ICS 35.220.01
L 63

团 体 标 准

T/ZBLM 0001-2018

数据备份与恢复服务能力成熟度测评规范

The test and evaluation specifications for data backup and recovery server capability maturity

2018-12-01 发布 2019-01-01 实施

北京信息灾备技术产业联盟 发布

目　　次

前　言

本部分按照GB/T 1.1—2009给出的规则起草。

本标准由北京信息灾备技术产业联盟提出并归口。

本标准主要起草单位：国家电子计算机质量监督检验中心（北京尊冠科技有限公司）、国家金卡工程信息存储系统测评中心、厦门纳网科技股份有限公司、华为技术有限公司、灾备技术国家工程实验室、北京邮电大学、北京众享比特科技有限公司、中兴通讯股份有限公司、北京银河七星科技有限公司、中国大唐集团科学技术研究院有限公司、北京星云泰科技有限公司。

本标准主要起草人：阳小珊、田雄军、陈迎锋、李辉、曾宪章、周景才、杨晓平、辛阳、李正文、杨光灿、陈鸿刚、刘根、杨长清、李志立、张伟、赵廷涛。

数据备份与恢复服务能力成熟度测评规范

1 范围

本标准规定了企业或组织（以下统称组织）进行电子数据备份所达到的数据备份恢复服务能力成熟度的评测标准。

本标准适用于任何组织对电子数据备份所达到的数据保护能力的评估。

本标准仅适用于电子数据的备份和恢复，不包括应用高可用和业务容灾等内容。

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 20988-2007 信息安全技术 信息系统灾难恢复规范

GB/T 29765-2013 信息安全技术 数据备份与恢复产品技术要求与测试评价方法

3 术语、定义和缩略语

3.1 术语和定义

GB/T 20988-2007 和 GB/T 29765-2013界定的以及下列术语和定义适用于本文件。

3.1.1

数据 data

泛指组织信息系统相关数据，包括业务数据、应用系统、中间件和操作系统等。

3.1.2

数据备份 data backup

是指拷贝或归档数据的过程，以便于在数据丢失时能够恢复原始数据。

3.1.3

数据恢复 data restore

是指利用数据备份所产生的备份数据将目标数据还原为某一备份时间点的内容或状态的过程。

3.1.4

备份对象 backup object

是指需要进行备份的数据集合，可以是文件、数据库、虚拟机、操作系统和存储容器等。

3.1.5

备份介质 backup media

是指用于存放备份数据的物理载体，如磁盘、磁带和光盘等。

3.1.6

备份系统 backup system

是指实现数据备份和数据恢复的相关软件和硬件所组成的系统。

3.1.7

云备份 cloud backup

是指以云计算的形式为用户提供备份恢复服务。

3.1.8

全量备份 full backup

备份所有指定的数据对象的过程,不论这些数据自上次备份后是否被更改,是增量备份的基础。

3.1.9

差异备份 differential backup

仅备份自上次全量备份以后发生变化的所有数据对象，使用差异备份进行恢复时，只需要上次完全备份和自上次完全备份后的累积增量备份。

3.1.10

增量备份 incremental backup

备份自上次完全备份或增量备份后更改过的数据对象。使用增量备份恢复数据时,需要最新的完全备份和自最新完全备份后的所有增量备份。

3.1.11

热备 hot backup

是指在信息系统运行过程中直接备份，对正在运行的系统没有任何影响，并保证备份数据的一致性。

3.1.12

冷备 code backup

是指在信息系统停止运行的情况下进行备份。

3.1.13

暖备 warm backup

是指在信息系统运行的情况下进行备份，会对业务系统有一定的影响，如通过加锁等方式保证数据的一致性。

3.1.14

数据加密 data encryption

是指利用密码技术对信息进行加密，实现信息隐蔽，从而起到保护信息安全的作用。

3.1.15

安全审计 security audit

是指对系统中与安全有关的活动的相关信息进行识别、记录、存储和分析。信息安全审计的记录用于检查网络上发生了哪些与安全有关的活动，谁（哪个用户）对这个活动负责。

3.1.16

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持的关键业务功能。

3.1.17

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。

3.1.18

恢复时间目标 recovery time objective

灾难发生后,信息系统或业务功能从停顿到必须恢复的时间要求。

3.1.19

恢复点目标 recovery point objective

灾难发生后,系统和数据必须恢复到的时间点要求。

3.1.20

完整性校验 integrity check

是通过核对数据校验码确认数据完整性的过程。

3.1.21

数据转存 data dump

是指当某种数据的存储介质发生质变,比如纸介的保存受到场地限制或者易破损消失是需要转录成其他介质保存（如扫描成电子文档，或影像），另外原有的介质的读取（或存储设备淘汰）设备不支持时，需要及时采用其他的存储介质保存（如软盘、磁带、光盘等）。

