

DB43

湖南省地方标准

DB43/T 1843—2020

信息安全技术 区块链数据安全技术测评要求

Information security technology - Evaluation requirements
for blockchain data security technology

地方标准信息服务平台

2020-09-30发布

2020-12-30实施

湖南省市场监督管理局 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 等级测评概述..... 1

 4.1 等级测评方法..... 1

 4.2 单项测评..... 2

5 第一级测评要求..... 2

 5.1 数据存储测评要求 2

 5.2 数据传输测评要求 3

 5.3 数据访问测评要求 4

 5.4 区块数据测评要求 5

 5.5 数据管理测评要求 5

6 第二级测评要求..... 6

 6.1 数据存储测评要求 6

 6.2 数据传输测评要求 8

 6.3 数据访问测评要求 9

 6.4 区块数据测评要求 10

 6.5 数据管理测评要求 10

7 第三级测评要求..... 11

 7.1 数据存储测评要求 11

 7.2 数据传输测评要求 13

 7.3 数据访问测评要求 14

 7.4 区块数据测评要求 15

 7.5 数据管理测评要求 16

8 第四级测评要求..... 17

 8.1 数据存储测评要求 17

 8.2 数据传输测评要求 19

 8.3 数据访问测评要求 20

 8.4 区块数据测评要求 21

 8.5 数据管理测评要求 22

9 测评结论 23

 9.1 风险分析和评价 23

9.2 等级测评结论	23
参考文献	25

地方标准信息服务平台

前 言

本文件按照 GB/T 1.1—2020 给出的规则起草。

本文件由中共湖南省委网络安全和信息化委员会办公室提出。

本文件由湖南省区块链和分布式记账技术标准化技术委员会（筹）归口。

本文件起草单位：湖南链信安科技有限公司、湖南天河国云科技有限公司、湖南省东方区块链安全技术检测中心、湖南省人民政府发展研究中心、湖南天河云链科技有限公司。

本文件主要起草人：梁琪、杨征、李财、陈昕、谭林、聂璐璐、梁亮、聂朗、尹海波、黄帅、汪武、柳兴、郭慧、殷新文、丁雅琪、沈浪、张祥、宋姝、姜载乐、刘齐平、郑婷婷、胡钦、邹曼瑜等。

地方标准信息服务平台

信息安全技术 区块链数据安全技术测评要求

1 范围

本文件规定了区块链数据安全技术测评指标要求。包括第一级、第二级、第三级和第四级区块链数据安全技术测评要求。

本文件适用于测评机构对区块链数据安全进行的测评工作，也适用于区块链技术开发者参考使用。

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—2010 信息安全技术 术语

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 术语和定义

GB/T 25069—2010、GB/T 29765—2013 界定的下列术语和定义适用于本文件。

3.1

区块 block

区块链中存放电子记录的块式数据结构。

3.2

区块激励 block reward

区块链体系给予区块生产者创建区块的奖励。

3.3

口令 password

用于身份鉴别的秘密的字、短语、数字或字符序列，通常是被默记的弱秘密。

[GB/T 25069—2010]

3.4

数据恢复 data recovery

利用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。

[GB/T 29765—2013]

4 等级测评概述

4.1 等级测评方法

等级测评实施的基本方法是针对待定的测评对象，采用相关的测评手段，遵从一定的测评规程，获取需要的证据数据，给出是否达到特定级别安全保护能力的评判。

本标准中针对每一个要求项的测评就构成一个单项测评,针对某个要求项的所有具体测评内容构成测评实施。根据调研结果,分析等级保护对象的业务流程和数据流,确定测评工作范围。结合等级保护对象的安全级别进行综合分析,测评对象可以根据类别加以描述,包括数据存储、数据传输、数据访问、区块数据、数据管理。

本标准中每个级别测评要求都包括数据存储测评要求、数据传输测评要求、数据访问测评要求、区块数据测评要求、数据管理测评要求五部分内容。

4.2 单项测评

单项测评是针对各安全要求项的测评,支持测评结果的可重复性和可再现性。本标准中单项测评包括测评指标、测评对象、测评实施和测评判定结果构成。

5 第一级测评要求

5.1 数据存储测评要求

5.1.1 数据存储机密性

该测评单元包括以下要求:

- a) 测评指标: 应保证数据存储机密性。
- b) 测评对象: 数据存储形式。
- c) 测评实施包括以下内容:
 - 1) 在数据存储过程中是否采用密文的形式进行存储。
- d) 测评判定: 如果以上测评实施内容为肯定,则符合本测评单元指标要求,否则不符合本测评单元指标要求。

5.1.2 数据存储完整性

该测评单元包括以下要求:

- a) 测评指标: 应保证数据存储完整性。
- b) 测评对象: 数据存储策略。
- c) 测评实施包括以下内容:
 - 1) 数据存储是否建立数据存储冗余策略和管理制度,及数据备份与恢复操作过程规范。
- d) 测评判定: 如果以上测评实施内容为肯定,则符合本测评单元指标要求,否则不符合本测评单元指标要求。

5.1.3 数据存储可靠性

该测评单元包括以下要求:

- a) 测评指标: 应保证数据存储可靠性。
- b) 测评对象: 数据存储策略类。
- c) 测评实施包括以下内容:
 - 1) 数据存储时是否具有存储策略类文档,文档内容包括但不限于存储管理制度和数据备份操作;
 - 2) 数据存储内容是否包含完整的用户访问记录、数据处理记录等内容。
- d) 测评判定: 如果以上测评实施内容均为肯定,则符合本测评单元指标要求,否则不符合或部分

符合本测评单元指标要求。

5.1.4 数据备份可用性

该测评单元包括以下要求：

- a) 测评指标：保证数据备份可用性。
- b) 测评对象：数据备份与恢复能力。
- c) 测评实施包括以下内容：
 - 1) 重要数据是否具有备份机制；
 - 2) 重要数据是否设置数据定期备份的策略。
- d) 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

