doi :10.3969/j.issn.1671-1122.2019.07.001

《信息安全技术 网络安全等级保护测评要求》（GB/T 28448–2019）标准解读

陈广勇[1]，祝国邦[2]，范春玲[2]

（1. 公安部信息安全等级保护评估中心，北京 100142；2. 公安部网络安全保卫局，北京 100741）

摘　要：《信息安全技术 网络安全等级保护测评要求》（GB/T 28448–2019）已正式发布实施。文章介绍了 GB/T 28448–2019 的修订背景和进程、与 GB/T 28448–2012 比较发生的主要变化、安全测评通用要求和安全测评扩展要求的主要内容等，目的是使用户更好地了解和掌握 GB/T 28448–2019 的内容。

关键词：等级保护；等级保护对象；等级测评；安全测评通用要求；安全测评扩展要求

中图分类号：TP309　**文献标识码：**A　**文章编号：**1671-1122（2019）07-0001-07

中文引用格式：陈广勇，祝国邦，范春玲.《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019）标准解读 [J]. 信息网络安全，2019，19（7）：1–7.

英文引用格式：CHEN Guangyong, ZHU Guobang, FAN Chunling. *Information Security Technology—Evaluation Requirement for Classified Protection of Cybersecurity*(GB/T 28448-2019) Standard Interpretation[J]. Netinfo Security, 2019, 19(7): 1–7.

Information Security Technology—Evaluation Requirement for Classified Protection of Cybersecurity(GB/T 28448-2019) Standard Interpretation

CHEN Guangyong[1], ZHU Guobang[2], FAN Chunling[2]

(1. *Information Classified Security Protection Evaluation Center of the Ministry of Public Security, Beijing* 100142, *China*; 2. *Cyber Security Department of the Ministry of Public Security, Beijing* 100741, *China*)

Abstract: *Evaluation requirements for classified protection of cybersecurity*(GB/T 28448-2019) will be formally implemented soon. This paper introduces the revision background and process of this standard, the main changes in comparison with GB/T 28448-2012, the main contents of security general requirements and security special requirements, etc., so that to the main contents can be understood better.

Key words: classified protection; classified protection object; evaluation for classified protection; security general requirements; security special requirements

收稿日期：2019–6–10

作者简介：陈广勇（1973—），男，天津，副研究员，硕士，主要研究方向为信息技术、网络安全；祝国邦（1979—），男，吉林，副研究员，硕士，主要研究方向为信息技术、网络安全、等级保护；范春玲（1976—），女，吉林，副研究员，硕士，主要研究方向为信息技术、网络安全、等级保护。

通信作者：陈广勇 chen.guangyong@cspec.org.cn

0 引言

信息系统等级保护系列国家标准在我国推行信息安全工作开展过程中发挥了重要作用，被广泛应用于网络安全职能部门、各行业和领域的网络安全管理部门及等级测评机构开展系统定级、安全建设整改、等级测评、安全自查和安全监督检查等相关工作[1]。但随着IT技术的飞速发展，特别是在云计算、移动互联、物联网、工业控制和大数据等新技术、新应用环境下，GB/T 22239-2008《信息安全技术 信息系统安全等级保护基本要求》和GB/T 28448-2012《信息安全技术 信息系统安全等级保护测评要求》[2,3]在应用过程中遇到了一些新的问题，在适用性、时效性、易用性、可操作性上需要进一步完善。2017年6月1日颁布实施的《中华人民共和国网络安全法》也要求各网络安全职能部门、各行业和领域的网络安全管理部门等配合落实国家网络安全等级保护制度[4]，需要同时对GB/T 22239-2008《信息安全技术 信息系统安全等级保护基本要求》和GB/T 28448-2012《信息安全技术 信息系统安全等级保护测评要求》进行修订[5]。为适应我国网络安全等级保护工作发展的需要，进一步与新版的GB/T 22239-2019[6,7]相协调，有必要对GB/T 28448-2012进行修订。

2014年，公安部第三研究所（公安部信息安全等级保护评估中心）根据国家标准编号制修订计划，牵头组织了对GB/T 28448-2012的修订工作，前后共有20多家单位、70多人参与修订工作。修订工作历经调查研究、草案形成、征求意见稿、送审稿和报批稿等过程[8,9]，收到了各行业职能部门、用户、专家的宝贵意见。2019年，《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019）国家标准正式实施。本文分析了GB/T 28448-2019发生的主要变化，解读其内容修订和等级测评工作变化等主要内容，以便读者更好地了解和掌握GB/T 28448-2019的内容。

