T/XXX

团　　体　　标　　准

T/ISEAA XXX- XXXX

网络安全等级保护大数据测评指南

Evaluation guide of Big data system for classified protection of cybersecurity

（征求意见稿）

20XX-XX-XX 发布　　20XX-XX-XX 实施

中关村信息安全测评联盟　　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。

本文件由中关村信息安全测评联盟提出并归口。

本文件起草单位：。

本文件主要起草人：。

引　言

为指导大数据安全等级保护测评工作的开展，对大数据测评等环节涉及到的工作难点提出详细的指导，帮助大数据等级保护对象的主管部门及网络运营者、测评机构对大数据等级保护对象开展安全等级保护状况测试评价工作，特制定本文件。

本文件是网络安全等级保护相关系列标准之一。

与本文件相关的标准包括：

——GB/T 22240 信息安全技术　网络安全等级保护定级指南；

——GB/T 22239 信息安全技术 网络安全等级保护基本要求；

——GB/T 28448 信息安全技术 网络安全等级保护测评要求；

——T/ISEAA 002-2021 信息安全技术 网络安全等级保护大数据基本要求。

网络安全等级保护大数据测评指南

1 范围

本文件规范了大数据等级保护对象的等级测评实施，规定了网络安全等级保护第二级到第四级大数据等级保护对象的安全测评要求，对第五级大数据等级保护对象的安全测评要求不在本文件中描述。

本文件适用于中关村信息安全测评联盟内部规范测评机构对大数据等级保护对象开展等级测评工作，也可以为主管部门及网络运营者对大数据等级保护对象开展安全自查工作提供参考。

注1：第五级大数据等级保护对象是非常重要的监督管理对象，对其有特殊的管理模式和安全要求，所以不在本文件中进行描述。

注2：本文件仅规定大数据等级保护对象的扩展安全要求的测评要求，安全通用要求的测评要求参见《GB/T 28448 信息安全技术 网络安全等级保护测评要求》。

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 22239 信息安全技术 网络安全等级保护基本要求
GB/T 22240 信息安全技术 网络安全等级保护定级指南
GB/T 25069 信息安全技术 术语
GB/T 28448 信息安全技术 网络安全等级保护测评要求
GB/T 28449 信息安全技术 网络安全等级保护测评过程指南
GB/T 35274 信息安全技术 大数据服务安全能力要求
GB/T 35295-2017 信息技术 大数据 术语
GB/T 35589-2017 信息技术 大数据 技术参考模型

3 术语和定义

GB/T 22239、GB/T 22240、GB/T 28448 和 GB/T 28449、GB/T 35274、GB/T 25069、GB/T 35589-2017、GB/T 35295-2017 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 22240、GB/T 35274、GB/T 35295-2017、GB/T 35589-2017 中的一些术语和定义。

3.1

大数据 big data

具有体量巨大、来源多样、生成极快、且多变等特征并且难以用传统数据体系结构有效处理的包含大量数据集的数据。

注：国际上，大数据的 4 个特征普遍不加修饰地直接用 volume、variety、velocity、variability 予以表述，并分别赋予了它们在大数据语境下的定义：

a）体量 volume：构成大数据的数据集的规模；

b）多样性 variety：数据可能来自多个数据仓库、数据领域或多种数据类型；

c）速度 velocity：单位时间的数据流量；

d）多变性 variability：大数据其他特征，即体量、速度和多样性等特征都处于多变状态。

[来源：GB/T 35295-2017，2.1.1]

3.2

数据生命周期 data lifecycle

数据从产生，经过数据采集、数据传输、数据存储、数据处理（如计算、分析、可视化等）、数据交换等，直至数据销毁等各种生存形态的演变过程。

[来源：GB/T 35274-2017，3.2]

3.3

大数据服务 big data service

支撑机构或个人对大数据采集、存储、使用和数据价值发现等数据生命周期相关的各种数据服务和系统服务。

注：大数据服务一般面对的是海量、异构、快速变化的结构化、半结构化和非结构化数据服务，且通过底层可伸缩的大数据平台和上层各种大数据应用的系统服务提供。

[来源：GB/T 35274-2017，3.4]

3.4

大数据资源 big data resources

具有或预期具有价值的大数据集合。

注：大数据资源多以电子形式存在。

[来源：GB/T 22240-2020，3.5]

3.5

大数据应用 big data application

执行数据生命周期相关的数据采集、数据传输、数据存储、数据处理（如计算、分析、可视化等）、数据交换、数据销毁等数据活动，运行在大数据平台，并提供大数据服务的各种应用系统。

[来源：GB/T 35274-2017，3.5]

3.6

大数据平台 big data platform

采用分布式存储和计算技术，提供大数据的访问和处理、支持大数据应用安全高效运行的软硬件集合，包括监视大数据的存储、输入/输出、操作控制等大数据服务软硬件基础设施。

[来源：GB/T 35274-2017，3.6]

3.7

大数据系统 classified cybersecurity protection target of big data

等级保护对象中与大数据相关的部分或全部，包括大数据平台、大数据应用、大数据资源及其组合，以及包含大数据平台、大数据应用、大数据资源的信息系统。

4 大数据安全测评实施要点

4.1 大数据等级保护对象测评概述

大数据等级保护对象的安全等级测评，是落实网络安全等级保护大数据相关安全要求，指导和监督大数据等级保护对象的安全建设和运行，提升大数据系统全生命周期各技术环节、管理环节安全性的重要措施。

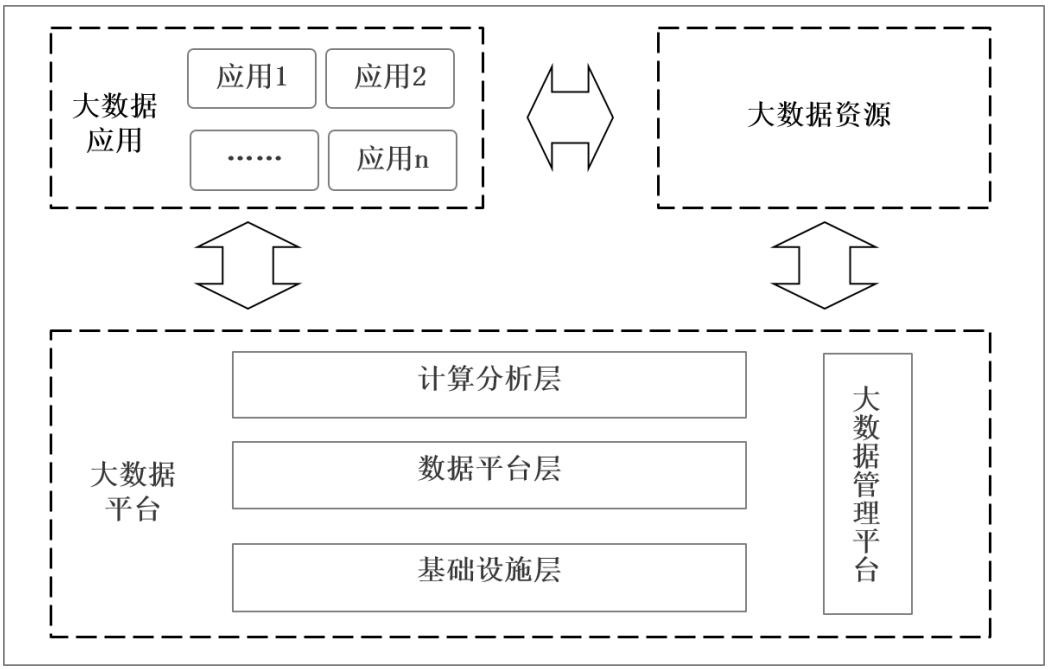

图 1 大数据相关等级保护对象的构成组件示意图

综合 GB/T 22240《信息安全技术 网络安全等级保护定级指南》给出的定级对象的基本特征，GB/T 35589-2017《信息技术 大数据 技术参考模型》给出的大数据参考架构，T/ISEAA 002-2021《信息安全技术 网络安全等级保护大数据基本要求》等对大数据等级保护对象的描述，可将大数据等级保护对象抽象为大数据资源、大数据应用、大数据平台 3 类组件，如图 1 所示。

大数据平台：为大数据应用提供资源和服务的支撑集成环境，包括基础设施层、数据平台层和计算分析层以及大数据管理平台等部分或者全部的功能。基础设施层提供物理或虚拟的计算、网络和存储能力；数据平台层提供结构化和非结构化数据的存储能力；计算分析层提供处理大量、高速、多样和多变数据的分析计算能力，大数据管理平台提供大数据平台的辅助服务能力。大数据平台可以为多个大数据应用及大数据资源提供服务。

大数据应用：基于大数据平台对数据执行处理过程，通常包括数据采集、数据传输、数据存储、数据处理、数据交换、数据销毁等环节。

大数据资源：为大数据平台和大数据应用提供基础数据的资源集合，具有数量巨大、来源多样、生成极快、且多变等特征并且难以用传统数据体系结构有效处理的包含大量数据集的数据。

在实际的信息系统中，大数据等级保护对象可能是一个独立的业务系统，也可能作为大型业务系统的组成部分。当大数据等级保护对象作为一个独立业务系统定级时，可直接按照定级范围识别测评对象的范围。当大数据等级保护对象作为大型业务系统的组成部分时，应首先进行大数据等级保护对象识别，即明确系统中哪一部分属于大数据相关资产，并仅对属于大数据相关资产的部分依据本文件开展测评。

根据 GB/T 28448-2019《信息安全技术 网络安全等级保护测评要求》给出的等级保护测评方法，本文件主要从不同形态大数据系统的识别、系统调研、测评对象确定、测评指标选取、测评实施要点、

基本要求条款测评方法等方面，为大数据系统测评过程各环节提供建议和指导，提升大数据系统测评工作的规范性和客观性，工作流程及要点如下。

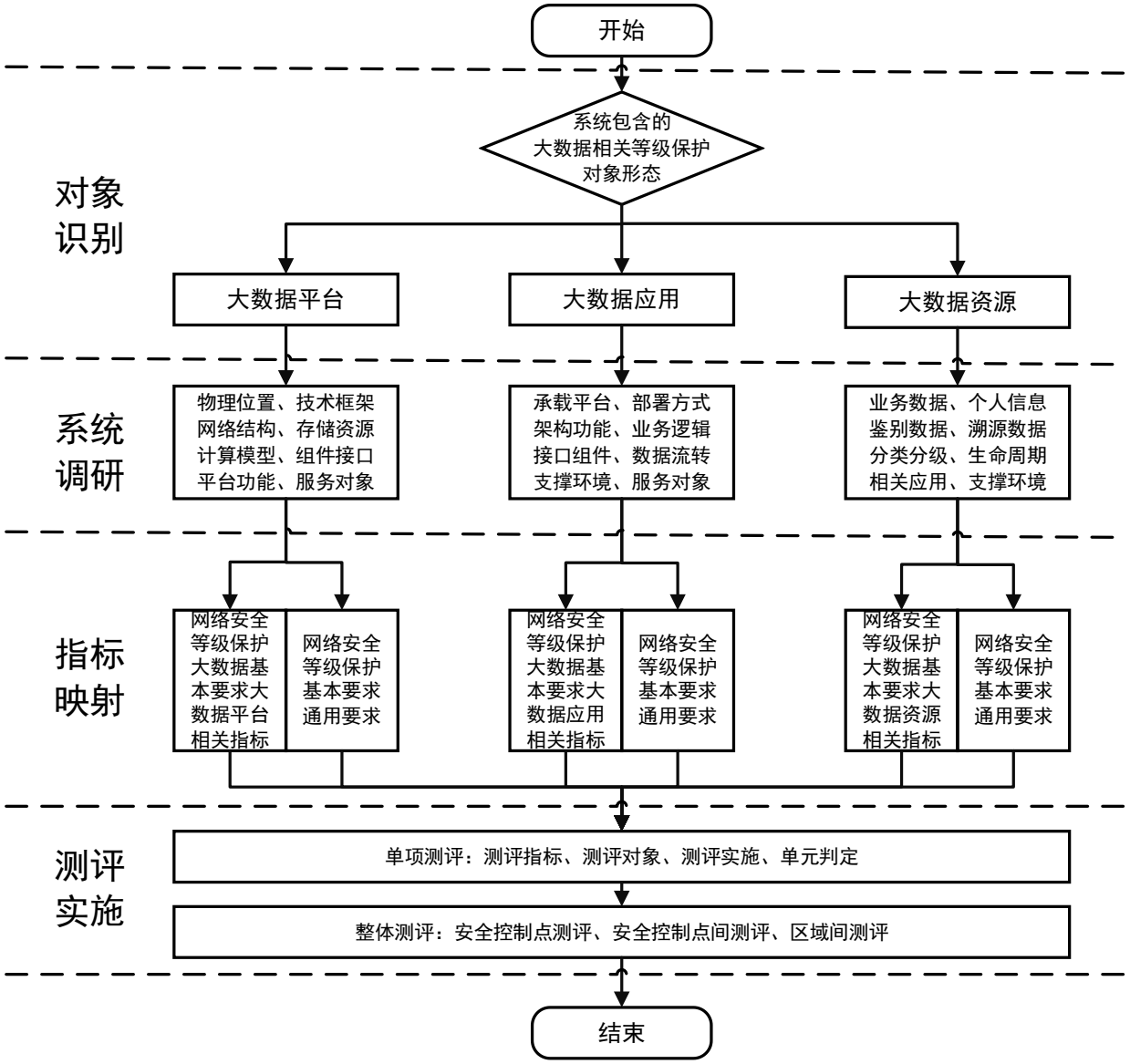

图 2 大数据等级保护对象测评工作流程及要点

4.2 系统调研

4.2.1 大数据资源调研

参考 GB/T 28449-2018《信息安全技术 网络安全等级保护测评过程指南》中的测评准备活动，测评机构通过查阅被测系统已有资料或使用系统调研表格的方式，了解整个系统的构成和保护情况以及责任部门相关情况。确定被测系统为大数据资源时，调研对象需覆盖各级各类的数据以及对应的安全防护需求，并重点关注重要业务数据、个人信息、鉴别数据、溯源数据等。

为全面了解被测系统中的各级各类数据，在信息收集和分析任务中应依据下表调研相关内容：

表 1 数据资源调研表

序号	数据类别	数据级别	安全防护需求	关联业务应用						是否出境
				数据采集	数据存储	数据处理	数据传输	数据交换	数据销毁	
1										
2										

其中，上表中的数据类别及数据级别并非被测等级保护定级对象的级别，而是由被测系统运营者根据行业数据分类分级规则或组织生产经营需求对企业自身数据确定的分类分级，可参照被测系统运营者的数据分类分级保护制度。

4.2.2 大数据应用调研

基于大数据平台对数据执行分析处理的业务应用系统应作为大数据应用，仅通过API接口调用大数据平台计算结果的业务应用系统不作为大数据应用。

确定被测系统为大数据应用时，调研对象包括数据类、应用部件类和系统支撑类。其中数据类对象调研时在按照4.2.1的表1调研外，还需关注大数据应用新生成的业务数据、配置数据、日志数据等。应用部件类调研时需覆盖重点关注数据全生命周期相关的业务应用系统、组件及提供服务的API接口，包括调研重点关注数据在流转过程中的流经对象，形成对应的数据流转图。系统支撑类调研时应包括大数据应用运维管理以及安全管理等相关的管理及支撑类系统或组件。

4.2.3 大数据平台调研

确定被测系统为大数据平台时，调研对象为提供资源和服务的支撑集成环境，包括基础设施层、数据平台层、计算分析层以及大数据管理平台等相关的服务组件及提供服务的 API 接口。另外，还需调研不同安全责任主体的数据、测试训练数据、平台提供的开发测试环境和数据分析挖掘模型等。

4.3 测评对象确定

4.3.1 大数据资源测评对象确定

大数据资源的测评对象不限于通用测评对象中的“关键数据类”，细化扩展为不同等级不同类别的各类数据。在大数据资源类测评对象选择之前，测评机构应将被测对象的数据级别映射为系统定级时考虑的业务信息安全保护等级，并在测评报告中明确映射的规则。应保证数据类的最高级别不低于其所属被测系统的业务信息安全保护等级。映射之后应形成如下表格：

表 2 数据选择矩阵表

数据级别	数据类别
一级数据	
二级数据	
三级数据	
四级数据	

在选择数据类测评对象时，可参考以下几个方面：

a） 根据被测系统的安全保护等级，确定选择测评对象所属级别，例如四级被测系统选择二、三、四级的数据；三级被测系统选择二、三级的数据；二级被测系统选择二级的数据；

b） 重点抽选重要业务数据和敏感数据，例如个人敏感信息、溯源数据等敏感数据类；

c） 根据信息内容、数据来源、存储方式、流动方式等不同，从上述两方面确定出的数据级别和类别中，选择出有代表性的数据类作为具体测评对象，而且高级别数据类应作为测评核心，增加抽样数量。数据类测评对象的存在形态可能是数据库、数据表、数据文件、字段名（列）、数据行以及其他非结构化数据等。

测评机构在选取大数据资源特殊测评对象时可参照下表：

表 3 大数据资源测评对象举例

大数据对象类型	测评对象举例
大数据资源	管理类：大数据安全策略类文档、大数据管理制度文档（如大数据安全工作的总体方针文档、数据分类分级保护制度、数据生命周期安全保护制度、数据资产管理制度、跨境数据管理制度、个人数据安全管理制度、以及其他数据安全保护相关的文档等）、系统设计及建设相关文档（如设计及建设方案、定级备案材料、供应商管理制度、供应商服务协议、数据安全协议、服务协议、用户须知、权责声明等其他材料）、运维记录表单（如制度评审记录、数据迁移记录、数据销毁记录、授权审批流记录、供应链安全事件记录、接口资产清单。 技术类：物理机房、业务数据、个人信息、敏感信息、配置数据、审计数据、溯源数据等。

4.3.2 大数据应用测评对象确定

针对已选出的数据类测评对象中的重要数据和敏感数据（如个人敏感信息、溯源数据和最高级别业务数据等），分别分析数据流转的流经对象及数据流转图。

应用部件类测评对象选择时需根据数据流转图和《信息安全技术 网络安全等级保护大数据基本要求》中与数据生命周期相关的要求，选择对数据类测评对象进行计算处理及安全保护的软硬件组件。

此外，大数据应用测评对象还应包括大数据应用运维管理以及安全管理等支撑类对象。

根据已经了解到的被测大数据系统信息，分析整个被测大数据系统及其涉及的业务应用系统，确定出本次测评的测评对象。最终明确大数据应用测评对象清单。

测评机构在选取大数据应用特殊测评对象时可参照下表：

表 4 大数据应用测评对象举例

大数据对象类型	测评对象举例
大数据应用	管理类：大数据安全策略类文档、大数据管理制度文档（如大数据安全工作的总体方针文档、数据分类分级保护制度、数据生命周期安全保护制度、数据资产管理制度、跨境数据管理制度、个人数据安全管理制度、以及其他数据安全保护相关的文档等）、系统设计及建设相关文档（如设计及建设方案、定级备案材料、供应商管理制度、供应商服务协议、数据安全协议、服务协议、用户须知、权责声明等其他材料）、运维记录表单（如制度评审记录、数据迁移记录、数据销毁记录、授权审批流记录、供应链安全事件记录、接口资产清单。 技术类：物理机房、大数据应用系统（如数据采集、数据传输、数据存储、数据处理、数据交换、数据销毁、API 接口应用等系统）、业务应用系统、数据库管理系统、数据共享过程中涉及到的数据共享接口、数据共享系统、系统共享软件、系统管理软件、中间件、业务数据、个人信息、敏感信息、配置数据、审计数据、溯源数据等。

