需求方的保密要求。包括但不限于以下内容：

a) 应建立并执行与灾难恢复服务相关的保密管理制度和流程；
b) 参与灾难恢复服务的人员应与灾难恢复服务需求方签订保密协议，并定期对保密协议的执行情况进行监督和检查；
c) 未经服务需求方允许，服务提供方不得向第三方披露与服务协议相关的敏感信息；
d) 未经服务需求方允许，服务提供方不得转卖、转租、转借服务工作环境中的可移动设备、介质、资料。

7.10 与供应商协调要求

7.10.1 供应商管理概述

服务提供方应根据服务需求方的灾难恢复要求，选择安全、可靠、适用的产品（包括用于灾难恢复的

硬件、软件和服务)供应商,同时服务提供方还应在服务过程中加强与产品供应商的协调与配合,共同满足服务需求方的灾难恢复服务要求。供应商协调要求包括供应商的选择、产品的采购。

7.10.2 供应商选择

服务提供方在灾难恢复服务过程选择产品供应商时应要求:

a) 供应商提供的产品具有服务需求方相类似的成功案例;
b) 供应商具有良好的财务状况和资信,能够按服务需求方的要求提供长期、稳定的产品;
c) 供应商提供的产品通过相关组织的安全认证;
d) 供应商提供的产品满足服务需求方所属行业的准入要求。

7.10.3 产品的采购

服务提供方根据服务需求方的灾难恢复要求,进行灾难恢复系统所需的产品采购时,应:

a) 判定采购的产品所采用的技术满足灾难恢复技术架构的要求;
b) 判定采购的产品配置满足灾难恢复系统的运行要求;
c) 判定采购的产品满足灾难恢复系统的运行维护要求;
d) 判定采购的产品满足灾难恢复服务的要求。

参 考 文 献

[1] GB/T 22080—2016 信息技术 安全技术 信息安全管理体系 要求(ISO 27001:2013,IDT)

[2] GB/T 29246—2017 信息技术 安全技术 信息安全管理体系 概述和词汇(ISO 27000:2016,IDT)

[3] GB/T 30146—2013 公共安全 业务连续性管理体系 要求(ISO 22301:2012,IDT)

[4] GB/T 31168—2014 信息安全技术 云计算服务安全能力要求

[5] ISO/IEC 20000:2011 Information technology—Service management—Requirements

[6] ISO/IEC 20243:2015 Information technology—Open Trusted Technology Provider Standard (O-TTPS)—Mitigating maliciously tainted and counterfeit products

[7] SS 507:2008 SINGAPORE STANDARD FOR Business continuity/disaster recovery (BC/DR) service providers

[8] NIST SP 800-34 Contingency Planning Guide for Information Technology System

[9] Professional Practices for Business Continuity Planners,DRI International

[10] Business Continuity Glossary,DRI International