5.1.5 数据恢复可用性

该测评单元包括以下要求：

- a) 测评指标：应保证数据恢复功能可用性。
- b) 测评对象：遇到故障时数据恢复能力。
- c) 测评实施包括以下内容：
 - 1) 是否具有数据故障处置预案。
- d) 测评判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

5.2 数据传输测评要求

5.2.1 数据传输机密性

该测评单元包括以下要求：

- a) 测评指标：应保证数据传输过程中区块链数据的机密性。
- b) 测评对象：数据传输策略。
- c) 测评实施包括以下内容：
 - 1) 数据传输过程是否采用加密技术；
 - 2) 数据传输是否在已授权节点之间进行。
- d) 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

5.2.2 数据传输完整性

该测评单元包括以下要求：

- a) 测评指标：应保证数据传输过程中区块链数据的完整性。
- b) 测评对象：数据传输策略。
- c) 测评实施包括以下内容：
 - 1) 在数据传输过程中是否提供数据完整性验证协议。
- d) 测评判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

5.2.3 数据传输可靠性

该测评单元包括以下要求：

- a) 测评指标：应保证数据传输过程中区块链数据的可靠性。
- b) 测评对象：数据传输策略。
- c) 测评实施包括以下内容：
 - 1) 传输连接建立之前，是否对发送方和接收方进行身份鉴别操作，例如利用密码技术进行初始化会话验证；
 - 2) 数据传输过程中是否采用加解密技术。
- d) 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

5.2.4 数据传输可用性

该测评单元包括以下要求：

- a) 测评指标：应保证数据传输过程中区块链数据的可用性。
- b) 测评对象：数据传输策略。
- c) 测评实施包括以下内容：
 - 1) 通过传输接收到的数据是否与系统采用统一时间标准。
- d) 测评判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

5.3 数据访问测评要求

5.3.1 访问权限控制

该测评单元包括以下要求：

- a) 测评指标：应保证设置数据访问控制权限、访问控制策略。
- b) 测评对象：数据访问权限控制功能。
- c) 测评实施包括以下内容：
 - 1) 是否具有数据访问权限控制策略。
- d) 测评判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

5.3.2 数据访问处理

该测评单元包括以下要求：

- a) 测评指标：应保证数据处理时明确处理的目的和范围、遵守数据使用规范。
- b) 测评对象：数据访问流程。
- c) 测评实施包括以下内容：
 - 1) 是否根据法律法规要求，明确数据处理的目的和范围；
 - 2) 是否设置数据访问处理规范类文档及相关违规处理的惩戒措施。
- d) 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

5.3.3 加密访问控制

该测评单元包括以下要求：

- a) 测评指标：应保证对数据进行加密访问控制、数据访问权限设置采用多私钥规则以及属性加密

等规则。

- b) 测评对象：数据访问权限控制。
- c) 测评实施包括以下内容：
 - 1) 数据是否通过加密方式进行访问控制。
- d) 测评判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

5.3.4 数据服务

该测评单元包括以下要求：

- a) 测评指标：应指定数据服务安控制策略和明确安全规范。
- b) 测评对象：数据服务功能。
- c) 测评实施包括以下内容：
 - 1) 数据服务是否制定安全控制策略，明确规定使用服务的安全限制和安全控制措施，如身份鉴别、授权策略、访问控制机制、签名、时间戳、安全协议等。
- d) 测评判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

5.4 区块数据测评要求

5.4.1 区块激励机制

该测评单元包括以下要求：

- a) 测评指标：应保证设置合法、合理的区块激励机制。
- b) 测评对象：区块激励机制。
- c) 测评实施包括以下内容：
 - 1) 是否具有区块激励机制。
- d) 测评判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

5.4.2 区块防攻击能力

该测评单元包括以下要求：

- a) 测评指标：应保证区块大小在安全范围内，并具备一定的防攻击能力。
- b) 测评对象：区块程序。
- c) 测评实施包括以下内容：
 - 1) 区块大小是否在安全范围内。
- d) 测评判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

5.5 数据管理测评要求

5.5.1 数据管理制度

该测评单元包括以下要求：

- a) 测评指标：应制定区块链数据安全工作的总体方针、数据安全策略。
- b) 测评对象：总体方针策略类文档、数据安全管理制度类文档。

c) 测评实施包括以下内容：

- 1) 数据安全工作的总体方针和安全策略文件是否明确规定数据安全工作的总体目标范围、原则以及各类安全策略等；
- 2) 数据管理制度是否覆盖数据库、区块数据、数据存储、数据传输等管理内容。

d) 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

5.5.2 数据管理机构

该测评单元包括以下要求：

a) 测评指标：应设立适合区块链系统的数据管理机构。

b) 测评对象：数据制度。

c) 测评实施包括以下内容：

- 1) 各类数据变更记录是否针对数据存储变更、数据操作记录、数据访问等事项进行及时记录。

d) 测评判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

5.5.3 数据管理人员

该测评单元包括以下要求：

a) 测评指标：应配备完善的数据管理人员体系。

b) 测评对象：数据管理制度。

c) 测评实施包括以下内容：

- 1) 是否制定数据服务人力资源安全策略，明确不同岗位人员在数据生命周期各阶段数据服务和系统服务相关的工作范畴和安全管控措施；
- 2) 是否制定数据服务人员招聘、录用、上岗、调岗、离岗、考核、选拔等人员安全管理制度；
- 3) 是否在录用重要岗位人员前对其进行背景调查，确保符合相关的法律、法规合同和道德要求，并与所有涉及数据服务岗位人员签订安全责任协议；
- 4) 是否在重要岗位人员调离或终止劳动合同时，与其签订保密协议。

d) 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6 第二级测评要求

6.1 数据存储测评要求

6.1.1 数据存储机密性

该测评单元包括以下要求：

a) 测评指标：应保证数据存储机密性。

b) 测评对象：数据存储形式。

c) 测评实施包括以下内容：

- 1) 在数据存储过程中是否采用密文的形式进行存储；
- 2) 在数据存储时是否设置用户访问权限；
- 3) 数据信息是否进行安全保护分级。

- d) 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.2 数据存储完整性

该测评单元包括以下要求：

- a) 测评指标：应保证数据存储完整性。
- b) 测评对象：数据存储策略。
- c) 测评实施包括以下内容：
 - 1) 数据存储是否建立数据存储冗余策略和管理制度，及数据备份与恢复操作过程规范；
 - 2) 数据存储是否具有数据完整性验证机制。
- d) 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.3 数据存储可靠性