3.2 缩略语

以下缩略语适用于本文件。

RPO: 恢复点目标（Recovery Point Objective）

RTO: 恢复时间目标（Recovery Time Objective）

DBR：数据备份与恢复（Data Backup and Recovery）

4 概述

4.1 能力成熟度

数据备份是组织信息安全最基本也是最重要的数据保护方式。数据备份和恢复的能力反映了组织在面对灾难时的抗风险能力。数据备份与恢复能力成熟度将组织的数据备份保护能力划分为不同的等级，主要用于衡量组织的数据备份安全保护所达到水平。

4.2 成熟度等级划分

数据备份与恢复能力成熟度共划分为六个等级：分别是DBR1、DBR2、DBR3、DBR4、DBR5和DBR6。

4.2.1 DBR1：基本支持级

DBR1为基本保护级，是指组织会定期对所要求的数据做一定的数据备份，并将备份数据进行场外存放，具有数据恢复预案。

- 定期对所要求的数据备份，并进行场外存放。
- 制定介质存取、验证和转储的管理制度。
- 完整测试和演练的灾难恢复预案。

4.2.2 DBR2：备用场地支持级

在DBR1的基础上，组织会对所要求的数据进行有计划的数据备份，并对备份数据进行定期的有效性验证，但对数据备份的管理和恢复尚处于人工管理的初级阶段。

- 预定时间调配数据,通信线路和网络设备。
- 备用场地管理制度。
- 设备及网络紧急供货协议。

4.2.3 DBR3：电子传输和部分设备支持级

在DBR2的基础上,组织会对所有要求的数据采用专业的备份系统进行数据的备份、恢复和管理，对于备份数据的存取具有相应的管理制度，对于备份系统有相应的管理制度。

- 配置部分数据,通信线路和网络设备。
- 每天实现多次的数据电子传输。
- 备用场地配置专职的运行管理人员。

4.2.4 DBR4：电子传输及完整设备支持级

在DBR3的基础上，组织对于所要求的数据的备份和恢复提出了一定的性能要求，采用专业的软硬件备份系统进行备份恢复的实施和管理，建立了较为完善的管理制度和人员配置，基本能够保证业务的开展不受灾难发生的影响。

- 配置全部数据处理系统、通信线路和网络设备。
- 备用数据处理系统或网络设备处于就绪状态。

4.2.5 DBR5：实时数据传输及完整设备支持级

在DBR 4的基础上，组织对所要求的数据的备份和恢复的性能提出了较高的要求，基本达到RPO＝0，RTO达到分钟级别，具有完善的管理制度和配置了满足需求的人员，基本保证业务不被中断。

- 实现远程数据复制技术。

- 备用网络也具备自动或集中切换能力。

4.2.6 DBR6：数据零丢失和远程集群支持级

在DBR 5的基础上，组织对所要求的数据的备份和恢复能力已达到极高水平，能够达到RPO=0，RTO近似于0的标准，具有完善的基础设施、管理制度，配置了满足需求的人员，能够保证业务的连续性。

- 实现远程数据实时备份，实现零丢失。
- 应用软件可以实现实时无缝切换。
- 远程集群系统的实时监控和自动切换能力。

4.3 数据等级划分

为了有效的实施数据备份，组织的数据资产需要进行分级管理。由于各个组织业务的不同，所关注的数据的侧重点也不同，因此，数据等级划分需要根据组织的具体情况实施。在此仅给出数据等级划分的参考原则。该原则按照数据的机密性、完整性和可用性将组织数据资产划分为三个等级。具体数据资产价值评估方法见《附录A 数据资产价值评估》。

4.3.1 I 级

I级数据是组织的核心数据，包括组织机密数据、核心业务数据和核心业务系统等，此部分数据的泄漏、丢失或损坏，会对组织正常运转和核心业务开展产生重大影响，甚至造成重大财产损失。

