ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 31500—2024
代替 GB/T 31500—2015

网络安全技术　存储介质数据恢复服务安全规范

Cybersecurity technology—Security specification of data recovery service for storage media

2024-10-26 发布　　2025-05-01 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

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 31500—2015《信息安全技术　存储介质数据恢复服务要求》，与GB/T 31500—2015相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 更改了文件的适用范围（见第1章，2015年版的第1章）；
b) 增加了“逻辑故障”“镜像数据”“数据恢复服务”等术语和定义，更改了“存储介质”的术语和定义（见第3章）；
c) 更改了“保密性原则”的相关要求，增加了“合规原则”和“分级原则”条款（见第4章，2015年版的第4章）；
d) 增加了总体要求（见第5章）；
e) 更改了从业机构的相关要求，将要求进一步划分为两类，并对应细化了条款（见6.1，2015年版的5.1）；
f) 更改了从业人员的相关要求，将要求进一步划分为两类，并对应细化了条款（见6.2，2015年版的5.2）；
g) 更改了“环境”的相关要求，细化了服务场所、设施设备、储存介质的相关条款（见6.3，2015年版的5.3、5.4、7.3、7.4）；
h) 增加了“质量控制”要求（见6.4）；
i) 增加了“安全审计”要求（见6.5）；
j) 更改了“安全实施要求”的相关要求，将“服务过程要求”改为“安全实施要求”（见第7章、2015年版的第6章）；
k) 增加了“安全管理评价方法”，描述了第6章安全管理要求的评价方法（见第8章）；
l) 增加了“安全实施评价方法”，描述了第7章安全实施要求的评价方法（见第9章）；
m) 增加了规范性附录A（见附录A）。

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：国家信息中心、联想（北京）有限公司、中国科学院信息工程研究所、司法鉴定科学研究院、中国电子技术标准化研究院、中电长城网际系统应用有限公司、北京源堡科技有限公司、云领信息技术（天津）有限公司。

本文件主要起草人：王笑强、王佳慧、魏连、张羽、朱雪峰、李汝鑫、冯维淼、郭弘、闵京华、高亚楠、李冉、赵晓乐、王晓振、梁露露、弥宝鑫、刘祎然、王庆德、杨绍亮、李岩、赵榛、贾成罡、刘俊。

本文件及其所代替文件的历次版本发布情况为：

——2015年首次发布为GB/T 31500—2015；
——本次为第一次修订。

网络安全技术　存储介质数据恢复服务安全规范

1　范围

本文件确立了存储介质数据恢复服务的安全原则、规定了安全管理要求和安全实施要求，描述了满足安全管理要求和安全实施要求的评价方法。

本文件适用于指导存储介质数据恢复服务机构针对非涉及国家秘密的数据恢复服务的实施和管理、存储介质数据恢复服务机构的自评价和第三方监督评审，以及存储服务使用单位采购数据恢复服务的评价。

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 25069—2022　信息安全技术　术语

GB/T 42446—2023　信息安全技术　网络安全从业人员能力一般要求

GB 50073　洁净厂房设计规范

GB 50174　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

电子数据　electronic data

基于计算机应用和通信等电子化技术手段形成的客观资料，用以表示文字、图形符号、多媒体等信息。

注：电子数据包括以电子形式存储、处理或传输的静态数据和动态数据。

3.2

存储介质　storage medium

存储媒体

承载电子数据（3.1）的各类载体或设备，包括但不限于计算机硬盘、磁带、软盘、光盘、各种形式的存储卡、存储芯片等。

［来源：GB/T 25069—2022，3.94，有修改］

3.3

数据恢复　data recovery

通过专门的计算机软硬件技术，再生成（复原）存储介质（3.2）内已经丢失或被破坏的电子数据（3.1）的过程。

3.4

数据恢复服务　data recovery service

利用数据恢复技术开展数据恢复的经营活动。

3.5

镜像生成　imaging generation

通过逐比特复制，获得与被复制数据完全一致的电子数据(3.1)的过程。

3.6

镜像数据　mirror data

镜像生成(3.5)产生的数据。

3.7

硬件故障　physical fault

由于存储介质(3.2)硬件损坏而造成数据无法访问的故障。

注：一般是指电路故障、机械故障、固件故障等。

3.8

逻辑故障　logical damage

由于存储介质(3.2)中数据损坏而造成用户数据无法访问的故障。

注：一般是指操作系统故障、应用程序故障、用户误操作、计算机病毒破坏等。

3.9

开盘修复　interior disk repairing

打开存储介质盘体或拆取存储芯片，修复存储介质(3.2)硬件故障(3.7)的操作。

3.10

数据销毁　data destruction

使用数据覆盖、介质消磁、硬件破坏等技术手段，清除存储介质(3.2)上部分或全部数据的操作。

3.11

写保护　write protect

保证存储介质(3.2)中电子数据(3.1)无法被修改的防护措施。

3.12

远程数据恢复　remote data recovery

通过网络实现的数据恢复服务(3.4)方式。

4　原则

实施存储介质数据恢复服务遵循如下基本安全原则：

a)　合规原则：符合涉及数据恢复的法律法规和标准；

b)　可用性原则：恢复的数据可被授权用户正确访问和使用；

c)　保密性原则：服务过程中用户的个人信息及存储介质中的数据不被非授权个人、实体处理，核心岗位至少 2 名人员同时参与；

d)　完整性原则：数据恢复过程中确保用户送修存储介质中的数据不被更改；

e)　可审计原则：确保数据恢复服务实施各流程的操作可追溯；

f)　分级原则：数据恢复服务机构根据数据恢复服务需求方要求提供分级服务。

5 总体要求

存储介质数据恢复服务是数据处理的一种特殊形式，是网络安全保障的重要环节。存储介质数据恢复服务机构向存储介质数据恢复服务需求方提供存储介质数据恢复服务，应满足第6章的要求，存储介质数据恢复服务机构向对存储介质数据恢复服务有更高安全要求的服务需求方（如党政机关、大型机构、关键信息基础设施运营者等）提供存储介质数据恢复服务时，还应满足第7章的要求。