该测评单元包括以下要求：

- a) 测评指标：应保证数据存储可靠性。
- b) 测评对象：数据存储策略类。
- c) 测评实施包括以下内容：
 - 1) 数据存储时是否具有存储策略类文档，文档内容包括但不限于存储管理制度和数据备份操作；
 - 2) 数据存储内容是否包含完整的用户访问记录、数据处理记录等内容；
 - 3) 数据存储是否建立数据的细颗粒度审计机制。
- d) 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.4 数据备份可用性

该测评单元包括以下要求：

- a) 测评指标：保证数据备份可用性。
- b) 测评对象：数据备份与恢复能力。
- c) 测评实施包括以下内容：
 - 1) 重要数据是否具有备份机制；
 - 2) 重要数据是否设置数据定期备份的策略；
 - 3) 是否采用分散式方式进行数据备份；
 - 4) 是否建立备份操作过程规范，包括备份日志记录规范。
- d) 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.5 数据恢复可用性

该测评单元包括以下要求：

- a) 测评指标：应保证数据恢复功能可用性。
- b) 测评对象：遇到故障时数据恢复能力。
- c) 测评实施包括以下内容：

- 1) 是否具有数据故障处置预案;
 - 2) 故障预案是否能及时解决故障并迅速恢复数据;
 - 3) 是否建立恢复操作过程规范, 包括恢复日志记录规范;
 - 4) 在节点重新接入区块时, 是否能重新恢复数据。
- d) 测评判定: 如果以上测评实施内容均为肯定, 则符合本测评单元指标要求, 否则不符合或部分符合本测评单元指标要求。

6.2 数据传输测评要求

6.2.1 数据传输机密性

该测评单元包括以下要求:

- a) 测评指标: 应保证数据传输过程中区块链数据的机密性。
- b) 测评对象: 数据传输策略。
- c) 测评实施包括以下内容:
 - 1) 数据传输过程是否采用加密技术;
 - 2) 数据传输是否在已授权节点之间进行;
 - 3) 机密和绝密数据是否在传输过程中使用数字签名。
- d) 测评判定: 如果以上测评实施内容均为肯定, 则符合本测评单元指标要求, 否则不符合或部分符合本测评单元指标要求。

6.2.2 数据传输完整性

该测评单元包括以下要求:

- a) 测评指标: 应保证数据传输过程中区块链数据的完整性。
- b) 测评对象: 数据传输策略。
- c) 测评实施包括以下内容:
 - 1) 在数据传输过程中是否提供数据完整性验证协议;
 - 2) 数据传输协议是否能够保证业务数据的传输完整性。
- d) 测评判定: 如果以上测评实施内容为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.2.3 数据传输可靠性

该测评单元包括以下要求:

- a) 测评指标: 应保证数据传输过程中区块链数据的可靠性。
- b) 测评对象: 数据传输策略。
- c) 测评实施包括以下内容:
 - 1) 传输连接建立之前, 是否对发送方和接收方进行身份鉴别操作, 例如利用密码技术进行初始化会话验证;
 - 2) 数据传输过程中是否采用加解密技术;
 - 3) 数据传输是否采用满足数据传输安全策略的相应安全控制措施, 如安全通道、可信通道、数据加密等。
- d) 测评判定: 如果以上测评实施内容均为肯定, 则符合本测评单元指标要求, 否则不符合或部分符合本测评单元指标要求。

6.2.4 数据传输可用性

该测评单元包括以下要求：

- a) 测评指标：应保证数据传输过程中区块链数据的可用性。
- b) 测评对象：数据传输策略。
- c) 测评实施包括以下内容：
 - 1) 通过传输接收到的数据是否与系统采用统一时间标准；
 - 2) 是否具备对传输数据的可用性进行检测的能力。
- d) 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.3 数据访问测评要求

6.3.1 访问权限控制

该测评单元包括以下要求：

- a) 测评指标：应保证设置数据访问控制权限、访问控制策略。
- b) 测评对象：数据访问权限控制功能。
- c) 测评实施包括以下内容：
 - 1) 是否具有数据访问权限控制策略；
 - 2) 针对系统中安全相关的操作，例如备份作业、日志访问、策略管理等，是否具备安全策略；
 - 3) 是否具有访问错误次数限制机制，例如当异常操作次数超过三次时，应能阻止该用户的进一步操作尝试。
- d) 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.3.2 数据访问处理

该测评单元包括以下要求：

- a) 测评指标：应保证数据处理时明确处理的目的和范围、遵守数据使用规范。
- b) 测评对象：数据访问流程。
- c) 测评实施包括以下内容：
 - 1) 是否根据法律法规要求，明确数据处理的目的和范围；
 - 2) 是否设置数据访问处理规范类文档及相关违规处理的惩戒措施；
 - 3) 是否建立特定操作日志文档，记录和管理区块链数据访问处理活动中的相关操作。
- d) 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.3.3 加密访问控制

该测评单元包括以下要求：

- a) 测评指标：应保证对数据进行加密访问控制、数据访问权限设置采用多私钥规则以及属性加密等规则。
- b) 测评对象：数据访问权限控制。
- c) 测评实施包括以下内容：
 - 1) 数据是否通过加密方式进行访问控制；

