

- d) 单元判定:如果 1)~3)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。

B.2.4.2 测评单元(BDS-L2-02)

该测评单元包括以下要求:

- a) 测评指标:应以书面方式约定大数据平台提供者的权限与责任、各项服务内容和具体技术指标等,尤其是安全服务内容。
- b) 测评对象:服务合同、协议和服务水平协议、安全声明等。
- c) 测评实施:应核查服务合同、协议或服务水平协议、安全声明等,是否规范了大数据平台提供者的权限与责任,覆盖管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等方面的内容;是否规定了大数据平台的各项服务内容(含安全服务)和具体指标、服务期限等,并有双方签字或盖章。
- d) 单元判定: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。

B.2.5 安全运维管理

B.2.5.1 测评单元(BDS-L2-01)

该测评单元包括以下要求:

- a) 测评指标:应建立数字资产安全管理策略,对数据全生命周期的操作规范、保护措施、管理人员职责等进行规定,包括并不限于数据采集、存储、处理、应用、流动、销毁等过程。
- b) 测评对象:数字资产安全管理策略。
- c) 测评实施包括以下内容:
 - 1) 应核查大数据平台和大数据应用数字资产安全管理策略是否明确资产的安全管理目标、原则和范围;
 - 2) 应核查大数据平台和大数据应用数字资产安全管理策略是否明确各类数据全生命周期(包括并不限于数据采集、存储、处理、应用、流动、销毁等过程)的操作规范和保护措施,是否与数字资产的安全类别级别相符;
 - 3) 应核查大数据平台和大数据应用数字资产安全管理策略是否明确管理人员的职责。
- d) 单元判定:如果 1)~3)均为肯定,则符合本单元测评指标要求,否则不符合或部分符合本单元测评指标要求。

B.3 第三级安全评估方法

B.3.1 安全物理环境

B.3.1.1.1 测评单元(BDS-L3-01)

该测评单元包括以下要求:

- a) 测评指标:应保证承载大数据存储、处理和分析的设备机房位于中国境内。
- b) 测评对象:大数据平台管理员和大数据平台建设方案。
- c) 测评实施包括以下内容:
 - 1) 应访谈大数据平台管理员大数据平台的存储节点、处理节点、分析节点和大数据管理平台等承载大数据业务和数据的软硬件是否均位于中国境内;
 - 2) 应核查大数据平台建设方案中是否明确大数据平台的存储节点、处理节点、分析节点和大

数据管理平台等承载大数据业务和数据的软硬件均位于中国境内。

- d) 单元判定:如果 1)和 2)均为肯定,则符合本单元测评指标要求,否则不符合或部分符合本单元测评指标要求。

B.3.2 安全通信网络

B.3.2.1.1 测评单元(BDS-L3-01)

该测评单元包括以下要求:

- a) 测评指标:应保证大数据平台不承载高于其安全保护等级的大数据应用。
- b) 测评对象:大数据平台和业务应用系统定级材料。
- c) 测评实施:应核查大数据平台和大数据平台承载的大数据应用系统相关定级材料,大数据平台安全保护等级是否不低于其承载的业务应用系统。
- d) 单元判定:如果以上测评实施内容为肯定,则符合本单元测评指标要求,否则不符合本单元测评指标要求。

B.3.2.1.2 测评单元(BDS-L3-02)

该测评单元包括以下要求:

- a) 测评指标:应保证大数据平台的管理流量与系统业务流量分离。
- b) 测评对象:网络架构和大数据平台。
- c) 测评实施包括以下内容:
 - 1) 应核查网络架构和配置策略能否采用带外管理或策略配置等方式实现管理流量和业务流量分离;
 - 2) 应核查大数据平台管理流量与大数据服务业务流量是否分离,核查所采取的技术手段和流量分离手段;
 - 3) 应测试验证大数据平台管理流量与业务流量是否分离。
- d) 单元判定:如果 1)~3)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。

B.3.3 安全计算环境

B.3.3.1 测评单元(BDS-L3-01)

该测评单元包括以下要求:

- a) 测评指标:大数据平台应对数据采集终端、数据导入服务组件、数据导出终端、数据导出服务组件的使用实施身份鉴别。
- b) 测评对象:数据采集终端、导入服务组件、业务应用系统、数据管理系统和系统管理软件等。
- c) 测评实施包括以下内容:
 - 1) 应核查数据采集终端、用户或导入服务组件、数据导出终端、数据导出服务组件在登录时是否采用了身份鉴别措施;
 - 2) 应测试验证身份鉴别措施是否能够不被绕过。
- d) 单元判定:如果 1)和 2)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。

B.3.3.2 测评单元(BDS-L3-02)

该测评单元包括以下要求:

- a) 测评指标:大数据平台应能对不同客户的大数据应用实施标识和鉴别。
- b) 测评对象:大数据平台、大数据应用系统和系统管理软件等。
- c) 测评实施包括以下内容:
 - 1) 应核查大数据平台是否对大数据应用实施身份鉴别措施;
 - 2) 应测试验证身份鉴别措施是否能够不被绕过。
- d) 单元判定:如果 1)和 2)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。

B.3.3.3 测评单元(BDS-L3-03)

该测评单元包括以下要求:

- a) 测评指标:大数据平台应为大数据应用提供集中管控其计算和存储资源使用状况的能力。
- b) 测评对象:大数据平台和大数据应用。
- c) 测评实施包括以下内容:
 - 1) 应核查大数据平台是否为大数据应用提供计算和存储资源集中管控的模块;
 - 2) 应建立大数据应用测试账户,核查大数据平台是否支持计算和存储资源集中监测和集中管控功能。
- d) 单元判定:如果 1)和 2)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。

B.3.3.4 测评单元(BDS-L3-04)

该测评单元包括以下要求:

- a) 测评指标:大数据平台应对其提供的辅助工具或服务组件,实施有效管理。
- b) 测评对象:辅助工具、服务组件和大数据平台。
- c) 测评实施包括以下内容:
 - 1) 应核查提供的辅助工具或服务组件是否可以安装、部署、升级和卸载等;
 - 2) 应核查提供的辅助工具或服务组件是否提供日志;
 - 3) 应核查大数据平台是否采用技术手段或管理手段对辅助工具或服务组件进行统一管理,避免组件冲突。
- d) 单元判定:如果 1)~3)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。

B.3.3.5 测评单元(BDS-L3-05)

该测评单元包括以下要求:

- a) 测评指标:大数据平台应屏蔽计算、内存、存储资源故障,保障业务正常运行。
- b) 测评对象:设计文档、建设文档、计算节点和存储节点。
- c) 测评实施包括以下内容:
 - 1) 应核查设计文档或建设文档等是否具备屏蔽计算、内存、存储资源故障的措施和技术手段;
 - 2) 应测试验证单一计算节点或存储节点关闭时,是否不影响业务正常运行。
- d) 单元判定:如果 1)和 2)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。

B.3.3.6 测评单元(BDS-L3-06)

该测评单元包括以下要求:

- a) 测评指标:大数据平台应提供静态脱敏和去标识化的工具或服务组件技术。
- b) 测评对象:设计或建设文档、大数据应用和大数据平台。
- c) 测评实施包括以下内容:
 - 1) 应核查大数据平台设计或建设文档是否具备数据静态脱敏和去标识化措施或方案,如核查工具或服务组件是否具备配置不同的脱敏算法的能力;
 - 2) 应核查静态脱敏和去标识化工具或服务组件是否进行了策略配置;
 - 3) 应核查大数据平台是否为大数据应用提供静态脱敏和去标识化的工具或服务组件技术;
 - 4) 应测试验证脱敏后的数据是否实现对敏感信息内容的屏蔽和隐藏,验证脱敏处理是否具备不可逆性。
- d) 单元判定:如果 1)~4)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。

B.3.3.7 测评单元(BDS-L3-07)

该测评单元包括以下要求:

- a) 测评指标:对外提供服务的大数据平台,平台或第三方只有在大数据应用授权下才可以对大数据应用的数据资源进行访问、使用和管理。
- b) 测评对象:大数据平台、大数据应用系统、数据管理系统和系统设计文档等。
- c) 测评实施包括以下内容:
 - 1) 应核查是否由授权主体负责配置访问控制策略;
 - 2) 应核查授权主体是否依据安全策略配置了主体对客体的访问规则;
 - 3) 应测试验证是否不存在可越权访问情形。
- d) 单元判定:如果 1)~3)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。

B.3.3.8 测评单元(BDS-L3-08)

该测评单元包括以下要求:

- a) 测评指标:大数据平台应提供数据分类分级安全管理功能,供大数据应用针对不同类别级别的数据采取不同的安全保护措施。
- b) 测评对象:大数据平台、大数据应用系统、数据管理系统和系统设计文档等。
- c) 测评实施包括以下内容:
 - 1) 应访谈管理员是否依据行业相关数据分类分级规范制定数据分类分级策略;
 - 2) 应核查大数据平台是否具有分类分级管理功能,是否依据分类分级策略对数据进行分类和等级划分;大数据平台是否能够为大数据应用提供分类分级安全管理功能;
 - 3) 应核查大数据平台、大数据应用和数据管理系统等对不同类别级别的数据在标识、使用、传输和存储等方面采取何种安全防护措施,进而根据不同需要对关键数据进行重点防护。
- d) 单元判定:如果 1)~3)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。

B.3.3.9 测评单元(BDS-L3-09)

该测评单元包括以下要求:

- a) 测评指标:大数据平台应提供设置数据安全标记功能,基于安全标记的授权和访问控制措施,满足细粒度授权访问控制管理能力要求。
- b) 测评对象:大数据平台、数据管理系统和系统设计文档等。

- c) 测评实施包括以下内容：
 - 1) 应核查大数据平台是否依据安全策略对数据设置安全标记；
 - 2) 应核查大数据平台是否为大数据应用提供基于安全标记的细粒度访问控制授权能力；
 - 3) 应测试验证依据安全标记是否实现主体对客体细粒度的访问控制管理功能。
- d) 单元判定：如果 1)～3) 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。

B.3.3.10 测评单元(BDS-L3-10)

该测评单元包括以下要求：

- a) 测评指标：大数据平台应在数据采集、存储、处理、分析等各个环节，支持对数据进行分类分级处置，并保证安全保护策略保持一致。
- b) 测评对象：数据采集终端、导入服务组件、大数据应用系统、数据管理系统和系统管理软件等。
- c) 测评实施包括以下内容：
 - 1) 应访谈管理员是否依据行业相关数据分类分级规范制定数据分类分级策略；
 - 2) 应核查数据是否依据分类分级策略在数据采集、处理、分析过程中进行分类和等级划分；
 - 3) 应核查是否采取有效措施保障机构内部数据安全保护策略的一致性。
- d) 单元判定：如果 1)～3) 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。

B.3.3.11 测评单元(BDS-L3-11)

该测评单元包括以下要求：

- a) 测评指标：涉及重要数据接口、重要服务接口的调用，应实施访问控制，包括但不限于数据处理、使用、分析、导出、共享、交换等相关操作。
- b) 测评对象：大数据平台、大数据应用系统、数据管理系统和系统管理软件等。
- c) 测评实施包括以下内容：
 - 1) 应核查大数据平台或大数据应用系统是否面向重要数据接口、重要服务接口的调用提供有效访问控制措施；
 - 2) 应核查访问控制措施是否包括但不限于数据处理、使用、分析、导出、共享、交换等相关操作；
 - 3) 应测试验证访问控制措施是否不被绕过。
- d) 单元判定：如果 1)～3) 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。

B.3.3.12 测评单元(BDS-L3-12)