6 安全管理要求

6.1 机构

6.1.1 一般要求

从业机构一般要求如下：

a） 应具备合法经营资格，具备依法缴纳税收的良好记录；
b） 法定代表人、董事、合伙人以及高层管理人员应无犯罪行为记录且未被列入失信被执行人；
c） 应具备与开展数据恢复业务相匹配的专业技术团队；
d） 应具备保护用户数据安全、防止数据泄露的防护措施。

6.1.2 增强要求

从业机构增强要求如下：

a） 应是在中华人民共和国境内依法成立1年以上的法人；
b） 应设立数据安全管理机构，协调配置必要的人力、物力、资金等资源保障用户数据安全；
c） 数据安全管理机构负责人应由从业机构最高负责人担任，成员应包括机构高层管理人员和业务负责人，将负责人和工作职责描述记录在文档之中，并向全机构进行通告；
d） 应建立业务全流程数据安全权限管理制度，进行必要的职责分离以防止对恢复数据未经授权的访问和数据泄露，必要时关键核心岗位应配置至少2人同时操作；
e） 应建立数据安全应急处置和报告机制，发生数据安全事件时及时启动应急响应机制，采取措施防止危害扩大，消除安全隐患，并记录处置过程，包括人员、时间、对象、方式等关键信息；
f） 应提高数据安全意识，制定业务培训制度，包括，开展安全意识教育和培训，为所有员工（包括管理层）制定并实施培训计划，定期对相关人员进行安全意识培训、技术培训和技能考核，并对过程和结果进行记录；
g） 定期开展数据安全各项管理制度执行情况的内部监督检查、评审和改进。

6.2 人员

6.2.1 一般要求

从业人员一般要求如下：

a） 应配合机构对拟任职人员进行的信息网络犯罪记录调查和信用调查；
b） 应配合机构对拟任职人员的任职审查和任职资格确认；
c） 应遵守机构制定的从业人员管理制度，如关键岗位人员签订保密协议，说明与职位和安全相关的要求及其责任，说明接触用户数据人员的保密义务和要求，并为任职人员分配唯一的身份标识，定期进行尽职考核并进行奖惩；
d） 应与从业机构签署劳动合同，无历史违规行为或事件的声明、相关离职要求等文件和声明；

e) 应具有良好的计算机应用知识，熟悉计算机系统结构、数据存储原理等专业知识；
f) 应具备 2 年以上数据安全服务项目经验，熟悉数据安全基本知识，如数据安全基本概念、数据安全技术、数据安全保障等，具备 GB/T 42446—2023 中 K01-001，K01-002、K01-003、K01-004、K01-005、K03、K10-003 所要求知识和 S01、S02-02-002、S02-17-002 中技能；
g) 实施存储介质逻辑故障恢复的技术人员应掌握各种应用操作系统、文件系统的基础理论知识和相关软件和设备使用方法，具有处理逻辑故障的能力；
h) 实施存储介质硬件故障恢复的技术人员应掌握各类集成电路、硬盘结构、存储芯片的基础理论知识和相关软件和设备使用方法，具有处理硬件故障的能力。

6.2.2 增强要求

从业人员增强要求如下：
a) 应建立临时人员（包含短期工作人员或第三方合作人员）职责文档，应明确短期工作人员或第三方合作人员（例如代岗人员、学生、实习生等）的要求和责任；
b) 临时人员不应参与重要数据级别以上的数据恢复业务服务。

6.3 环境

6.3.1 服务场所

6.3.1.1 一般要求

服务场所一般要求如下。
a) 应具有与服务基本相匹配的独立的、面积适宜的、配备相关设备和消防设施的服务场所。
b) 应根据不同的功能划分相互独立的用户接待区、数据恢复工作区和管理办公区。
c) 应具备独立的工作场所，专门用于数据恢复的技术实施。实施送修介质开盘修复操作应在不低于六级洁净等级的洁净环境中进行。洁净环境建设要求应满足 GB 50073 中第 3 章的空气洁净度等级要求。
d) 服务场所应安装密码门禁系统，只允许数据恢复工作人员进入，其他人员进入应经过审批，并留存电子或纸质版记录。
e) 服务场所应安装录像监控系统，监控范围应覆盖整个服务场所，且录像记录应至少保存 3 个月。
f) 应设置安全管理员并定期检查服务场所设备设施的运转情况，查验相关日志信息，及时排查故障隐患。
g) 服务场所内的资料、数据、配置参数等信息应妥善保管，未经批准不应以任何形式提供给其他无关人员。

6.3.1.2 增强要求

服务场所增强要求如下：
a) 应安装双向刷卡和具有商用密码产品认证证书的门禁系统密码门禁/生物识别系统，只允许被授权数据恢复工作人员进入，其他人员进入应经过审批；
b) 应建立服务场所资料、数据、软硬件配置参数清单，所有信息应分类保存，执行严格的审核制度访问，未经批准不应以任何形式提供给其他无关人员；
c) 应建立服务场所安全区域管理制度，访问登记制度，并定期核查执行情况；服务场所应设立处理重要数据级别以上的安全区域，在安全区域建立适当的进入控制措施以确保只有得到授权的人员才能进入；外部人员访问该区域前先提出书面申请，经批准后由专人全程陪同或监

督，并登记备案。

6.3.2 设施设备

6.3.2.1 一般要求

设施设备一般要求如下：

a) 应按照附录 A 配备实施数据恢复服务需要的软、硬件工具；
b) 应建立设备维护和管理清单；
c) 应做到所有设备专机专用，定机定责，不应安装使用与数据恢复无关的应用程序；
d) 应区分用于远程数据恢复的计算机，在数据恢复过程中，除用于远程数据恢复的计算机外，其他设备不应连接互联网；通过网络传输的数据文件应经过加密；
e) 未经批准，不应改变现有设备的配置；
f) 存储介质管理应遵循易取易存原则，集中存放、分类管理（包括用户盘、工作盘、备件盘）；
g) 应建立专用的存储介质库，并指定存储介质管理员负责存储介质库的维护和管理工作；
h) 应建立并严格执行存储介质出入库管理制度，未经批准，不应将存储介质带出服务场所；
i) 应建立存储介质档案，对存储介质逐一编号，详细记录其品牌、型号、容量、序列号及性能等信息；
j) 用户存储介质应粘贴唯一性标签，同一工作单的用户存储介质应集中放置一处，并在专门防磁、防静电的存储环境中保存。