4.3.3 大数据平台测评对象确定

大数据平台测评对象包括基础设施层、数据平台层、计算分析层以及大数据管理平台等相关的服务组件及接口，选择原则依据GB/T 28449 附录D.1测评对象确定准则确定。

测评机构在选取大数据平台特殊测评对象时可参照下表：

表 5 大数据平台测评对象举例

大数据对象类型	测评对象举例
大数据平台	管理类：大数据安全策略类文档、大数据管理制度文档（如大数据安全工作的总体方针文档、数据分类分级保护制度、数据生命周期安全保护制度、数据资产管理制度、跨境数据管理制度、个人数据安全管理制度、以及其他数据安全保护相关的文档等）、系统设计及建设相关文档（如设计及建设方案、定级备案材料、供应商管理制度、供应商服务协议、数据安全协议、服务协议、用户须知、权责声明等其他材料）、运维记录表单（如制度评审记录、数据迁移记录、数据销毁记录、授权审批流记录、供应链安全事件记录、接口资产清单。 技术类测评对象涉及基础设施层、数据平台层、计算分析层以及大数据管理平台等模块，其具体对象包括但不限于： 1.基础设施层：交换机、服务器、存储设备等； 2.数据平台层：Hadoop、分布式文件系统（HDFS）、分布式数据库（HBase）、Hive 及资源管理器（YARN）等； 3.计算分析层：联邦学习平台、安全多方计算平台、同态加密平台等各种算法模型平台，以及其他服务组件； 4.大数据管理平台：运维管理软件（如 Ganglia、Nagios、Apache Hadoop 其组件包括 HDFS、MapReduce）；流处理系统 Apache Storm、Apache Samza 等；混合处理系统 Apache Spark，Apache FlinkImpala、Spark 等；信息交互通信框架层如 Hue、Sqoop、Flume、Kafka 等；数据防泄漏系统；数据监控系统；业务系统应用接口层如数据流入平台的接口、数据流出平台或者应用的接口等；以及其他服务组件。 5.大数据平台相关的物理机房、业务数据、个人信息、敏感信息、配置数据、审计数据、溯源数据等。

4.4 测评指标确定

测评指标选择时可以参考以下步骤：

a） 根据被测系统的定级结果，即：根据被测评系统的业务信息安全保护等级和系统服务安全保护等级，得出被测系统的系统服务保证类（A 类）安全要求、业务信息安全类（S 类）安全要求以及通用安全保护类（G 类）安全要求的组合情况。

b） 根据被测系统的系统服务保证类（A 类）安全要求、业务信息安全类（S 类）安全要求及通用安全保护类（G 类）安全要求的组合情况，从 GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》、行业规范中选择相应等级的安全通用要求作为基本测评指标。

c） 根据被测系统的大数据形态，从 T/ISEAA 002-2021《信息安全技术 网络安全等级保护大数据基本要求》中选择相应的大数据扩展要求指标。

d） 根据被测系统实际情况，确定不适用测评指标。

e） 根据测评委托单位所属行业及被测系统业务自身需求，确定特殊测评指标。

4.5 测评实施关注点

大数据系统结构复杂，参与角色众多，其安全保护由各安全责任主体共同参与，因此，需明确各责任主体的安全职责，实现目标同步，责任共担。在对大数据系统开展等级测评过程中，应根据被测定级对象所承担的安全保护职责，对测评关注点进行相应调整。对于不同类型的被测定级对象而言，其测评实施关注点也不同，具体如下：

1）大数据平台定级对象应重点关注自身安全保护能力以及为大数据应用、大数据资源提供的安全服务能力两方面。

针对大数据平台处理框架组件/产品的测评，其侧重点主要集中在以下几个方面：

——处理框架组件/产品自身是否因为版本或代码修改原因造成组件/产品存在安全漏洞问题；

——对处理框架组件/产品及部署的相关运维管理平台中的用户身份鉴别、访问控制等控制措施进行重点测评；

——确保对处理框架组件/产品的日志进行记录，并对相关日志信息进行统一管理和综合审计；

——对存储的数据是否进行相关加密处理，以及数据分片是否能对原始数据进行还原处理。

2）大数据应用定级对象应重点关注自身安全保护能力以及数据收集、使用、加工、传输等过程中实施的数据安全保护策略及保护能力。

3）大数据资源定级对象应重点关注数据安全保护策略在全生命周期的实施情况和保护能力。

——应梳理数据资产，并明确数据资产类型、数据量、存放位置、数据关联系统、数据共享情况、数据出境情况等；

——重点测评数据安全管控措施，包括数据访问权限管控、数据泄露管控、数据接口管控等。

5 第二级安全测评要求

5.1 安全物理环境

5.1.1 基础设施位置

5.1.1.1 测评单元（L2-PES-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：物理机房、机房管理员。

c) 测评实施：应核查大数据相关的管理系统、业务系统以及数据资源所在的存储节点、处理节点、分析节点等的软硬件设备所在的物理机房是否均位于中国境内。

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。

5.2 安全通信网络

5.2.1 网络架构

5.2.1.1 测评单元（L2-CNS-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和大数据资源。

b) 测评对象：大数据平台、大数据应用、大数据资源及业务应用系统的定级备案材料，服务协议、用户须知等其他材料。

c) 测评实施包括以下内容：

1） 应访谈管理人员并核查大数据平台的服务协议、用户须知等相关材料，其中是否明确告知用户，大数据平台不承载高于其安全保护等级的大数据应用和大数据资源；
2） 应访谈管理人员并核查大数据平台及其所承载的大数据应用系统、大数据资源的相关定级备案材料，大数据平台安全保护等级是否不低于其承载的大数据应用和大数据资源的安全保护等级。

d） 单元判定：如果 1）-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

5.3 安全计算环境

5.3.1 身份鉴别

5.3.1.1 测评单元（L2-CES-01）

该测评单元包括以下要求：

a） 测评指标：大数据系统提供的重要外部调用接口应进行身份鉴别。
b） 测评对象：大数据平台、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对重要外部调用接口进行身份鉴别；
2） 应测试验证调用接口的身份认证功能是否有效，是否无法被绕过。
d） 单元判定：如果 1）-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。

5.3.2 访问控制

5.3.2.1 测评单元（L2-CES-02）

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，平台或第三方应在服务客户授权下才可以对其数据资源进行访问、使用和管理。
b） 测评对象：大数据管理平台、相关授权审批文档和数据安全保护相关管理制度文档。
c） 测评实施包括以下内容：
1） 应核查对服务客户的数据资源进行访问、使用和管理时，是否具备必要的授权机制，包括授权流程、授权方式、授权内容等；
2） 应核查大数据平台，平台或第三方是否具有服务客户数据资源的访问、使用和管理权限，如果具有，核查是否有相关授权证明。
d） 单元判定：如果 1）-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。

5.3.2.2 测评单元（L2-CES-03）

该测评单元包括以下要求：

a） 测评指标：应对数据进行分类分级管理。
b） 测评对象：大数据资源、大数据应用、大数据平台、系统设计及建设方案文档等。
c） 测评实施包括以下内容：
1） 应核查系统设计及建设方案文档中是否具备数据分类分级标识的相关设计；
2） 应核查大数据系统是否依据相关设计对数据进行分类分级标识；
3） 应测试验证数据分级分类标识是否有效。

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，否则不符合本单元测评指标要求。

5.3.2.3 测评单元（L2-CES-04）

该测评单元包括以下要求：

a) 测评指标：应采取技术手段对数据采集终端、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进行限制。
b) 测评对象：大数据采集终端、数据导入服务组件、数据导出终端、数据导出服务组件等。
c) 测评实施包括以下内容：
   1) 应核查是否具备对相关终端和组件的使用进行限制的技术手段，如身份鉴别、权限控制、操作审计等；
   2) 应测试验证所使用的限制措施是否有效，是否无法被绕过。
d) 单元判定：如果 1）-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。

5.3.2.4 测评单元（L2-CES-05）

该测评单元包括以下要求：

a) 测评指标：应最小化各类接口操作权限。
b) 测评对象：大数据应用、大数据平台中的各类接口。
c) 测评实施：应核查各类接口的操作权限是否为其实现功能所需的最小权限。
d) 单元判定：如果以上测评实施为肯定，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。

5.3.2.5 测评单元（L2-CES-06）

该测评单元包括以下要求：

a) 测评指标：应最小化数据使用、分析、导出、共享、交换的数据集。
b) 测评对象：大数据资源、大数据应用、大数据平台、系统设计及建设方案文档等。
c) 测评实施包括以下内容：
   1) 应核查系统设计及建设方案文档，是否遵循数据集最小化原则，包含但不限于数据的使用、分析、导出、共享、交换等过程；
   2) 应核查在数据使用、分析、导出、共享、交换过程中是否不存在非必要的数据集。
d) 单元判定：如果 1）-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。

5.3.3 安全审计

5.3.3.1 测评单元（L2-CES-07）

该测评项单元包含以下要求：

a) 测评指标：大数据系统应对其提供的重要接口的调用情况以及各类重要账号的操作情况进行审计。
b) 测评对象：大数据管理平台和大数据应用系统等。
c) 测评实施：
   1) 应核查大数据系统是否开启相关审计功能，审计功能工作是否正常，是否存在审计记录等；
   2) 应核查大数据系统的审计内容是否包括重要接口的调用情况和各类重要账号的操作情况。

d) 单元判定：如果 1)-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。

5.3.3.2 测评单元（L2-CES-08）

该测评项单元包含以下要求：

a) 测评指标：应保证大数据系统服务商对服务客户数据的操作可被服务客户审计。
b) 测评对象：大数据管理平台、大数据应用系统和服务组件等。
c) 测评实施：应核查是否能够保证大数据系统服务商对服务客户数据的操作（如增、删、改、查等操作）可被服务客户审计。
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。

5.3.4 数据完整性

5.3.4.1 测评单元（L2-CES-09）

该测评单元包括以下要求：

a) 测评指标：应采用技术手段对数据交换过程进行数据完整性检测。
b) 测评对象：数据交换接口、数据共享接口、数据共享系统及系统共享软件等。
c) 测评实施包括以下内容：
   1) 应核查数据在交换过程中是否采用技术手段进行数据完整性检测,如校验技术或密码技术等；
   2) 应测试验证数据完整性校验措施是否有效。
d) 单元判定：如果 1）-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。

5.3.4.2 测评单元（L2-CES-10）

该测评单元包括以下要求：

a) 测评指标：数据在存储过程中的完整性保护应满足数据提供方系统的安全保护要求。
b) 测评对象：大数据应用系统、大数据管理平台、数据提供方合同及数据安全协议、系统定级备案材料、系统设计及建设方案文档等。
c) 测评实施包括以下内容：
   1) 应核查系统设计及建设方案文档、数据提供方合同、数据安全协议以及系统定级备案材料，是否明确对数据存储过程的完整性保护需求；
   2) 应核查存储完整性保护措施是否满足数据提供方的完整性保护需求；
   3) 应测试验证数据存储完整性保护措施是否有效。
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。

5.3.5 数据保密性

5.3.5.1 测评单元（L2-CES-11）

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：大数据平台设计及建设方案文档、静态脱敏和去标识化工具或服务组件等。

c) 测评实施包括以下内容：
   1) 应核查大数据平台系统设计及建设方案中是否提供数据静态脱敏和去标识化相关措施；
   2) 应核查静态脱敏和去标识化工具或服务组件是否支持静态脱敏和去标识化相关策略配置；
   3) 应测试验证静态脱敏和去标识化措施是否有效。
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。

5.3.5.2 测评单元（L2-CES-12）

该测评单元包括以下要求：
a) 测评指标：应依据相关安全策略对数据进行静态脱敏和去标识化处理。
b) 测评对象：大数据管理平台、业务应用系统、数据管理系统和系统设计及建设方案文档等。
c) 测评实施包括以下内容：
   1) 应核查系统设计及建设方案，是否明确了数据安全策略，是否具有数据静态脱敏和去标识化相关需求；
   2) 应核查是否依据数据安全策略对数据进行静态脱敏和去标识化处理，包括但不限于业务数据、日志文件等；
   3) 应测试验证静态脱敏和去标识化措施是否有效。
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。

5.3.5.3 测评单元（L2-CES-13）

该测评单元包括以下要求：
a) 测评指标：数据在存储过程中的保密性保护应满足数据提供方系统的安全保护要求。
b) 测评对象：大数据应用系统、大数据管理平台、数据提供方合同及数据安全协议、系统设计及建设方案文档和系统定级备案材料等。
c) 测评实施包括以下内容：
   1) 应核查数据提供方合同、数据安全协议以及系统定级备案材料，明确对数据存储过程的保密性保护需求；
   2) 应核查存储保密性保护措施是否满足数据提供方的保密性保护需求；
   3) 应测试验证数据存储保密性保护措施是否有效。
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。

5.3.6 数据备份与恢复

5.3.6.1 测评单元（L2-CES-14）

该测评单元包括以下要求：
a) 测评指标：备份数据应采取与原数据一致的安全保护措施。
b) 测评对象：配置数据和业务数据等备份数据。
c) 测评实施包括以下内容：
   1) 应核查备份数据的安全保护措施是否与原数据一致，安全保护措施包括但不限于备份数据的访问控制、操作审计、存储保密性和存储完整性、传输保密性和传输完整性等保护措施；
   2) 应测试验证备份数据相关保护措施的有效性是否与原数据保护措施一致。

d) 单元判定：如果 1）-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。

5.3.7 剩余信息保护

5.3.7.1 测评单元（L2-CES-15）

该测评单元包括以下要求：

a) 测评指标：大数据平台应提供主动迁移功能，数据整体迁移的过程中应杜绝数据残留。
b) 测评对象：系统设计及建设方案文档、数据迁移记录和相关配置等。
c) 测评实施包括以下内容：
   1) 应核查大数据平台系统设计及建设方案中是否提供主动迁移功能，是否具备整体迁移过程杜绝数据残留相关措施；
   2) 应核查主动迁移功能是否可用，包括相关配置项是否有效等；
   3) 应核查整体迁移完成后是否采取技术措施对原存储空间进行完全清除，包括但不限于索引表删除、低级格式化、重写覆盖、消磁以及物理销毁等。
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。

5.3.7.2 测评单元（L2-CES-16）

该测评单元包括以下要求：

a) 测评指标：大数据平台应能够根据服务客户提出的数据销毁要求和方式实施数据销毁。
b) 测评对象：系统设计及建设方案文档、相关操作记录等。
c) 测评实施包括以下内容：
   1) 应核查大数据平台系统设计及建设方案，是否支持多种数据销毁功能，包括但不限于索引表删除、低级格式化、重写覆盖、消磁以及物理销毁等；
   2) 应核查大数据平台是否提供渠道供服务客户提出数据销毁要求和方式，包括但不限于数据安全协议、服务协议、用户须知、权责声明、系统工单等；
   3) 应核查数据销毁记录是否与服务客户提出的要求和方式一致。
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。

5.3.8 个人信息保护

5.3.8.1 测评单元（L2-CES-17）

该测评单元包括以下要求：

a) 测评指标：采集、处理、使用、转让、共享、披露个人信息应在个人信息处理的授权同意范围内，并保留操作审计记录。
b) 测评对象：大数据平台、大数据应用、大数据资源所关联的个人信息数据。
c) 测评实施包括以下内容：
   1) 应核查是否明确个人信息处理的授权同意范围，包括但不限于知悉范围、留存期限、流转路径等；
   2) 应核查采集、处理、使用、转让、共享、披露个人信息是否未超出个人信息处理的授权同意范围；

3) 应核查采集、处理、使用、转让、共享、披露个人信息是否保留审计记录，审计记录内容是否符合国家法律法规对于个人信息安全审计的相关要求。

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。

5.3.8.2 测评单元（L2-CES-18）

该测评单元包括以下要求：

a) 测评指标：应采取措施防止在数据处理、使用、分析、导出、共享、交换等过程中识别出个人身份信息。

b) 测评对象：大数据平台、大数据应用、大数据资源所关联的系统设计及建设方案文档等。

c) 测评实施包括以下内容：

1) 应核查系统设计及建设方案文档，是否在数据处理、使用、分析、导出、共享、交换等过程中具备相关措施防止个人身份信息被识别，包括但不限于脱敏、匿名、泛化、去标识化等；

2) 应测试验证所使用的措施是否有效。

d) 单元判定：如果 1）-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。

5.3.8.3 测评单元（L2-CES-19）

该测评单元包括以下要求：

a) 测评指标：对个人信息的重要操作应设置内部审批流程,审批通过后才能对个人信息进行相应的操作。

b) 测评对象：大数据平台、大数据应用、大数据资源所关联的系统设计及建设方案文档和安全策略文档等。

c) 测评实施包括以下内容：

1) 应核查系统设计及建设方案和安全策略文档是否明确了对个人信息的重要操作的内部审批流程，包括但不限于批量导出、修改、销毁、备份、恢复等；

2) 应访谈管理人员，了解审批通过是否为实施重要操作的必备前置条件。

d) 单元判定：如果 1）-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。

5.4 安全管理中心

5.4.1 系统管理

5.4.1.1 测评单元（L2-SMC-01）

该测评单元包括以下要求：

a) 测评指标：大数据平台应为服务客户提供管理其计算和存储资源使用状况的能力。

b) 测评对象：大数据管理平台。

c) 测评实施包括以下内容：

1) 应核查大数据平台是否为服务客户提供管理其计算和存储资源使用状况的能力,包括但不限于查询、监控、申请变更等；

2) 应测试验证提供给客户的管理功能是否有效，是否不存在无法管理的情况。

d) 单元判定：如果 1）-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。

5.4.1.2 测评单元（L2-SMC-02）

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、服务组件和大数据管理平台等。
c) 测评实施包括以下内容：
   1) 应核查大数据管理平台是否具备对其提供的辅助工具或服务组件进行管理的能力，包括但不限于辅助工具或服务组件的安装、部署、监控、优化、升级、卸载、身份鉴别、访问权限管理、操作审计等；
   2) 应测试验证大数据平台提供的辅助工具或服务组件的安全管理措施是否有效，是否不存在无法管理的情况。
d) 单元判定：如果 1）-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。

5.4.1.3 测评单元（L2-SMC-03）

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：系统设计及建设方案文档、计算分析层相关节点等。
c) 测评实施包括以下内容：
   1) 应核查是否具备屏蔽计算、内存、存储资源故障的措施和技术手段，相关措施是否正常运行；
   2) 应测试验证相关措施的有效性，是否不存在部分计算节点或存储节点故障时，业务无法正常运行的情况。
d) 单元判定：如果 1）-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。

5.4.1.4 测评单元（L2-SMC-04）

该测评单元包括以下要求：

a) 测评指标：大数据平台在系统维护、在线扩容等情况下，应保证大数据应用和大数据资源的正常业务处理能力。
b) 测评对象：大数据管理平台、系统维护及扩容测试记录等文档。
c) 测评实施包括以下内容：
   1) 应核查大数据平台在系统维护、在线扩容等情况下，是否采取技术手段保证大数据应用和大数据资源的正常业务处理能力；
   2) 应测试验证所采取的技术手段是否有效，是否不存在部分大数据应用和大数据资源的正常业务处理无法开展的情况。
d) 单元判定：如果 1）-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。

5.5 安全管理制度

5.5.1 安全策略

5.5.1.1 测评单元（L2-PSS-01）

该测评单元包括以下要求：

a) 测评指标：应制定大数据安全工作的总体方针和安全策略，阐明本机构大数据安全工作的目标、范围、原则和安全框架等相关内容。
b) 测评对象：大数据安全工作的总体方针、安全策略类文档。
c) 测评实施包括以下内容：
   1) 应访谈并核查是否具有大数据安全工作的总体方针和安全策略相关文档；
   2) 应核查相关文档中是否明确机构大数据安全工作的总体目标、范围、原则和安全框架等相关内容。
d) 单元判定：如果 1）-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。