1 标准主要内容变化

1.1 标准文本结构变化

GB/T 28448-2019标准文本分为12章，3个附录。第1章、第2章、第3章为标准的常规性描述，包括范围、规范性引用文件、术语和定义；第4章为缩略语；第5章概要描述了安全等级保护测评方法及单项测评和整体测评的构成。

第6章、第7章、第8章、第9章为重点章节，分别描述了第一级、第二级、第三级、第四级测评要求，以及每级如何遵从GB/T 22239-2019的框架描述实施测评工作。每个级别都由五部分内容组成，包括安全通用要求、云计算、移动互联、物联网和工业控制系统等相关测评实施内容。安全技术方面从安全物理环境、安全通信网络、安全区域边界、安全计算环境和安全管理中心5个方面展开；安全管理方面从安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理5个方面展开，与《基本要求》形成了相互对照、和谐统一的标准文本结构。

第10章为略掉的第五级测评要求。第11章描述了系统整体测评方法，在单项测评的基础上，从系统整体的角度综合考虑如何进行系统性的测评。分别从安全控制点测评、安全控制点间测评和区域间测评（包含层面间测评）等3个方面进行描述，分析了在进行系统整体测评时需要考虑的内容。第12章概要说明了测评结论的得出方法及测评结论主要包括的内容等。

附录A描述了各种测评方法的测评强度，并具体描述了针对不同等级保护对象的测评强度。附录B描述了大数据的可参考安全评估方法。附录C描述了测评指标编码规则及专用缩略语。

1.2 等级测评内容的变化

由于等级保护对象的内涵发生变化，GB/T 28448-2019按照应用领域分为安全测评通用要求和安全测评扩展要求。安全测评通用要求是指不管等级保护对

象形态如何，均需遵循的安全测评要求。安全测评扩展要求是指针对云计算安全扩展要求、大数据安全扩展要求、移动互联安全扩展要求、物联网安全扩展要求和工业控制系统安全扩展要求提出的特殊安全测评要求。

1.3 等级测评技术框架的变化

等级测评技术框架由原标准的单元测评和整体测评调整为单项测评和整体测评。

单项测评是针对安全控制点下的各安全要求项的测评，支持测评结果的可重复性和可再现性。单项测评由四部分内容组成，分别是测评指标、测评对象、测评实施和单元判定。修订后的单项测评中测评指标更加细化，由针对原标准中的安全控制点的测评调整为针对安全控制点下的安全要求项的测评，更有助于测评实施工作的开展。

整体测评是在单项测评基础上，对定级对象整体安全保护能力的判断。整体测评内容由原标准的安全控制点间测评、层面间测评和区域间测评等方面调整为安全控制点测评、安全控制点间测评和区域间测评（包含层面间测评）。

另外，为了更好地让测评人员明确测评工作的作用对象，在测评单元中增加测评对象。测评对象是指等级测评过程中不同测评方法作用的对象，主要涉及相关配套制度文档、设备设施及人员等。

1.4 测评方法的变化

测评方法包括访谈、核查和测试。访谈是指测评人员通过引导等级保护对象相关人员进行有目的、有针对性的交流，帮助测评人员理解、澄清或取得证据的过程。核查是指测评人员通过对测评对象（如各类设备、各类系统软件和制度文档等）进行观察、查验和分析，帮助测评人员理解、澄清或取得证据的过程。测试是指测评人员使用预定的方法/工具使测评对象产生特定的结果，并将运行结果与预期的结果进行比对的过程。

新版标准在配置核查和测试验证方面要求更加严格。测评结果判定要求采信配置核查结果，同时要求对安全策略进行测试验证。测试验证包括漏洞扫描、策略有效性验证、数据抓包分析、数据通信监听、数据备份恢复、应急响应和渗透测试等。

1.5 测评要求在级差上的变化

等级测评强度由测评广度和测评深度来描述。测评广度越大，范围越大，包含的测评对象就越多，测评实际投入程度越高。测评深度越深，越需要在细节上展开，测评实际投入程度也越高。表1从测评广度和测评深度两方面详细分析了不同测评方法的测评力度在不同级别的等级保护对象安全测评中的具体体现。

表 1 不同级别的等级保护对象的测评力度要求

测评力度	测评方法	第一级	第二级	第三级	第四级
广度	访谈	测评对象在种类和数量上抽样，种类和数量都较少	测评对象在种类和数量上抽样，种类和数量都较多	测评对象在数量上抽样，在种类上基本覆盖	测评对象在数量上抽样，在种类上全部覆盖
	核查				
	测试				
深度	访谈	简要	充分	较全面	全面
	核查				
	测试	功能测试	功能测试	功能测试和测试验证	功能测试和测试验证