社会影响：数据的丢失、泄露、损坏将对国家、社会产生重大影响或重大经济损失的；

单位影响：数据的丢失、泄露、损坏将对单位的关键业务造成重大的经济损失的；

用户影响：数据的丢失、泄露、损坏客户不能容忍的。

4.3.2 II 级

II级数据是组织的重要数据，包括组织中的非公开数据、非核心但重要的业务系统和数据等，此部分数据的泄漏、丢失或损坏，会造成组织效能下降，对于业务开展有一定的影响，但不会导致业务停顿。

数据的丢失、泄露、损坏将影响单位部分关键业务造成较大影响或经济损失的；

数据的丢失、泄露、损坏将对单位和用户具有一定容忍度的。

4.3.3 III 级

III级数据是组织的普通数据，包括一些公开信息以及一些非重要系统和数据等，此部分数据的泄漏、丢失或损坏不会对组织造成任何影响或影响极低。

数据的丢失、泄露、损坏将影响单位非关键业务并造成一定经济损失的；

数据的丢失、泄露、损坏将允许在一定时间内可以补救的。

5 基本要求

5.1 管理要求

5.1.1 人员配置

对数据备份与恢复的人员配置要求分为以下三级:

a) 具有兼职数据备份支持人员，负责进行数据的备份和恢复。

b) 具有专职数据备份支持人员，负责组织数据梳理，备份恢复的实施及管理。

c) 具有 7 x 24 专职数据备份支持人员，负责组织数据梳理，备份恢复的实施和管理。

5.1.2 管理规范

对数据备份与恢复的管理规范要求分为以下三级：

a) 制定了基本的数据备份与恢复的管理规范，规定了备份范围和核心的数据备份与恢复的操作流程，介质存取、验证和转储的管理制度，以及完整测试和演练的灾难恢复预案。

b) 在 A 基础上，制定了较为完善的数据备份与恢复的管理规范，内容包括备份范围、备份与恢复性能要求、操作流程、备份数据访问管理制度等。

c) 在 B 基础上，制定了完善的数据备份与恢复的管理制度，明确了数据备份管理架构、人员构成、访问控制、备份数据生命周期管理等。

5.1.3 人员培训

对数据备份与恢复的人员培训要求分为以下二级：

a) 由内部 IT 人员定期提供数据备份基础知识培训。

b) 由厂商或专家定期提供数据备份专业知识技能培训。

5.2 技术要求

5.2.1 备份范围

对数据备份与恢复的备份范围要求分为以下三级：

a) 备份范围只涵盖 I 级核心数据。

b) 备份范围涵盖 I 级和 II 级数据。

c) 备份范围涵盖 I 级、II 级和 III 级数据。

5.2.2 备份对象

对数据备份与恢复的备份对象要求分为以下三类：

a) 备份对象只涵盖业务数据，主要包括文件和数据库。

b) 备份对象在业务数据基础上，还包括应用系统和中间件。

c) 备份对象在业务数据、业务系统基础上还提供基础支撑系统备份，如操作系统、虚拟机、容器等。

5.2.3 备份方法

对数据备份与恢复的备份方法要求分为以下三类：

a) 提供数据冷备支持。

b) 提供数据暖备支持。

c) 提供数据热备支持。

5.2.4 备份周期

对数据备份与恢复的备份周期要求分为以下五类：

a) 全量备份至少每周一次。

b) 全量备份至少每天一次。

c) 全量备份至少每天一次、增量 / 差异数据备份达到小时级。
d) 全量备份至少每天一次、增量 / 差异数据备份达到分钟级。
e) 提供持续数据保护。

5.2.5 保存时长

对数据备份与恢复的保存时长要求分为以下五类:
a) 数据保存至少 6 个月以上。
b) 数据保存至少 1 年以上。
c) 数据保存至少 3 年以上。
d) 数据保存至少 6 年以上。
e) 数据保存至少 10 年以上。

5.2.6 备份介质

对数据备份与恢复的备份介质要求分为以下两类:
a) 支持离线备份介质，如磁带、光盘等。
b) 支持在线备份介质，如磁盘、SSD 等。

5.2.7 保存位置

对数据备份与恢复的保存位置要求分为以下四类:
a) 提供数据场外保存。
b) 提供数据远程单节点保存，包括数据在云中的备份。
c) 提供本地加远程单节点保存，包括数据在云中的备份。
d) 提供本地加远程多节点保存，数据需要支持多个云提供商。