5.5.1.2 测评单元（L2-PSS-02）

该测评单元包括以下要求：

a) 测评指标：大数据安全策略应覆盖数据生命周期相关的数据安全，内容至少包括目的、范围、岗位、责任、管理层承诺、内外部协调及合规性要求等。
b) 测评对象：安全策略类文档。
c) 测评实施包括以下内容：
   1) 应访谈并核查是否具有大数据安全策略相关文档；
   2) 应核查大数据安全策略文档内容是否覆盖数据生命周期相关的数据安全，至少包含目的、范围、岗位、责任、管理层承诺、内外部协调及合规性要求等。
d) 单元判定：如果 1）-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。

5.6 安全管理机构

5.6.1 授权和审批

5.6.1.1 测评单元（L2-ORS-01）

该测评单元包括以下要求：

a) 测评指标：数据的采集应获得数据源管理者的授权，确保符合数据收集最小化原则。
b) 测评对象：数据源管理者、数据安全保护相关管理制度文档及记录表单类文档等。
c) 测评实施包括以下内容：
   1) 应访谈数据源管理者并核查相关制度，是否要求对数据的采集需获得授权，是否遵循最小化授权原则；
   2) 应核查是否具有数据采集相关的授权记录，授权内容是否符合数据收集最小化原则，是否与相关制度要求一致。
d) 单元判定：如果 1）-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。

5.6.2 审核和检查

5.6.2.1 测评单元（L2-ORS-02）

该测评单元包括以下要求：

a) 测评指标：应定期对个人信息安全保护措施的有效性进行常规安全检查。
b) 测评对象：信息/网络安全主管、数据安全保护相关管理制度文档等。
c) 测评实施包括以下内容：
   1) 应访谈信息/网络安全主管并核查数据安全保护相关管理制度，是否对个人信息安全保护措施的有效性进行常规安全检查；
   2) 应核查是否具有常规安全检查相关记录，检查内容是否覆盖个人信息安全保护措施的有效性检查，检查频率、检查方法以及检查内容等是否与管理制度要求一致，记录内容是否详尽。
d) 单元判定：如果 1）-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。

5.7 安全建设管理

5.7.1 服务供应商选择

5.7.1.1 测评单元（L2-CMS-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和大数据资源提供相应等级的安全保护能力。
b) 测评对象：安全策略类文档、数据安全保护相关管理制度文档和大数据平台定级备案材料、等级测评报告等。
c) 测评实施包括以下内容：
   1) 应访谈系统建设负责人并核查相关制度，是否根据业务系统的安全保护等级选择具有相应等级安全保护能力的大数据平台；
   2) 应核查大数据平台和大数据应用、大数据资源的定级备案材料，大数据平台是否与所承载的大数据应用和大数据资源具有相应或高于的安全保护能力。
   3) 应核查所使用的大数据平台的网络安全等级保护测评报告，报告时间和报告结论是否符合网络安全等级保护相关要求。
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。

5.7.1.2 测评单元（L2-CMS-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和大数据平台使用者的权限与责任、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：供应商服务协议及数据安全协议等。
c) 测评实施包括以下内容：
   1) 应核查供应商服务协议、数据安全协议以及用户须知等相关材料，是否明确了大数据服务提供者和使用者的权限与责任，核查内容是否覆盖大数据服务内容、安全服务内容，是否明确服务范围、服务指标、职责划分、访问授权、隐私保护、行为准则、违约责任等；
   2) 应核查大数据平台供应商服务协议、数据安全协议以及用户须知等相关材料的有效性，是否具有双方签字及盖章，是否处于有效期内等。
d) 单元判定：如果 1）-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。

5.7.2 供应链管理

5.7.2.1 测评单元（L2-CMS-03）

该测评单元包括以下要求：

a) 测评指标：应确保供应商的选择符合国家有关规定。

b) 测评对象：建设负责人。

c) 测评实施包括以下内容：

1) 应访谈系统建设负责人并核查相关材料，供应商的选择过程是否符合国家有关规定，包括但不限于招投标流程、合同签约流程、价款支付方式等；

2) 应访谈系统建设负责人并核查相关材料，供应商的选择结果是否符合国家有关规定，包括但不限于供应商的建设服务资质、安全服务资质、集成服务资质、密码服务资质以及产品销售许可等。

d) 单元判定：如果 1）-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。

5.7.3 数据源管理

5.7.3.1 测评单元（L2-CMS-04）

该测评单元包括以下要求：

a) 测评指标：应通过合法正当的渠道获取各类数据。

b) 测评对象：供应商服务协议、数据安全协议及记录表单类文档等。

c) 测评实施包括以下内容：

1) 应对照获取的数据类核查供应商服务协议及数据安全协议，是否均通过合法正当的渠道获取各类数据；

2) 如果获取的渠道数据用于提供大数据平台服务，应核查相关系统、合同或协议等是否对渠道进行了明示。

d) 单元判定：如果 1）-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。

5.8 安全运维管理

5.8.1 资产管理

5.8.1.1 测评单元（L2-MMS-01）

该测评单元包括以下要求：

a) 测评指标：应建立数据资产安全管理策略，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，包括但不限于数据采集、传输、存储、处理、交换、销毁等过程。

b) 测评对象：数据资产安全管理策略、操作记录及提供数据保护的相关产品或组件。

c) 测评实施包括以下内容：

1) 应访谈并核查是否建立数据资产安全管理策略，策略是否明确各类数据全生命周期的操作规范、保护措施、管理人员职责，包括但不限于数据采集、传输、存储、处理、交换、销毁等过程；

2) 应核查数据采集、传输、存储、处理、交换、销毁等过程中的数据保护措施和相关记录是否与数据资产安全管理策略一致。

d) 单元判定：如果 1）-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。

5.8.1.2 测评单元（L2-MMS-02）

该测评单元包括以下要求：

a) 测评指标：应对数据资产进行登记，建立数据资产清单。

b) 测评对象：数据资产安全管理策略、数据资产清单等。

c) 测评实施包括以下内容：

1) 应访谈管理员是否定期对数据资产进行梳理和登记，是否形成数据资产清单；

2) 应核查数据资产清单是否全面，是否覆盖重要数据，包括但不限于业务数据、标识数据、密钥数据、审计数据、溯源数据、脱敏数据、个人数据、配置数据、备份数据等。

d) 单元判定：如果 1）-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。

5.8.2 介质管理

5.8.2.1 测评单元（L2-MMS-03）

该测评单元包括以下要求：

a) 测评指标：应在中国境内对数据进行清除或销毁。

b) 测评对象：数据管理员及数据清除、销毁过程记录。

c) 测评实施包括以下内容：

1) 应访谈数据管理员，数据清除或销毁是否在中国境内开展；

2) 应核查数据清除、销毁相关记录，是否依据要求在中国境内对数据进行清除或销毁。

d) 单元判定：如果 1）-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。

5.8.3 网络和系统安全管理

5.8.3.1 测评单元（L2-MMS-04）

该测评单元包括以下要求：

a) 测评指标：应建立对外数据接口安全管理机制，所有的接口调用均应获得授权和批准。

b) 测评对象：安全策略类文档、数据安全保护相关管理制度文档、授权审计记录、大数据系统审计模块等。

c) 测评实施包括以下内容：

1) 应访谈安全管理人员并核查相关管理制度，是否建立大数据网络和系统安全管理机制，是否要求所有的接口调用均应获得授权和批准；

2) 应核查相关授权和审批记录，记录内容是否全面，授权和审批过程是否合规，是否与管理制度要求一致。

d) 单元判定：如果 1）-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。

6 第三级安全测评要求

6.1 安全物理环境

6.1.1 基础设施位置

6.1.1.1 测评单元（L3-PES-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：物理机房、机房管理员。

c) 测评实施：应核查大数据相关的管理系统、业务系统以及数据资源所在的存储节点、处理节点、分析节点等的软硬件设备所在的物理机房是否均位于中国境内。

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。

6.2 安全通信网络

6.2.1 网络架构

6.2.1.1 测评单元（L3-CNS-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和大数据资源。

b) 测评对象：大数据平台、大数据应用、大数据资源及业务应用系统的定级备案材料，服务协议、用户须知等其他材料。

c) 测评实施包括以下内容：

1) 应访谈管理人员并核查大数据平台的服务协议、用户须知等相关材料，其中是否明确告知用户，大数据平台不承载高于其安全保护等级的大数据应用和大数据资源；

2) 应访谈管理人员并核查大数据平台及其所承载的大数据应用系统、大数据资源的相关定级备案材料，大数据平台安全保护等级是否不低于其承载的大数据应用和大数据资源的安全保护等级。

d) 单元判定：如果 1）-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。

6.2.1.2 测评单元（L3-CNS-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：大数据平台基础设施层的网络架构。

c) 测评实施包括以下内容：

1) 应核查大数据平台基础设施层的网络架构、策略配置或相关组件，是否采用带外管理等方式实现管理流量与系统业务流量分离；

2) 应测试验证大数据平台的管理流量与系统业务流量是否分离。

d) 单元判定：如果 1）-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。

6.2.1.3 测评单元（L3-CNS-03）

该测评单元包括以下要求：

a) 测评指标：应提供开放接口或开放性安全服务，允许客户接入第三方安全产品或在大数据平台选择第三方安全服务。

b） 测评对象：大数据平台设计及建设方案文档、开放接口或提供开放性安全服务的组件。
c） 测评实施包括以下内容：
1） 应核查接口设计文档或开放性服务技术文档是否提供开放接口以及是否允许接入第三方安全产品或服务；
2） 应核查大数据平台服务客户是否可以接入第三方安全产品或在大数据平台选择第三方安全服务。
d） 单元判定：如果 1）-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。

6.3 安全计算环境

6.3.1 身份鉴别

6.3.1.1 测评单元（L3-CES-01）

该测评单元包括以下要求：
a） 测评指标：大数据平台应提供双向认证功能，能对不同客户的大数据应用、大数据资源进行双向身份鉴别。
b） 测评对象：大数据平台设计及建设方案文档、大数据平台等。
c） 测评实施包括以下内容：
1） 应核查大数据平台设计及建设方案文档中是否具备双向身份认证功能设计；
2） 应核查大数据平台是否能对不同客户的大数据应用、大数据资源进行双向身份认证；
3） 应测试验证双向身份认证功能是否有效，是否无法被绕过。
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。

6.3.1.2 测评单元（L3-CES-02）

该测评单元包括以下要求：
a） 测评指标：应采用口令和密码技术组合的鉴别技术对使用数据采集终端、数据导入服务组件、数据导出终端、数据导出服务组件的主体实施身份鉴别。
b） 测评对象：数据采集终端、数据导入服务组件、数据导出终端、数据导出服务组件等。
c） 测评实施包括以下内容：
1） 应核查相关终端和组件是否对使用主体实施基于口令和密码技术组合的身份鉴别；
2） 应测试验证口令和密码技术组合的身份鉴别措施是否有效，是否无法被绕过。
d） 单元判定：如果 1）-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。

6.3.1.3 测评单元（L3-CES-03）

该测评单元包括以下要求：
a） 测评指标：应对向大数据系统提供数据的外部实体实施身份鉴别。
b） 测评对象：大数据应用、大数据平台中提供外部数据接收功能的接口或服务组件。
c） 测评实施包括以下内容：
1） 应核查是否对向大数据系统提供数据的外部实体实施身份鉴别；
2） 应测试验证所采取的身份鉴别措施是否有效，是否无法被绕过。

d) 单元判定：如果 1）-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。

6.3.1.4 测评单元（L3-CES-04）

该测评单元包括以下要求：

a) 测评指标：大数据系统提供的各类外部调用接口应依据调用主体的操作权限实施相应强度的身份鉴别。
b) 测评对象：大数据应用、大数据平台中的外部调用接口。
c) 测评实施包括以下内容：
   1) 应核查大数据系统提供的各类外部调用接口是否对调用接口的主体划分操作权限，如分为读权限和写权限等；
   2) 应核查大数据系统提供的各类外部调用接口是否依据调用主体的不同操作权限，实施相应强度的身份鉴别，如对具备写权限的主体实施基于口令和密码技术组合的身份鉴别，对具备读权限的主体实施基于口令的身份鉴别等；
   3) 应测试验证身份鉴别措施是否有效，是否无法被绕过。
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。

6.3.2 访问控制

6.3.2.1 测评单元（L3-CES-05）

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，平台或第三方应在服务客户授权下才可以对其数据资源进行访问、使用和管理。
b) 测评对象：大数据管理平台、相关授权审批文档和数据安全保护相关管理制度文档。
c) 测评实施包括以下内容：
   1) 应核查对服务客户的数据资源进行访问、使用和管理时，是否具备必要的授权机制，包括授权流程、授权方式、授权内容等；
   2) 应核查大数据平台，平台或第三方是否具有服务客户数据资源的访问、使用和管理权限，如果具有，核查是否有相关授权证明。
d) 单元判定：如果 1）-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。

6.3.2.2 测评单元（L3-CES-06）

该测评单元包括以下要求：

a) 测评指标：大数据系统应提供数据分类分级标识功能。
b) 测评对象：大数据资源、大数据应用、大数据平台、系统设计及建设方案文档等。
c) 测评实施包括以下内容：
   1) 应核查系统设计及建设方案文档中是否具备数据分类分级标识的相关设计；
   2) 应核查大数据系统是否依据相关设计对数据进行分类分级标识；
   3) 应测试验证数据分级分类标识是否有效。
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，否则不符合本单元测评指标要求。

6.3.2.3 测评单元（L3-CES-07）

该测评单元包括以下要求：

a) 测评指标：应在数据采集、传输、存储、处理、交换及销毁等各个环节，根据数据分类分级标识对数据进行不同处置，最高等级数据的相关保护措施不低于第三级安全要求，安全保护策略在各环节保持一致。

b) 测评对象：大数据资源、大数据应用、大数据平台、系统管理软件及系统设计及建设方案文档等。

c) 测评实施包括以下内容：

1) 应核查系统设计及建设方案文档中是否具备数据分类分级保护策略及功能的相关设计；

2) 应核查在数据采集、传输、存储、处理、交换及销毁等各个环节，是否基于相关策略对数据进行不同处置；

3) 应核查最高等级数据的相关保护措施是否不低于第三级安全要求；

4) 应核查在数据采集、传输、存储、处理、交换及销毁等各个环节的安全保护策略强度是否一致。

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。

6.3.2.4 测评单元（L3-CES-08）

该测评单元包括以下要求：

a) 测评指标：大数据系统应对其提供的各类接口的调用实施访问控制，包括但不限于数据采集、处理、使用、分析、导出、共享、交换等相关操作。

b) 测评对象：大数据应用、大数据平台中的各类接口等。

c) 测评实施包括以下内容：

1) 应核查大数据系统是否对各类接口的调用提供访问控制措施，包括但不限于数据采集、处理、使用、分析、导出、共享、交换等相关操作；

2) 应测试验证调用接口的访问控制措施是否有效，是否无法被绕过。

d) 单元判定：如果 1）-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。

6.3.2.5 测评单元（L3-CES-09）

该测评单元包括以下要求：

a) 测评指标：应最小化各类接口操作权限。

b) 测评对象：大数据应用、大数据平台中的各类接口。

c) 测评实施：应核查各类接口的操作权限是否为其实现功能所需的最小权限。

d) 单元判定：如果以上测评实施为肯定，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。

6.3.2.6 测评单元（L3-CES-10）

该测评单元包括以下要求：

a) 测评指标：应最小化数据使用、分析、导出、共享、交换的数据集。

b) 测评对象：大数据资源、大数据应用、大数据平台、系统设计及建设方案文档等。

c) 测评实施包括以下内容：

1) 应核查系统设计及建设方案文档,是否遵循数据集最小化原则,包含但不限于数据的使用、分析、导出、共享、交换等过程;
2) 应核查在数据使用、分析、导出、共享、交换过程中是否不存在非必要的数据集。

d) 单元判定:如果 1)-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。

6.3.2.7 测评单元(L3-CES-11)

该测评单元包括以下要求:

a) 测评指标:大数据系统应提供隔离不同客户应用数据资源的能力。
b) 测评对象:大数据应用、大数据平台及系统设计及建设方案文档。
c) 测评实施包括以下内容:
1) 应核查系统设计及建设方案文档,是否具备隔离不同客户应用数据资源的功能设计;
2) 应核查不同客户应用数据资源之间是否已实现隔离措施;
3) 应测试验证不同客户应用数据资源的隔离措施是否有效。
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,否则不符合本单元测评指标要求。

6.3.2.8 测评单元(L3-CES-12)

该测评项单元包含以下要求:

a) 测评指标:应对重要数据的数据流转、泄露和滥用情况进行监控,及时对异常数据操作行为进行预警,并能够对突发的严重异常操作及时定位和阻断。
b) 测评对象:大数据平台中的数据防泄漏系统、数据监控系统或相关服务组件。
c) 测评实施包括以下内容:
1) 应核查是否对重要数据的数据流转、泄露和滥用情况进行监控;
2) 应核查是否对异常数据操作行为进行预警,如非授权导出、修改等操作;
3) 应核查是否能够对突发的严重异常操作及时定位和阻断,如非授权导出、修改、销毁等操作。
4) 应测试验证相关监控、预警、定位和阻断措施是否有效。
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。

6.3.3 安全审计

6.3.3.1 测评单元(L3-CES-13)

该测评项单元包含以下要求:

a) 测评指标:大数据系统应保证不同客户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:大数据管理平台和大数据应用系统等。
c) 测评实施包括以下内容:
1) 应核查大数据系统是否通过物理隔离或逻辑隔离方式对不同客户的审计数据进行隔离存放;
2) 应核查大数据系统是否提供集中审计功能,是否可对不同客户的审计数据进行收集汇总和集中分析。

d) 单元判定：如果 1)-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。

6.3.3.2 测评单元（L3-CES-14）

该测评项单元包含以下要求：

a) 测评指标：大数据系统应对其提供的各类接口的调用情况以及各类账号的操作情况进行审计。
b) 测评对象：大数据管理平台和大数据应用系统等。
c) 测评实施包括以下内容：
   1) 应核查大数据系统是否开启相关审计功能,审计功能工作是否正常,是否存在审计记录等；
   2) 应核查大数据系统的审计内容是否包括各类接口的调用情况和各类账号的操作情况。
d) 单元判定：如果 1)-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。

6.3.3.3 测评单元（L3-CES-15）

该测评项单元包含以下要求：

a) 测评指标：应保证大数据系统服务商对服务客户数据的操作可被服务客户审计。
b) 测评对象：大数据管理平台、大数据应用系统和服务组件等。
c) 测评实施：应核查是否能够保证大数据系统服务商对服务客户数据的操作（如增、删、改、查等操作）可被服务客户审计。
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。

6.3.4 入侵防范

6.3.4.1 测评单元（L3-CES-16）

该测评单元包括以下要求：

a) 测评指标：应对所有进入系统的数据进行检测，避免出现恶意数据输入。
b) 测评对象：系统设计及建设方案文档、大数据管理平台、大数据应用系统、数据采集终端和数据导入服务组件、具备数据检测/监测功能的设备或相关组件等。
c) 测评实施包括以下内容：
   1) 应核查系统设计及建设方案中是否具备对输入的数据进行检测以及恶意数据识别的措施；
   2) 应核查是否启用数据检测和恶意数据识别相关措施，是否配置相应检测和识别策略，检测和识别策略是否完善；
   3) 应测试验证输入数据的检测以及恶意数据识别是否有效。
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。

6.3.5 数据完整性

6.3.5.1 测评单元（L3-CES-17）

该测评单元包括以下要求：

a) 测评指标：应采用技术手段对数据交换过程进行数据完整性检测。
b) 测评对象：数据交换接口、数据共享接口、数据共享系统及系统共享软件等。
c) 测评实施包括以下内容：