测评的广度和深度落实到访谈、核查和测试3种不同的测评方法上，能够体现出测评实施过程中访谈、核查和测试的投入程度的不同。对于不同等级的测评工作的强度可由以下3个方面来体现：

1）使用不同测评方法

在实际现场测评实施过程中，安全技术方面的测评方法以配置核查和测试验证为主。安全管理方面可以使用访谈方式进行测评。使用不同测评方法能体现出测评实施过程中访谈、核查和测试的测评强度的不同。

2）不同级别测评对象范围不同

第一级和第二级测评对象的范围为关键设备，第三级为主要设备，第四级为所有设备。不同级别测评对象范围不同，能体现出测评实施过程中访谈、核查和测试的测评广度的不同。

3）不同级别现场测评实施工作不同

第一级和二级以核查安全机制为主，第三级和第四级先核查安全机制，再测试验证安全策略的有效性。

2 新标准下的等级测评

2.1 标准使用

在针对某级别等级保护对象进行等级测评时，无论该等级保护对象使用何种特定技术或处于何种特定的应用场景，都必须使用安全测评通用要求对等级保护对象进行测评，再结合等级保护对象采用的具体技术架构或应用场景选用相关安全测评扩展要求进行等级测评。例如，某单位的等级保护对象采用了云计算技术和大数据技术，在进行等级测评时，首先使用GB/T 28448中的安全测评通用要求部分，再使用大数据安全测评扩展要求部分和云计算安全测评扩展要求部分进行等级测评。

2.2 测评对象选择

由于新技术新应用的迅速发展，等级保护对象的形态发生了变化，导致等级测评对象也发生了变化。以云计算平台和传统信息系统的测评对象为例，测评对象选择如表2所示。

表 2 测评对象选择

安全类或层面	云计算平台测评对象	传统测评对象
安全物理环境	机房及基础设施	机房及基础设施
安全通信网络	网络结构、通信传输设备、可信验证设备、虚拟化网络结构	传统网络设备、传统安全设备、传统网络结构
安全区域边界	网络设备、安全设备、虚拟网络设备、虚拟安全设备	传统网络设备、传统安全设备、传统网络结构
安全计算环境	网络设备、安全设备、虚拟网络设备、虚拟安全设备、物理机、宿主机、虚拟机、虚拟机监视器、云管理平台、数据库管理系统、终端、应用系统、云应用开发平台、中间件、云业务管理系统、配置文件、镜像文件、快照、业务数据、用户隐私、鉴别信息等	传统主机、数据库管理系统、终端、应用系统、中间件、配置文件、业务数据、用户隐私、鉴别信息等

由表2可以看出，与传统信息系统相比，采用新技术新应用的等级保护对象的测评对象发生了很大变化。在进行等级测评时，应根据被测等级保护对象采用新技术新应用的情况，依据测评对象选择规则合理选择测评对象。

2.3 测评作业指导书开发

测评作业指导书的开发包括安全物理环境（包括相应的安全扩展要求）、安全通信网络（包括相应的安全扩展要求）、安全区域边界（包括相应的安全扩展要求）、安全计算环境（包括相应的安全扩展要求）、安全管理中心（包括云计算安全扩展要求）和安全管理（包括相应的安全扩展要求）等方面，其中，安全物理环境、安全通信网络、安全区域边界、安全管理中心和安全管理等为全局性测评，安全计算环境需要根据设备类型和型号分别制定作业指导书。

以云计算平台的安全区域边界和安全计算环境为例，安全区域边界属于全局性测评，此部分测评作业指导书的指标项和测评实施项来源于安全测评通用要求和云计算安全测评扩展要求中的相关部分。由于安全计算环境部分的测评作业指导书与设备类型和型号相关，所以可能涉及的作业指导书包括路由器（包括虚拟路由器）安全测评作业指导书、交换机（包括虚拟交换机）安全测评作业指导书、防火墙（包括虚拟防火墙）安全测评作业指导书、操作系统（包括虚拟机）安全测评作业指导书、数据库安全测评作业指导书、宿主机操作系统安全测评作业指导书和云操作系统安全测评作业指导书等。

2.4 单项测评

单项测评从安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理、安全物理环境、安全通信网络、安全区域边界、安全计算环境和安全管理中心十个方面逐一展开。

1）安全物理环境单项测评

安全物理环境的单项测评主要针对机房的基础物理设施环境及相关的硬件设备和介质等进行。部分安全物理环境安全的测评涉及终端所在的办公场地。测评的主要内容包括物理位置选择、物理访问控制、防雷、防火、防水、防潮、防盗窃、防破坏、温湿度控制、电力供应、电磁防护等。测评对象包括各种制度类、规程类、记录和证据类等文档，各类安全管理人