2) 数据访问权限设置是否采用属性加密方法进行访问权限控制。

- d) 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.3.4 数据服务

该测评单元包括以下要求：

- a) 测评指标：应指定数据服务安控制策略和明确安全规范。
- b) 测评对象：数据服务功能。
- c) 测评实施包括以下内容：
 - 1) 数据服务是否制定安全控制策略，明确规定使用服务的安全限制和安全控制措施，如身份鉴别、授权策略、访问控制机制、签名、时间戳、安全协议等；
 - 2) 数据服务是否明确安全规范，包括服务名称、服务参数、服务安全要求等，具备对服务不安全参数进行限制或过滤能力，为服务提供异常处理能力。
- d) 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.4 区块数据测评要求

6.4.1 区块激励机制

该测评单元包括以下要求：

- a) 测评指标：应保证设置合法、合理的区块激励机制。
- b) 测评对象：区块激励机制。
- c) 测评实施包括以下内容：
 - 1) 是否具有区块激励机制；
 - 2) 区块激励机制是否合理、合法。
- d) 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.4.2 区块防攻击能力

该测评单元包括以下要求：

- a) 测评指标：应保证区块大小在安全范围内，并具备一定的防攻击能力。
- b) 测评对象：区块程序。
- c) 测评实施包括以下内容：
 - 1) 区块大小是否在安全范围内；
 - 2) 区块是否能有效防御竞态攻击等同类攻击；
 - 3) 区块是否能有效防御芬尼攻击等同类攻击；
 - 4) 区块是否能有效防御 51%算力攻击等同类攻击。
- d) 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.5 数据管理测评要求

6.5.1 数据管理制度

该测评单元包括以下要求：

- a) 测评指标：应制定区块链数据安全工作的总体方针、数据安全策略。
- b) 测评对象：总体方针策略类文档、数据安全管理制度类文档。
- c) 测评实施包括以下内容：
 - 1) 数据安全工作的总体方针和安全策略文件是否明确规定数据安全工作的总体目标范围、原则以及各类安全策略等；
 - 2) 数据管理制度是否覆盖数据库、区块数据、数据存储、数据传输等管理内容；
 - 3) 数据安全管理人员是否定期对数据安全管理制度合理性和适用性进行评审修订。
- d) 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.5.2 数据管理机构

该测评单元包括以下要求：

- a) 测评指标：应设立适合区块链系统的数据管理机构。
- b) 测评对象：数据制度。
- c) 测评实施包括以下内容：
 - 1) 各类数据变更记录是否针对数据存储变更、数据操作记录、数据访问等事项进行及时记录；
 - 2) 是否建立安全领导小组，指定机构最高管理者或授权代表担任小组组长，并明确组长责任与权力；
 - 3) 是否建立机构内部监督管理职能部门，对数据管理和各用户操作行为进行安全监督管理。
- d) 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.5.3 数据管理人员

该测评单元包括以下要求：

- a) 测评指标：应配备完善的数据管理人员体系。
- b) 测评对象：数据管理制度。
- c) 测评实施包括以下内容：
 - 1) 是否制定数据服务人力资源安全策略，明确不同岗位人员在数据生命周期各阶段数据服务和系统服务相关的工作范畴和安全管控措施；
 - 2) 是否制定数据服务人员招聘、录用、上岗、调岗、离岗、考核、选拔等人员安全管理制度；
 - 3) 是否在录用重要岗位人员前对其进行背景调查，确保符合相关的法律、法规合同和道德要求，并与所有涉及数据服务岗位人员签订安全责任协议；
 - 4) 是否在重要岗位人员调离或终止劳动合同时，与其签订保密协议；
 - 5) 是否明确数据服务重要岗位的兼职和轮岗、权限分离、多人共管等安全管理要求；
 - 6) 是否建立人员安全责任奖惩管理制度，并按照规定对造成数据服务损失的人员给予相应的处理，记录并保存相关信息。
- d) 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7 第三级测评要求

7.1 数据存储测评要求

7.1.1 数据存储机密性

该测评单元包括以下要求：

- a) 测评指标：应保证数据存储机密性。
- b) 测评对象：数据存储形式。
- c) 测评实施包括以下内容：
 - 1) 在数据存储过程中是否采用密文的形式进行存储；
 - 2) 在数据存储时是否设置用户访问权限；
 - 3) 数据信息是否进行安全保护分级。
- d) 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.2 数据存储完整性

该测评单元包括以下要求：

- a) 测评指标：应保证数据存储完整性。
- b) 测评对象：数据存储策略。
- c) 测评实施包括以下内容：
 - 1) 数据存储是否建立数据存储冗余策略和管理制度，及数据备份与恢复操作过程规范；
 - 2) 数据存储是否具有数据完整性验证机制。
- d) 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.3 数据存储可靠性

该测评单元包括以下要求：

- a) 测评指标：应保证数据存储可靠性。
- b) 测评对象：数据存储策略类。
- c) 测评实施包括以下内容：
 - 1) 数据存储时是否具有存储策略类文档，文档内容包括但不限于存储管理制度和数据备份操作；
 - 2) 数据存储内容是否包含完整的用户访问记录、数据处理记录等内容；
 - 3) 数据存储是否建立数据的细颗粒度审计机制；
 - 4) 数据存储架构是否可伸缩，以满足数据量持续增长、数据分类分级存储等需求。
- d) 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.4 数据备份可用性

该测评单元包括以下要求：

- a) 测评指标：保证数据备份可用性。
- b) 测评对象：数据备份与恢复能力。
- c) 测评实施包括以下内容：
 - 1) 重要数据是否具有备份机制；
 - 2) 重要数据是否设置数据定期备份的策略；

- 3) 是否采用分散式方式进行数据备份;
- 4) 是否建立备份操作过程规范, 包括备份日志记录规范;
- 5) 是否明确数据逻辑存储隔离授权与操作规范、确保具备数据存储安全隔离能力。
- d) 测评判定: 如果以上测评实施内容均为肯定, 则符合本测评单元指标要求, 否则不符合或部分符合本测评单元指标要求。

7.1.5 数据恢复可用性

该测评单元包括以下要求:

- a) 测评指标: 应保证数据恢复功能可用性。
- b) 测评对象: 遇到故障时数据恢复能力。
- c) 测评实施包括以下内容:
 - 1) 是否具有数据故障处置预案;
 - 2) 故障预案是否能及时解决故障并迅速恢复数据;
 - 3) 是否建立恢复操作过程规范, 包括恢复日志记录规范;
 - 4) 在节点重新接入区块时, 是否能重新恢复数据;
 - 5) 在数据故障时是否具备自动恢复能力。
- d) 测评判定: 如果以上测评实施内容均为肯定, 则符合本测评单元指标要求, 否则不符合或部分符合本测评单元指标要求。

7.2 数据传输测评要求

7.2.1 数据传输机密性

该测评单元包括以下要求:

- a) 测评指标: 应保证数据传输过程中区块链数据的机密性。
- b) 测评对象: 数据传输策略。
- c) 测评实施包括以下内容:
 - 1) 数据传输过程是否采用加密技术;
 - 2) 数据传输是否在已授权节点之间进行;
 - 3) 机密和绝密数据是否在传输过程中使用数字签名;
 - 4) 数字签名的密钥的类型、属性以及密钥长度是否达到安全需求。
- d) 测评判定: 如果以上测评实施内容均为肯定, 则符合本测评单元指标要求, 否则不符合或部分符合本测评单元指标要求。

7.2.2 数据传输完整性

该测评单元包括以下要求:

- a) 测评指标: 应保证数据传输过程中区块链数据的完整性。
- b) 测评对象: 数据传输策略。
- c) 测评实施包括以下内容:
 - 1) 在数据传输过程中是否提供数据完整性验证协议;
 - 2) 数据传输协议是否能够保证业务数据的传输完整性。
- d) 测评判定: 如果以上测评实施内容为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

7.2.3 数据传输可靠性

该测评单元包括以下要求：

- a) 测评指标：应保证数据传输过程中区块链数据的可靠性。
- b) 测评对象：数据传输策略。
- c) 测评实施包括以下内容：
 - 1) 传输连接建立之前，是否对发送方和接收方进行身份鉴别操作，例如利用密码技术进行初始化会话验证；
 - 2) 数据传输过程中是否采用加解密技术；
 - 3) 数据传输是否采用满足数据传输安全策略的相应安全控制措施，如安全通道、可信通道、数据加密等；
 - 4) 重要数据传输时是否采用隐蔽、随机化等方式的传输协议，或者采用专用的传输协议等，保障数据传输过程中数据安全性。
- d) 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.2.4 数据传输可用性

该测评单元包括以下要求：

- a) 测评指标：应保证数据传输过程中区块链数据的可用性。
- b) 测评对象：数据传输策略。
- c) 测评实施包括以下内容：
 - 1) 通过传输接收到的数据是否与系统采用统一时间标准；
 - 2) 是否具备对传输数据的可用性进行检测的能力；
 - 3) 数据传输过程中是否具有数据自动矫正机制。
- d) 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.3 数据访问测评要求

7.3.1 访问权限控制

该测评单元包括以下要求：

- a) 测评指标：应保证设置数据访问控制权限、访问控制策略。
- b) 测评对象：数据访问权限控制功能。
- c) 测评实施包括以下内容：
 - 1) 是否具有数据访问权限控制策略；
 - 2) 针对系统中安全相关的操作，例如备份作业、日志访问、策略管理等，是否具备安全策略；
 - 3) 是否具有访问错误次数限制机制，例如当异常操作次数超过三次时，应能阻止该用户的进一步操作尝试；
 - 4) 是否具有访问超时锁定功能，例如在设定时间段内没有任何操作，系统会自动终止会话，需要再次进行身份鉴别才能够重新操作。
- d) 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.3.2 数据访问处理

该测评单元包括以下要求：

- a) 测评指标：应保证数据处理时明确处理的目的和范围、遵守数据使用规范。
- b) 测评对象：数据访问流程。
- c) 测评实施包括以下内容：
 - 1) 是否根据法律法规要求，明确数据处理的目的和范围；
 - 2) 是否设置数据访问处理规范类文档及相关违规处理的惩戒措施；
 - 3) 是否建立特定操作日志文档，记录和管理区块链数据访问处理活动中的相关操作；
 - 4) 是否设置风险评估体系，评估数据访问处理结果，避免数据处理过程中涉及到相关敏感等重要数据。
- d) 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.3.3 加密访问控制

该测评单元包括以下要求：

- a) 测评指标：应保证对数据进行加密访问控制、数据访问权限设置采用多私钥规则以及属性加密等规则。
- b) 测评对象：数据访问权限控制。
- c) 测评实施包括以下内容：
 - 1) 数据是否通过加密方式进行访问控制；
 - 2) 数据访问权限设置是否采用属性加密方法进行访问权限控制；
 - 3) 数据访问权限设置是否采用多层加密规则。
- d) 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.3.4 数据服务

该测评单元包括以下要求：

- a) 测评指标：应指定数据服务安全控制策略和明确安全规范。
- b) 测评对象：数据服务功能。
- c) 测评实施包括以下内容：
 - 1) 数据服务是否制定安全控制策略，明确规定使用服务的安全限制和安全控制措施，如身份鉴别、授权策略、访问控制机制、签名、时间戳、安全协议等；
 - 2) 数据服务是否明确安全规范，包括服务名称、服务参数、服务安全要求等，具备对服务不安全参数进行限制或过滤能力，为服务提供异常处理能力；
 - 3) 数据服务调用是否采用安全通道、加密传输等机制。
- d) 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.4 区块数据测评要求

7.4.1 区块激励机制

该测评单元包括以下要求：

- a) 测评指标：应保证设置合法、合理的区块激励机制。
- b) 测评对象：区块激励机制。
- c) 测评实施包括以下内容：
 - 1) 是否具有区块激励机制；
 - 2) 区块激励机制是否合理、合法；
 - 3) 区块激励机制设置是否能使得共识节点最大化自身收益的个体行为与区块链系统的安全性和有效性相契合；
 - 4) 区块激励机制设置是否能使得大规模节点形成稳定的共识。
- d) 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.4.2 区块防攻击能力