1) 应核查数据在交换过程中是否采用技术手段进行数据完整性检测，如校验技术或密码技术等；
2) 应测试验证数据完整性校验措施是否有效。

d) 单元判定：如果 1）-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。

6.3.5.2 测评单元（L3-CES-18）

该测评单元包括以下要求：

a) 测评指标：数据在存储过程中的完整性保护应满足数据提供方系统的安全保护要求。
b) 测评对象：大数据应用系统、大数据管理平台、数据提供方合同及数据安全协议、系统定级备案材料、系统设计及建设方案文档等。
c) 测评实施包括以下内容：
1) 应核查系统设计及建设方案文档、数据提供方合同、数据安全协议以及系统定级备案材料，是否明确对数据存储过程的完整性保护需求；
2) 应核查存储完整性保护措施是否满足数据提供方的完整性保护需求；
3) 应测试验证数据存储完整性保护措施是否有效。
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。

6.3.6 数据保密性

6.3.6.1 测评单元（L3-CES-19）

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：大数据平台设计及建设方案文档、静态脱敏和去标识化工具或服务组件等。
c) 测评实施包括以下内容：
1) 应核查大数据平台系统设计及建设方案中是否提供数据静态脱敏和去标识化相关措施；
2) 应核查静态脱敏和去标识化工具或服务组件是否支持静态脱敏和去标识化相关策略配置；
3) 应测试验证静态脱敏和去标识化措施是否有效。
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。

6.3.6.2 测评单元（L3-CES-20）

该测评单元包括以下要求：

a) 测评指标：应依据相关安全策略和数据分类分级标识对数据进行静态脱敏和去标识化处理。
b) 测评对象：大数据管理平台、业务应用系统、数据管理系统和系统设计及建设方案文档等。
c) 测评实施包括以下内容：
1) 应核查系统设计及建设方案，是否明确了数据安全策略和数据分类分级标识，是否具有数据静态脱敏和去标识化相关需求；
2) 应核查是否依据相关数据安全策略和数据分类分级标识对数据进行静态脱敏和去标识化处理，包括但不限于业务数据、日志文件等；
3) 应测试验证静态脱敏和去标识化措施是否有效。
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。

6.3.6.3 测评单元（L3-CES-21）

该测评单元包括以下要求：

a) 测评指标：数据在存储过程中的保密性保护应满足数据提供方系统的安全保护要求。

b) 测评对象：大数据应用系统、大数据管理平台、数据提供方合同及数据安全协议、系统设计及建设方案文档和系统定级备案材料等。

c) 测评实施包括以下内容：

1) 应核查数据提供方合同、数据安全协议以及系统定级备案材料，明确对数据存储过程的保密性保护需求；

2) 应核查存储保密性保护措施是否满足数据提供方的保密性保护需求；

3) 应测试验证数据存储保密性保护措施是否有效。

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。

6.3.6.4 测评单元（L3-CES-22）

该测评单元包括以下要求：

a) 测评指标：应采取技术措施保证汇聚大量数据时不暴露敏感信息。

b) 测评对象：大数据管理平台、服务组件和系统设计及建设方案文档等。

c) 测评实施包括以下内容：

1) 应核查系统设计及建设方案文档，是否分析了汇聚大量数据可能暴露敏感信息的情况，若有相关情况，是否设计相关技术措施保证汇聚大量数据时不暴露敏感信息；

2) 应测试验证采用的技术措施是否有效。

d) 单元判定：如果 1）-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。

6.3.6.5 测评单元（L3-CES-23）

该测评单元包括以下要求：

a) 测评指标：可采用多方计算、同态加密等数据隐私计算技术实现数据共享的安全性。

b) 测评对象：大数据管理平台、业务应用系统、数据管理系统和系统设计及建设方案文档等。

c) 测评实施包括以下内容：

1) 应核查系统设计及建设方案文档，是否采取多方安全计算、同态加密、联邦学习等数据隐私计算技术实现数据共享的安全性；

2) 应测试验证是否有效使用多方安全计算、同态加密、联邦学习等数据隐私计算技术措施。

d) 单元判定：如果 1）-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。

6.3.7 数据备份与恢复

6.3.7.1 测评单元（L3-CES-24）

该测评单元包括以下要求：

a) 测评指标：备份数据应采取与原数据一致的安全保护措施。

b) 测评对象：配置数据和业务数据等备份数据。

c) 测评实施包括以下内容：

1) 应核查备份数据的安全保护措施是否与原数据一致，安全保护措施包括但不限于备份数据的访问控制、操作审计、存储保密性和存储完整性、传输保密性和传输完整性等保护措施；
2) 应测试验证备份数据相关保护措施的有效性是否与原数据保护措施一致。

d) 单元判定：如果 1）-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。

6.3.7.2 测评单元（L3-CES-25）

该测评单元包括以下要求：

a) 测评指标：大数据平台应保证用户数据存在若干个可用的副本，各副本之间的内容应保持一致。
b) 测评对象：大数据管理平台、存储系统及相关组件。
c) 测评实施包括以下内容：
1) 应核查大数据平台是否对用户数据进行多副本存储，是否存在若干个可用的副本；
2) 应测试验证各副本是否完整、可用，各副本内容是否一致。
d) 单元判定：如果 1）-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。

6.3.7.3 测评单元（L3-CES-26）

该测评单元包括以下要求：

a) 测评指标：应提供对关键溯源数据的异地备份。
b) 测评对象：大数据资源、大数据应用、大数据平台所关联的关键溯源数据。
c) 测评实施包括以下内容：
1) 应核查是否存在关键溯源数据；
2) 应核查关键溯源数据是否进行异地备份，备份策略和相关配置是否合理；
3) 应测试验证关键溯源数据备份措施是否有效。
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。

6.3.8 剩余信息保护

6.3.8.1 测评单元（L3-CES-27）

该测评单元包括以下要求：

a) 测评指标：大数据平台应提供主动迁移功能，数据整体迁移的过程中应杜绝数据残留。
b) 测评对象：系统设计及建设方案文档、数据迁移记录和相关配置等。
c) 测评实施包括以下内容：
1) 应核查大数据平台系统设计及建设方案中是否提供主动迁移功能，是否具备整体迁移过程杜绝数据残留相关措施；
2) 应核查主动迁移功能是否可用，包括相关配置项是否有效等；
3) 应核查整体迁移完成后是否采取技术措施对原存储空间进行完全清除，包括但不限于索引表删除、低级格式化、重写覆盖、消磁以及物理销毁等。
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。

6.3.8.2 测评单元（L3-CES-28）

该测评单元包括以下要求：

a) 测评指标：应基于数据分类分级保护策略，明确数据销毁要求和方式。
b) 测评对象：大数据资源、大数据应用、大数据平台所关联的数据分类分级保护制度和执行情况等。
c) 测评实施包括以下内容：
   1) 应核查是否具有数据分类分级保护策略，是否明确了不同级别和不同类型数据的销毁要求和销毁方式；
   2) 应核查数据销毁方式是否有效，销毁结果是否与相关保护策略要求一致。
d) 单元判定：如果 1）-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。

6.3.8.3 测评单元（L3-CES-29）

该测评单元包括以下要求：
a) 测评指标：大数据平台应能够根据服务客户提出的数据销毁要求和方式实施数据销毁。
b) 测评对象：系统设计及建设方案文档、相关操作记录等。
c) 测评实施包括以下内容：
   1) 应核查大数据平台系统设计及建设方案，是否支持多种数据销毁功能，包括但不限于索引表删除、低级格式化、重写覆盖、消磁以及物理销毁等；
   2) 应核查大数据平台是否提供渠道供服务客户提出数据销毁要求和方式，包括但不限于数据安全协议、服务协议、用户须知、权责声明、系统工单等；
   3) 应核查数据销毁记录是否与服务客户提出的要求和方式一致。
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。

6.3.9 个人信息保护

6.3.9.1 测评单元（L3-CES-30）

该测评单元包括以下要求：
a) 测评指标：采集、处理、使用、转让、共享、披露个人信息应在个人信息处理的授权同意范围内，并保留操作审计记录。
b) 测评对象：大数据平台、大数据应用、大数据资源所关联的个人信息数据。
c) 测评实施包括以下内容：
   1) 应核查是否明确个人信息处理的授权同意范围，包括但不限于知悉范围、留存期限、流转路径等；
   2) 应核查采集、处理、使用、转让、共享、披露个人信息是否未超出个人信息处理的授权同意范围；
   3) 应核查采集、处理、使用、转让、共享、披露个人信息是否保留审计记录，审计记录内容是否符合国家法律法规对于个人信息安全审计的相关要求。
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。

6.3.9.2 测评单元（L3-CES-31）

该测评单元包括以下要求：
a) 测评指标：应采取措施防止在数据处理、使用、分析、导出、共享、交换等过程中识别出个人身份信息。

b) 测评对象：大数据平台、大数据应用、大数据资源所关联的系统设计及建设方案文档等。
c) 测评实施包括以下内容：
   1) 应核查系统设计及建设方案文档，是否在数据处理、使用、分析、导出、共享、交换等过程中具备相关措施防止个人身份信息被识别，包括但不限于脱敏、匿名、泛化、去标识化等；
   2) 应测试验证所使用的措施是否有效。
d) 单元判定：如果 1）-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。

6.3.9.3 测评单元（L3-CES-32）

该测评单元包括以下要求：
a) 测评指标：对个人信息的重要操作应设置内部审批流程,审批通过后才能对个人信息进行相应的操作。
b) 测评对象：大数据平台、大数据应用、大数据资源所关联的系统设计及建设方案文档和安全策略文档等。
c) 测评实施包括以下内容：
   1) 应核查系统设计及建设方案和安全策略文档是否明确了对个人信息的重要操作的内部审批流程，包括但不限于批量导出、修改、销毁、备份、恢复等；
   2) 应访谈管理人员，了解审批通过是否为实施重要操作的必备前置条件。
d) 单元判定：如果 1）-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。

6.3.9.4 测评单元（L3-CES-33）

该测评单元包括以下要求：
a) 测评指标：保存个人信息的时间应满足最小化要求，并能够对超出保存期限的个人信息进行删除或匿名化处理。
b) 测评对象：大数据平台、大数据应用、大数据资源所关联的安全管理相关文档和记录。
c) 测评实施包括以下内容：
   1) 应核查安全管理相关文档，是否根据法律法规、行业标准和单位实际情况确定个人信息的保存时间要求；
   2) 应核查是否存在对超出保存期限的个人信息进行删除或匿名化处理的相关配置或操作记录；
   3) 应测试验证个人信息删除或匿名化处理是否有效。
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。

6.3.10 数据溯源

6.3.10.1 测评单元（L3-CES-34）

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。
b) 测评对象：大数据平台、大数据应用、大数据资源所关联的溯源数据、系统设计及建设方案文档等；
c) 测评实施包括以下内容：

1） 应核查系统设计及建设方案是否具有跟踪和记录数据采集、处理、分析和挖掘等过程相关措施；
2） 应核查是否启用跟踪和记录数据采集、处理、分析和挖掘等过程的相关措施，是否保留溯源数据；
3） 应测试验证是否能够基于溯源数据重现相应过程。

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。

6.3.10.2 测评单元（L3-CES-35）

该测评单元包括以下要求：

a） 测评指标：溯源数据应满足数据业务要求和合规审计要求；
b） 测评对象：大数据平台、大数据应用、大数据资源所关联的溯源数据、系统设计及建设方案文档等。
c） 测评实施包括以下内容：
1） 应核查系统设计及建设方案及相关安全管理制度，是否明确了溯源数据的数据业务要求和合规审计要求。
2） 应核查所记录的溯源数据是否满足数据业务要求；
3） 应核查所记录的溯源数据是否满足法律法规、部门规章、组织内部合规等的合规审计要求。
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。

6.3.10.3 测评单元（L3-CES-36）

该测评单元包括以下要求：

a） 测评指标：应采取技术手段保证数据源的真实可信；
b） 测评对象：大数据应用、大数据资源、大数据平台的数据平台层、计算分析层以及大数据管理平台等模块及系统设计及建设方案文档等。
c） 测评实施包括以下内容：
1） 应核查外部数据导入时是否采用数字签名等技术手段保证数据源的真实可信；
2） 应测试验证所使用的技术手段是否有效。
d） 单元判定：如果 1）-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。

6.4 安全管理中心

6.4.1 系统管理

6.4.1.1 测评单元（L3-SMC-01）

该测评单元包括以下要求：

a） 测评指标：大数据平台应为服务客户提供管理其计算和存储资源使用状况的能力。
b） 测评对象：大数据管理平台。
c） 测评实施包括以下内容：
1） 应核查大数据平台是否为服务客户提供管理其计算和存储资源使用状况的能力，包括但不限于查询、监控、申请变更等；
2） 应测试验证提供给客户的管理功能是否有效，是否不存在无法管理的情况。

d) 单元判定：如果 1）-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。

6.4.1.2 测评单元（L3-SMC-02）

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、服务组件和大数据管理平台等。
c) 测评实施包括以下内容：
   1) 应核查大数据管理平台是否具备对其提供的辅助工具或服务组件进行管理的能力，包括但不限于辅助工具或服务组件的安装、部署、监控、优化、升级、卸载、身份鉴别、访问权限管理、操作审计等；
   2) 应测试验证大数据平台提供的辅助工具或服务组件的安全管理措施是否有效，是否不存在无法管理的情况。
d) 单元判定：如果 1）-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。

6.4.1.3 测评单元（L3-SMC-03）

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：系统设计及建设方案文档、计算分析层相关节点等。
c) 测评实施包括以下内容：
   1) 应核查是否具备屏蔽计算、内存、存储资源故障的措施和技术手段，相关措施是否正常运行；
   2) 应测试验证相关措施的有效性，是否不存在部分计算节点或存储节点故障时，业务无法正常运行的情况。
d) 单元判定：如果 1）-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。

6.4.1.4 测评单元（L3-SMC-04）

该测评单元包括以下要求：

a) 测评指标：大数据平台在系统维护、在线扩容等情况下，应保证大数据应用和大数据资源的正常业务处理能力。
b) 测评对象：大数据管理平台、系统维护及扩容测试记录等文档。
c) 测评实施包括以下内容：
   1) 应核查大数据平台在系统维护、在线扩容等情况下，是否采取技术手段保证大数据应用和大数据资源的正常业务处理能力；
   2) 应测试验证所采取的技术手段是否有效，是否不存在部分大数据应用和大数据资源的正常业务处理无法开展的情况。
d) 单元判定：如果 1）-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。

6.4.2 集中管控

6.4.2.1 测评单元（L3-SMC-05）

测评单元包括以下要求：

a) 测评指标：应对大数据系统提供的各类接口的使用情况进行集中审计和监测，并在发生问题时提供报警。
b) 测评对象：大数据系统集中审计功能模块。
c) 测评实施包括以下内容：
   1) 应核查是否能够对各类接口的使用进行集中审计和监测；
   2) 应核查是否保存有至少 6 个月的审计数据和监测数据；
   3) 应核查是否能够在接口使用异常的情况下进行报警。
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。

6.5 安全管理制度

6.5.1 安全策略

6.5.1.1 测评单元（L3-PSS-01）

该测评单元包括以下要求：

a) 测评指标:应制定大数据安全工作的总体方针和安全策略,阐明本机构大数据安全工作的目标、范围、原则和安全框架等相关内容。
b) 测评对象：大数据安全工作的总体方针、安全策略类文档。
c) 测评实施包括以下内容：
   1) 应访谈并核查是否具有大数据安全工作的总体方针和安全策略相关文档；
   2) 应核查相关文档中是否明确机构大数据安全工作的总体目标、范围、原则和安全框架等相关内容。
d) 单元判定：如果 1）-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。

6.5.1.2 测评单元（L3-PSS-02）

该测评单元包括以下要求：

a) 测评指标：大数据安全策略应覆盖数据生命周期相关的数据安全，内容至少包括目的、范围、岗位、责任、管理层承诺、内外部协调及合规性要求等。
b) 测评对象：安全策略类文档。
c) 测评实施包括以下内容：
   1) 应访谈并核查是否具有大数据安全策略相关文档；
   2) 应核查大数据安全策略文档内容是否覆盖数据生命周期相关的数据安全，至少包含目的、范围、岗位、责任、管理层承诺、内外部协调及合规性要求等。
d) 单元判定：如果 1）-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。

6.6 安全管理机构

6.6.1 授权和审批

6.6.1.1 测评单元（L3-ORS-01）

该测评单元包括以下要求：

a) 测评指标：数据的采集应获得数据源管理者的授权，确保符合数据收集最小化原则。
b) 测评对象：数据源管理者、数据安全保护相关管理制度文档及记录表单类文档等。
c) 测评实施包括以下内容：
   1) 应访谈数据源管理者并核查相关制度，是否要求对数据的采集需获得授权，是否遵循最小化授权原则；
   2) 应核查是否具有数据采集相关的授权记录，授权内容是否符合数据收集最小化原则，是否与相关制度要求一致。
d) 单元判定：如果 1）-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。

6.6.1.2 测评单元（L3-ORS-02）

该测评单元包括以下要求：
a) 测评指标：应建立数据导入、导出、集成、分析、交换、交易、共享及公开的授权审批控制流程，赋予数据活动主体的最小操作权限、最小数据集和权限有效时长，依据流程实施相关控制并记录过程，及时回收过期的数据访问权限。
b) 测评对象：数据安全保护相关管理制度文档及记录表单类文档等。
c) 测评实施包括以下内容：
   1) 应核查管理制度类文档是否明确数据的导入、导出、集成、分析、交换、交易、共享及公开的授权审批流程；
   2) 应核查管理制度类文档是否明确过期的数据访问权限回收流程及方式方法等，审批内容是否涵盖数据活动主体的最小操作权限、最小数据集和权限有效时长；
   3) 应核查是否具有相关控制记录，记录内容是否与数据安全保护相关管理制度要求一致。
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。

6.6.1.3 测评单元（L3-ORS-03）

该测评单元包括以下要求：
a) 测评指标：应建立跨境数据的评估、审批及监管控制流程，并依据流程实施相关控制并记录过程。
b) 测评对象：数据安全保护相关管理制度文档和记录表单类文档等。
c) 测评实施包括以下内容：
   1) 应核查数据安全保护相关管理制度中是否明确跨境数据的评估、审批及监管控制流程；
   2) 应核查是否具有相关控制的记录，记录内容是否与数据安全保护相关管理制度要求一致；
   3) 应核查数据出境是否符合国家相关部门的有关管理规定。
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。

6.6.2 审核和检查

6.6.2.1 测评单元（L3-ORS-04）

该测评单元包括以下要求：
a) 测评指标：应定期对个人信息安全保护措施的有效性进行常规安全检查。
b) 测评对象：信息/网络安全主管、数据安全保护相关管理制度文档等。
c) 测评实施包括以下内容：

1） 应访谈信息/网络安全主管并核查数据安全保护相关管理制度，是否对个人信息安全保护措施的有效性进行常规安全检查；
2） 应核查是否具有常规安全检查相关记录，检查内容是否覆盖个人信息安全保护措施的有效性检查，检查频率、检查方法以及检查内容等是否与管理制度要求一致，记录内容是否详尽。

d） 单元判定：如果1）-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。

6.7 安全建设管理

6.7.1 服务供应商选择

6.7.1.1 测评单元（L3-CMS-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和大数据资源提供相应等级的安全保护能力。
b） 测评对象：安全策略类文档、数据安全保护相关管理制度文档和大数据平台定级备案材料、等级测评报告等。
c） 测评实施包括以下内容：
1） 应访谈系统建设负责人并核查相关制度，是否根据业务系统的安全保护等级选择具有相应等级安全保护能力的大数据平台；
2） 应核查大数据平台和大数据应用、大数据资源的定级备案材料，大数据平台是否与所承载的大数据应用和大数据资源具有相应或高于的安全保护能力；
3） 应核查所使用的大数据平台的网络安全等级保护测评报告，报告时间和报告结论是否符合网络安全等级保护相关要求。
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。