5.2.8 数据校验

对数据备份与恢复的数据校验要求分为以下两类:
a) 备份完成时进行备份数据完整性校验。
b) 定期进行备份数据完整性校验。

5.2.9 恢复粒度

对数据备份与恢复的恢复粒度要求分为以下三级:
a) 只支持全量恢复，即只能恢复每次备份的全部内容。
b) 支持细粒度恢复，如文件级别的单文件或文件夹恢复，数据库备份的单表恢复。
c) 支持操作系统 / 虚拟机 / 容器备份的的内部单文件恢复。

5.2.10 恢复演练

对数据备份与恢复的恢复演练要求分为以下四类:
a) 提供每年一次的恢复演练。
b) 提供半年一次的恢复演练。
c) 提供每月一次的恢复演练。
d) 提供每周一次的恢复演练。

5.2.11 备份工具

对数据备份与恢复的备份工具要求分为以下三类:

a) 通过手工拷贝或脚本进行数据备份。
b) 专业备份软件。
c) 专业备份软件和备份硬件。

5.2.12 数据迁移

对数据备份与恢复的数据迁移要求分为以下两类:

a) 支持同一备份系统不同版本之间的数据迁移。
b) 支持不同备份系统之间的数据转换迁移。

5.2.13 恢复点目标

对数据备份与恢复的恢复点目标要求分为以下四类:

a) RPO 支持 1 天至 7 天。
b) RPO 支持数小时到 1 天。
c) RPO 支持 0 到 30 分钟。
d) RPO 为 0，能保证数据不丢失。

5.2.14 恢复时间目标

对数据备份与恢复的恢复时间目标要求分为以下六类:

a) 数据恢复时间在 2 天以上。
b) 数据恢复时间在 24 小时以上。
c) 数据恢复时间在 12 小时以上。
d) 数据恢复时间在 1 小时以上。
e) 数据恢复时间在 1 分钟以上。
f) 数据恢复时间在 1 分钟以内。

5.2.15 数据加密

对数据备份与恢复的保存位置要求分为以下七类:

a) 支持数据的加密存储。
b) 支持数据的加密传输和存储。
c) 支持数据的源端加密、加密传输和存储。
d) 加密强度－弱。
e) 加密强度－中。
f) 加密强度－强。
g) 支持国密算法。

5.2.16 访问控制

对数据备份与恢复的访问控制要求分为以下五类:

a) 身份鉴别－口令系统。
b) 身份鉴别－智能卡 / 证书 / 生物特征。
c) 身份鉴别－多因子认证，综合应用 A / B 两种鉴权方式。
d) 提供基于功能的权限控制。
e) 提供基于数据的权限控制。

5.2.17 安全审计

对数据备份与恢复的安全审计要求分为以下四级:

a) 提供用户身份鉴别日志审计，包括用户注册、登录、注销等。

b) 在 A 基础上，提供用户操作审计，包括策略配置、系统配置等。

c) 在 B 基础上，提供备份恢复作业执行情况审计，包括备份作业执行信息、恢复作业执行信息、资源占用信息等。

d) 在 C 基础上，审计日志的查询、导出和删除需要授权访问。

5.2.18 数据转存

对数据转储的要求如下:

a) 组织提供存储介质转存工具，支持纸质介质的电子化。

b) 组织提供存储介质转存工具，支持将软盘、光盘、磁带、磁盘等介质的数据本地转存到新的介质。

c) 组织提供存储介质转存工具，提供介质异地转存功能。

5.2.19 备用系统

对备用的数据处理系统、通信线路和网络设备的要求分为如下五级:

a) 灾难发生时，能在预定时间内调配所需的数据处理设备、通信线路和网络设备到位。

b) 配备部分数据处理设备、通信线路和相应的网络设备。

c) 配备灾难恢复所需的全部数据处理设备、通信线路和网络设备，并处于就绪状态。

d) 配备灾难恢复所需的全部数据处理设备、通信线路和网络设备，具有自动和集中切换能力。

e) 配备与生产系统相同等级的数据处理系统、通信线路和网络设备，且处于运行状态，具有实时监控和自动切换能力。

6 测评方法

6.1 管理要求

本节提出了对管理要求的测评方法，包括预置条件、测评步骤和结果判定。

6.1.1 人员配置

a) 预置条件

1) 数据备份和恢复系统已建设完成；

2) 测试人员到被测机构现场进行评估。

b) 测评步骤

1) 检查组织人员配置，确认是否有数据备份人员岗位设置；

2) 检查组织人员配置，确认是否有 7 x 24 数据备份人员支持。

c) 结果判定

根据 5.1.1 的要求进行判定。

6.1.2 管理规范

a) 预置条件

1) 数据备份与恢复系统已建设完成；

2) 被测机构提供备份恢复相关管理规范文件；
3) 测试人员到被测机构现场进行评估。

b) 测评步骤

1) 检查组织的数据备份和恢复管理规范文件，确认是否规定了备份范围及备份与恢复的流程；
2) 检查组织的数据备份和恢复管理规范文件，确认是否规定了备份恢复性能要求、操作流程、备份数据访问管理制度；
3) 检查组织的数据备份和恢复管理规范文件，确认是否规定了备份恢复管理架构、访问控制、恢复演练等。