该测评单元包括以下要求：

- a) 测评指标：应保证区块大小在安全范围内，并具备一定的防攻击能力。
- b) 测评对象：区块程序。
- c) 测评实施包括以下内容：
 - 1) 区块大小是否在安全范围内；
 - 2) 区块是否能有效防御竞态攻击等同类攻击；
 - 3) 区块是否能有效防御芬尼攻击等同类攻击；
 - 4) 区块是否能有效防御 51%算力攻击等同类攻击。
- d) 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.5 数据管理测评要求

7.5.1 数据管理制度

该测评单元包括以下要求：

- a) 测评指标：应制定区块链数据安全工作的总体方针、数据安全策略。
- b) 测评对象：总体方针策略类文档、数据安全管理制度类文档。
- c) 测评实施包括以下内容：
 - 1) 数据安全工作的总体方针和安全策略文件是否明确规定数据安全工作的总体目标范围、原则以及各类安全策略等；
 - 2) 数据管理制度是否覆盖数据库、区块数据、数据存储、数据传输等管理内容；
 - 3) 数据安全管理人员是否定期对数据安全管理制度合理性和适用性进行评审修订；
 - 4) 是否设置专门的人员负责制定数据安全管理制度。
- d) 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.5.2 数据管理机构

该测评单元包括以下要求：

- a) 测评指标：应设立适合区块链系统的数据管理机构。
- b) 测评对象：数据制度。

c) 测评实施包括以下内容：

- 1) 各类数据变更记录是否针对数据存储变更、数据操作记录、数据访问等事项进行及时记录；
- 2) 是否建立安全领导小组，指定机构最高管理者或授权代表担任小组组长，并明确组长责任与权力；
- 3) 是否建立机构内部监督管理职能部门，对数据管理和各用户操作行为进行安全监督管理；
- 4) 机构最高管理者或组长是否明确了安全岗位和岗位用户职责；
- 5) 数据安全主管是否配备了系统管理员、数据安全管理员等必需岗位；
- 6) 数据安全各岗位职责文档是否明确了各岗位职责；
- 7) 是否制定数据安全追责制度，定期对责任部门或安全岗位组织安全检查，形成检查报告。

d) 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.5.3 数据管理人员

该测评单元包括以下要求：

a) 测评指标：应配备完善的数据管理人员体系。

b) 测评对象：数据管理制度。

c) 测评实施包括以下内容：

- 1) 是否制定数据服务人力资源安全策略，明确不同岗位人员在数据生命周期各阶段数据服务和系统服务相关的工作范畴和安全管控措施；
- 2) 是否制定数据服务人员招聘、录用、上岗、调岗、离岗、考核、选拔等人员安全管理制度；
- 3) 是否在录用重要岗位人员前对其进行背景调查，确保符合相关的法律、法规合同和道德要求，并与所有涉及数据服务岗位人员签订安全责任协议；
- 4) 是否在重要岗位人员调离或终止劳动合同时，与其签订保密协议；
- 5) 是否明确数据服务重要岗位的兼职和轮岗、权限分离、多人共管等安全管理要求；
- 6) 是否建立人员安全责任奖惩管理制度，并按照规定对造成数据服务损失的人员给予相应的处理，记录并保存相关信息；
- 7) 是否建立第三方人员安全管理制度，对接触个人信息、重要数据等数据的人员进行审批和登记，并要求签署保密协议，定期对这些人员行为进行安全审查。

d) 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8 第四级测评要求

8.1 数据存储测评要求

8.1.1 数据存储机密性

该测评单元包括以下要求：

a) 测评指标：应保证数据存储机密性。

b) 测评对象：数据存储形式。

c) 测评实施包括以下内容：

- 1) 在数据存储过程中是否采用密文的形式进行存储；
- 2) 在数据存储时是否设置用户访问权限；

- 3) 数据信息是否进行安全保护分级;
- 4) 敏感信息的主体是否采用匿名化方式存储。
- d) 测评判定: 如果以上测评实施内容均为肯定, 则符合本测评单元指标要求, 否则不符合或部分符合本测评单元指标要求。

8.1.2 数据存储完整性

该测评单元包括以下要求:

- a) 测评指标: 应保证数据存储完整性。
- b) 测评对象: 数据存储策略。
- c) 测评实施包括以下内容:
 - 1) 数据存储是否建立数据存储冗余策略和管理制度, 及数据备份与恢复操作过程规范;
 - 2) 数据存储是否具有数据完整性验证机制。
- d) 测评判定: 如果以上测评实施内容均为肯定, 则符合本测评单元指标要求, 否则不符合或部分符合本测评单元指标要求。

8.1.3 数据存储可靠性

该测评单元包括以下要求:

- a) 测评指标: 应保证数据存储可靠性。
- b) 测评对象: 数据存储策略类。
- c) 测评实施包括以下内容:
 - 1) 数据存储时是否具有存储策略类文档, 文档内容包括但不限于存储管理制度和数据备份操作;
 - 2) 数据存储内容是否包含完整的用户访问记录、数据处理记录等内容;
 - 3) 数据存储是否建立数据的细颗粒度审计机制;
 - 4) 数据存储架构是否可伸缩, 以满足数据量持续增长、数据分类分级存储等需求;
 - 5) 是否将不同类别和级别的数据分开存储, 并采取物理或逻辑隔离机制。
- d) 测评判定: 如果以上测评实施内容均为肯定, 则符合本测评单元指标要求, 否则不符合或部分符合本测评单元指标要求。

8.1.4 数据备份可用性

该测评单元包括以下要求:

- a) 测评指标: 保证数据备份可用性。
- b) 测评对象: 数据备份与恢复能力。
- c) 测评实施包括以下内容:
 - 1) 重要数据是否具有备份机制;
 - 2) 重要数据是否设置数据定期备份的策略;
 - 3) 是否采用分散式方式进行数据备份;
 - 4) 是否建立备份操作过程规范, 包括备份日志记录规范;
 - 5) 是否明确数据逻辑存储隔离授权与操作规范、确保具备数据存储安全隔离能力。
- d) 测评判定: 如果以上测评实施内容均为肯定, 则符合本测评单元指标要求, 否则不符合或部分符合本测评单元指标要求。