6.7.1.2 测评单元（L3-CMS-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和大数据平台使用者的权限与责任、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：供应商服务协议及数据安全协议等。
c） 测评实施包括以下内容：
1） 应核查供应商服务协议、数据安全协议以及用户须知等相关材料，是否明确了大数据服务提供者和使用者的权限与责任，核查内容是否覆盖大数据服务内容、安全服务内容，是否明确服务范围、服务指标、职责划分、访问授权、隐私保护、行为准则、违约责任等；
2） 应核查大数据平台供应商服务协议、数据安全协议以及用户须知等相关材料是否有效，是否具有双方签字及盖章，是否处于有效期内等。
d） 单元判定：如果1）-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。

6.7.2 供应链管理

6.7.2.1 测评单元（L3-CMS-03）

该测评单元包括以下要求：

a) 测评指标：应确保供应商的选择符合国家有关规定。

b) 测评对象：建设负责人。

c) 测评实施包括以下内容：

1) 应访谈系统建设负责人并核查相关材料，供应商的选择过程是否符合国家有关规定，包括但不限于招投标流程、合同签约流程、价款支付方式等；

2) 应访谈系统建设负责人并核查相关材料，供应商的选择结果是否符合国家有关规定，包括但不限于供应商的建设服务资质、安全服务资质、集成服务资质、密码服务资质以及产品销售许可等。

d) 单元判定：如果 1）-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。

6.7.2.2 测评单元（L3-CMS-04）

该测评单元包括以下要求：

a) 测评指标：应以书面方式约定数据交换、共享的接收方对数据的保护责任，并明确数据安全保护要求。

b) 测评对象：供应商服务协议及数据安全协议等。

c) 测评实施包括以下内容：

1) 应核查供应商服务协议及数据安全协议中是否建立数据交换、共享的数据保护责任要求，明确数据保护范围、保护内容、数据类型、数据分级分类保护等级及对不同等级数据的保护要求等内容；

2) 应核查合同或协议是否有双方签字或盖章，是否处于有效期内等。

d) 单元判定：如果 1）-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。

6.7.2.3 测评单元（L3-CMS-05）

该测评单元包括以下要求：

a) 测评指标：应将供应链安全事件信息或安全威胁信息及时传达到数据交换、共享的接收方。

b) 测评对象：供应链安全事件记录和供应商服务协议及数据安全协议等。

c) 测评实施：

1) 应核查供应链安全事件报告或威胁报告是否及时传达到数据交换、共享的接收方；

2) 应核查安全事件报告或威胁报告是否明确相关事件信息或威胁信息。

d) 单元判定：如果 1）-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。

6.7.3 数据源管理

6.7.3.1 测评单元（L3-CMS-06）

该测评单元包括以下要求：

a) 测评指标：应通过合法正当的渠道获取各类数据。

b) 测评对象：供应商服务协议、数据安全协议及记录表单类文档等。

c) 测评实施包括以下内容：

1) 应对照获取的数据类核查供应商服务协议及数据安全协议，是否均通过合法正当的渠道获取各类数据；

2) 如果获取的渠道数据用于提供大数据平台服务，应核查相关系统、合同或协议等是否对渠道进行了明示。

d) 单元判定：如果 1）-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。

6.8 安全运维管理

6.8.1 资产管理

6.8.1.1 测评单元（L3-MMS-01）

该测评单元包括以下要求：

a) 测评指标：应建立数据资产安全管理策略，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，包括但不限于数据采集、传输、存储、处理、交换、销毁等过程。

b) 测评对象：数据资产安全管理策略、操作记录及提供数据保护的相关产品或组件。

c) 测评实施包括以下内容：

1) 应访谈并核查是否建立数据资产安全管理策略，策略是否明确各类数据全生命周期的操作规范、保护措施、管理人员职责，包括但不限于数据采集、传输、存储、处理、交换、销毁等过程；

2) 应核查数据采集、传输、存储、处理、交换、销毁等过程中的数据保护措施和相关记录是否与数据资产安全管理策略一致。

d) 单元判定：如果 1）-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。

6.8.1.2 测评单元（L3-MMS-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相应强度的安全保护要求。

b) 测评对象：数据分类分级保护策略、操作记录及提供数据分类分级标记和保护的相关产品或组件。

c) 测评实施包括以下内容：

1) 应访谈并核查是否制定数据分类分级保护策略，数据分类分级保护策略是否明确了数据分类分级方法和依据、是否为不同类别级别的数据制定相应强度的安全保护要求；

2) 应核查数据分类分级保护策略是否已覆盖大数据系统重要数据，包括但不限于重要业务数据、标识数据、密钥数据、审计数据、溯源数据、脱敏数据、个人数据、配置数据、备份数据等；

3) 应核查数据保护相关记录，是否与分类分级保护策略要求一致。

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。

6.8.1.3 测评单元（L3-MMS-03）

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，如需要变更数据所属类别或级别，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。

6.8.1.4 测评单元（L3-MMS-04）

该测评单元包括以下要求：
a) 测评指标：应对数据资产和对外数据接口进行登记管理，建立相应的资产清单。
b) 测评对象：数据资产清单、对外数据接口清单。
c) 测评实施：
   1) 应访谈管理员是否定期对数据资产和对外接口进行梳理和登记，是否形成数据资产清单和对外接口清单；
   2) 应核查数据资产清单是否全面，是否覆盖重要数据，包括但不限于业务数据、标识数据、密钥数据、审计数据、溯源数据、脱敏数据、个人数据、配置数据、备份数据等；
   3) 应核查对外数据接口清单是否全面，是否覆盖所有重要接口，包括但不限于数据采集、数据交换、数据共享、API 应用等接口。
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。

6.8.2 介质管理

6.8.2.1 测评单元（L3-MMS-05）

该测评单元包括以下要求：
a) 测评指标：应在中国境内对数据进行清除或销毁。
b) 测评对象：数据管理员及数据清除、销毁过程记录。
c) 测评实施包括以下内容：
   1) 应访谈数据管理员，数据清除或销毁是否在中国境内开展；
   2) 应核查数据清除、销毁相关记录，是否依据要求在中国境内对数据进行清除或销毁。
d) 单元判定：如果 1）-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。

6.8.2.2 测评单元（L3-MMS-06）

该测评单元包括以下要求：
a) 测评指标：对存储重要数据的存储介质或物理设备应采取难恢复的技术手段，如物理粉碎、消磁、多次擦写等。
b) 测评对象：数据管理员、数据销毁执行记录。
c) 测评实施包括以下内容：
   1) 应访谈数据管理员，对存储重要数据的存储介质或物理设备在停用后是否采取如物理粉碎、消磁、多次擦写等技术处理手段进行数据销毁；

2) 应核查存储重要数据的存储介质或物理设备在停用后的数据销毁执行记录，记录内容是否包括被销毁对象原用途、容量、销毁方式、销毁时间、销毁实施人员等信息，销毁方式是否难以恢复。

d) 单元判定：如果 1）-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。

6.8.3 网络和系统安全管理

6.8.3.1 测评单元（L3-MMS-07）

该测评单元包括以下要求：

a) 测评指标：应建立对外数据接口安全管理机制，所有的接口调用均应获得授权和批准。

b) 测评对象：安全策略类文档、数据安全保护相关管理制度文档、授权审计记录、大数据系统审计模块等。

c) 测评实施包括以下内容：

1) 应访谈安全管理人员并核查相关管理制度，是否建立大数据网络和系统安全管理机制，是否要求所有的接口调用均应获得授权和批准；

2) 应核查相关授权和审批记录，记录内容是否全面，授权和审批过程是否合规，是否与管理制度要求一致。

d) 单元判定：如果 1）-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。

7 第四级安全测评要求

7.1 安全物理环境

7.1.1 基础设施位置

7.1.1.1 测评单元（L4-PES-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：物理机房、机房管理员。

c) 测评实施：应核查大数据相关的管理系统、业务系统以及数据资源所在的存储节点、处理节点、分析节点等的软硬件设备所在的物理机房是否均位于中国境内。

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。

7.2 安全通信网络

7.2.1 网络架构

7.2.1.1 测评单元（L4-CNS-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和大数据资源。

b) 测评对象：大数据平台、大数据应用、大数据资源及业务应用系统的定级备案材料，服务协议、用户须知等其他材料。

c) 测评实施包括以下内容：
   1) 应访谈管理人员并核查大数据平台的服务协议、用户须知等相关材料，其中是否明确告知用户，大数据平台不承载高于其安全保护等级的大数据应用和大数据资源；
   2) 应访谈管理人员并核查大数据平台及其所承载的大数据应用系统、大数据资源的相关定级备案材料，大数据平台安全保护等级是否不低于其承载的大数据应用和大数据资源的安全保护等级。
d) 单元判定：如果 1）-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。

7.2.1.2 测评单元（L4-CNS-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：大数据平台基础设施层的网络架构。
c) 测评实施包括以下内容：
   1) 应核查大数据平台基础设施层的网络架构、策略配置或相关组件，是否采用带外管理等方式实现管理流量与系统业务流量分离；
   2) 应测试验证大数据平台的管理流量与系统业务流量是否分离。
d) 单元判定：如果 1）-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。

7.2.1.3 测评单元（L4-CNS-03）

该测评单元包括以下要求：
a) 测评指标：应提供开放接口或开放性安全服务，允许客户接入第三方安全产品或在大数据平台选择第三方安全服务。
b) 测评对象：大数据平台设计及建设方案文档、开放接口或提供开放性安全服务的组件。
c) 测评实施包括以下内容：
   1) 应核查接口设计文档或开放性服务技术文档是否提供开放接口以及是否允许接入第三方安全产品或服务；
   2) 应核查大数据平台服务客户是否可以接入第三方安全产品或在大数据平台选择第三方安全服务。
d) 单元判定：如果 1）-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。

7.3 安全计算环境

7.3.1 身份鉴别

7.3.1.1 测评单元（L4-CES-01）

该测评单元包括以下要求：
a) 测评指标：大数据平台应提供双向认证功能，能对不同客户的大数据应用、大数据资源进行双向身份鉴别。
b) 测评对象：大数据平台设计及建设方案文档、大数据平台等。
c) 测评实施包括以下内容：
   1) 应核查大数据平台设计及建设方案文档中是否具备双向身份认证功能设计；

2） 应核查大数据平台是否能对不同客户的大数据应用、大数据资源进行双向身份认证；
3） 应测试验证双向身份认证功能是否有效，是否无法被绕过。

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。

7.3.1.2 测评单元（L4-CES-02）

该测评单元包括以下要求：

a） 测评指标：应采用口令和密码技术组合的鉴别技术对使用数据采集终端、数据导入服务组件、数据导出终端、数据导出服务组件的主体实施身份鉴别。
b） 测评对象：数据采集终端、数据导入服务组件、数据导出终端、数据导出服务组件等。
c） 测评实施包括以下内容：
1） 应核查相关终端和组件是否对使用主体实施基于口令和密码技术组合的身份鉴别；
2） 应测试验证口令和密码技术组合的身份鉴别措施是否有效，是否无法被绕过。
d） 单元判定：如果 1）-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。

7.3.1.3 测评单元（L4-CES-03）

该测评单元包括以下要求：

a） 测评指标：应对向大数据系统提供数据的外部实体实施身份鉴别。
b） 测评对象：大数据应用、大数据平台中提供外部数据接收功能的接口或服务组件。
c） 测评实施包括以下内容：
1） 应核查是否对向大数据系统提供数据的外部实体实施身份鉴别；
2） 应测试验证所采取的身份鉴别措施是否有效，是否无法被绕过。
d） 单元判定：如果 1）-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。

7.3.1.4 测评单元（L4-CES-04）

该测评单元包括以下要求：

a） 测评指标:大数据系统提供的各类外部调用接口应依据调用主体的操作权限实施相应强度的身份鉴别。
b） 测评对象：大数据应用、大数据平台中的外部调用接口。
c） 测评实施包括以下内容：
1） 应核查大数据系统提供的各类外部调用接口是否对调用接口的主体划分操作权限,如分为读权限和写权限等；
2） 应核查大数据系统提供的各类外部调用接口是否依据调用主体的不同操作权限,实施相应强度的身份鉴别，如对具备写权限的主体实施基于口令和密码技术组合的身份鉴别，对具备读权限的主体实施基于口令的身份鉴别等；
3） 应测试验证身份鉴别措施是否有效，是否无法被绕过。
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。

7.3.2 访问控制

7.3.2.1 测评单元（L4-CES-05）

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，平台或第三方应在服务客户授权下才可以对其数据资源进行访问、使用和管理。

b) 测评对象：大数据管理平台、相关授权审批文档和数据安全保护相关管理制度文档。

c) 测评实施包括以下内容：

1) 应核查对服务客户的数据资源进行访问、使用和管理时，是否具备必要的授权机制，包括授权流程、授权方式、授权内容等；

2) 应核查大数据平台，平台或第三方是否具有服务客户数据资源的访问、使用和管理权限，如果具有，核查是否有相关授权证明。

d) 单元判定：如果 1）-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。

7.3.2.2 测评单元（L4-CES-06）

该测评单元包括以下要求：

a) 测评指标：大数据系统应提供数据分类分级标识功能。

b) 测评对象：大数据资源、大数据应用、大数据平台、系统设计及建设方案文档等。

c) 测评实施包括以下内容：

1) 应核查系统设计及建设方案文档中是否具备数据分类分级标识的相关设计；

2) 应核查大数据系统是否依据相关设计对数据进行分类分级标识；

3) 应测试验证数据分级分类标识是否有效。

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，否则不符合本单元测评指标要求。

7.3.2.3 测评单元（L4-CES-07）

该测评单元包括以下要求：

a) 测评指标：应在数据采集、传输、存储、处理、交换及销毁等各个环节，支持对数据进行分类分级处置，最高等级数据的相关保护措施不低于第四级安全要求，安全保护策略在各环节保持一致。

b) 测评对象：大数据资源、大数据应用、大数据平台、系统管理软件及系统设计及建设方案文档等。

c) 测评实施包括以下内容：

1) 应核查系统设计及建设方案文档中是否具备数据分类分级保护策略及功能的相关设计；

2) 应核查在数据采集、传输、存储、处理、交换及销毁等各个环节，是否基于相关策略对数据进行不同处置；

3) 应核查最高等级数据的相关保护措施是否不低于第四级安全要求；

4) 应核查在数据采集、传输、存储、处理、交换及销毁等各个环节的安全保护策略强度是否一致。

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。

7.3.2.4 测评单元（L4-CES-08）

该测评单元包括以下要求：

a) 测评指标：大数据系统应具备设置数据安全标记功能，并基于安全标记进行访问控制。

b） 测评对象：大数据资源、大数据应用、大数据平台、系统设计及建设方案文档等。
c） 测评实施包括以下内容：
1） 应核查系统设计及建设方案文档中是否具备设置数据安全标记的功能设计；
2） 应核查大数据系统是否对数据设置了安全标记；
3） 应核查大数据系统是否基于设置的安全标记进行访问控制；
4） 应测试验证基于安全标记的访问控制措施是否有效，是否无法被绕过。
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。

7.3.2.5 测评单元（L4-CES-09）

该测评单元包括以下要求：
a） 测评指标：大数据系统应对其提供的各类接口的调用实施访问控制，包括但不限于数据采集、处理、使用、分析、导出、共享、交换等相关操作。
b） 测评对象：大数据应用、大数据平台中的各类接口等。
c） 测评实施包括以下内容：
1） 应核查大数据系统是否对各类接口的调用提供访问控制措施，包括但不限于数据采集、处理、使用、分析、导出、共享、交换等相关操作；
2） 应测试验证调用接口的访问控制措施是否有效，是否无法被绕过。
d） 单元判定：如果 1）-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。

7.3.2.6 测评单元（L4-CES-10）

该测评单元包括以下要求：
a） 测评指标：应最小化各类接口操作权限。
b） 测评对象：大数据应用、大数据平台中的各类接口。
c） 测评实施：应核查各类接口的操作权限是否为其实现功能所需的最小权限。
d） 单元判定：如果以上测评实施为肯定，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。

7.3.2.7 测评单元（L4-CES-11）

该测评单元包括以下要求：
a） 测评指标：应最小化数据使用、分析、导出、共享、交换的数据集。
b） 测评对象：大数据资源、大数据应用、大数据平台、系统设计及建设方案文档等。
c） 测评实施包括以下内容：
1） 应核查系统设计及建设方案文档,是否遵循数据集最小化原则,包含但不限于数据的使用、分析、导出、共享、交换等过程；
2） 应核查在数据使用、分析、导出、共享、交换过程中是否不存在非必要的数据集。
d） 单元判定：如果 1）-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。

7.3.2.8 测评单元（L4-CES-12）

该测评单元包括以下要求：
a） 测评指标：大数据系统应提供隔离不同客户应用数据资源的能力。

b) 测评对象：大数据应用、大数据平台及系统设计及建设方案文档。
c) 测评实施包括以下内容：
   1) 应核查系统设计及建设方案文档，是否具备隔离不同客户应用数据资源的功能设计；
   2) 应核查不同客户应用数据资源之间是否已实现隔离措施；
   3) 应测试验证不同客户应用数据资源的隔离措施是否有效。
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，否则不符合本单元测评指标要求。

7.3.2.9 测评单元（L4-CES-13）

该测评单元包括以下要求：
a) 测评指标：应采用技术手段限制在终端输出重要数据。
b) 测评对象：大数据资源、大数据应用、大数据平台、系统设计及建设方案文档等。
c) 测评实施包括以下内容：
   1) 应核查系统设计及建设方案文档中是否具备限制在终端输出重要数据的技术手段，包括但不限于身份鉴别、权限校验、操作审计、添加水印等；
   2) 应核查是否使用相关技术手段限制在终端输出重要数据；
   3) 应测试验证限制在终端输出重要数据的技术手段是否有效。
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，否则不符合本单元测评指标要求。

7.3.2.10 测评单元（L4-CES-14）

该测评项单元包含以下要求：
a) 测评指标：应对重要数据的数据流转、泄露和滥用情况进行监控，及时对异常数据操作行为进行预警，并能够对突发的严重异常操作及时定位和阻断。
b) 测评对象：大数据平台中的数据防泄漏系统、数据监控系统或相关服务组件。
c) 测评实施包括以下内容：
   1) 应核查是否对重要数据的数据流转、泄露和滥用情况进行监控；
   2) 应核查是否对异常数据操作行为进行预警，如非授权导出、修改等操作；
   3) 应核查是否能够对突发的严重异常操作及时定位和阻断，如非授权导出、修改、销毁等操作。
   4) 应测试验证相关监控、预警、定位和阻断措施是否有效。
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。

7.3.3 安全审计

7.3.3.1 测评单元（L4-CES-15）

该测评项单元包含以下要求：
a) 测评指标：大数据系统应保证不同客户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：大数据管理平台、大数据应用系统和服务组件等。
c) 测评实施包括以下内容：
   1) 应核查大数据系统是否通过物理隔离或逻辑隔离方式对不同客户的审计数据进行隔离存放；

