ICS 35.040
L 80

中华人民共和国国家标准

GB/T 28448—2019
代替 GB/T 28448—2012

信息安全技术
网络安全等级保护测评要求

Information security technology—
Evaluation requirement for classified protection of cybersecurity

2019-05-10 发布　　2019-12-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准代替 GB/T 28448—2012《信息安全技术　信息系统安全等级保护测评要求》，与 GB/T 28448—2012 相比，主要变化如下：

——将标准名称变更为《信息安全技术　网络安全等级保护测评要求》；

——每个级别增加了云计算安全测评扩展要求、移动互联安全测评扩展要求、物联网安全测评扩展要求和工业控制系统安全测评扩展要求等内容；

——增加了等级测评、测评对象、云服务商和云服务客户等相关术语和定义（见第 3 章，2012 年版的第 3 章）；

——将针对控制点的单元测评细化调整为针对要求项的单项测评，删除了“测评框架”（见 2012 年版的 4.1）和“等级测评内容”（见 2012 年版的 4.2）；

——增加了大数据可参考安全评估方法（见附录 B）和测评单元编号说明（见附录 C）。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息安全标准化技术委员会（SAC/TC 260）提出并归口。

本标准起草单位：公安部第三研究所（公安部信息安全等级保护评估中心）、中国电子技术标准化研究院、国家信息中心、中国科学院信息工程研究所（信息安全国家重点实验室）、北京大学、新华三技术有限公司、成都科来软件有限公司、中国移动通信集团有限公司、北京鼎普科技股份有限公司、北京微步在线科技有限公司、北京梆梆安全科技有限公司、北京迅达云成科技有限公司、中国电子科技集团公司第十五研究所（信息产业信息安全测评中心）、公安部第一研究所、北京信息安全测评中心、国家能源局信息中心（电力行业信息安全等级保护测评中心）、全球能源互联网研究院、北京卓识网安技术股份有限公司、中国电力科学研究院、南京南瑞集团公司、国电南京自动化股份有限公司、南方电网科学研究院、中国电子信息产业集团公司第六研究所、工业和信息化部计算机与微电子发展研究中心（中国软件评测中心）、启明星辰信息技术集团股份有限公司、北京烽云互联科技有限公司、华普科工（北京）有限公司。

本标准主要起草人：陈广勇、李明、黎水林、马力、曲洁、于东升、艾春迪、郭启全、葛波蔚、祝国邦、陆磊、张宇翔、毕马宁、沙淼淼、李升、胡红升、陈雪鸿、袁静、章恒、张益、毛澍、王斌、尹湘培、王勇、高亚楠、焦安春、赵劲涛、于俊杰、徐衍龙、马晓波、江雷、黄顺京、朱建兴、苏艳芳、禄凯、何申、霍珊珊、于运涛、陈震、任卫红、孙惠平、万晓兰、马红霞、薛锋、赵林林、刘金刚、胡越宁、周晓雪、李亚军、杨洪起、孟召瑞、李飞、王江波、阚志刚、刘健、陶源、李秋香、许凤凯、王绍杰、李晨旸、李凌、朱世顺、张五一、陈华军、张洁昕、张彪、李汪蔚、王雪、蔡学琳、胡娟、刘静、周峰、郝鑫、马闽、段伟恒。

本标准所代替标准的历次版本发布情况为：

——GB/T 28448—2012。

引　言

为了配合《中华人民共和国网络安全法》的实施，同时适应云计算、移动互联、物联网和工业控制等新技术、新应用情况下网络安全等级保护工作的开展，需对 GB/T 28448—2012 进行修订。同时，作为测评指标进行引用的 GB/T 22239—2008 也启动了修订工作。修订的思路和方法依据 GB/T 22239 调整的内容，针对共性安全保护需求提出安全测评通用要求，针对云计算、移动互联、物联网和工业控制等新技术、新应用领域的个性安全保护需求提出安全测评扩展要求，形成新的《信息安全技术　网络安全等级保护测评要求》标准。

本标准是网络安全等级保护相关系列标准之一。

与本标准相关的标准包括：

——GB/T 25058　信息安全技术　信息系统安全等级保护实施指南；

——GB/T 22240　信息安全技术　信息系统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 25070　信息安全技术　网络安全等级保护安全设计技术要求；

——GB/T 28449　信息安全技术　网络安全等级保护测评过程指南。

信息安全技术
网络安全等级保护测评要求

1 范围

本标准规定了不同级别的等级保护对象的安全测评通用要求和安全测评扩展要求。

本标准适用于安全测评服务机构、等级保护对象的运营使用单位及主管部门对等级保护对象的安全状况进行安全测评并提供指南，也适用于网络安全职能部门进行网络安全等级保护监督检查时参考使用。

注：第五级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测评要求，所以不在本标准中进行描述。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB 17859—1999 计算机信息系统 安全保护等级划分准则

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 25069 信息安全技术 术语

GB/T 25070—2019 信息安全技术 网络安全等级保护安全设计技术要求

GB/T 28449—2018 信息安全技术 网络安全等级保护测评过程指南

GB/T 31167—2014 信息安全技术 云计算服务安全指南

GB/T 31168—2014 信息安全技术 云计算服务安全能力要求

GB/T 32919—2016 信息安全技术 工业控制系统安全控制应用指南

3 术语和定义

GB 17859—1999、GB/T 25069、GB/T 22239—2019、GB/T 25070—2019、GB/T 31167—2014、GB/T 31168—2014 和 GB/T 32919—2016 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 31167—2014 和 GB/T 31168—2014 中的一些术语和定义。

3.1

访谈 interview

测评人员通过引导等级保护对象相关人员进行有目的的(有针对性的)交流以帮助测评人员理解、澄清或取得证据的过程。

3.2

核查 examine

测评人员通过对测评对象(如制度文档、各类设备及相关安全配置等)进行观察、查验和分析，以帮助测评人员理解、澄清或取得证据的过程。

3.3

测试 test

测评人员使用预定的方法/工具使测评对象(各类设备或安全配置)产生特定的结果，将运行结果与

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