c) 结果判定

根据 5.1.2 的要求进行判定。

6.1.3 人员培训

a) 预置条件

1) 数据备份与恢复系统已建设完成；
2) 被测机构具有备份恢复管理制度规范；
3) 被测机构提供培训计划和相关记录；
4) 测试人员到被测机构现场进行评估。

b) 测评步骤

1) 检查组织规范和制度，确认是否为全体员工提供内部数据备份基础知识的相关培训；
2) 检查组织规范和制度，确认是否邀请厂商或专家提供数据备份专业知识技能培训。

c) 结果判定

根据 5.1.3 的要求进行判定。

6.2 技术要求

6.2.1 备份范围

a) 预置条件

1) 被测机构已完成数据等级划分工作；
2) 测试人员具有访问备份数据的权限。

b) 测评步骤

1) 检查备份策略和备份数据，确认是否包含所有 I 级核心数据；
2) 检查备份策略和备份数据，确认是否包含所有 I 级和 II 级数据；
3) 检查备份策略和备份数据，确认是否包含所有 I 级、II 级和 III 级数据。

c) 结果判定

根据 5.2.1 的要求进行判定。

6.2.2 备份对象

a) 预置条件

1) 数据备份与恢复系统已建设完成；
2) 被测机构为测试人员提供数据备份与恢复系统测试帐号；
3) 测试人员具有查看和使用数据备份与恢复系统的权限。

b) 测评步骤

1) 检查备份系统和备份数据，确认是否支持文件备份和数据库备份；
2) 检查备份系统和备份数据，确认是否支持组织所用应用系统和中间件的备份；
3) 检查备份系统和备份数据，确认是否支持操作系统、虚拟机和容器的备份。

c) 结果判定

根据 5.2.2 的要求进行判定。

6.2.3 备份方法

a) 预置条件

测试人员具有查看备份数据和备份工具的权限。

b) 测评步骤

1) 检查组织备份方法，确认是否采用冷备方式实现数据备份；
2) 检查组织备份方法，确认是否采用暖备方式实现数据备份；
3) 检查组织备份方法，确认是否采用热备方式实现数据备份。

c) 结果判定

根据 5.2.3 的要求进行判定。

6.2.4 备份频率

a) 预置条件

1) 数据备份与恢复系统已建设完成；
2) 数据备份与恢复系统提供备份频率配置接口；
3) 被测机构为测试人员提供数据备份与恢复系统测试帐号；
4) 测试人员具有访问备份策略配置的权限。

b) 测评步骤

1) 检查组织的备份系统和备份数据，确认是否支持每周一次全量备份的备份频率，并已实施；
2) 检查组织的备份系统和备份数据，确认是否支持每天一次全量备份的备份频率，并已实施；
3) 检查组织的备份系统和备份数据，确认是否支持小时级别的备份频率，并已实施；
4) 检查组织的备份系统和备份数据，确认是否支持分钟级别的备份频率，并已实施；
5) 检查组织的备份系统和备份数据，确认是否提供持续数据保护，并已实施。

c) 结果判定

根据 5.2.4 的要求进行判定。

6.2.5 保存时长

a) 预置条件

1) 数据备份与恢复系统已建设完成；
2) 数据备份与恢复系统提供备份数据和存储容量统计报表；
3) 被测机构为测试人员提供数据备份与恢复系统测试帐号；
4) 测试人员具有访问用户存储和备份数据的权限。

b) 测评步骤

1) 检查组织的备份系统和备份介质，确认是否支持 6 个月以上的备份数据存储；
2) 检查组织的备份系统和备份介质，确认是否支持 1 年以上的备份数据存储；
3) 检查组织的备份系统和备份介质，确认是否支持 3 年以上的备份数据存储；
4) 检查组织的备份系统和备份介质，确认是否支持 6 年以上的备份数据存储；
5) 检查组织的备份系统和备份介质，确认是否支持 10 年以上的备份数据存储。