6.3.2.2 增强要求

设施设备增强要求如下：

a) 应做到所有设备专机专用，定人定岗定机定责，不应安装使用与数据恢复无关的应用程序；
b) 未经批准，不应提供远程数据恢复服务；
c) 应建立设备变更制度，未经批准，不应改变现有设备的配置，对软硬件配置的重大变更，应先形成方案文件，经论证并获得相关负责人批准后，由具备资格的技术人员进行更改，并保留更改和操作记录；
d) 应建立设备使用记录清单，专用设备只能由被授权人员进行操作；
e) 应定期检测设备运转情况，进行必要的升级维护，保障设备运转正常并详细记录检查情况和问题改进；
f) 应建立出入库登记制度，并定期盘点，详细记录制度执行情况；
g) 设立安全管理员对存储介质的管理过程进行监督；
h) 应建立存储介质访问和生命周期管理机制，记录使用情况以及相关责任人，定期盘点，存储介质报废不再使用，及时进行信息彻底删除或物理销毁；
i) 应选择合格合规的设施设备供应商，确保设备使用的安全性、可用性和可追溯性。

6.4 质量控制

6.4.1 一般要求

质量控制一般要求如下：

a) 应建立服务质量目标；
b) 应确认质量控制人，制定业务执行流程手册；
c) 应制定并实行质量抽查要求和实施流程文档；
d) 应建立便捷的数据安全投诉举报机制，明确界定数据安全投诉举报机制的事项、内容、范围，及

时受理、处置数据安全投诉举报并记录处理情况。

6.4.2 增强要求

质量控制增强要求如下：

a) 应制定建立和实施质量控制体系，具备质量体系认证资质，包括确认质量控制人，质量体系文件有质量手册、程序文件、业务执行流程手册和管理流程手册等，并定期对质量体系的执行进行检查和审核，同时对潜在的不合格项制定预防措施并进行跟踪和验证，确保机构实施的一致性和结果有效性；

b) 应制定并实行质量抽查制度，包括质量抽查要求和实施流程文档，并对用户进行回访，对过程及结果进行详细记录，并分析和利用反馈以改进服务，严格执行，对数据恢复进度和恢复结果以及服务承诺多维度进行抽查，抽查结果应详细记录，每月抽查次数不低于4次；

c) 应建立便捷的数据安全投诉举报机制，及时受理、处置数据安全投诉举报，控制知悉范围，并对过程及整改结果进行详细记录。

6.5 安全审计

6.5.1 一般要求

应对数据恢复服务管理和实施过程进行内部审计，明确审计的时间间隔，对审计发现的问题应及时整改。

6.5.2 增强要求

安全审计增强要求如下：

a) 应对数据恢复服务管理和实施过程进行内部或外部审计，对审计发现的问题应及时整改；

b) 审计内容应包括数据安全组织管理审计、制度与规范管理审计，人员与意识培训管理审计，数据恢复服务场所审计，数据恢复服务过程审计等；

c) 应采用措施保证审计日志和记录的完整性和抗抵赖性，只允许授权人员查看相关记录，并规定审计记录存储时间。

7 安全实施要求

7.1 概述

存储介质数据恢复的实施过程包括介质接收、介质检测、数据恢复、数据交付、数据销毁5个环节，其主要工作内容应至少包括：

a) 介质接收：接收存储介质并记录存储介质情况；

b) 介质检测：判断存储介质故障类型，制定数据恢复方案；

c) 数据恢复：排除存储介质故障，提取可用数据；

d) 数据交付：将数据恢复结果交付给用户；

e) 数据销毁：销毁数据恢复结果和数据恢复操作过程中产生的所有相关数据信息；

f) 上述各环节责任人对操作及结果进行记录并签字。

7.2 介质接收

7.2.1 一般要求

介质接收环节一般要求如下：

a) 应检查送修存储介质，记录其基本情况，包括类型、品牌、型号、序列号及外观特征；
b) 应指导用户描述送修存储介质的故障现象，包括故障出现前后的操作、故障表现，并记录上述信息；
c) 应指导用户描述需要恢复的数据特征，并记录上述信息；
d) 应告知用户数据恢复实施的相关风险及后果、用户及数据恢复服务机构的职责；
e) 用户与数据恢复服务机构应签署服务协议，协议拟定见附录 B，协议基本内容包括存储介质的基本情况、存储介质的归属权、修复需求、修复风险及各方责任和义务。在服务实施前，应与服务需求方明确约定数据安全保护的相关条款，包括服务过程中涉及的个人信息（如身份信息等）、业务数据、系统数据、安全数据及其他相关资料的保护要求。

7.2.2 增强要求

此项要求无内容。

7.3 介质检测

7.3.1 一般要求

介质检测环节一般要求如下：

a) 应检测送修存储介质故障类型，判断本机构是否具备实施条件；若不具备实施条件，应中止数据恢复操作并返还给用户送修存储介质，并对用户说明无法实施的原因；
b) 对于具备实施条件的，应根据故障类型制定恢复方案，方案包括技术路线、使用方法、软硬件工具、人员时间安排和操作方法等。

7.3.2 增强要求

此项要求无内容。

7.4 数据恢复

7.4.1 一般要求

数据恢复环节一般要求如下。

a) 应根据存储介质检测结果实施数据恢复操作；需要实施送修介质开盘修复操作应获得用户书面授权，并在符合要求的洁净环境中实施。
b) 当存储介质能正常读取后，通过只读方式对原始存储介质实施镜像，镜像完成后，逻辑故障的排除应在镜像数据上进行。
c) 恢复出的可用数据应保存在专用数据存储设备中，不应覆盖镜像数据或用户的原始数据。严禁将恢复出的用户数据存储在个人存储介质中。
d) 实施远程数据恢复时，双方均应在符合本文件服务场所要求的环境中进行，并由专人相互配合，共同完成数据恢复技术操作。
e) 实施远程数据恢复时，应采取保证系统安全及数据安全传输的措施。
f) 应对原始数据进行保护，不应更改和删除原始存储介质上的数据。