该测评单元包括以下要求：

- a) 测评指标：应在数据清洗和转换过程中对重要数据进行保护，以保证重要数据清洗和转换后的一致性，避免数据失真，并在产生问题时能有效还原和恢复。
- b) 测评对象：管理员、清洗和转换的数据、数据清洗和转换工具或脚本。
- c) 测评实施包括以下内容：
 - 1) 应访谈数据清洗转换相关管理员，询问数据清洗后是否较少出现失真或一致性破坏的情况；
 - 2) 应核查清洗和转换的数据，重要数据清洗前后的字段或者内容是否具备一致性，能否避免数据失真；

- 3) 应核查数据清洗和转换工具或脚本,重要数据是否具备回滚机制等,在产生问题时可进行有效还原和恢复。
- d) 单元判定:如果 1)~3)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。

B.3.3.13 测评单元(BDS-L3-13)

该测评单元包括以下要求:

- a) 测评指标:应跟踪和记录数据采集、处理、分析和挖掘等过程,保证溯源数据能重现相应过程,溯源数据满足合规审计要求。
- b) 测评对象:数据溯源措施或系统和大数据系统。
- c) 测评实施包括以下内容:
 - 1) 应核查数据溯源措施或系统是否对数据采集、处理、分析和挖掘等过程进行溯源;
 - 2) 应核查重要业务数据处理流程是否包含在数据溯源范围中;
 - 3) 应测试验证大数据平台是否对测试产生的数据采集、处理、分析或挖掘的过程进行了记录,是否可溯源测试过程;
 - 4) 应核查是否能支撑数据业务要求,确保重要业务数据可溯源;
 - 5) 对于自研发溯源措施或系统,应核查溯源数据能否满足合规审计要求;
 - 6) 对于采购的溯源措施或系统,应核查系统是否符合国家产品和服务合规审计要求,溯源数据是否符合合规审计要求。
- d) 单元判定:如果 1)~6)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。

B.3.3.14 测评单元(BDS-L3-14)

该测评单元包括以下要求:

- a) 测评指标:大数据平台应保证不同客户大数据应用的审计数据隔离存放,并提供不同客户审计数据收集汇总和集中分析的能力。
- b) 测评对象:大数据应用的审计数据。
- c) 测评实施包括以下内容:
 - 1) 应核查对外提供服务的大数据平台,审计数据存储方式和不同大数据应用的审计数据是否隔离存放;
 - 2) 应核查大数据平台是否提供不同客户审计数据收集汇总和集中分析的能力。
- d) 单元判定:如果 1)和 2)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。

B.3.4 安全建设管理

B.3.4.1 测评单元(BDS-L3-01)

该测评单元包括以下要求:

- a) 测评指标:应选择安全合规的大数据平台,其所提供的大数据平台服务应为其所承载的大数据应用提供相应等级的安全保护能力。
- b) 测评对象:大数据应用建设负责人、大数据平台资质及安全服务能力报告和大数据平台服务合同等。
- c) 测评实施包括以下内容:

- 1) 应访谈大数据应用建设负责人,所选择的大数据平台是否满足国家的有关规定;
 - 2) 应查阅大数据平台相关资质及安全服务能力报告,是否大数据平台能为其所承载的大数据应用提供相应等级的安全保护能力;
 - 3) 应核查大数据平台提供者的相关服务合同,是否大数据平台提供了其所承载的大数据应用相应等级的安全保护能力。
- d) 单元判定:如果 1)~3)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。

B.3.4.2 测评单元(BDS-L3-02)

该测评单元包括以下要求:

- a) 测评指标:应以书面方式约定大数据平台提供者的权限与责任、各项服务内容和具体技术指标等,尤其是安全服务内容。
- b) 测评对象:服务合同、协议或服务水平协议、安全声明等。
- c) 测评实施:应核查服务合同、协议或服务水平协议、安全声明等,是否规范了大数据平台提供者的权限与责任,覆盖管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等方面的内容;是否规定了大数据平台的各项服务内容(含安全服务)和具体指标、服务期限等,并有双方签字或盖章。
- d) 单元判定: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。

B.3.4.3 测评单元(BDS-L3-03)

该测评单元包括以下要求:

- a) 测评指标:应明确约束数据交换、共享的接收方对数据的保护责任,并确保接收方有足够或相当的安全防护能力。
- b) 测评对象:数据交换、共享策略和数据交换、共享合同、协议等。
- c) 测评实施包括以下内容:
 - 1) 应核查是否建立数据交换、共享的策略,确保内容覆盖对接收方安全防护能力的约束性要求;
 - 2) 应核查数据交换、共享的合同或协议是否明确数据交换、共享的接收方对数据的保护责任。
- d) 单元判定:如果 1)和 2)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。

B.3.5 安全运维管理

B.3.5.1 测评单元(BDS-L3-01)

该测评单元包括以下要求:

- a) 测评指标:应建立数字资产安全管理策略,对数据全生命周期的操作规范、保护措施、管理人员职责等进行规定,包括并不限于数据采集、存储、处理、应用、流动、销毁等过程。
- b) 测评对象:数字资产安全管理策略。
- c) 测评实施包括以下内容:
 - 1) 应核查大数据平台和大数据应用数字资产安全管理策略是否明确资产的安全管理目标、原则和范围;

- 2) 应核查大数据平台和大数据应用数字资产安全管理策略是否明确各类数据全生命周期(包括并不限于数据采集、存储、处理、应用、流动、销毁等过程)的操作规范和保护措施,是否与数字资产的安全类别级别相符;
- 3) 应核查大数据平台和大数据应用数字资产安全管理策略是否明确管理人员的职责。
- d) 单元判定:如果 1)~3)均为肯定,则符合本单元测评指标要求,否则不符合或部分符合本单元测评指标要求。

B.3.5.2 测评单元(BDS-L3-02)

该测评单元包括以下要求:

- a) 测评指标:应制定并执行数据分类分级保护策略,针对不同类别级别的数据制定不同的安全保护措施。
- b) 测评对象:数据分类分级保护策略。
- c) 测评实施包括以下内容:
 - 1) 应核查大数据平台和大数据应用数据分类分级保护策略是否针对不同类别级别的数据制定不同的安全保护措施;
 - 2) 应核查数据操作记录是否按照大数据平台和大数据应用数据分类分级保护策略对数据实施保护。
- d) 单元判定:如果 1)和 2)均为肯定,则符合本单元测评指标要求,否则不符合或部分符合本单元测评指标要求。

B.3.5.3 测评单元(BDS-L3-03)

该测评单元包括以下要求:

- a) 测评指标:应在数据分类分级的基础上,划分重要数字资产范围,明确重要数据进行自动脱敏或去标识的使用场景和业务处理流程。
- b) 测评对象:数据安全相关要求和大数据平台建设方案。
- c) 测评实施包括以下内容:
 - 1) 应核查数据安全相关要求是否划分重要数字资产范围,是否明确重要数据自动脱敏或去标识的使用场景和业务处理流程;
 - 2) 应核查数据自动脱敏或去标识的使用场景和业务处理流程是否和管理要求相符。
- d) 单元判定:如果 1)和 2)均为肯定,则符合本单元测评指标要求,否则不符合或部分符合本单元测评指标要求。

B.3.5.4 测评单元(BDS-L3-04)

该测评单元包括以下要求:

- a) 测评指标:应定期评审数据的类别和级别,如需要变更数据的类别或级别,应依据变更审批流程执行变更。
- b) 测评对象:数据管理员,数据管理相关制度和数据变更记录表单。
- c) 测评实施包括以下内容:
 - 1) 应访谈数据管理员,是否定期评审数据的类别和级别,如需要变更数据的类别或级别时,是否依据变更审批流程执行;
 - 2) 应核查数据管理相关制度,是否要求对数据的类别和级别进行定期评审,是否提出数据类别或级别变更的审批要求;
 - 3) 应核查数据变更记录表单,是否依据变更审批流程执行变更。

- d) 单元判定:如果 1)~3)均为肯定,则符合本单元测评指标要求,否则不符合或部分符合本单元测评指标要求。

B.4 第四级安全评估方法

B.4.1 安全物理环境

B.4.1.1.1 测评单元(BDS-L4-01)

该测评单元包括以下要求:

- a) 测评指标:应保证承载大数据存储、处理和分析的设备机房位于中国境内。
- b) 测评对象:大数据平台管理员和大数据平台建设方案。
- c) 测评实施包括以下内容:
 - 1) 应访谈大数据平台管理员大数据平台的存储节点、处理节点、分析节点和大数据管理平台等承载大数据业务和数据的软硬件是否均位于中国境内;
 - 2) 应核查大数据平台建设方案中是否明确大数据平台的存储节点、处理节点、分析节点和大数据管理平台等承载大数据业务和数据的软硬件均位于中国境内。
- d) 单元判定:如果 1)和 2)均为肯定,则符合本单元测评指标要求,否则不符合或部分符合本单元测评指标要求。

B.4.2 安全通信网络

B.4.2.1.1 测评单元(BDS-L4-01)

该测评单元包括以下要求:

- a) 测评指标:应保证大数据平台不承载高于其安全保护等级的大数据应用。
- b) 测评对象:大数据平台和业务应用系统定级材料。
- c) 测评实施:应核查大数据平台和大数据平台承载的大数据应用系统相关定级材料,大数据平台安全保护等级是否不低于其承载的业务应用系统。
- d) 单元判定:如果以上测评实施内容为肯定,则符合本单元测评指标要求,否则不符合本单元测评指标要求。

B.4.2.1.2 测评单元(BDS-L4-02)

该测评单元包括以下要求:

- a) 测评指标:应保证大数据平台的管理流量与系统业务流量分离。
- b) 测评对象:网络架构和大数据平台。
- c) 测评实施包括以下内容:
 - 1) 应核查网络架构和配置策略能否采用带外管理或策略配置等方式实现管理流量和业务流量分离;
 - 2) 应核查大数据平台管理流量与大数据服务业务流量是否分离,核查所采取的技术手段和流量分离手段;
 - 3) 应测试验证大数据平台管理流量与业务流量是否分离。
- d) 单元判定:如果 1)和 3)或 2)和 3)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。

B.4.3 安全计算环境

B.4.3.1 测评单元(BDS-L4-01)

该测评单元包括以下要求：

- a) 测评指标：大数据平台应对数据采集终端、数据导入服务组件、数据导出终端、数据导出服务组件的使用实施身份鉴别。
- b) 测评对象：数据采集终端、导入服务组件、业务应用系统、数据管理系统和系统管理软件等。
- c) 测评实施包括以下内容：
 - 1) 应核查数据采集终端、用户或导入服务组件、数据导出终端、数据导出服务组件在登录时是否采用了身份鉴别措施；
 - 2) 应测试验证身份鉴别措施是否能够不被绕过。
- d) 单元判定：如果 1) 和 2) 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。

B.4.3.2 测评单元(BDS-L4-02)

该测评单元包括以下要求：

- a) 测评指标：大数据平台应能对不同客户的大数据应用实施标识和鉴别。
- b) 测评对象：大数据平台、大数据应用系统和系统管理软件等。
- c) 测评实施包括以下内容：
 - 1) 应核查大数据平台是否对大数据应用实施身份鉴别措施；
 - 2) 应测试验证身份鉴别措施是否能够不被绕过。
- d) 单元判定：如果 1) 和 2) 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。

B.4.3.3 测评单元(BDS-L4-03)

该测评单元包括以下要求：

- a) 测评指标：大数据平台应为大数据应用提供集中管控其计算和存储资源使用状况的能力。
- b) 测评对象：大数据平台和大数据应用。
- c) 测评实施包括以下内容：
 - 1) 应核查大数据平台是否为大数据应用提供计算和存储资源集中管控的模块；
 - 2) 应建立大数据应用测试账户，核查大数据平台是否支持计算和存储资源集中监测和集中管控功能。
- d) 单元判定：如果 1) 和 2) 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。

B.4.3.4 测评单元(BDS-L4-04)