2） 应核查大数据系统是否提供集中审计功能，是否可对不同客户的审计数据进行收集汇总和集中分析。

d） 单元判定：如果 1)-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。

7.3.3.2 测评单元（L4-CES-16）

该测评项单元包含以下要求：

a） 测评指标：大数据系统应对其提供的各类接口的调用情况以及各类账号的操作情况进行审计。

b） 测评对象：大数据管理平台和大数据应用系统等。

c） 测评实施包括以下内容：

1） 应核查大数据系统是否开启相关审计功能，审计功能工作是否正常，是否存在审计记录等；

2） 应核查大数据系统的审计内容是否包括各类接口的调用情况和各类账号的操作情况。

d） 单元判定：如果 1)-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。

7.3.3.3 测评单元（L4-CES-17）

该测评项单元包含以下要求：

a） 测评指标：应保证大数据系统服务商对服务客户数据的操作可被服务客户审计。

b） 测评对象：大数据管理平台、大数据应用系统和服务组件等。

c） 测评实施：应核查是否能够保证大数据系统服务商对服务客户数据的操作（如增、删、改、查等操作）可被服务客户审计。

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。

7.3.4 入侵防范

7.3.4.1 测评单元（L4-CES-18）

该测评单元包括以下要求：

a） 测评指标：应对所有进入系统的数据进行检测，避免出现恶意数据输入。

b） 测评对象：系统设计及建设方案文档、大数据管理平台、大数据应用系统、数据采集终端和数据导入服务组件、具备数据检测/监测功能的设备或相关组件等。

c） 测评实施包括以下内容：

1） 应核查系统设计及建设方案中是否具备对输入的数据进行检测以及恶意数据识别的措施；

2） 应核查是否启用数据检测和恶意数据识别相关措施，是否配置相应检测和识别策略，检测和识别策略是否完善；

3） 应测试验证输入数据的检测以及恶意数据识别是否有效。

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。

7.3.5 数据完整性

7.3.5.1 测评单元（L4-CES-19）

该测评单元包括以下要求：

a） 测评指标：应采用技术手段对数据交换过程进行数据完整性检测。

b) 测评对象：数据交换接口、数据共享接口、数据共享系统及系统共享软件等。
c) 测评实施包括以下内容：
   1) 应核查数据在交换过程中是否采用技术手段进行数据完整性检测，如校验技术或密码技术等；
   2) 应测试验证数据完整性校验措施是否有效。
d) 单元判定：如果 1）-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。

7.3.5.2 测评单元（L4-CES-20）

该测评单元包括以下要求：
a) 测评指标：数据在存储过程中的完整性保护应满足数据提供方系统的安全保护要求。
b) 测评对象：大数据应用系统、大数据管理平台、数据提供方合同及数据安全协议、系统定级备案材料、系统设计及建设方案文档等。
c) 测评实施包括以下内容：
   1) 应核查系统设计及建设方案文档、数据提供方合同、数据安全协议以及系统定级备案材料，是否明确对数据存储过程的完整性保护需求；
   2) 应核查存储完整性保护措施是否满足数据提供方的完整性保护需求；
   3) 应测试验证数据存储完整性保护措施是否有效。
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。

7.3.6 数据保密性

7.3.6.1 测评单元（L4-CES-21）

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：大数据平台设计及建设方案文档、静态脱敏和去标识化工具或服务组件等。
c) 测评实施包括以下内容：
   1) 应核查大数据平台系统设计及建设方案中是否提供数据静态脱敏和去标识化相关措施；
   2) 应核查静态脱敏和去标识化工具或服务组件是否支持静态脱敏和去标识化相关策略配置；
   3) 应测试验证静态脱敏和去标识化措施是否有效。
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。

7.3.6.2 测评单元（L4-CES-22）

该测评单元包括以下要求：
a) 测评指标：应依据相关安全策略和数据分类分级标识对数据进行静态脱敏和去标识化处理。
b) 测评对象：大数据管理平台、业务应用系统、数据管理系统和系统设计及建设方案文档等。
c) 测评实施包括以下内容：
   1) 应核查系统设计及建设方案，是否明确了数据安全策略和数据分类分级标识，是否具有数据静态脱敏和去标识化相关需求；
   2) 应核查是否依据相关数据安全策略和数据分类分级标识对数据进行静态脱敏和去标识化处理，包括但不限于业务数据、日志文件等；
   3) 应测试验证静态脱敏和去标识化措施是否有效。

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。

7.3.6.3 测评单元（L4-CES-23）

该测评单元包括以下要求：

a) 测评指标：数据在存储过程中的保密性保护应满足数据提供方系统的安全保护要求。
b) 测评对象：大数据应用系统、大数据管理平台、数据提供方合同及数据安全协议、系统设计及建设方案文档和系统定级备案材料等。
c) 测评实施包括以下内容：
   1) 应核查数据提供方合同、数据安全协议以及系统定级备案材料，明确对数据存储过程的保密性保护需求；
   2) 应核查存储保密性保护措施是否满足数据提供方的保密性保护需求；
   3) 应测试验证数据存储保密性保护措施是否有效。
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。

7.3.6.4 测评单元（L4-CES-24）

该测评单元包括以下要求：

a) 测评指标：应采取技术措施保证汇聚大量数据时不暴露敏感信息。
b) 测评对象：大数据管理平台、服务组件和系统设计及建设方案文档等。
c) 测评实施包括以下内容：
   1) 应核查系统设计及建设方案文档，是否分析了汇聚大量数据可能暴露敏感信息的情况，若有相关情况，是否设计相关技术措施保证汇聚大量数据时不暴露敏感信息；
   2) 应测试验证采用的技术措施是否有效。
d) 单元判定：如果1）-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。

7.3.6.5 测评单元（L4-CES-25）

该测评单元包括以下要求：

a) 测评指标：可采用多方计算、同态加密等数据隐私计算技术实现数据共享的安全性。
b) 测评对象：大数据管理平台、业务应用系统、数据管理系统和系统设计及建设方案文档等
c) 测评实施包括以下内容：
   1) 应核查系统设计及建设方案文档，是否采取多方安全计算、同态加密、联邦学习等数据隐私计算技术实现数据共享的安全性；
   2) 应测试验证是否有效使用多方安全计算、同态加密、联邦学习等数据隐私计算技术措施。
d) 单元判定：如果1）-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。

7.3.7 数据备份与恢复

7.3.7.1 测评单元（L4-CES-26）

该测评单元包括以下要求：

a) 测评指标：备份数据应采取与原数据一致的安全保护措施。
b) 测评对象：配置数据和业务数据等备份数据。

c) 测评实施包括以下内容：
   1) 应核查备份数据的安全保护措施是否与原数据一致，安全保护措施包括但不限于备份数据的访问控制、操作审计、存储保密性和存储完整性、传输保密性和传输完整性等保护措施；
   2) 应测试验证备份数据相关保护措施的有效性是否与原数据保护措施一致。
d) 单元判定：如果 1）-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。

7.3.7.2 测评单元（L4-CES-27）

该测评单元包括以下要求：
a) 测评指标：大数据平台应保证用户数据存在若干个可用的副本，各副本之间的内容应保持一致。
b) 测评对象：大数据管理平台、存储系统及相关组件。
c) 测评实施包括以下内容：
   1) 应核查大数据平台是否对用户数据进行多副本存储，是否存在若干个可用的副本；
   2) 应测试验证各副本是否完整、可用，各副本内容是否一致。
d) 单元判定：如果 1）-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。

7.3.7.3 测评单元（L4-CES-28）

该测评单元包括以下要求：
a) 测评指标：应提供对关键溯源数据的异地备份。
b) 测评对象：大数据资源、大数据应用、大数据平台所关联的关键溯源数据。
c) 测评实施包括以下内容：
   1) 应核查是否存在关键溯源数据；
   2) 应核查关键溯源数据是否进行异地备份，备份策略和相关配置是否合理；
   3) 应测试验证关键溯源数据备份措施是否有效。
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。

7.3.8 剩余信息保护

7.3.8.1 测评单元（L4-CES-29）

该测评单元包括以下要求：
a) 测评指标：大数据平台应提供主动迁移功能，数据整体迁移的过程中应杜绝数据残留。
b) 测评对象：系统设计及建设方案文档、数据迁移记录和相关配置等。
c) 测评实施包括以下内容：
   1) 应核查大数据平台系统设计及建设方案中是否提供主动迁移功能，是否具备整体迁移过程杜绝数据残留相关措施；
   2) 应核查主动迁移功能是否可用，包括相关配置项是否有效等；
   3) 应核查整体迁移完成后是否采取技术措施对原存储空间进行完全清除，包括但不限于索引表删除、低级格式化、重写覆盖、消磁以及物理销毁等。
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。

7.3.8.2 测评单元（L4-CES-30）

该测评单元包括以下要求：

a) 测评指标：应基于数据分类分级保护策略，明确数据销毁要求和方式。

b) 测评对象：大数据资源、大数据应用、大数据平台所关联的数据分类分级保护制度和执行情况等。

c) 测评实施包括以下内容：

1) 应核查是否具有数据分类分级保护策略，是否明确了不同级别和不同类型数据的销毁要求和销毁方式；

2) 应核查数据销毁方式是否有效，销毁结果是否与相关保护策略要求一致。

d) 单元判定：如果 1）-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。

7.3.8.3 测评单元（L4-CES-31）

该测评单元包括以下要求：

a) 测评指标：大数据平台应能够根据服务客户提出的数据销毁要求和方式实施数据销毁。

b) 测评对象：系统设计及建设方案文档、相关操作记录等。

c) 测评实施包括以下内容：

1) 应核查大数据平台系统设计及建设方案，是否支持多种数据销毁功能，包括但不限于索引表删除、低级格式化、重写覆盖、消磁以及物理销毁等；

2) 应核查大数据平台是否提供渠道供服务客户提出数据销毁要求和方式，包括但不限于数据安全协议、服务协议、用户须知、权责声明、系统工单等；

3) 应核查数据销毁记录是否与服务客户提出的要求和方式一致。

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。

7.3.9 个人信息保护

7.3.9.1 测评单元（L4-CES-32）

该测评单元包括以下要求：

a) 测评指标：采集、处理、使用、转让、共享、披露个人信息应在个人信息处理的授权同意范围内，并保留操作审计记录。

b) 测评对象：大数据平台、大数据应用、大数据资源所关联的个人信息数据。

c) 测评实施包括以下内容：

1) 应核查是否明确个人信息处理的授权同意范围，包括但不限于知悉范围、留存期限、流转路径等；

2) 应核查采集、处理、使用、转让、共享、披露个人信息是否未超出个人信息处理的授权同意范围；

3) 应核查采集、处理、使用、转让、共享、披露个人信息是否保留审计记录，审计记录内容是否符合国家法律法规对于个人信息安全审计的相关要求。

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。

7.3.9.2 测评单元（L4-CES-33）

该测评单元包括以下要求：

a) 测评指标：应采取措施防止在数据处理、使用、分析、导出、共享、交换等过程中识别出个人身份信息。
b) 测评对象：大数据平台、大数据应用、大数据资源所关联的系统设计及建设方案文档等。
c) 测评实施包括以下内容：
   1) 应核查系统设计及建设方案文档，是否在数据处理、使用、分析、导出、共享、交换等过程中具备相关措施防止个人身份信息被识别，包括但不限于脱敏、匿名、泛化、去标识化等；
   2) 应测试验证所使用的措施是否有效。
d) 单元判定：如果 1）-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。

7.3.9.3 测评单元（L4-CES-34）

该测评单元包括以下要求：
a) 测评指标：对个人信息的重要操作应设置内部审批流程,审批通过后才能对个人信息进行相应的操作。
b) 测评对象：大数据平台、大数据应用、大数据资源所关联的系统设计及建设方案文档和安全策略文档等。
c) 测评实施包括以下内容：
   1) 应核查系统设计及建设方案和安全策略文档是否明确了对个人信息的重要操作的内部审批流程，包括但不限于批量导出、修改、销毁、备份、恢复等；
   2) 应访谈管理人员，了解审批通过是否为实施重要操作的必备前置条件。
d) 单元判定：如果 1）-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。

7.3.9.4 测评单元（L4-CES-35）

该测评单元包括以下要求：
a) 测评指标：保存个人信息的时间应满足最小化要求，并能够对超出保存期限的个人信息进行删除或匿名化处理。
b) 测评对象：大数据平台、大数据应用、大数据资源所关联的安全管理相关文档和记录。
c) 测评实施包括以下内容：
   1) 应核查安全管理相关文档，是否根据法律法规、行业标准和单位实际情况确定个人信息的保存时间要求；
   2) 应核查是否存在对超出保存期限的个人信息进行删除或匿名化处理的相关配置或操作记录；
   3) 应测试验证个人信息删除或匿名化处理是否有效。
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。

7.3.10 数据溯源

7.3.10.1 测评单元（L4-CES-36）

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。

b） 测评对象：大数据平台、大数据应用、大数据资源所关联的溯源数据、系统设计及建设方案文档等；
c） 测评实施包括以下内容：
1） 应核查系统设计及建设方案是否具有跟踪和记录数据采集、处理、分析和挖掘等过程相关措施；
2） 应核查是否启用跟踪和记录数据采集、处理、分析和挖掘等过程的相关措施，是否保留溯源数据；
3） 应测试验证是否能够基于溯源数据重现相应过程。
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。

7.3.10.2 测评单元（L4-CES-37）

该测评单元包括以下要求：
a） 测评指标：应对重要数据的全生命周期实现数据审计，保证数据活动的所有操作可追溯。
b） 测评对象：大数据平台、大数据应用、大数据资源所关联的溯源数据。
c） 测评实施包括以下内容：
1） 应核查是否对重要数据的全生命周期进行数据审计,包括但不限于数据采集、传输、存储、处理、交换、销毁等数据活动；
2） 应测试验证针对重要数据的审计措施是否有效，是否可追溯数据活动的所有操作。
d） 单元判定：如果 1）-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。

7.3.10.3 测评单元（L4-CES-38）

该测评单元包括以下要求：
a） 测评指标：溯源数据应满足数据业务要求和合规审计要求。
b） 测评对象：大数据平台、大数据应用、大数据资源所关联的溯源数据、系统设计及建设方案文档等。
c） 测评实施包括以下内容：
1） 应核查系统设计及建设方案及相关安全管理制度,是否明确了溯源数据的数据业务要求和合规审计要求。
2） 应核查所记录的溯源数据是否满足数据业务要求；
3） 应核查所记录的溯源数据是否满足法律法规、部门规章、组织内部合规等的合规审计要求。
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。

7.3.10.4 测评单元（L4-CES-39）

该测评单元包括以下要求：
a） 测评指标：应采取技术手段保证溯源数据真实性和保密性。
b） 测评对象：大数据平台、大数据应用、大数据资源所关联的溯源数据、系统设计及建设方案文档。
c） 测评实施包括以下内容：
1） 应核查是否采用数字签名等技术手段保证溯源数据的真实性；

2) 应核查是否采取密码技术保证溯源数据的保密性，密码技术包括但不限于密码算法、密码协议、密码产品、密码模块等；
3) 应测试验证所使用的技术手段是否有效。

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。

7.3.10.5 测评单元（L4-CES-40）

该测评单元包括以下要求：

a) 测评指标：应采取技术手段保证数据源的真实可信。
b) 测评对象：大数据应用、大数据资源、大数据平台的数据平台层、计算分析层以及大数据管理平台等模块及系统设计及建设方案文档等。
c) 测评实施包括以下内容：
   1) 应核查外部数据导入时是否采用数字签名等技术手段保证数据源的真实可信；
   2) 应测试验证所使用的技术手段是否有效。
d) 单元判定：如果 1）-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。

7.4 安全管理中心

7.4.1 系统管理

7.4.1.1 测评单元（L4-SMC-01）

该测评单元包括以下要求：

a) 测评指标：大数据平台应为服务客户提供管理其计算和存储资源使用状况的能力。
b) 测评对象：大数据管理平台。
c) 测评实施包括以下内容：
   1) 应核查大数据平台是否为服务客户提供管理其计算和存储资源使用状况的能力，包括但不限于查询、监控、申请变更等；
   2) 应测试验证提供给客户的管理功能是否有效，是否不存在无法管理的情况。
d) 单元判定：如果 1）-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。

7.4.1.2 测评单元（L4-SMC-02）

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、服务组件和大数据管理平台等。
c) 测评实施包括以下内容：
   1) 应核查大数据管理平台是否具备对其提供的辅助工具或服务组件进行管理的能力，包括但不限于辅助工具或服务组件的安装、部署、监控、优化、升级、卸载、身份鉴别、访问权限管理、操作审计等；
   2) 应测试验证大数据平台提供的辅助工具或服务组件的安全管理措施是否有效，是否不存在无法管理的情况。
d) 单元判定：如果 1）-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。

7.4.1.3 测评单元（L4-SMC-03）

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：系统设计及建设方案文档、计算分析层相关节点等。
c) 测评实施包括以下内容：
   1) 应核查是否具备屏蔽计算、内存、存储资源故障的措施和技术手段，相关措施是否正常运行；
   2) 应测试验证相关措施的有效性，是否不存在部分计算节点或存储节点故障时，业务无法正常运行的情况。
d) 单元判定：如果 1）-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。

7.4.1.4 测评单元（L4-SMC-04）

该测评单元包括以下要求：

a) 测评指标：大数据平台在系统维护、在线扩容等情况下，应保证大数据应用和大数据资源的正常业务处理能力。
b) 测评对象：大数据管理平台、系统维护及扩容测试记录等文档。
c) 测评实施包括以下内容：
   1) 应核查大数据平台在系统维护、在线扩容等情况下，是否采取技术手段保证大数据应用和大数据资源的正常业务处理能力。
   2) 应测试验证所采取的技术手段是否有效，是否不存在部分大数据应用和大数据资源的正常业务处理无法开展的情况。
d) 单元判定：如果 1）-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。

7.4.2 集中管控

7.4.2.1 测评单元（L4-SMC-05）

测评单元包括以下要求：

a) 测评指标：应对大数据系统提供的各类接口的使用情况进行集中审计和监测，并在发生问题时提供报警。
b) 测评对象：大数据系统集中审计功能模块。
c) 测评实施包括以下内容：
   1) 应核查是否能够对各类接口的使用进行集中审计和监测；
   2) 应核查是否保存有至少 6 个月的审计数据和监测数据；
   3) 应核查是否能够在接口使用异常的情况下进行报警。
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。

7.5 安全管理制度

7.5.1 安全策略

7.5.1.1 测评单元（L4-PSS-01）

该测评单元包括以下要求：

a) 测评指标：应制定大数据安全工作的总体方针和安全策略，阐明本机构大数据安全工作的目标、范围、原则和安全框架等相关内容。
b) 测评对象：大数据安全工作的总体方针、安全策略类文档。
c) 测评实施包括以下内容：
   1) 应访谈并核查是否具有大数据安全工作的总体方针和安全策略相关文档；
   2) 应核查相关文档中是否明确机构大数据安全工作的总体目标、范围、原则和安全框架等相关内容。
d) 单元判定：如果 1）-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。

7.5.1.2 测评单元（L4-PSS-02）

该测评单元包括以下要求：

a) 测评指标：大数据安全策略应覆盖数据生命周期相关的数据安全，内容至少包括目的、范围、岗位、责任、管理层承诺、内外部协调及合规性要求等。
b) 测评对象：安全策略类文档。
c) 测评实施包括以下内容：
   1) 应访谈并核查是否具有大数据安全策略相关文档；
   2) 应核查大数据安全策略文档内容是否覆盖数据生命周期相关的数据安全，至少包含目的、范围、岗位、责任、管理层承诺、内外部协调及合规性要求等。
d) 单元判定：如果 1）-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。

7.6 安全管理机构

7.6.1 授权和审批

7.6.1.1 测评单元（L4-ORS-01）

该测评单元包括以下要求：

a) 测评指标：数据的采集应获得数据源管理者的授权，确保符合数据收集最小化原则。
b) 测评对象：数据源管理者、数据安全保护相关管理制度文档及记录表单类文档等。
c) 测评实施包括以下内容：
   1) 应访谈数据源管理者并核查相关制度，是否要求对数据的采集需获得授权，是否遵循最小化授权原则；
   2) 应核查是否具有数据采集相关的授权记录，授权内容是否符合数据收集最小化原则，是否与相关制度要求一致。
d) 单元判定：如果 1）-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。