员和机房各类基础设备。其中，各类安全管理人员主要为安全主管、系统管理员、审计管理员、安全管理员和其他相关人员；机房各类基础设备包括电子门禁系统、机房监控系统、防盗报警系统、防感应雷措施、火灾自动检测、报警和灭火、温湿度自动调控、UPS、备用发电系统和屏蔽机柜/机房等。

2）安全通信网络单项测评

安全通信网络的单项测评主要针对组织中的数据通信网络进行，由网络设备、安全设备和通信链路及其组件构成，目的是保证等级保护对象各个部分进行安全通信传输。测评内容主要包括网络架构、通信传输和可信验证等。测评对象包括路由器、交换机、无线接入设备和防火墙等提供网络通信功能的设备或相关组件，综合网管系统和相应设计/验收文档等。

3）安全区域边界单项测评

安全区域边界的单项测评主要针对系统边界进行，系统边界一般包括整网互联边界和不同级别系统之间的边界。测评内容主要包括边界防护、访问控制、入侵防范、恶意代码、反垃圾邮件防范和安全审计等。测评对象包括网闸、防火墙、路由器、交换机和无线接入网关设备等提供访问控制功能的设备或相关组件，抗APT攻击系统、网络回溯系统、威胁情报检测系统、抗DDoS攻击系统和入侵保护系统或相关组件，防病毒网关和UTM等提供防恶意代码功能的系统或相关组件，防垃圾邮件网关等提供防垃圾邮件功能的系统或相关组件，终端管理系统或相关设备等。

4）安全计算环境单项测评

安全计算环境的单项测评主要针对构成等级保护对象的所有设备节点进行。测评内容主要包括身份鉴别、访问控制、安全审计、可信验证、入侵防范、恶意代码防范、数据完整性、数据保密性、数据备份恢复和个人信息保护等。测评对象包括终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟网络设备）、安全设备（包括虚拟安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等、提供可信验证的设备或组件和提供集中审计功能的系统等。

5）安全管理中心单项测评

安全管理中心的单项测评主要针对相关的集中安全管理系统进行。测评内容主要包括系统管理、审计管理、安全管理和集中管控等。测评对象主要包括提供集中系统管理功能的系统、安全审计系统等提供集中审计功能的系统和综合网管系统等提供运行状态监测功能的系统等。

6）安全管理方面的单项测评

安全管理方面的单项测评主要包括安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维5个方面。测评对象主要包括人员和文档。人员包括系统管理员、安全审计员、安全管理员、机房管理员和文档管理员等。文档包括管理文档（策略、制度、规程），记录类文档（会议记录、运维记录）和其他类文档（机房验收证明等）。

2.5 整体测评

等级保护对象整体测评需要从安全控制点测评、安全控制点间测评和区域间测评等方面进行综合安全分析，从而给出等级测评结论。

1）安全控制点测评

安全控制点测评是指对单个控制点中所有要求项的符合程度进行分析和判定。在单项测评完成后，如果该安全控制点下的所有要求项为符合，则该安全控制点符合；否则，为不符合或部分符合。

2）安全控制点间测评

安全控制点间测评的目的是确定安全问题之间的关联对定级对象整体安全保护能力的影响，所以需要从同一安全类或层面内的两个或两个以上不同安全控

制点间的测评结果进行关联综合分析。在单项测评工作完成后应进行安全控制点间测评，汇总统计定级对象的某个安全控制点中的要求项存在不符合或部分符合的情况，综合分析在同一安全类或层面内是否存在不同安全控制点之间具有增强或削弱的作用（如物理访问控制和防盗窃、身份鉴别和访问控制等）。同时分析是否存在与该要求项具有相似的安全功能的安全技术措施或管理措施等相关工作。

根据安全控制点间测评结果，综合分析判断其相对应的安全保护能力是否缺失，如果经过综合分析其相关联的安全问题不会造成定级对象整体安全保护能力的缺失，则该安全控制点测评结果应调整为符合。

3）区域间测评

区域间测评的目的是确定安全问题之间的关联对定级对象整体安全保护能力的影响，所以需要从不同功能区域间或不同控制方式之间的关联进行测评分析。在单项测评工作完成后应进行区域间测评，汇总统计定级对象的某个安全控制点下的安全要求项不符合或部分符合的情况。分析在互连互通的不同安全区域之间，是否存在区域间安全功能的相互增强或削弱等作用，重点分析定级对象的访问控制路径，如不同功能区域间的数据流流向和控制方式。