7.4.2 增强要求

此项要求无内容。

7.5 数据交付

7.5.1 一般要求

数据交付环节一般要求如下：

a) 数据恢复实施方案完成后，应对照用户的委托要求评价数据恢复的结果，并如实告知用户，由用户对恢复结果进行确认；
b) 应提供数据恢复交付清单，并有核实记录；
c) 数据恢复结果宜以用户可用的形式交付，双方另有约定的从其约定；
d) 数据交付时，应完整归还用户送修的存储介质；
e) 如需远程交付，应使用符合密码相关国家标准的加密方式进行数据加密。

7.5.2 增强要求

此项要求无内容。

7.6 数据销毁

7.6.1 一般要求

数据销毁环节一般要求如下：

a) 数据交付完成后，应根据协议约定及时销毁数据恢复结果及操作过程中产生的所有相关数据信息；
b) 应在销毁审批后以不可逆方式销毁数据及其副本内容。

7.6.2 增强要求

数据销毁环节增强要求如下：

a) 重要数据级别以上的数据，应在销毁审批后实施现场销毁，并在必要情况下实施数据恢复验证；
b) 应建立数据销毁审批机制和管理制度，明确销毁对象、销毁策略和操作规程。建立数据销毁审批机制并记录审批操作过程，设置销毁相关监督角色，监督操作过程，并记录数据销毁操作时间、操作人、操作方式。

8 安全管理评价方法

8.1 机构

8.1.1 一般要求评价方法

机构一般要求评价方法、预期结果和结果判定如下。

a) 评价方法：
   1) 查看机构的法律地位证明文件，如机构组织机构代码证和成立证明文件等，核查其经营范围；
   2) 查看管理层无犯罪行为记录和无失信行为记录名单；
   3) 查看从事数据恢复服务的人员资质、相关工作记录、流程文档、人员值班记录等；
   4) 查看相关文件，访谈相关人员，检查是否制定保护用户数据安全、防止数据泄露的防护措施。

b） 预期结果：

1） 具备合法经营资格，经营范围（业务范围）包含数据恢复服务或相关表述；

2） 法定代表人、董事、合伙人以及高层管理人员无犯罪行为记录且未被列入失信人员名单；

3） 配备与从事服务类别相适应的技术团队；

4） 具备保护用户数据安全、防止数据泄露的防护措施。

c） 结果判定：实际评价结果与预期结果一致则判定符合，其他情况判定不符合。

8.1.2 增强要求评价方法

机构增强要求评价方法、预期结果和结果判定如下。

a） 评价方法：

1） 查看机构的法律地位证明文件，如组织机构代码证和成立证明文件等；

2） 查看数据安全管理机构架构文件、成立记录文件、相关发文、安全管理工作记录等，访谈相关人员，是否设立了数据安全管理机构，是否配备了不同角色的安全管理人员，包括权限审核人员、安全操作人员等；

3） 查看数据安全管理机构制度文件，访谈机构负责人和关键岗位人员，是否由机构主要负责人担任其领导职务，是否明确其成员构成，构成角色及相关职责；是否配备了与业务相配备的安全管理人员；

4） 查看数据安全权限管理制度和相关规范文件，并访谈相关人员，查看规范文件是否包含不同人员角色权限对应关系，是否覆盖授权、审批、核查等职责，是否详细说明防止数据泄露的防护措施；

5） 查看数据安全应急处理相关制度文件，查看应急记录文件，访问应急处理负责人和相关人，检查是否定期开展演练；

6） 查看培训制度和相关记录文件，检查是否开展了培训和考核，是否包括具体培训内容、方式、周期等，是否对过程和结果进行记录；

7） 查看数据安全管理规则制度文件和工作记录文件，检查安全管理人员是否参与业务决策，检查是否定期检查，是否及时改进。

b） 预期结果：

1） 具备合法经营资格，在中华人民共和国境内依法成立 1 年以上；

2） 设立了数据安全管理机构，并实际开展了数据安全管理工作；

3） 数据安全管理机构负责人由从业机构最高负责人担任，成员包括机构高层管理人员和业务负责人，相应人员岗位职责明确合理并知悉；

4） 具备业务全流程数据安全权限管理制度，包括不同人员角色权限对应关系，是否覆盖授权、审批、核查等职责，详细说明防止数据泄露的防护措施；

5） 具备数据安全应急处置和报告制度，发生数据安全事件时及时上报并启动应急响应机制，详细记录应急处理记录，定期开展应急演练并记录演练情况；

6） 具备数据安全意识和业务培训制度，包括培训计划、培训内容、培训过程和考核方式，并详细记录；

7） 开展了数据安全各项管理制度执行情况的内部监督检查、评审和改进，并详细记录。

c） 结果判定：实际评价结果与预期结果一致则判定符合，其他情况判定不符合。

8.2 人员

8.2.1 一般要求评价方法

人员一般要求评价方法、预期结果和结果判定如下。

a) 评价方法。
   1) 查看人员档案和相关证明文件等。
   2) 查看人员档案和资格证明，调查人员从业经历、项目经历等。
   3) 查看从业人员相关管理制度，访谈相关人员，检查是否权责分明，是否有和关键岗位人员签订保密协议、离职要求等，是否有尽职考核（包括数据安全）记录文件，是否有奖惩记录文件；岗位职责变化或终结时，是否及时对相应权限进行调整。
   4) 查看人员劳动合同等文件。
   5) 查看人员资格证明、培训记录、考核记录等，组织安全意识和技能考试[对应 6.2.1 要求中条款 d)、e)、f)、g)]。
b) 预期结果。
   1) 人员无犯罪记录、无不良信用记录。
   2) 任职人员具备与从事业务相匹配的资格和能力。
   3) 具备人员管理制度，权责分明，定职定岗，并定期进行尽职考核，进行奖惩，记录完整。
   4) 机构与人员建立劳动关系；机构使用劳务派遣人员，满足《中华人民共和国劳动合同法》《劳务派遣暂行规定》关于劳务派遣人员工作岗位和用工比例的要求。退休返聘人员签订有书面协议。
   5) 具备匹配的知识能力结构和安全意识 6.2.1 要求中条款 d)、e)、f)、g)。
c) 结果判定：实际评价结果与预期结果一致则判定符合，其他情况判定不符合。