7.6.1.2 测评单元（L4-ORS-02）

该测评单元包括以下要求：

a) 测评指标：应建立数据导入、导出、集成、分析、交换、交易、共享及公开的授权审批控制流程，赋予数据活动主体的最小操作权限、最小数据集和权限有效时长，依据流程实施相关控制并记录过程，及时回收过期的数据访问权限。

b） 测评对象：数据安全保护相关管理制度文档及记录表单类文档等。
c） 测评实施包括以下内容：
1） 应核查管理制度类文档是否明确数据的导入、导出、集成、分析、交换、交易、共享及公开的授权审批流程;
2） 应核查管理制度类文档是否明确过期的数据访问权限回收流程及方式方法等,审批内容是否涵盖数据活动主体的最小操作权限、最小数据集和权限有效时长；
3） 应核查是否具有相关控制记录，记录内容是否与数据安全保护相关管理制度要求一致。
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。

7.6.1.3 测评单元（L4-ORS-03）

该测评单元包括以下要求：
a） 测评指标：应建立跨境数据的评估、审批及监管控制流程，并依据流程实施相关控制并记录过程。
b） 测评对象：数据安全保护相关管理制度文档和记录表单类文档等。
c） 测评实施包括以下内容：
1） 应核查数据安全保护相关管理制度中是否明确跨境数据的评估、审批及监管控制流程；
2） 应核查是否具有相关控制的记录，记录内容是否与数据安全保护相关管理制度要求一致；
3） 应核查数据出境是否符合国家相关部门的有关管理规定。
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。

7.6.2 审核和检查

7.6.2.1 测评单元（L4-ORS-04）

该测评单元包括以下要求：
a） 测评指标：应定期对个人信息安全保护措施的有效性进行常规安全检查。
b） 测评对象：信息/网络安全主管、数据安全保护相关管理制度文档等。
c） 测评实施包括以下内容：
1） 应访谈信息/网络安全主管并核查数据安全保护相关管理制度，是否对个人信息安全保护措施的有效性进行常规安全检查；
2） 应核查是否具有常规安全检查相关记录,检查内容是否覆盖个人信息安全保护措施的有效性检查，检查频率、检查方法以及检查内容等是否与管理制度要求一致，记录内容是否详尽。
d） 单元判定：如果 1）-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。

7.7 安全建设管理

7.7.1 服务供应商选择

7.7.1.1 测评单元（L4-CMS-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和大数据资源提供相应等级的安全保护能力。

b) 测评对象：安全策略类文档、数据安全保护相关管理制度文档和大数据平台定级备案材料、等级测评报告等。

c) 测评实施包括以下内容：

1) 应访谈系统建设负责人并核查相关制度，是否根据业务系统的安全保护等级选择具有相应等级安全保护能力的大数据平台；

2) 应核查大数据平台和大数据应用、大数据资源的定级备案材料，大数据平台是否与所承载的大数据应用和大数据资源具有相应或高于的安全保护能力；

3) 应核查所使用的大数据平台的网络安全等级保护测评报告，报告时间和报告结论是否符合网络安全等级保护相关要求。

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。

7.7.1.2 测评单元（L4-CMS-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和大数据平台使用者的权限与责任、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：供应商服务协议及数据安全协议等。

c) 测评实施包括以下内容：

1) 应核查供应商服务协议、数据安全协议以及用户须知等相关材料，是否明确了大数据服务提供者和使用者的权限与责任，核查内容是否覆盖大数据服务内容、安全服务内容，是否明确服务范围、服务指标、职责划分、访问授权、隐私保护、行为准则、违约责任等；

2) 应核查大数据平台供应商服务协议、数据安全协议以及用户须知等相关材料的有效性，是否具有双方签字及盖章，是否处于有效期内等。

d) 单元判定：如果 1）-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。

7.7.2 供应链管理

7.7.2.1 测评单元（L4-CMS-03）

该测评单元包括以下要求：

a) 测评指标：应确保供应商的选择符合国家有关规定。

b) 测评对象：建设负责人。

c) 测评实施包括以下内容：

1) 应访谈系统建设负责人并核查相关材料，供应商的选择过程是否符合国家有关规定，包括但不限于招投标流程、合同签约流程、价款支付方式等；

2) 应访谈系统建设负责人并核查相关材料，供应商的选择结果是否符合国家有关规定，包括但不限于供应商的建设服务资质、安全服务资质、集成服务资质、密码服务资质以及产品销售许可等。

d) 单元判定：如果 1）-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。

7.7.2.2 测评单元（L4-CMS-04）

该测评单元包括以下要求：

a) 测评指标：应以书面方式约定数据交换、共享的接收方对数据的保护责任，并明确数据安全保护要求。
b) 测评对象：供应商服务协议及数据安全协议等。
c) 测评实施包括以下内容：
   1) 应核查供应商服务协议及数据安全协议中是否建立数据交换、共享的数据保护责任要求，明确数据保护范围、保护内容、数据类型、数据分级分类保护等级及对不同等级数据的保护要求等内容；
   2) 应核查合同或协议是否有双方签字或盖章，是否处于有效期内等。
d) 单元判定：如果 1）-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。

7.7.2.3 测评单元（L4-CMS-05）

该测评单元包括以下要求：
a) 测评指标：应将供应链安全事件信息或安全威胁信息及时传达到数据交换、共享的接收方。
b) 测评对象：供应链安全事件记录和供应商服务协议及数据安全协议等。
c) 测评实施：
   1) 应核查供应链安全事件报告或威胁报告是否及时传达到数据交换、共享的接收方；
   2) 应核查安全事件报告或威胁报告是否明确相关事件信息或威胁信息。
d) 单元判定：如果 1）-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。

7.7.3 数据源管理

7.7.3.1 测评单元（L4-CMS-06）

该测评单元包括以下要求：
a) 测评指标：应通过合法正当的渠道获取各类数据。
b) 测评对象：供应商服务协议、数据安全协议及记录表单类文档等。
c) 测评实施包括以下内容：
   1) 应对照获取的数据类核查供应商服务协议及数据安全协议，是否均通过合法正当的渠道获取各类数据；
   2) 如果获取的渠道数据用于提供大数据平台服务，应核查相关系统、合同或协议等是否对渠道进行了明示。
d) 单元判定：如果 1）-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。

7.8 安全运维管理

7.8.1 资产管理

7.8.1.1 测评单元（L4-MMS-01）

该测评单元包括以下要求：
a) 测评指标：应建立数据资产安全管理策略，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，包括但不限于数据采集、传输、存储、处理、交换、销毁等过程。
b) 测评对象：数据资产安全管理策略、操作记录及提供数据保护的相关产品或组件。
c) 测评实施包括以下内容：

1) 应访谈并核查是否建立数据资产安全管理策略，策略是否明确各类数据全生命周期的操作规范、保护措施、管理人员职责，包括但不限于数据采集、传输、存储、处理、交换、销毁等过程；
2) 应核查数据采集、传输、存储、处理、交换、销毁等过程中的数据保护措施和相关记录是否与数据资产安全管理策略一致。

d) 单元判定：如果 1）-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。

7.8.1.2 测评单元（L4-MMS-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相应强度的安全保护要求。
b) 测评对象：数据分类分级保护策略、操作记录及提供数据分类分级标记和保护的相关产品或组件。
c) 测评实施包括以下内容：
1) 应访谈并核查是否制定数据分类分级保护策略，数据分类分级保护策略是否明确了数据分类分级方法和依据、是否为不同类别级别的数据制定相应强度的安全保护要求；
2) 应核查数据分类分级保护策略是否已覆盖大数据系统重要数据，包括但不限于重要业务数据、标识数据、密钥数据、审计数据、溯源数据、脱敏数据、个人数据、配置数据、备份数据等；
3) 应核查数据保护相关记录，是否与分类分级保护策略要求一致。
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。

7.8.1.3 测评单元（L4-MMS-03）

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，如需要变更数据所属类别或级别，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。

7.8.1.4 测评单元（L4-MMS-04）

该测评单元包括以下要求：

a) 测评指标：应对数据资产和对外数据接口进行登记管理，建立相应的资产清单。
b) 测评对象：数据资产清单、对外数据接口清单。
c) 测评实施：

1） 应访谈管理员是否定期对数据资产和对外接口进行梳理和登记，是否形成数据资产清单和对外接口清单；
2） 应核查数据资产清单是否全面，是否覆盖重要数据，包括但不限于业务数据、标识数据、密钥数据、审计数据、溯源数据、脱敏数据、个人数据、配置数据、备份数据等；
3） 应核查对外数据接口清单是否全面，是否覆盖所有重要接口，包括但不限于数据采集、数据交换、数据共享、API 应用等接口。

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。

7.8.2 介质管理

7.8.2.1 测评单元（L4-MMS-05）

该测评单元包括以下要求：

a） 测评指标：应在中国境内对数据进行清除或销毁。
b） 测评对象：数据管理员及数据清除、销毁过程记录。
c） 测评实施包括以下内容：
1） 应访谈数据管理员，数据清除或销毁是否在中国境内开展；
2） 应核查数据清除、销毁相关记录，是否依据要求在中国境内对数据进行清除或销毁。
d） 单元判定：如果 1）-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。

7.8.2.2 测评单元（L4-MMS-06）

该测评单元包括以下要求：

a） 测评指标：对存储重要数据的存储介质或物理设备应采取难恢复的技术手段，如物理粉碎、消磁、多次擦写等。
b） 测评对象：数据管理员、数据销毁执行记录。
c） 测评实施包括以下内容：
1） 应访谈数据管理员，对存储重要数据的存储介质或物理设备在停用后是否采取如物理粉碎、消磁、多次擦写等技术处理手段进行数据销毁；
2） 应核查存储重要数据的存储介质或物理设备在停用后的数据销毁执行记录，记录内容是否包括被销毁对象原用途、容量、销毁方式、销毁时间、销毁实施人员等信息，销毁方式是否难以恢复。
d） 单元判定：如果 1）-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。

7.8.3 网络和系统安全管理

7.8.3.1 测评单元（L4-MMS-07）

该测评单元包括以下要求：

a） 测评指标：应建立对外数据接口安全管理机制，所有的接口调用均应获得授权和批准。
b） 测评对象：安全策略类文档、数据安全保护相关管理制度文档、授权审计记录、大数据系统审计模块等。
c） 测评实施包括以下内容：

1) 应访谈安全管理人员并核查相关管理制度，是否建立大数据网络和系统安全管理机制，是否要求所有的接口调用均应获得授权和批准；
2) 应核查相关授权和审批记录，记录内容是否全面，授权和审批过程是否合规，是否与管理制度要求一致。

d) 单元判定：如果 1）-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。

8 第五级安全测评要求

略。

附 录 A
（规范性附录）
测评单元编号说明

A.1 测评单元编码规则

测评单元编号为三组数据，格式为 XX—XXX—XX，各组含义和编码规则如下：

第 1 组由 2 位组成，第 1 位为字母 L，第 2 位为数字，其中数字 1 为第一级，2 为第二级，3 为第三级，4 为第四级，5 为第五级。

第 2 组由 3 位字母组成。字母代表类：PES 为安全物理环境， CNS 为安全通信网络，ABS 为安全区域边界，CES 为安全计算环境，SMC 为安全管理中心，PSS 为安全管理制度，ORS 为安全管理机构，HRS 为安全管理人员，CMS 为安全建设管理，MMS 为安全运维管理。

第 3 组由 2 位数字组成，按类对基本要求中的要求项进行顺序编号。

示例：测评单元编号为 L2-PES-01，代表源自安全测评要求部分的第二级安全物理环境类的第 1 个指标。

A.2 专用缩略语

下列专用缩略语适用于本文件。

ABS：安全区域边界（Area Boundary Security）
CES：安全计算环境（Computing Environment Security）
CMS：安全建设管理（Construction Management Security）
CNS：安全通信网络（Communication Network Security）
MMS：安全运维管理（Maintenance Management Security）
ORS：安全管理机构（Organization and Resource Security）
PES：安全物理环境（Physical Environment Security）
PSS：安全管理制度（Policy and System Security）
HRS: 安全管理人员（Human Resource Security）
SMC：安全管理中心（Security Management Center）

附 录 B
（资料性附录）
大数据等级保护对象与安全要求映射

不同类型大数据等级保护对象与 T/ISEAA 002-2021《信息安全技术网络安全等级保护大数据基本要求》安全要求的映射关系见表 B.1。

表 B.1 大数据等级保护对象类型与测评指标映射表

类别	控制点	要求项	保护等级	适用保护对象类型
安全物理环境	基础设施位置	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。	二 三 四	包含大数据平台、大数据应用或大数据资源的定级对象
安全通信网络	网络架构	b)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和大数据资源；	二 三 四	包含大数据平台、大数据应用或大数据资源的定级对象
		c)应保证大数据平台的管理流量与系统业务流量分离；	三 四	包含大数据平台的定级对象
		d)应提供开放接口或开放性安全服务，允许客户接入第三方安全产品或在大数据平台选择第三方安全服务。	三 四	包含大数据平台的定级对象
安全计算环境	身份鉴别	b)大数据系统提供的重要外部调用接口应进行身份鉴别。	二	包含大数据平台或大数据应用的定级对象
		b)大数据平台应提供双向认证功能，能对不同客户的大数据应用、大数据资源进行双向身份鉴别；	三 四	包含大数据平台的定级对象
		c)应采用口令和密码技术组合的鉴别技术对使用数据采集终端、数据导入服务组件、数据导出终端、数据导出服务组件的主体实施身份鉴别；	三 四	包含大数据平台、大数据应用或大数据资源的定级对象
		d)应对向大数据系统提供数据的外部实体实施身份鉴别；	三 四	包含大数据平台的定级对象
		e)大数据系统提供的各类外部调用接口应依据调用主体的操作权限实施相应强度的身份鉴别。	三 四	包含大数据平台、大数据应用或大数据资源的定级对象
	访问控制	b)对外提供服务的大数据平台，平台或第三方应在服务客户授权下才可以对其数据资源进行访问、使用和管理；	二 三 四	包含大数据平台或大数据应用的定级对象
		c)应对数据进行分类分级管理；	二	包含大数据平台、大数据应用或大数据资源的定级对象
		c)大数据系统应提供数据分类分级标识功能；	三 四	包含大数据平台的定级对象
		d)应采取技术手段对数据采集终端、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进行限制；	二	包含大数据平台、大数据应用或大数据资源的定级对象
		d)应在数据采集、传输、存储、处理、交换及销毁等各个环节，根据数据分类分级标识对数据进行不同处置，最高等级数据的相关保护措施不低于第三级安全要求，安全保护策略在各环节保持一致；	三	包含大数据平台、大数据应用或大数据资源的定级对象
		d)应在数据采集、传输、存储、处理、交换及销毁等各个环节，支持对数据进行分类分级处置，最高等级数据的相关保护措施不低于第四级安全要求，安全保护策略在各环节保持一致；	四	包含大数据平台、大数据应用或大数据资源的定级对象

类别	控制点	要求项	保护等级	适用保护对象类型
		e)应最小化各类接口操作权限；（二级） f)应最小化各类接口操作权限；（三级） g)应最小化各类接口操作权限；（四级）	二 三	包含大数据平台、大数据应用或大数据资源的定级对象
		e)大数据系统应具备设置数据安全标记功能，并基于安全标记进行访问控制；	四	包含大数据平台或大数据资源的定级对象
		e)大数据系统应对其提供的各类接口的调用实施访问控制，包括但不限于数据采集、处理、使用、分析、导出、共享、交换等相关操作；（三级） f)大数据系统应对其提供的各类接口的调用实施访问控制，包括但不限于数据采集、处理、使用、分析、导出、共享、交换等相关操作；（四级）	三 四	包含大数据平台、大数据应用或大数据资源的定级对象
		f)应最小化数据使用、分析、导出、共享、交换的数据集；（二级） g)应最小化数据使用、分析、导出、共享、交换的数据集；（三级） h)应最小化数据使用、分析、导出、共享、交换的数据集；（四级）	二 三 四	包含大数据平台、大数据应用或大数据资源的定级对象
		h)大数据系统应提供隔离不同客户应用数据资源的能力；（三级） i)大数据系统应提供隔离不同客户应用数据资源的能力；（四级）	三 四	包含大数据平台的定级对象
		i)应对重要数据的数据流转、泄露和滥用情况进行监控，及时对异常数据操作行为进行预警，并能够对突发的严重异常操作及时定位和阻断。（三级） k)应对重要数据的数据流转、泄露和滥用情况进行监控，及时对异常数据操作行为进行预警，并能够对突发的严重异常操作及时定位和阻断。（四级）	三 四	包含大数据平台、大数据应用或大数据资源的定级对象
		i)应采用技术手段限制在终端输出重要数据。（三级） j)应采用技术手段限制在终端输出重要数据；（四级）	三 四	包含大数据平台、大数据应用或大数据资源的定级对象
	安全审计	b)大数据系统应对其提供的**重要**接口的调用情况以及各类**重要**账号的操作情况进行审计；	二	包含大数据平台、大数据应用或大数据资源的定级对象
		b)大数据系统应保证不同客户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；	三 四	包含大数据平台、大数据应用或大数据资源的定级对象
		c)大数据系统应对其提供的**各类**接口的调用情况以及各类账号的操作情况进行审计；	三 四	包含大数据平台、大数据应用或大数据资源的定级对象
		c)应保证大数据系统服务商对服务客户数据的操作可被服务客户审计。（二级） d)应保证大数据系统服务商对服务客户数据的操作可被服务客户审计。（三、四级）	二 三 四	包含大数据平台或大数据应用的定级对象
	入侵防范	b)应对所有进入系统的数据进行检测，避免出现恶意数据输入。	三 四	包含大数据平台或大数据应用的定级对象
	数据完整性	b)应采用技术手段对数据交换过程进行数据完整性检测；	二 三 四	包含大数据平台、大数据应用或大数据资源的定级对象
		c)数据在存储过程中的完整性保护应满足数据提供方系统的安全保护要求。	二 三 四	包含大数据平台、大数据应用或大数据资源的定级对象
	数据保密性	b)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；	二 三	包含大数据平台的定级对象

类别	控制点	要求项	保护等级	适用保护对象类型
			四	
		b)应依据相关安全策略对数据进行静态脱敏和去标识化处理；	二	包含大数据平台、大数据应用或大数据资源的定级对象
		c)应依据相关安全策略和数据**分类分级标识**对数据进行静态脱敏和去标识化处理；	三 四	包含大数据平台、大数据应用或大数据资源的定级对象
		d)数据在存储过程中的保密性保护应满足数据提供方系统的安全保护要求；	三 四	包含大数据平台、大数据应用或大数据资源的定级对象
		e)应采取技术措施保证汇聚大量数据时不暴露敏感信息；	三 四	包含大数据平台、大数据应用或大数据资源的定级对象
		f)可采用多方计算、同态加密等数据隐私计算技术实现数据共享的安全性。	三 四	包含大数据平台、大数据应用或大数据资源的定级对象
	数据备份恢复	b)备份数据应采取与原数据一致的安全保护措施；	二 三 四	包含大数据平台、大数据应用或大数据资源的定级对象
		c)大数据平台应保证用户数据存在若干个可用的副本，各副本之间的内容应保持一致；	三 四	包含大数据平台的定级对象
		d)应提供对关键溯源数据的异地备份。	三 四	包含大数据平台或大数据资源的定级对象
	剩余信息保护	b)大数据平台应提供主动迁移功能，数据整体迁移的过程中应杜绝数据残留；	二 三 四	包含大数据平台、大数据应用或大数据资源的定级对象
		c)应基于数据分类分级保护策略，明确数据销毁要求和方式；	三 四	包含大数据平台、大数据应用或大数据资源的定级对象
		c)大数据平台应能够根据服务客户提出的数据销毁要求和方式实施数据销毁。(二级) d)大数据平台应能够根据服务客户提出的数据销毁要求和方式实施数据销毁。(三级、四级)	二 三 四	包含大数据平台的定级对象
	个人信息保护	b)采集、处理、使用、转让、共享、披露个人信息应在个人信息处理的授权同意范围内，并保留操作审计记录；	二 三 四	包含大数据平台、大数据应用或大数据资源的定级对象
		c)应采取措施防止在数据处理、使用、分析、导出、共享、交换等过程中识别出个人身份信息；	二 三 四	包含大数据平台、大数据应用或大数据资源的定级对象
		d)对个人信息的重要操作应设置内部审批流程,审批通过后才能对个人信息进行相应的操作。	二 三 四	包含大数据平台、大数据应用或大数据资源的定级对象
		e)保存个人信息的时间应满足最小化要求，并能够对超出保存期限的个人信息进行删除或匿名化处理。	三 四	包含大数据平台、大数据应用或大数据资源的定级对象

