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.4.3.15 测评单元(BDS-L4-15)

该测评单元包括以下要求:

a) 测评指标:大数据平台应具备对不同类别、不同级别数据全生命周期区分处置的能力。

b) 测评对象:设计文档或建设文档和大数据平台。

c) 测评实施包括以下内容:

1) 应核查设计文档或建设文档是否具备对不同类别、不同级别数据区分处置的策略或措施;

2) 应核查大数据平台不同类别、不同级别数据是否在全生命周期区分处置。

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.4.4 安全建设管理

#### B.4.4.1 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.4.4.2 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.4.4.3 测评单元（BDS-L4-03）

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.4.5 安全运维管理

#### B.4.5.1 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.4.5.2 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.4.5.3 测评单元(BDS-L4-03)

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：数据安全管理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) 应核查数据安全管理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.4.5.4 测评单元(BDS-L4-04)

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。

# 附 录 C
（规范性附录）
测评单元编号说明

## C.1 测评单元编码规则

测评单元编号为三组数据，格式为××—××××—××，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4位组成，前3位为字母，第4位为数字。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。数字代表应用场景：1为安全测评通用要求部分，2为云计算安全测评扩展要求部分，3为移动互联安全测评扩展要求部分，4为物联网安全测评扩展要求部分，5为工业控制系统安全测评扩展要求部分。

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L1-PES1-01，代表源自安全测评通用要求部分的第一级安全物理环境类的第1个指标。

## C.2 大数据可参考安全评估方法编号说明

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

第1组由3位组成，BDS代表大数据可参考安全评估方法。

第2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3组由2位数字组成，按照基本要求中的安全控制措施进行顺序编号。

**示例**：测评单元编号为BDS-L1-01，代表源自大数据可参考安全评估方法的第一级的第1个指标。

## C.3 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）

BDS：大数据系统（Bigdata System）

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）

HRS：安全管理人员（Human Resource 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）

SMC：安全管理中心（Security Management Center）

# 参 考 文 献


[1] GB/T 18336.1—2015 信息技术 安全技术 信息技术安全评估准则 第1部分:简介和一般模型

[2] GB/T 18336.2—2015 信息技术 安全技术 信息技术安全评估准则 第2部分:安全功能组件

[3] GB/T 18336.3—2015 信息技术 安全技术 信息技术安全评估准则 第3部分:安全保障组件

[4] GB/T 20269—2006 信息安全技术 信息系统安全管理要求

[5] GB/T 20270—2006 信息安全技术 网络基础安全技术要求

[6] GB/T 20271—2006 信息安全技术 信息系统通用安全技术要求

[7] GB/T 20272—2006 信息安全技术 操作系统安全技术要求

[8] GB/T 20273—2006 信息安全技术 数据库管理系统安全技术要求

[9] GB/T 20282—2006 信息安全技术 信息系统安全工程管理要求

[10] GB/T 30976.1—2014 工业控制系统信息安全 第1部分:评估规范

[11] GB/T 30976.2—2014 工业控制系统信息安全 第2部分:验收规范

[12] GB 50174—2017 数据中心设计规范

[13] YD/T 2437—2012 物联网总体框架与技术要求

[14] YDB 101—2012 物联网安全需求

[15] ISO/IEC 27000:2013 Information technology—Security techniques—Information security management systems—Overview and vocabulary

[16] ISO/IEC 27001:2013 Information technology—Security techniques—Information security management system—Requirements

[17] ISO/IEC 27002:2013 Information Technology—Security Techniques—Code of practice for information security controls

[18] ISO/IEC 27003:2013 Information technology—Security techniques—Information security management system implementation—Guidance

[19] IEC 62264-1 Enterprise—control system integration—Part 1: Models and terminology

[20] IEC 62443-1-1 Industrial communication networks—network and system security—Part 1-1: terminology, concepts and models

[21] IEC 62443-3-2 Industrial communication networks—Network and system security—Part 3-2: Security assurance levels for zones and conduits

[22] IEC 62443-3-3 Industrial communication networks—Network and system security—Part 3-3: System security requirements and security levels

[23] NIST Special Publication 800-53A:Assessing Security and Privacy Controls in Federal Information Systems and Organizations

[24] NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security

中 华 人 民 共 和 国
国 家 标 准
信息安全技术
网络安全等级保护测评要求
GB/T 28448—2019
*
中 国 标 准 出 版 社 出 版 发 行
北京市朝阳区和平里西街甲 2 号(100029)
北京市西城区三里河北街 16 号(100045)
网址:www.spc.org.cn
服务热线:400-168-0010
2019 年 4 月第一版
*
书号:155066·1-62443



GB/T 28448-2019