该测评单元包括以下要求：

- a) 测评指标：大数据平台应对其提供的辅助工具或服务组件，实施有效管理。
- b) 测评对象：辅助工具、服务组件和大数据平台。
- c) 测评实施包括以下内容：
 - 1) 应核查提供的辅助工具或服务组件是否可以安装、部署、升级和卸载等；
 - 2) 应核查提供的辅助工具或服务组件是否提供日志；

- 3) 应核查大数据平台是否采用技术手段或管理手段对辅助工具或服务组件进行统一管理,避免组件冲突。
- d) 单元判定:如果 1)~3)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。

B.4.3.5 测评单元(BDS-L4-05)

该测评单元包括以下要求:

- a) 测评指标:大数据平台应屏蔽计算、内存、存储资源故障,保障业务正常运行。
- b) 测评对象:设计文档、建设文档、计算节点和存储节点。
- c) 测评实施包括以下内容:
 - 1) 应核查设计文档或建设文档等是否具备屏蔽计算、内存、存储资源故障的措施和技术手段;
 - 2) 应测试验证单一计算节点或存储节点关闭时,是否不影响业务正常运行。
- d) 单元判定:如果 1)和 2)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。

B.4.3.6 测评单元(BDS-L4-06)

该测评单元包括以下要求:

- a) 测评指标:大数据平台应提供静态脱敏和去标识化的工具或服务组件技术。
- b) 测评对象:设计或建设文档、大数据应用和大数据平台。
- c) 测评实施包括以下内容:
 - 1) 应核查大数据平台设计或建设文档是否具备数据静态脱密和去标识化措施或方案,如核查工具或服务组件是否具备配置不同的脱敏算法的能力;
 - 2) 应核查静态脱敏和去标识化工具或服务组件是否进行了策略配置;
 - 3) 应核查大数据平台是否为大数据应用提供静态脱敏和去标识化的工具或服务组件技术;
 - 4) 应测试验证脱敏后的数据是否实现对敏感信息内容的屏蔽和隐藏,验证脱敏处理是否具备不可逆性。
- d) 单元判定:如果 1)~4)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。

B.4.3.7 测评单元(BDS-L4-07)

该测评单元包括以下要求:

- a) 测评指标:对外提供服务的大数据平台,平台或第三方只有在大数据应用授权下才可以对大数据应用的数据资源进行访问、使用和管理。
- b) 测评对象:大数据平台、大数据应用系统、数据管理系统和系统设计文档等。
- c) 测评实施包括以下内容:
 - 1) 应核查是否由授权主体负责配置访问控制策略;
 - 2) 应核查授权主体是否依据安全策略配置了主体对客体的访问规则;
 - 3) 应测试验证是否不存在可越权访问情形。
- d) 单元判定:如果 1)~3)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。

B.4.3.8 测评单元(BDS-L4-08)

该测评单元包括以下要求:

- a) 测评指标:大数据平台应提供数据分类分级安全管理功能,供大数据应用针对不同类别级别的数据采取不同的安全保护措施。
- b) 测评对象:大数据平台、大数据应用系统、数据管理系统和系统设计文档等。
- c) 测评实施包括以下内容:
 - 1) 应访谈管理员是否依据行业相关数据分类分级规范制定数据分类分级策略;
 - 2) 应核查大数据平台是否具有分类分级管理功能,是否依据分类分级策略对数据进行分类和等级划分;大数据平台是否能够为大数应用提供分类分级安全管理功能;
 - 3) 应核查大数据平台、大数据应用和数据管理系统等对不同类别级别的数据在标识、使用、传输和存储等方面采取何种安全防护措施,进而根据不同需要对关键数据进行重点防护。
- d) 单元判定:如果 1)~3)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。

B.4.3.9 测评单元(BDS-L4-09)

该测评单元包括以下要求:

- a) 测评指标:大数据平台应提供设置数据安全标记功能,基于安全标记的授权和访问控制措施,满足细粒度授权访问控制管理能力要求。
- b) 测评对象:大数据平台、数据管理系统和系统设计文档等。
- c) 测评实施包括以下内容:
 - 1) 应核查大数据平台是否依据安全策略对数据设置安全标记;
 - 2) 应核查大数据平台是否为大数应用提供基于安全标记的细粒度访问控制授权能力;
 - 3) 应测试验证依据安全标记是否实现主体对客体细粒度的访问控制管理功能。
- d) 单元判定:如果 1)~3)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。