8.2.2 增强要求评价方法

人员增强要求评价方法、预期结果和结果判定如下。

a) 评价方法：
   1) 查看临时人员职责文档，是否包括短期工作人员或第三方合作人员（例如代岗人员、学生、实习生等）的要求和责任；
   2) 查看临时人员职责文档，业务操作记录等，是否未参与重要数据恢复。
b) 预期结果：
   1) 具备临时人员职责文档，包括短期工作人员或第三方合作人员（例如代岗人员、学生、实习生等）的要求和责任；
   2) 临时人员未参与重要数据级别以上的恢复服务。
c) 结果判定：实际评价结果与预期结果一致则判定符合，其他情况判定不符合。

8.3 环境

8.3.1 服务场所

8.3.1.1 一般要求评价方法

服务场所一般要求评价方法、预期结果和结果判定如下。

a) 评价方法。
   1) 查看服务场所面积、功能分区、配套设施等，核查服务场所的属性，确认机构是否对服务场所具有完全的使用权。
   2) 查看制度和资料文档，访谈从业人员，是否划分了不同的功能区。
   3) 查看服务场所配置、访谈相关人员，是否满足六级洁净等级的洁净环境。
   4) 查看服务场所设施、进入记录和审批记录，检查服务场所是否安装密码门禁系统，人员是否按要求进入。

5） 查看服务场所设施、录像记录，是否安装录像监控系统，监控范围是否覆盖整个服务场所，录像记录保存时间。

6） 查看相关文件记录，是否设立安全管理人；是否定期检查服务场所设备设施的运转情况，查验相关日志信息，是否及时排查故障隐患。

7） 查看服务场所配置文件记录，服务场所内的资料、数据、配置参数等信息是否归档，是否有审批访问记录。

b） 预期结果。

1） 具有和从事业务相匹配的、独立的、布局合理的、配备相关设备和消防设施的服务场所，如机构自有产权的，提供产权证明；为上级配置、出资方调配的，提供上级、出资方的产权证明及其对机构具有完全使用权的声明（或授权）；机构非自有产权的，提供租赁、借用合同（期限不少于1年）及产权证复印件。如涉及转租，提供所有环节的租赁合同，且合同中不应有“不允许对外转租”等限制性字样。

2） 根据不同的功能划分了相互独立的用户接待区、数据恢复工作区和管理办公区。

3） 具备独立的场所，专门用于数据恢复的技术实施。实施送修介质开盘修复操作应在不低于六级洁净等级的洁净环境中进行。按照GB 50174建设要求检查服务场所建设是否满足。