c) 结果判定

根据 5.2.5 的要求进行判定。

6.2.6 备份介质

a) 预置条件

1) 被测机构提供备份介质中备份数据的访问工具；

2) 测试人员具有访问备份介质和检查备份数据的权限。

b) 测评步骤

1) 检查组织的备份介质，确认是否包含磁带、光盘等，并且备份系统提供该类介质支持；

2) 检查组织的备份介质，确认是否包含磁盘、SSD 或云存储等，并且备份系统提供该类介质支持。

c) 结果判定

根据 5.2.6 的要求进行判定。

6.2.7 保存位置

a) 预置条件

测试人员具有访问备份数据的权限。

b) 测评步骤

1) 检查组织备份数据，确认是否提供场外位置保存；

2) 检查组织备份数据，确认是否提供远程数据保存，包括云存储，确认数据保存位置是否具有 C 级数据中心资质；

3) 检查组织备份数据，确认是否存在本地和远程单点保存，确认数据保存位置是否具有 B 级数据中心资质；

4) 检查组织备份数据，确认是否提供本地和远程多点保存，确认数据保存位置是否具有 B 级或 A 级数据中心资质。

c) 结果判定

根据 5.2.7 的要求进行判定。

6.2.8 数据校验

a) 预置条件

1) 数据备份与恢复系统已建设完成；

2) 数据备份与恢复系统提供查看数据完整性校验机制的接口；

3) 被测机构为测试人员提供数据备份与恢复系统测试帐号；

4) 测试人员具有查看数据完整性校验机制的权限。

b) 测评步骤

1) 通过检查备份系统和备份数据，确认是否提供备份完成时对备份数据进行完整性校验的功能；

2) 通过检查备份系统和备份数据，确认是否提供定期进行备份数据完整性校验的功能。

c) 结果判定

根据 5.2.8 的要求进行判定。

6.2.9 恢复粒度

a) 预置条件

1) 数据备份与恢复系统已建设完成；
2) 被测机构为测试人员提供数据备份与恢复系统测试帐号；
3) 测试人员具有访问数据备份系统数据恢复功能的权限。

b) 测评步骤
1) 通过数据恢复测试，确认是否只能进行数据的全量恢复；
2) 通过数据恢复测试，确认是否能够进行细粒度的数据恢复，包括单文件／文件夹恢复、数据库单表恢复等；
3) 通过数据恢复测试，确认是否支持操作系统／虚拟机／容器备份的内部单文件恢复。

c) 结果判定
根据 5.2.9 的要求进行判定。

6.2.10 恢复演练

a) 预置条件
1) 数据备份与恢复系统已建设完成；
2) 被测机构已制定备份恢复管理制度规范；
3) 被测机构为测试人员提供数据备份与恢复系统测试帐号；
4) 测试人员具有访问数据备份与恢复系统恢复演练支持功能的权限。

b) 测评步骤
1) 检查组织备份管理制度，确认是否具有每年一次恢复演练的要求，并且备份系统提供相应支持；
2) 检查组织备份管理制度，确认是否具有每半年一次恢复演练的要求，并且备份系统提供相应支持；
3) 检查组织备份管理制度，确认是否具有每三个月一次恢复演练的要求，并且备份系统提供相应支持；
4) 检查组织备份管理制度，确认是否具有每个月一次恢复演练的要求，并且备份系统提供相应支持。

c) 结果判定
根据 5.2.10 的要求进行判定。

6.2.11 备份工具

a) 预置条件
1) 组织已经开始进行数据备份；
2) 测试人员具有访问被测组织备份工具和备份数据的权限。

b) 测评步骤
1) 检查组织所采用的备份工具，确认是否仅通过手工拷贝或脚本实现数据备份；
2) 检查组织所采用的备份工具，确认是否通过专业备份软件实现数据备份；
3) 检查组织所采用的备份工具，确认是否通过专业备份软件和专业硬件实现数据备份。

c) 结果判定
根据 5.2.11 的要求进行判定。

6.2.12 数据迁移

a) 预置条件
1) 数据备份与恢复系统已建设完成；

2) 数据备份与恢复系统提供备份数据导出功能；
3) 被测机构提供其数据备份系统所支持数据迁移的备份系统；
4) 被测机构为测试人员提供数据备份与恢复系统测试帐号；
5) 测试人员具有所有备份系统的数据导入和导出权限。