B.4.3.10 测评单元(BDS-L4-10)

该测评单元包括以下要求:

- a) 测评指标:大数据平台应在数据采集、存储、处理、分析等各个环节,支持对数据进行分类分级处置,并保证安全保护策略保持一致。
- b) 测评对象:数据采集终端、导入服务组件、大数据应用系统、数据管理系统和系统管理软件等。
- c) 测评实施包括以下内容:
 - 1) 应访谈管理员是否依据行业相关数据分类分级规范制定数据分类分级策略;
 - 2) 应核查数据是否依据分类分级策略在数据采集、处理、分析过程中进行分类和等级划分;
 - 3) 应核查是否采取有效措施保障机构内部数据安全保护策略的一致性。
- d) 单元判定:如果 1)~3)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。

B.4.3.11 测评单元(BDS-L4-11)

该测评单元包括以下要求:

- a) 测评指标:涉及重要数据接口、重要服务接口的调用,应实施访问控制,包括但不限于数据处理、使用、分析、导出、共享、交换等相关操作。
- b) 测评对象:大数据平台、大数据应用系统、数据管理系统和系统管理软件等。
- c) 测评实施包括以下内容:
 - 1) 应核查大数据平台或大数据应用系统是否面向重要数据接口、重要服务接口的调用提供

有效访问控制措施；

- 2) 应核查访问控制措施是否包括但不限于数据处理、使用、分析、导出、共享、交换等相关操作；
- 3) 应测试验证访问控制措施是否不被绕过。
- d) 单元判定：如果 1)～3) 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。

B.4.3.12 测评单元(BDS-L3-12)

该测评单元包括以下要求：

- a) 测评指标：应在数据清洗和转换过程中对重要数据进行保护，以保证重要数据清洗和转换后的一致性，避免数据失真，并在产生问题时能有效还原和恢复。
- b) 测评对象：管理员、清洗和转换的数据、数据清洗和转换工具或脚本。
- c) 测评实施包括以下内容：
 - 1) 应访谈数据清洗转换相关管理员，询问数据清洗后是否较少出现失真或一致性破坏的情况；
 - 2) 应核查清洗和转换的数据，重要数据清洗前后的字段或者内容是否具备一致性，能否避免数据失真；
 - 3) 应核查数据清洗和转换工具或脚本，重要数据是否具备回滚机制等，在产生问题时可进行有效还原和恢复。
- d) 单元判定：如果 1)～3) 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。

B.4.3.13 测评单元(BDS-L3-13)

该测评单元包括以下要求：

- a) 测评指标：应跟踪和记录数据采集、处理、分析和挖掘等过程，保证溯源数据能重现相应过程，溯源数据满足合规审计要求。
- b) 测评对象：数据溯源措施或系统和大数据系统。
- c) 测评实施包括以下内容：
 - 1) 应核查数据溯源措施或系统是否对数据采集、处理、分析和挖掘等过程进行溯源；
 - 2) 应核查重要业务数据处理流程是否包含在数据溯源范围中；
 - 3) 应测试验证大数据平台是否对测试产生的数据采集、处理、分析或挖掘的过程进行了记录，是否可溯源测试过程；
 - 4) 应核查是否能支撑数据业务要求，确保重要业务数据可溯源；
 - 5) 对于自研发溯源措施或系统，应核查溯源数据能否满足合规审计要求；
 - 6) 对于采购的溯源措施或系统，应核查系统是否符合国家产品和服务合规审计要求，溯源数据是否符合合规审计要求。
- d) 单元判定：如果 1)～6) 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。

B.4.3.14 测评单元(BDS-L4-14)

该测评单元包括以下要求：

- a) 测评指标：大数据平台应保证不同客户大数据应用的审计数据隔离存放，并提供不同客户审计数据收集汇总和集中分析的能力。