4） 安装密码门禁系统，除数据恢复人员，进入都有审批记录。

5） 安装录像监控系统，监控范围覆盖整个服务场所，且录像记录保存3个月以上。

6） 安全管理员应定期检查服务场所设备设施的运转情况，查验相关日志信息，及时排查故障隐患。

7） 服务场所内的资料、数据、配置参数等信息归档保存，访问均有审批记录。

c） 结果判定：实际评价结果与预期结果一致则判定符合，其他情况判定不符合。

8.3.1.2 增强要求评价方法

服务场所增强要求评价方法、预期结果和结果判定如下。

a） 评价方法：

1） 查看服务场所设施、进入记录和审批记录，检查服务场所是否双向刷卡和密码门禁/生物识别系统，人员是否按要求进入；

2） 查看服务场所配置文件记录，服务场所内的资料、数据、配置参数等信息是否分类归档，是否有严格的审批制度和审批访问记录；

3） 查看服务场所设施和制度文件，检查是否设立处理重要数据的安全区域，是否建立服务场所安全区域管理制度，访问登记制度。

b） 预期结果：

1） 安装双向刷卡和密码门禁/生物识别系统，除数据恢复人员，进入都有审批记录；

2） 服务场所内的资料、数据、配置参数等信息分类归档保存，访问均执行审批记录；

3） 设立处理重要数据级别以上的安全区域，具备服务场所安全区域管理制度，访问登记制度。

c） 结果判定：实际评价结果与预期结果一致则判定符合，其他情况判定不符合。

8.3.2 设施设备

8.3.2.1 一般要求评价方法

设施设备一般要求评价方法、预期结果和结果判定如下：

a） 评价方法。

1） 查看设施设备，是否按照表 1 配备实施数据恢复服务需要的软、硬件工具。

2） 查看设备维护和管理清单。

3） 查看设备使用文件等，检查设备是否分类，专机专用，查看系统应用程序。

4） 查看是否有专门用于远程数据恢复的计算机，除用于远程数据恢复的计算机外，其他设备是否未连接互联网；核验通过网络传输的数据文件是否经过加密。

5） 查看设备配置变更记录，是否完整并有审批记录。

6） 查看存储介质管理是否易取易存，集中存放、分类管理（包括用户盘、工作盘、备件盘）。

7） 查看存储介质库，是否专用，访谈存储介质管理员，是否指定存储介质管理员负责对存储介质库的维护和管理工作。

8） 查看存储介质出入库管理制度，检查是否严格执行存储介质出入库管理制度，审批记录是否完整。

9） 查看存储介质档案，是否包括：存储介质逐一编号，详细记录其品牌、型号、容量、序列号及性能等信息。

10） 查看用户存储介质是否粘贴唯一性标签，同一工作单的用户存储介质是否集中放置一处，并在专门防磁、防静电的存储环境中保存。

b） 预期结果。

1） 按照表 1 配备实施数据恢复服务需要的软、硬件工具。

2） 具备设备维护和管理清单。

3） 所有设备专机专用，定机定责，没有安装使用与数据恢复无关的应用程序。

4） 有专门实施远程数据恢复的计算机，在数据恢复过程中，除用于远程数据恢复的计算机外，其他设备未连接互联网；通过网络传输的数据文件经过了加密。

5） 设备配置变更均有记录。

6） 存储介质管理遵循易取易存原则，集中存放、分类管理（包括用户盘、工作盘、备件盘）。

7） 具备专用的存储介质库，并指定存储介质管理员负责对存储介质库的维护和管理工作。

8） 严格执行存储介质出入库管理制度，未经批准，不能将存储介质带出服务场所。

9） 具备存储介质档案，包括：对存储介质逐一编号，详细记录其品牌、型号、容量、序列号及性能等信息。

10） 用户存储介质粘贴唯一性标签，同一工作单的用户存储介质集中放置一处，并在专门防磁、防静电的存储环境中保存。

c） 结果判定：实际评价结果与预期结果一致则判定符合，其他情况判定不符合。

8.3.2.2 增强要求评价方法

设施设备增强要求评价方法、预期结果和结果判定如下：

a） 评价方法：

1） 查看设备使用文件等，检查设备是否分类，专机专用，定人定岗定机定责，查看系统应用程序；

2） 查看记录文件，访问相关人员，查看是否未经批准提供远程数据恢复服务；

3） 查看设备配置变更记录，针对软硬件配置的重大变更，是否包括方案文件，论证记录，批准记录，实施人员是否是具备资格的技术人员；

4） 查看设备使用记录清单，是否专用设备只由被授权人员进行操作，是否加入外来移动存储介质；

5） 查看出入库登记制度，是否定期盘点，详细记录制度执行情况；

6） 查看设备配置变更记录等文件，检查是否定期检测设备运转情况，进行必要的升级维护，并详细记录检查周期和问题改进；
7） 访谈安全管理员，查看相关记录文件，是否对存储介质的管理过程进行监督；
8） 查看存储介质访问和生命周期管理机制，访谈相关人员，是否记录使用情况以及相关责任人，定期盘点，存储介质报废不再使用，是否及时进行信息彻底删除或物理销毁；
9） 查看设施设备供应商协议和供应商资质。

b） 预期结果：
1） 所有设备专机专用，定人定岗定机定责，没有安装使用与数据恢复无关的应用程序；
2） 不提供远程数据恢复服务；
3） 对软硬件配置的重大变更，具备方案文件，论证文件，批准记录等，由具备资格的技术人员进行更改；
4） 具备设备使用记录清单，专用设备只能由被授权人员进行操作，无外来存储设备；
5） 具备出入库登记制度，并定期盘点；
6） 定期检测设备运转情况，进行必要的升级维护，并详细记录检查周期和问题改进；
7） 已设立安全管理员对存储介质的管理过程进行监督；
8） 具备存储介质访问和生命周期管理机制，记录使用情况以及相关责任人，定期盘点，存储介质报废不再使用，及时进行信息彻底删除或物理销毁；
9） 设施设备供应商合格合规，并有详细采购文档记录确保可追溯性。

c） 结果判定：实际评价结果与预期结果一致则判定符合，其他情况判定不符合。

8.4 质量控制

8.4.1 一般要求评价方法

质量控制一般要求评价方法、预期结果和结果判定如下：

a） 评价方法：
1） 查看质量控制目标等相关文件和记录，访谈各级人员是否知悉；
2） 查看业务执行流程手册，访谈质量控制人；
3） 查看质量抽查要求和实施流程文档等相关文件；
4） 检查是否制定投诉举报机制文件或条款，检查用户是否可见，查看投诉举报受理及处理记录，检查处置是否及时合理。

b） 预期结果：
1） 建立了质量控制目标，各级人员均知悉；
2） 具备业务执行流程手册并在项目中应用；
3） 具备质量抽查要求和实施流程文档，并在项目中应用；
4） 具备便捷的数据安全投诉举报机制，并及时受理、处置、记录。

c） 结果判定：实际评价结果与预期结果一致则判定符合，其他情况判定不符合。

8.4.2 增强要求评价方法

质量控制增强要求评价方法、预期结果和结果判定如下：

a） 评价方法：
1） 查看质量控制体系相关制度文件和资质文件，是否包括确认质量控制人，质量体系文件有质量手册、程序文件、业务执行流程手册和管理流程手册等，并定期对质量体系的执行进行检查和审核，同时对潜在的不合格项制定预防措施并进行跟踪和验证；

2） 查看质量抽查制度，是否包括质量抽查要求和实施流程文档，是否对用户进行回访，严格执行，对数据恢复进度和恢复结果以及服务承诺多维度进行抽查，是否详细记录抽查结果；

3） 检查是否制定投诉举报机制文件或条款，检查用户是否可见，查看投诉举报受理及处理记录，检查处置是否及时合理，是否有整改结果详细记录。

b） 预期结果：

1） 具备质量控制体系，具备质量体系认证资质，确认质量控制人，质量体系文件包括质量手册、程序文件、业务执行流程手册和管理流程手册等，并定期对质量体系的执行进行检查和审核，并对潜在的不合格项制定预防措施并进行跟踪和验证；

2） 具备质量抽查制度，包括质量抽查要求和实施流程文档，并对用户进行回访，严格执行，对数据恢复进度和恢复结果以及服务承诺多维度进行抽查，抽查结果应详细记录；

3） 具备便捷的数据安全投诉举报机制，严格执行并及时受理、处置、记录，并对整改结果进行详细记录。

c） 结果判定：实际评价结果与预期结果一致则判定符合，其他情况判定不符合。

8.5 安全审计

8.5.1 一般要求评价方法

安全审计一般要求评价方法、预期结果和结果判定如下。

a） 评价方法：

查看历史审计报告和访谈审计负责人，是否对数据恢复服务管理和过程实施审计。

b） 预期结果：

定期对数据恢复服务管理和过程实施内部审计。

c） 结果判定：实际评价结果与预期结果一致则判定符合，其他情况判定不符合。

8.5.2 增强要求评价方法

安全审计增强要求评价方法、预期结果和结果判定如下。

a） 评价方法：

1） 查看历史审计报告和访谈审计负责人，是否对数据恢复服务管理和过程实施审计；

2） 查看历史审计报告，检查审计内容是否包括数据安全组织管理审计、制度与规范管理审计，人员与意识培训管理审计，数据恢复服务场所审计，数据恢复服务过程审计等，访谈审计负责人是否明确审计内容和方式；