b) 测评步骤

1) 通过备份系统功能测试，确认是否备份系统本身或通过辅助工具支持统一备份不同版本之间的数据迁移；
2) 通过备份系统功能测试，确认是否备份系统本身或通过辅助工具支持不同备份系统之间的数据迁移。

c) 结果判定

根据 5.2.12 的要求进行判定。

6.2.13 恢复点目标

a) 预置条件

1) 数据备份与恢复系统已建设完成；
2) 被测机构为测试人员提供数据备份与恢复系统测试帐号；
3) 测试人员具有进行数据备份和恢复的权限。

b) 测评步骤

1) 通过数据恢复测试，确认是否恢复点目标在 1 天至 7 天之间；
2) 通过数据恢复测试，确认是否恢复点目标在数小时到 1 天之间；
3) 通过数据恢复测试，确认是否恢复点目标在 0 到 30 分钟之间；
4) 通过数据恢复测试，确认是否恢复点目标为 0，即数据不会丢失。

c) 结果判定

根据 5.2.13 的要求进行判定。

6.2.14 恢复时间目标

a) 预置条件

1) 数据备份与恢复系统已建设完成；
2) 被测机构为测试人员提供数据备份与恢复系统测试帐号；
3) 测试人员具有进行数据备份和恢复的权限。

b) 测评步骤

1) 通过数据恢复测试，确认是否数据恢复时间在 2 天以上；
2) 通过数据恢复测试，确认是否数据恢复时间在 24 小时以上；
3) 通过数据恢复测试，确认是否数据恢复时间在 12 小时以上；
4) 通过数据恢复测试，确认是否数据恢复时间在 1 小时以上；
5) 通过数据恢复测试，确认是否数据恢复时间在 1 分钟以上；
6) 通过数据恢复测试，确认是否数据恢复时间在 1 分钟以内。

c) 结果判定

根据 5.2.14 的要求进行判定。

6.2.15 数据加密

a) 预置条件

1) 数据备份与恢复系统已建设完成；

2) 数据备份与恢复系统提供查看加密方式的接口；
3) 数据备份与恢复系统提供查看存储备份数据的接口；
4) 被测机构为测试人员提供数据备份与恢复系统测试帐号；
5) 测试人员具有查看备份加密方式和备份数据的权限。

b) 测评步骤
1) 检查组织备份数据的加密方式，确认是否支持数据的加密存储；
2) 检查组织备份数据的加密方式，确认是否支持数据的加密传输和存储；
3) 检查组织备份数据的加密方式，确认是否支持数据的源端加密、加密传输和加密存储；
4) 检查组织备份数据的加密方式，确认是否加密强度为弱；
5) 检查组织备份数据的加密方式，确认是否加密强度为中；
6) 检查组织备份数据的加密方式，确认是否加密强度为强；
7) 检查组织备份数据的加密方式，确认是否支持国密算法。

c) 结果判定
根据 5.2.15 的要求进行判定。

6.2.16 访问控制

a) 预置条件
1) 数据备份与恢复系统已建设完成；
2) 数据备份与恢复系统支持用户身份认证和数据授权访问；
3) 被测机构为测试人员提供数据备份与恢复系统测试帐号；
4) 测试人员具有查看身份认证和权限控制功能的权限。

b) 测评步骤
1) 检查组织备份系统和数据的访问控制方式，确认是否采用口令系统进行身份鉴别；
2) 检查组织备份系统和数据的访问控制方式，确认是否采用智能卡、证书、生物特征等方式进行身份鉴别；
3) 检查组织备份系统和数据的访问控制方式，确认是否采用多因子认证方式进行身份鉴别；
4) 检查组织备份系统和数据的访问控制方式，确认是否采用基于功能的权限控制；
5) 检查组织备份系统和数据的访问控制方式，确认是否采用基于数据的权限控制。

c) 结果判定
根据 5.2.16 的要求进行判定。

6.2.17 安全审计

a) 预置条件
1) 数据备份与恢复系统已建设完成；
2) 数据备份与恢复系统提供安全审计日志功能；
3) 被测机构为测试人员提供数据备份与恢复系统测试帐号；
4) 测试人员具有访问安全审计日志的权限。

b) 测评步骤
1) 检查组织审计日志，确认是否包含用户注册、登录、注销等信息；
2) 检查组织审计日志，确认是否包含用户操作审计信息；
3) 检查组织审计日志，确认是否包含备份恢复作业执行情况信息；
4) 检查组织审计日志，确认是否审计日志的访问需要授权。