类别	控制点	要求项	保护等级	适用保护对象类型
	数据溯源	a)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；	三 四	包含大数据平台、大数据应用或大数据资源的定级对象
		b)应对重要数据的全生命周期实现数据审计，保证数据活动的所有操作可追溯；	四	包含大数据平台、大数据应用或大数据资源的定级对象
		b)溯源数据应满足数据业务要求和合规审计要求；（三级） c)溯源数据应满足数据业务要求和合规审计要求；（四级）	三 四	包含大数据平台、大数据应用或大数据资源的定级对象
		c)应采取技术手段保证数据源的真实可信。(三级) e)应采取技术手段保证数据源的真实可信。（四级）	三	包含大数据平台、大数据应用或大数据资源的定级对象
		d)应采取技术手段保证溯源数据真实性和保密性；	四	包含大数据平台、大数据应用或大数据资源的定级对象
安全管理中心	系统管理	b)大数据平台应为服务客户提供管理其计算和存储资源使用状况的能力；	二 三 四	包含大数据平台的定级对象
		c)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；	二 三 四	包含大数据平台的定级对象
		d)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；	二 三 四	包含大数据平台的定级对象
		e)大数据平台在系统维护、在线扩容等情况下，应保证大数据应用和大数据资源的正常业务处理能力。	二 三 四	包含大数据平台的定级对象
	集中管控	b)应对大数据系统提供的各类接口的使用情况进行集中审计和监测，并在发生问题时提供报警。	三 四	包含大数据平台的定级对象
安全管理制度	安全策略	b)应制定大数据安全工作的总体方针和安全策略，阐明本机构大数据安全工作的目标、范围、原则和安全框架等相关内容；	二 三 四	包含大数据平台、大数据应用或大数据资源的定级对象
		c)大数据安全策略应覆盖数据生命周期相关的数据安全，内容至少包括目的、范围、岗位、责任、管理层承诺、内外部协调及合规性要求等。	二 三 四	包含大数据平台、大数据应用或大数据资源的定级对象
安全管理机构	授权和审批	b)数据的采集应获得数据源管理者的授权，确保符合数据收集最小化原则。	二 三 四	包含大数据平台、大数据应用或大数据资源的定级对象
		c)应建立数据导入、导出、集成、分析、交换、交易、共享及公开的授权审批控制流程，赋予数据活动主体的最小操作权限、最小数据集和权限有效时长，依据流程实施相关控制并记录过程，及时回收过期的数据访问权限；	三 四	包含大数据平台、大数据应用或大数据资源的定级对象
		d)应建立跨境数据的评估、审批及监管控制流程，并依据流程实施相关控制并记录过程。	三 四	包含大数据平台、大数据应用或大数据资源的定级对象

类别	控制点	要求项	保护等级	适用保护对象类型
	审核和检查	b)应定期对个人信息安全保护措施的有效性进行常规安全检查。	二 三 四	包含大数据平台、大数据应用或大数据资源的定级对象
安全建设管理	服务供应商选择	b)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和大数据资源提供相应等级的安全保护能力；	二 三 四	包含大数据平台、大数据应用或大数据资源的定级对象
		c)应以书面方式约定大数据平台提供者和大数据平台使用者的权限与责任、各项服务内容和具体技术指标等，尤其是安全服务内容。	二 三 四	包含大数据平台、大数据应用或大数据资源的定级对象
	供应链管理	a)应确保供应商的选择符合国家有关规定；	二 三 四	包含大数据平台、大数据应用或大数据资源的定级对象
		b)应以书面方式约定数据交换、共享的接收方对数据的保护责任，并明确数据安全保护要求；	三 四	包含大数据平台、大数据应用或大数据资源的定级对象
		c)应将供应链安全事件信息或安全威胁信息及时传达到数据交换、共享的接收方。	三 四	包含大数据平台、大数据应用或大数据资源的定级对象
	数据源管理	应通过合法正当的渠道获取各类数据。	二 三 四	包含大数据平台、大数据应用或大数据资源的定级对象
安全运维管理	资产管理	b)应建立数据资产安全管理策略，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，包括但不限于数据采集、传输、存储、处理、交换、销毁等过程；	二 三 四	包含大数据平台、大数据应用或大数据资源的定级对象
		c)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相应强度的安全保护要求；	三 四	包含大数据平台、大数据应用或大数据资源的定级对象
		d)应定期评审数据的类别和级别，如需要变更数据所属类别或级别，应依据变更审批流程执行变更；	三 四	包含大数据平台、大数据应用或大数据资源的定级对象
		c)应对数据资产进行登记，建立数据资产清单。	二	包含大数据平台、大数据应用或大数据资源的定级对象
		e)应对数据资产和对外数据接口进行登记管理，建立相应的资产清单。	三 四	包含大数据平台、大数据应用或大数据资源的定级对象
	介质管理	b)应在中国境内对数据进行清除或销毁。	二 三 四	包含大数据平台、大数据应用或大数据资源的定级对象
		c)对存储重要数据的存储介质或物理设备应采取难恢复的技术手段，如物理粉碎、消磁、多次擦写等。	三 四	包含大数据平台、大数据应用或大数据资源的定级对象
	网络和系统安全管理	b)应建立对外数据接口安全管理机制，所有的接口调用均应获得授权和批准。	二 三 四	包含大数据平台、大数据应用或大数据资源的定级对象

附 录 C
（资料性附录）
高风险判例场景

C.1 安全物理环境

C.1.1 基础设施物理位置不当

本判例包括以下内容：

a） 标准要求：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） 适用范围：第二级及以上大数据系统。

c） 问题描述：承载大数据业务和数据的基础设施，例如存储、处理、分析等功能的各类服务器、存储设备、网络设备、存储节点、处理节点、分析节点和大数据管理平台等软硬件不在中国境内。

d） 可能的缓解措施及风险评价：无。

C.2 安全通信网络

C.2.1 大数据平台等级低于承载的大数据应用或大数据资源等级

本判例包括以下内容：

a） 标准要求：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和大数据资源。

b） 适用范围：第二级及以上大数据系统。

c） 问题描述（任意）：

1） 大数据平台承载高于其安全保护等级（SxAx）的大数据应用或大数据资源；

2） 大数据应用或大数据资源部署在低于其安全保护等级（SxAx）的大数据平台上；

3） 大数据应用或大数据资源部署在未进行等级保护测评、测评报告超出有效期或者等级测评结论为差的大数据平台上。

d） 可能的缓解措施及风险评价：无。

C.3 安全计算环境

C.3.1 重要外部调用接口身份鉴别功能缺失

本判例包括以下内容：

a） 标准要求：大数据系统提供的重要外部调用接口应进行身份鉴别。

b） 适用范围：第二级及以上大数据系统。

c） 问题描述（任意）：

1） 大数据系统的重要外部调用接口无身份鉴别功能，或存在被绕过的情况；

2） 重要外部调用接口存在空口令或弱口令。

d） 可能的缓解措施及风险评价：无。

C.3.2 外部实体身份鉴别功能缺失

本判例包括以下内容：

a） 标准要求：应对向大数据系统提供数据的外部实体实施身份鉴别。

b） 适用范围：第三级及以上大数据系统。

c） 问题描述（任意）：

1） 为大数据系统提供数据的外部实体或接口未实施身份鉴别，或存在是否鉴别被绕过的情况；

2） 为大数据系统提供数据的外部接口存在空口令或弱口令。

d） 可能的缓解措施及风险评价：提供数据的外部实体或接口有其他的身份鉴别措施、访问控制措施或有效的管理制度，能够有效控制或降低身份鉴别功能的缺失带来的风险时可酌情降低风险。

C.3.3 身份鉴别强度不足

本判例包括以下内容：

a） 标准要求：大数据系统提供的各类外部调用接口应依据调用主体的操作权限实施相应强度的身份鉴别。

b） 适用范围：第三级及以上大数据系统。

c） 问题描述：大数据系统的数据调用接口存在访问控制策略缺陷，经测试验证可越权访问系统或其他用户的数据，例如：存在非授权访问系统数据、平行越权漏洞、垂直越权漏洞等。

d） 可能的缓解措施及风险评价：

1） 对于部署在可控网络环境的系统，可从现有的防护措施、用户行为监控等角度进行综合风险分析，根据分析结果，酌情判定风险等级；

2） 可从非授权访问模块的重要程度、影响程度，越权访问的难度等角度进行综合风险分析，根据分析结果，酌情判定风险等级。

C.3.4 大数据平台双向认证功能缺失

本判例包括以下内容：

a） 标准要求：大数据平台应提供双向认证功能，能对不同客户的大数据应用、大数据资源进行双向身份鉴别。

b） 适用范围：第四级及以上大数据系统。

c） 问题描述：大数据平台未提供双向认证功能。

d） 可能的缓解措施及风险评价：结合访问控制权限、其他防护技术措施、相关管理制度、是否对外提供服务等酌情判定风险等级。例如大数据平台不对外提供服务，可根据内部相关防护措施及实际防护效果进行综合风险分析，酌情判定风险等级。

C.3.5 数据采集、导入或导出终端或组件身份鉴别功能缺失

本判例包括以下内容：

a） 标准要求：应采用口令和密码技术组合的鉴别技术对使用数据采集终端、数据导入服务组件、数据导出终端、数据导出服务组件的主体实施身份鉴别。

b） 适用范围：第三级及以上大数据系统。

c） 问题描述（任意）：

1） 未对使用数据采集终端、数据导入服务组件、数据导出终端、数据导出服务组件的主体采用口令和密码技术组合鉴别技术进行身份鉴别；

2） 存在弱口令或弱密码算法的。

d） 可能的缓解措施及风险评价：

1） 在身份鉴别过程中，多次采用同一种鉴别技术进行身份鉴别，且每次鉴别信息不相同，例如两次口令认证措施（两次口令不同），可根据实际措施效果，酌情判定风险等级；

2） 在完成重要操作前的不同阶段使用不同的鉴别方式进行身份鉴别，可根据实际措施效果，酌情判定风险等级；
3） 对于用户群体为互联网个人用户的情况，可从行业主管部门的要求、用户身份被滥用后对系统或个人造成的影响等角度进行综合风险分析，根据分析结果，酌情判定风险等级；
4） 对于采取登录地址限制、绑定设备等其他技术手段减轻用户身份被滥用的威胁的情况，可从措施所起到的防护效果等角度进行综合风险分析，根据分析结果，酌情判定风险等级。

C.3.6 未授权的数据资源调用

本判例包括以下内容：
a） 标准要求：对外提供服务的大数据平台，平台或第三方应在服务客户授权下才可以对其数据资源进行访问、使用和管理。
b） 适用范围：第二级及以上大数据系统。
c） 问题描述（任意）：
1） 大数据平台对客户数据资源访问的授权机制缺失，对于客户的数据资源访问无限制；
2） 大数据平台的访问控制措施或策略存在缺陷,可越权访问、查看、操作服务客户或其他用户的数据，例如：存在非授权访问其他数据资源、平行权限漏洞、垂直越权漏洞等。
d） 可能的缓解措施及风险评价：如大数据平台和数据资源属于同一运营者，或调用数据资源对象的是同一运营者内部的大数据应用，且存在纸质/电子授权流程时，可根据实际情况，酌情判定风险等级。

C.3.7 数据分类分级标识功能缺失

本判例包括以下内容：
a） 标准要求：大数据系统应提供数据分类分级标识功能。
b） 适用范围：第三级及以上大数据系统。
c） 问题描述：大数据系统未提供数据分类分级标识功能。
d） 可能的缓解措施及风险评价：无。

C.3.8 访问控制机制存在缺陷

本判例包括以下内容：
a） 标准要求：大数据系统应对其提供的各类接口的调用实施访问控制，包括但不限于数据采集、处理、使用、分析、导出、共享、交换等相关操作。
b） 适用范围：第三级及以上大数据系统。
c） 问题描述（所有）：
1） 接口访问控制策略存在缺陷，可越权访问系统接口模块或查看、操作其他用户的数据。如存在平行权限漏洞、低权限用户越权访问高权限功能模块、用户可以通过接口请求非授权的资源或功能等；
2） 接口调用的访问控制策略配置不当或控制措施失效。
d） 可能的缓解措施及风险评价：
1） 对于部署在可控网络环境的大数据系统，可从现有的防护措施、用户行为监控等角度进行综合风险分析，根据分析结果，酌情判定风险等级；
2） 可从非授权访问模块的重要程度、影响程度、越权访问的难度等角度进行综合风险分析，根据分析结果，酌情判定风险等级。

C.3.9 数据导出控制缺失

本判例包括以下内容：

a） 标准要求：应最小化数据使用、分析、导出、共享、交换的数据集。

b） 适用范围：第二级及以上大数据应用、大数据资源。

c） 问题描述：数据导出功能无法进行资源量导出限制。

d） 可能的缓解措施及风险评价：无。

C.3.10 不同客户的审计数据隔离存放措施缺失

本判例包括以下内容：

a） 标准要求：大数据系统应保证不同客户的审计数据隔离存放。

b） 适用范围：第三级及以上大数据系统。

c） 问题描述：大数据系统不同客户的审计数据未做物理隔离也未做逻辑隔离。

d） 可能的缓解措施及风险评价：无。

C.3.11 重要接口、重要账号审计措施缺失

本判例包括以下内容：

a） 标准要求：大数据系统应对其提供的重要接口的调用情况以及各类重要账号的操作情况进行审计。

b） 适用范围：第二级及以上大数据系统。

c） 问题描述（所有）：

1） 系统无任何日志审计功能，无法对其提供的重要接口的调用情况以及重要账号的操作情况进行审计；

2） 未采取其他审计措施或其他审计措施存在漏记、旁路等缺陷，无法对系统提供的重要接口的调用情况以及重要账号的操作情况进行溯源。

d） 可能的缓解措施及风险评价：对于日志记录不全或有审计数据但无直观展示等情况，可从审计记录内容、事件追溯范围等角度进行综合风险分析，根据分析结果，酌情判定风险等级。

C.3.12 进入系统的恶意数据检测措施缺失

本判例包括以下内容：

a） 标准要求：应对所有进入系统的数据进行检测，避免出现恶意数据输入。

b） 适用范围：第三级及以上大数据系统。

c） 问题描述：无任何对重复数据、不可用数据、缺失数据、错误数据、格式不一致的数据、内容不一致的数据、异常数据、恶意代码等恶意数据输入行为的检测技术。

d） 可能的缓解措施及风险评价：无。

C.3.13 数据交换过程数据完整性保护措施缺失

本判例包括以下内容：

a） 标准要求：应采用技术手段对数据交换过程进行数据完整性检测。

b） 适用范围：第二级及以上大数据系统。

c） 问题描述：重要数据交换过程中无任何完整性保护措施，一旦数据遭受篡改，将对系统或者个人造成重大影响。

d） 可能的缓解措施及风险评价：在可控的网络中传输的情形，可从已采取安全措施，数据篡改的可能性进行综合分析，根据分析结果酌情判定风险等级。

C.3.14 大数据平台不支持静态脱敏和去标识化

本判例包括以下内容：

a） 标准要求：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） 适用范围：第二级及以上大数据平台。

c） 问题描述：大数据平台未提供静态脱敏和去标识化的工具或服务组件技术。

d） 可能的缓解措施及风险评价：无。

C.3.15 数据未脱敏

本判例包括以下内容：

a） 标准要求：应依据相关安全策略和数据分类分级标识对数据进行静态脱敏和去标识化处理。

b） 适用范围：第三级及以上大数据系统。

c） 问题描述（任意）：

1） 展示页面、存储数据或数据传输过程中存在未依据安全策略进行脱敏和去标识化的业务数据或个人敏感信息；

2） 日志文件中存储记录了未脱敏的数据接口配置、数据样本、SQL 语句等数据。

d） 可能的缓解措施及风险评价：无。

C.3.16 大量数据汇聚暴露敏感信息

本判例包括以下内容：

a） 标准要求：应采用技术措施保证汇聚大量数据时不暴露敏感信息。

b） 适用范围：第三级及以上大数据系统。

c） 问题描述：大数据系统在数据汇聚时存在暴露敏感信息的安全隐患或发生过暴露敏感信息的安全事件。

d） 可能的缓解措施及风险评价：无。

C.3.17 关键溯源数据未异地备份

本判例包括以下内容：

a） 标准要求：应提供对关键溯源数据的异地备份。

b） 适用范围：第三级及以上大数据系统。

c） 问题描述：关键溯源数据无异地备份措施或异地备份措施无法满足业务或行业主管部门要求。

d） 可能的缓解措施及风险评价：无。

C.3.18 越权处理个人信息

本判例包括以下内容：

a） 标准要求：采集、处理、使用、转让、共享、披露个人信息应在个人信息处理的授权同意范围内，并保留操作审计记录。

b） 适用范围：第二级及以上大数据系统。

c） 问题描述：超出个人信息处理的授权同意范围处理个人信息。

d） 可能的缓解措施及风险评价：无。

C.4 安全管理中心

C.4.1 接口监测措施缺失

本判例包括以下内容：

a） 标准要求：应对大数据系统提供的各类接口的使用情况进行集中审计和监测，并在发生问题时提供报警。
b） 适用范围：第三级及以上大数据系统。
c） 问题描述：对各类接口使用情况无任何监测措施，发生问题时无法提供报警。
d） 可能的缓解措施及风险评价：无。

C.5 安全管理机构

C.5.1 授权和审批缺失

本判例包括以下内容：
a） 标准要求：应建立数据导入、导出、集成、分析、交换、交易、共享及公开的授权审批控制流程，赋予数据活动主体的最小操作权限、最小数据集和权限有效时长，依据流程实施相关控制并记录过程，及时回收过期的数据访问权限。
b） 适用范围：第三级及以上大数据系统。
c） 问题描述（任意）：
1） 未建立数据导入、导出、集成、分析、交换、交易、共享及公开的授权审批控制流程和制度，并且数据访问权限管理无序，存在非授权访问、操作数据的情况；
2） 数据访问权限过期未及时收回，并导致数据安全事件的。
d） 可能的缓解措施及风险评价：无。

C.5.2 跨境数据未评估

本判例包括以下内容：
a） 标准要求：应建立跨境数据的评估、审批及监管控制流程，并依据流程实施相关控制并记录过程。
b） 适用范围：第三级及以上大数据系统。
c） 问题描述：数据出境前未开展评估、审批及监管控制。
d） 可能的缓解措施及风险评价：无。

C.6 安全运维管理

C.6.1 对外数据接口调用未获授权

本判例包括以下内容：
a） 标准要求：应建立对外数据接口安全管理机制，所有的接口调用均应获得授权和审批。
b） 适用范围：第二级及以上大数据系统。
c） 问题描述：未对所有对外数据接口调用进行授权。
d） 可能的缓解措施及风险评价：无。