3） 查看历史审计报告、记录文件、审计日志等，是否采用措施保证审计日志和记录的完整性和抗抵赖性，审计记录是否完整、是否规定审计记录存储时间。

b） 预期结果：

1） 定期对数据恢复服务管理和过程实施内部/外部审计；

2） 审计报告包括数据安全组织管理审计、制度与规范管理审计，人员与意识培训管理审计，数据恢复服务场所审计，数据恢复服务生存周期和过程审计等；

3） 已采用措施保证审计日志和记录的完整性和抗抵赖性，审计记录完整，已规定审计记录存储时间。

c） 结果判定：实际评价结果与预期结果一致则判定符合，其他情况判定不符合。

9 安全实施评价方法

9.1 介质接收

9.1.1 基本要求评价方法

介质接收安全实施一般要求评价方法、预期结果和结果判定如下。

a) 评价方法：
   1) 查看数据恢复工作单等记录档案文件，检查是否记录送修存储介质的基本情况，包括类型、品牌、型号、序列号及外观特征；
   2) 查看数据恢复工作单等记录档案文件，检查是否记录送修存储介质的故障现象；
   3) 查看数据恢复工作单等记录档案文件，检查是否记录需要恢复的数据特征，包括要恢复的数据目录和文件名及文件类型；
   4) 查看用户风险告知书等记录文件，访谈客服人员，检查是否告知用户数据恢复实施的相关风险及后果、用户及数据恢复服务机构的职责；
   5) 查看服务协议档案文件，检查协议内容，包括存储介质的基本情况、归属权、修复需求、修复风险及各方责任和义务。

b) 预期结果：
   1) 具备数据恢复工作单档案文件，并详细记录送修存储介质的基本情况，包括类型、品牌、型号、序列号及外观特征；
   2) 详细记录送修存储介质的故障现象；
   3) 详细记录需要恢复的数据特征，包括要恢复的数据目录和文件名及文件类型；
   4) 用户签署风险告知书，明确告知用户数据恢复实施的相关风险及后果、用户及数据恢复服务机构的职责；
   5) 用户签署服务协议，协议内容包括存储介质的基本情况、归属权、修复需求、修复风险及各方责任和义务。

c) 结果判定：实际评价结果与预期结果一致则判定符合，其他情况判定不符合。

9.1.2 增强要求评价方法

此项要求无内容。

9.2 介质检测

9.2.1 一般要求评价方法

介质检测安全实施一般要求评价方法、预期结果和结果判定如下。

a) 评价方法。
   1) 查看数据恢复过程记录文件，是否包括检测过程和故障类型；访谈客服和工作人员，在不具备实施条件下的处理方式。
   2) 查看数据恢复方案记录文件，是否包括技术路线、使用方法、软硬件工具、人员时间安排和操作方法等。

b) 预期结果。
   1) 具备数据恢复过程记录文件，包括检测过程和故障类型，并在不具备实施条件下，记录原因和返还时间、方式等。
   2) 查看数据恢复方案记录文件，包括技术路线、使用方法、软硬件工具、人员时间安排和操作

方法等。

c) 结果判定：实际评价结果与预期结果一致则判定符合，其他情况判定不符合。

9.2.2 增强要求评价方法

此项要求无内容。

9.3 数据恢复

9.3.1 基本要求评价方法

数据恢复环节安全实施一般要求评价方法、预期结果和结果判定如下。

a) 评价方法。

1) 查看用户书面授权书，是否明确告知需要实施送修介质开盘修复操作；访谈技术人员，开盘操作的地点和方式。

2) 访谈技术人员，检查实验室环境，是否通过只读方式对原始存储介质实施镜像，逻辑故障排除的执行方式。

3) 查看数据恢复过程记录文件，访谈技术人员，恢复出的可用数据是否保存在专用数据存储设备中。

4) 查看远程数据恢复过程记录文件，包括数据恢复操作地点，远程数据恢复的双方的操作环境、操作人员和操作方式。

5) 查看远程恢复数据记录文件，包括系统安全的检测，数据传输是否加密等。

6) 查看数据恢复过程记录文件，访谈技术人员，确认原始数据和数据恢复实施方式。

b) 预期结果。

1) 具备用户书面授权书，明确告知用户需要实施送修介质开盘修复操作，并在符合要求的洁净环境中实施。

2) 恢复过程中，通过只读方式对原始存储介质实施镜像，并且逻辑故障的排除是在镜像数据上进行。

3) 具备数据恢复过程记录文件，恢复出的可用数据保存在专用数据存储设备中。

4) 具备远程恢复过程记录文件，实施远程数据恢复时，双方均在符合本文件服务场所要求的环境中进行，并由专人相互配合，共同完成数据恢复技术操作。

5) 具备远程恢复过程记录文件，恢复实施前检测系统环境，并在数据传输时加密传输。

6) 具备数据恢复过程记录文件，存储介质可读后，所有操作在镜像完成。

c) 结果判定：实际评价结果与预期结果一致则判定符合，其他情况判定不符合。

9.3.2 增强要求评价方法

此项要求无内容。

9.4 数据交付

9.4.1 一般要求评价方法

数据交付环节安全实施一般要求评价方法、预期结果和结果判定如下：

a) 评价方法：

1) 查看数据恢复记录文件，数据恢复确认单，是否包括用户要求和结果比对，是否如实告知用户且用户对结果明确确认，包括签署数据恢复确认单；

2) 查看数据恢复记录文件，检查是否提供数据恢复交付清单，并有用户核实记录；

3） 查看数据恢复记录文件，检查数据交付的形式；
4） 查看数据恢复记录文件，包括交付归还用户送修的存储介质；
5） 查看数据恢复记录文件，访谈技术人员，远程交付的方式。

b） 预期结果：
1） 具备数据恢复记录文件，包括用户委托要求和结果比对，用户告知，恢复结果确认；
2） 具备数据恢复记录文件，包括提供数据恢复交付清单和用户确认；
3） 具备数据恢复记录文件，包括数据交付的形式；
4） 具备数据恢复记录文件，包括归还用户送修的存储介质和用户确认；
5） 具备数据恢复记录文件，包括远程交付的数据加密记录。