c) 结果判定

根据 5.2.17 的要求进行判定。

6.2.18 数据转存

a) 预置条件

1) 数据备份与恢复系统已建设完成；
2) 组织提供数据转存工具支持；
3) 测试人员具有访问使用数据转存工具的权限。

b) 测评步骤

1) 检查组织转储工具，确认是否支持纸质数据的电子化；
2) 检查组织转储工具，确认是否支持本地介质的数据转存功能；
3) 检查组织转储工具，确认是否支持异地介质的数据转存功能。

c) 结果判定

根据 5.2.18 的要求进行判定。

6.2.19 备用系统

a) 预置条件

1) 组织提供备用系统支持；
2) 测试人员具有访问备用系统的权限。

b) 测评步骤

1) 检查组织备用数据处理系统，确认是否具有与生产系统一致的能力，是否处于就绪状态或运行状态，是否具有自动切换能力；
2) 检查组织备用通信线路，确认是否具有与生产系统同等级的能力；
3) 检查组织备用网络设备，确认是否具有与生产系统同等级的能力，是否处于就绪或运行状态，是否具有自动切换能力。

c) 结果判定

根据 5.2.19 的要求进行判定。

7 评级要求

数据备份与恢复服务能力成熟度等级的评测需要遵循表1执行。

表 1 数据备份与恢复服务能力成熟度等级的评测表

序号	评测要素		评级要求					
			DBR1	DBR2	DBR3	DBR4	DBR5	DBR6
1	管理要求	5.1.1 人员配置	A	A	A	B	C	C
2		5.1.2 管理规范	A	A	B	B	C	C
3		5.1.3 人员培训	—	—	A	B	B	B
4	技术要求	5.2.1 备份范围	A	A	B	B	C	C
5		5.2.2 备份对象	A	A	B	B	C	C
6		5.2.3 备份方法	A|B	A|B	B	B	C	C
7		5.2.4 备份周期	A	A	B	C	D	E
8		5.2.5 保存时长	A	A	B	C	D	E
9		5.2.6 备份介质	B	B	B	B	AB	AB

10		5.2.7 保存位置	A	A	B	C	D	D
11		5.2.8 数据校验	A	A	A	B	B	B
12		5.2.9 恢复粒度	A	A	A	AB	AB	ABC
13		5.2.10 恢复演练	A	A	B	B	C	C
14		5.2.11 备份工具	A	A	B	B	C	C
15		5.2.12 数据迁移	A	A	B	B	B	B
16		5.2.13 恢复点目标	A	A	B	C	D	D
17		5.2.14 恢复时间目标	A	B	C	C	E	F
18		5.2.15 数据加密	-	AD	BE	CE	CF	CFG
19		5.2.16 访问控制	-	AD	AD	BD	CE	CE
20		5.2.17 安全审计	-	-	A	B	C	D
21		5.2.18 数据转存	-	-	A	AB	AB	AC
22		5.2.19 备用系统	-	A	B	C	D	E

说明：

1. 在上表中，每个值代表要达到该要求的等级，该项评测要素需要达到的最低标准；
2. 针对每一成熟度等级，需要满足所有评测要素的最低要求；
3. “-”表示对于该等级，此项评测要素不做要求。

附录 A.
（规范性附录）
数据资产价值评估标准

组织可按照机密性、完整性和可用性对数据资产进行评估分级，评估标准如下：

机密性

评分	描述
3	除工作职责必需之外，必须经过拥有者同意后方可使用或阅读。
2	仅签有保密协议的人员或主管机关可以使用。
1	为公开信息，不具机密性。

完整性

评分	描述
3	该数据的完整性可能影响法令是否遵循，会对该信息资产有重大影响且可能导致严重的业务中断。
2	该数据的完整性可能影响业务导致效能降低，但不致对业务造成停顿。
1	该数据的完整性对该信息资产的影响极低，且不会对业务运作的效能造成任何影响或影响极低。

可用性

评分	描述
3	该数据若未及时取得，可能直接影响营运业务或法令的遵循。
2	该数据若未及时取得，可能导致作业上的不便。
1	该资料并无时效性的问题。

数据资产价值计算公式：

数据资产价值 = 机密性评估值 + 完整性评估值 + 可用性评估值。

数据资产评级表

数据资产价值	评级
9	I 级
6 ～ 8	II 级
3 ～ 5	III 级