8.1.5 数据恢复可用性

该测评单元包括以下要求：

- a) 测评指标：应保证数据恢复功能可用性。
- b) 测评对象：遇到故障时数据恢复能力。
- c) 测评实施包括以下内容：
 - 1) 是否具有数据故障处置预案；
 - 2) 故障预案是否能及时解决故障并迅速恢复数据；
 - 3) 是否建立恢复操作过程规范，包括恢复日志记录规范；
 - 4) 在节点重新接入区块时，是否能重新恢复数据；
 - 5) 在数据故障时是否具备自动恢复能力；
 - 6) 是否具有数据分析能力，例如基于数据驱动的误用检测、安全事件检测等相关能力。
- d) 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.2 数据传输测评要求

8.2.1 数据传输机密性

该测评单元包括以下要求：

- a) 测评指标：应保证数据传输过程中区块链数据的机密性。
- b) 测评对象：数据传输策略。
- c) 测评实施包括以下内容：
 - 1) 数据传输过程是否采用加密技术；
 - 2) 数据传输是否在已授权节点之间进行；
 - 3) 机密和绝密数据是否在传输过程中使用数字签名；
 - 4) 数字签名的密钥的类型、属性以及密钥长度是否达到安全需求；
 - 5) 敏感数据传输时，是否采用用户口令、生物特征、密钥等加密传输策略。
- d) 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.2.2 数据传输完整性

该测评单元包括以下要求：

- a) 测评指标：应保证数据传输过程中区块链数据的完整性。
- b) 测评对象：数据传输策略。
- c) 测评实施包括以下内容：
 - 1) 在数据传输过程中是否提供数据完整性验证协议；
 - 2) 数据传输协议是否能够保证业务数据的传输完整性。
- d) 测评判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.2.3 数据传输可靠性

该测评单元包括以下要求：

- a) 测评指标：应保证数据传输过程中区块链数据的可靠性。

- b) 测评对象：数据传输策略。
- c) 测评实施包括以下内容：
 - 1) 传输连接建立之前，是否对发送方和接收方进行身份鉴别操作，例如利用密码技术进行初始化会话验证；
 - 2) 数据传输过程中是否采用加解密技术；
 - 3) 数据传输是否采用满足数据传输安全策略的相应安全控制措施，如安全通道、可信通道、数据加密等；
 - 4) 重要数据传输时是否采用隐蔽、随机化等方式的传输协议，或者采用专用的传输协议等，保障数据传输过程中数据安全性。
- d) 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.2.4 数据传输可用性

该测评单元包括以下要求：

- a) 测评指标：应保证数据传输过程中区块链数据的可用性。
- b) 测评对象：数据传输策略。
- c) 测评实施包括以下内容：
 - 1) 通过传输接收到的数据是否与系统采用统一时间标准；
 - 2) 是否具备对传输数据的可用性进行检测的能力；
 - 3) 数据传输过程中是否具有数据自动矫正机制。
- d) 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.3 数据访问测评要求

8.3.1 访问权限控制

该测评单元包括以下要求：

- a) 测评指标：应保证设置数据访问控制权限、访问控制策略。
- b) 测评对象：数据访问权限控制功能。
- c) 测评实施包括以下内容：
 - 1) 是否具有数据访问权限控制策略；
 - 2) 针对系统中安全相关的操作，例如备份作业、日志访问、策略管理等，是否具备安全策略；
 - 3) 是否具有访问错误次数限制机制，例如当异常操作次数超过三次时，应能阻止该用户的进一步操作尝试；
 - 4) 是否具有访问超时锁定功能，例如在设定时间段内没有任何操作，系统会自动终止会话，需要再次进行身份鉴别才能够重新操作。
- d) 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.3.2 数据访问处理

该测评单元包括以下要求：

- a) 测评指标：应保证数据处理时明确处理的目的和范围、遵守数据使用规范。
- b) 测评对象：数据访问流程。
- c) 测评实施包括以下内容：
 - 1) 是否根据法律法规要求，明确数据处理的目的和范围；
 - 2) 是否设置数据访问处理规范类文档及相关违规处理的惩戒措施；
 - 3) 是否建立特定操作日志文档，记录和管理区块链数据访问处理活动中的相关操作；
 - 4) 是否设置风险评估体系，评估数据访问处理结果，避免数据处理过程中涉及到相关敏感等重要数据。
- d) 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.3.3 加密访问控制

该测评单元包括以下要求：

- a) 测评指标：应保证对数据进行加密访问控制、数据访问权限设置采用多私钥规则以及属性加密等规则。
- b) 测评对象：数据访问权限控制。
- c) 测评实施包括以下内容：
 - 1) 数据是否通过加密方式进行访问控制；
 - 2) 数据访问权限设置是否采用属性加密方法进行访问权限控制；
 - 3) 数据访问权限设置是否采用多层加密规则；
 - 4) 数据访问权限设置是否同时采用多种密码学方法控制访问权限。
- d) 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.3.4 数据服务

该测评单元包括以下要求：

- a) 测评指标：应指定数据服务安控制策略和明确安全规范。
- b) 测评对象：数据服务功能。
- c) 测评实施包括以下内容：
 - 1) 数据服务是否制定安全控制策略，明确规定使用服务的安全限制和安全控制措施，如身份鉴别、授权策略、访问控制机制、签名、时间戳、安全协议等；
 - 2) 数据服务是否明确安全规范，包括服务名称、服务参数、服务安全要求等，具备对服务不安全参数进行限制或过滤能力，为服务提供异常处理能力；
 - 3) 数据服务调用是否采用安全通道、加密传输等机制；
 - 4) 数据服务是否具备访问的审计能力，并能为数据安全审计提供可配置的数据服务。
- d) 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.4 区块数据测评要求