c） 结果判定：实际评价结果与预期结果一致则判定符合，其他情况判定不符合。

9.4.2 增强要求评价方法

此项要求无内容。

9.5 数据销毁

9.5.1 一般要求评价方法

数据销毁安全实施一般要求评价方法、预期结果和结果判定如下。

a） 评价方法：
1） 查看数据销毁记录文件，包括销毁数据的方式和内容；
2） 查看销毁审批记录文件，以中立的视角观察操作流程，销毁数据的方式。

b） 预期结果：
1） 数据交付完成后，根据协议约定及时销毁数据恢复结果及操作过程中产生的所有相关数据信息；
2） 具备销毁审批制度，销毁审批后以不可逆方式销毁数据及其副本内容。

c） 结果判定：实际评价结果与预期结果一致则判定符合，其他情况判定不符合。

9.5.2 增强要求评价方法

数据销毁安全实施增强要求评价方法、预期结果和结果判定如下：

a） 评价方法：
1） 查看数据销毁记录文件，以中立的视角观察操作流程，检查重要数据是否有现场监督；
2） 查看数据销毁管理制度和策略，检查是否包括销毁流程、审批方式、操作人员、监督人员、记录内容；人员包括技术人员、审批人员、监督人员。

b） 预期结果：
1） 重要数据级别以上的数据恢复具备现场监督销毁；
2） 具备数据销毁策略和管理制度，明确销毁对象和流程。建立数据销毁审批机制并记录审批操作过程，设置销毁相关监督角色，监督操作过程，并记录数据销毁操作时间、操作人、操作方式。

c） 结果判定：实际评价结果与预期结果一致则判定符合，其他情况判定不符合。

附 录 A
（规范性）
数据恢复服务软、硬件工具基本配置要求

数据恢复服务软、硬件工具基本配置要求按表 A.1 的规定。

表 A.1 数据恢复服务软、硬件工具基本配置要求

序号	工具类别	配置要求	性质
1	数据恢复工作专用计算机及配套设备	a) 配置基本的正版操作系统和正版软件工作环境及必要的硬件配套设备； b) 写保护设备应有明确的写保护方向标识	必备
2	数据镜像工具	具备镜像功能的软件或硬件工具，其中硬件工具应具备写保护功能和输入输出方向标识	必备
3	数据销毁工具	具备数据销毁功能的软件或硬件工具	必备
4	软件操作工具	正版的软件工具，包括文件系统恢复工具、文件重构工具、文件修复工具、数据库恢复工具、磁盘阵列重组工具、远程数据恢复工具、十六进制编辑工具等	必备
5	备件库	应具备可用于硬件故障恢复的，可替代存储介质故障部分的零部件等备品备件	硬件故障恢复必备
6	硬件操作工具	洁净工作台、显微镜、开盘修复工具、焊接设备、固件操作工具、万用表、稳压电源和拆焊设备等	硬件故障恢复必备

附 录 B
（资料性）
数据恢复服务协议模板

数据恢复服务协议模板见图 B.1：

××恢复中心（以下简称"恢复中心"）与用户本着自愿、平等的原则，就用户委托恢复中心进行数据恢复的相关事宜，达成以下协议：

一、用户职责

1. 用户需要尽量详细地提供送修介质的相关信息；

2. 如用户送修介质为硬件故障，工程师需要使用恢复中心的备件为用户进行数据恢复，则用户只有该备件的使用权；如备件使用后数据恢复不成功，则用户无须支付任何费用；如备件使用后数据恢复成功，则用户需要额外支付备件使用费；

3. 经用户本人同意，恢复中心可为用户提供免费邮寄送修介质服务（大型设备另议），邮寄过程中发生的任何损失由快递公司按照相关条款赔偿，如用户需要投保，保费由用户承担；

4. 用户应按照约定支付数据恢复费用。

二、恢复中心职责

1. 尽力恢复用户的数据，在数据恢复过程中，保证用户存储介质的安全；

2. 承诺对恢复后的数据进行保密，不以任何形式泄露给第三方；

3. 数据恢复成功后，用户可当场验证数据，如恢复中心不具备验证环境，则此环境由用户提供；

4. 如未能成功恢复出用户所需数据，则不收取数据恢复费用（加急费、加班费除外）；

5. 用户确认并取走数据后，恢复中心应立即销毁用户所有数据（特殊要求另议）。

三、用户知悉以下信息并同意接受相关风险及其后果

1. 恢复中心尽力保证用户存储介质送修时的原始状态，但不排除在恢复过程中送修介质可能出现新的物理损坏，一旦发生意外，恢复中心对此不承担相关责任；

2. 由于技术处理的需要，在进行数据恢复过程中可能需要打开用户送修介质盘体，向用户确认并征得同意后，由此导致送修介质保修失效和不能再次使用等相关问题，恢复中心对此不承担相关责任。

四、其他事宜

1. 恢复中心进行数据恢复时，不负责恢复存储介质内的操作系统和应用软件；

2. 恢复中心在日常工作时间提供加急服务（一个工作日内交付数据），加急费为人民币×元，数据恢复不成功，加急费不退还；日常工作时间以外提供加班服务，加班费为×元/小时，不足半小时的按×元收取，拷贝数据时间算在加班时间之内，数据恢复不成功，加班费不退还；

3. 在恢复中心保留用户送修介质期间，如果因为不可抗力原因，如战争、地震、水灾等自然灾害以及其他不可预料的事件所带来的意外损失，恢复中心不承担相关责任；

4. 本协议自用户在数据恢复工作单（数据恢复工作单分三联，一联客服，一联技术部，一联用户，应包括用户基本信息、送修介质基本情况，故障现象，故障发生后做了什么操作，介质中需要恢复的数据目录和文件名及文件类型，送修须知，数据确认等等）签字之日起立即生效。

图 B.1 数据恢复服务协议模板

参 考 文 献

[1] GB/T 35273—2020 信息安全技术 个人信息安全规范
[2] GB/T 32914—2023 信息安全技术 网络安全服务能力要求
[3] GB/T 43697—2024 数据安全技术 数据分类分级规则
[4] 中华人民共和国劳动合同法(2012 年修正)
[5] 劳务派遣暂行规定(2014 年)