8.4.1 区块激励机制

该测评单元包括以下要求：

- a) 测评指标：应保证设置合法、合理的区块激励机制。
- b) 测评对象：区块激励机制。
- c) 测评实施包括以下内容：
 - 1) 是否具有区块激励机制；
 - 2) 区块激励机制是否合理、合法；
 - 3) 区块激励机制设置是否能使得共识节点最大化自身收益的个体行为与区块链系统的安全性和有效性相契合；
 - 4) 区块激励机制设置是否能使得大规模节点形成稳定的共识。
- d) 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.4.2 区块防攻击能力

该测评单元包括以下要求：

- a) 测评指标：应保证区块大小在安全范围内，并具备一定的防攻击能力。
- b) 测评对象：区块程序。
- c) 测评实施包括以下内容：
 - 1) 区块大小是否在安全范围内；
 - 2) 区块是否能有效防御竞态攻击等同类攻击；
 - 3) 区块是否能有效防御芬尼攻击等同类攻击；
 - 4) 区块是否能有效防御 51%算力攻击等同类攻击。
- d) 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.5 数据管理测评要求

8.5.1 数据管理制度

该测评单元包括以下要求：

- a) 测评指标：应制定区块链数据安全工作的总体方针、数据安全策略。
- b) 测评对象：总体方针策略类文档、数据安全管理制度类文档。
- c) 测评实施包括以下内容：
 - 1) 数据安全工作的总体方针和安全策略文件是否明确规定数据安全工作的总体目标范围、原则以及各类安全策略等；
 - 2) 数据管理制度是否覆盖数据库、区块数据、数据存储、数据传输等管理内容；
 - 3) 数据安全管理人员是否定期对数据安全管理制度合理性和适用性进行评审修订；
 - 4) 是否设置专门的人员负责制定数据安全管理制度。
- d) 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.5.2 数据管理机构

该测评单元包括以下要求：

- a) 测评指标：应设立适合区块链系统的数据管理机构。
- b) 测评对象：数据制度。

c) 测评实施包括以下内容：

- 1) 各类数据变更记录是否针对数据存储变更、数据操作记录、数据访问等事项进行及时记录；
- 2) 是否建立安全领导小组，指定机构最高管理者或授权代表担任小组组长，并明确组长责任与权力；
- 3) 是否建立机构内部监督管理职能部门，对数据管理和各用户操作行为进行安全监督管理；
- 4) 机构最高管理者或组长是否明确了安全岗位和岗位用户职责；
- 5) 数据安全主管是否配备了系统管理员、数据安全管理员等必需岗位；
- 6) 数据安全各岗位职责文档是否明确了各岗位职责；
- 7) 是否制定数据安全追责制度，定期对责任部门或安全岗位组织安全检查，形成检查报告。

d) 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.5.3 数据管理人员

该测评单元包括以下要求：

a) 测评指标：应配备完善的数据管理人员体系。

b) 测评对象：数据管理制度。

c) 测评实施包括以下内容：

- 1) 是否制定数据服务人力资源安全策略，明确不同岗位人员在数据生命周期各阶段数据服务和系统服务相关的工作范畴和安全管控措施；
- 2) 是否制定数据服务人员招聘、录用、上岗、调岗、离岗、考核、选拔等人员安全管理制度；
- 3) 是否在录用重要岗位人员前对其进行背景调查，确保符合相关的法律、法规合同和道德要求，并与所有涉及数据服务岗位人员签订安全责任协议；
- 4) 是否在重要岗位人员调离或终止劳动合同时，与其签订保密协议；
- 5) 是否明确数据服务重要岗位的兼职和轮岗、权限分离、多人共管等安全管理要求；
- 6) 是否建立人员安全责任奖惩管理制度，并按照规定对造成数据服务损失的人员给予相应的处理，记录并保存相关信息；
- 7) 是否建立第三方人员安全管理制度，对接触个人信息、重要数据等数据的人员进行审批和登记，并要求签署保密协议，定期对这些人员行为进行安全审查。

d) 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9 测评结论

9.1 风险分析和评价

等级测评报告中应对整体测评之后单项测评结果中的不符合项或部分符合项进行风险分析和评价。

采用风险分析的方法对单项测评结果中存在的不符合项或部分符合项，分析所产生的安全问题被威胁利用的可能性，判断其被威胁利用后对业务信息安全和系统服务安全造成影响的程度，综合评价这些不符合项或部分符合项对定级对象造成的安全风险。风险分析和评价应根据特定的条件和场景下展开，并对高风险的测试项予以预警。

9.2 等级测评结论

应结合各类的测评结论和对单项测评结果的风险分析给出等级测评结论：

- a) 符合：定级对象中未发现安全问题，等级测评结果中所有测评项的单项测评结果中部分符合和不符合项的统计结果全为 0。
- b) 基本符合：定级对象中存在安全问题，部分符合和不符合项的统计结果不全为 0，但存在的安全问题不会导致定级对象面临高等级安全风险。
- c) 不符合：定级对象中存在安全问题，部分符合项和不符合项的统计结果不全为 0，而且存在的安全问题会导致定级对象面临高等级安全风险。

地方标准信息服务平台

参 考 文 献

- [1] GB/T 28458—2012 信息安全技术 安全漏洞标识与描述规范.
- [2] GB/T 31495.2—2015 信息安全技术 信息安全保障指标体系及评价方法
- [3] 钱卫宁, 邵奇峰, 朱燕超, 等. 区块链与可信数据管理: 问题与方法[J]. 软件学报, 2018, 29(1): 150-159.
- [4] 韩璇, 袁勇, 王飞跃. 区块链安全问题: 研究现状与展望[J]. 自动化学报, 2019, 45(1): 206-225.
- [5] Lin I C , Liao T C . A Survey of Blockchain Security Issues and Challenges[J]. International Journal of Network Security, 2017, 19.
- [6] 黄永洪, 王惠莅, 伍前红. 区块链安全及标准化[J]. 信息技术与标准化, 2018, No.399(03):26-28.
-

地方标准信息服务平台