根据区域间测评结果，综合分析判断与其相对应的安全保护能力是否缺失，如果经过综合分析其相关联的安全问题不会造成定级对象整体安全保护能力的缺失，则该安全控制点测评结果应调整为符合。

2.6 测评结论形成

等级测评结论的形成需要分析汇总单项测评结果中存在的不符合项或部分符合项，采用风险分析方法对所有安全问题进行风险评价，通过整体测评再对安全问题进行关联分析，分析安全问题被威胁利用的可能性，判断其被威胁利用后对业务系统安全造成的影响程度。综合评价这些安全问题对定级对象造成的安全风险，并给出等级保护对象的等级测评结论。等级测评结论包括符合、基本符合和不符合3类，具体描述如下：

1）符合

定级对象未发现安全问题，单项测评结果中部分符合和不符合项的统计结果全为0，综合得分为100分。

2）基本符合

定级对象存在安全问题，部分符合和不符合项的统计结果不全为0，但存在的安全问题不会导致定级对象面临高等级安全风险，且综合得分不低于阈值。

3）不符合

定级对象存在安全问题，部分符合项和不符合项的统计结果不全为0，且存在的安全问题会导致定级对象面临高等级安全风险，或者综合得分低于阈值。

3 结束语

GB/T 28448-2019已经正式发布实施，与GB/T 28448-2012相比，其标准文本结构和内容都发生了很大变化，对安全测评服务机构、等级保护对象的运营使用单位及主管部门的等级保护推进工作产生较大影响。本文通过深入分析新标准GB/T 28448-2019的主要变化，着重介绍了如何基于新标准开展等级测评工作，从而帮助安全测评服务机构、等级保护对象的运营使用单位及主管部门更好地了解和掌握新标准的主要内容，同时也为网络安全职能部门开展执法检查提供参考。（责编 潘海洋）

参考文献：

[1] QU Jie, FAN Chunling, CHEN Guangyong, et al. Research on Establishment of Network Security Service Ability System for A New Era[J]. Netinfo Security, 2019, 19(1): 83-87.
曲洁，范春玲，陈广勇，等. 新时代下网络安全服务能力体系建设思路 [J]. 信息网络安全，2019，19（1）：83-87.

[2] GB/T 22239-2008. Information Security Technology-Baseline for Classified Protection of Information System Security[S]. Beijing:

Standards Press of China, 2008.
GB/T 22239–2008. 信息安全技术信息系统安全等级保护基本要求 [S]. 北京：中国标准出版社，2008.
[3] GB/T 28448–2012. Information Security Technology—Testing and Evaluation Requirement for Classified Protection of Information System[S]. Beijing: Standards Press of China, 2012.
GB/T 28448–2012. 信息安全技术信息系统安全等级保护测评要求 [S]. 北京：中国标准出版社，2012.
[4] Cybersecurity Law of the People's Republic of China[EB/OL]. http://www.npc.gov.cn/npc/, 2016–11–7.
中华人民共和国网络安全法 [EB/OL]. http://www.npc.gov.cn/npc/, 2016–11–7.
[5] GUO Qiquan. Training Course on Cybersecurity Law and Classified Protection of Cybersecurity[M]. Beijing: Publishing House of Electronics Industry, 2018.
郭启全 . 网络安全法与网络安全等级保护制度培训教程 [M]. 北京：电子工业出版社，2018.
[6] MA Li, ZHU Guobang, LU Lei, et al. *Baseline for Classified Protection of Cybersecurity*(GB/T 22239–2019) Standard Interpretation[J]. Netinfo Security, 2019, 19(2): 77–84.
马力，祝国邦，陆磊，等 .《网络安全等级保护基本要求》（GB/T 22239–2019）标准解读 [J]. 信息网络安全，2019，19（2）：77–84.
[7] GB/T 22239–2019. Information Security Technology—Baseline for Classified Protection of Cybersecurity[S]. Beijing: Standards Press of China, 2019.
GB/T 22239–2019. 信息安全技术网络安全等级保护基本要求 [S]. 北京：中国标准出版社，2019.
[8] National Information Security Standardization Technical Committee. Information Security Technology—Baseline for Classified Protection of Cybersecurity(Draft)[EB/OL]. https://www.tc260.org.cn/, 2018–10–31.
全国信息安全标准化技术委员会 . 信息安全技术网络安全等级保护基本要求（征求意见稿）[EB/OL]. https://www.tc260.org.cn/, 2018–10–31.
[9] National Information Security Standardization Technical Committee. Information Security Technology—Evaluation Requirement for Classified Protection of Cybersecurity(Draft)[EB/OL]. https://www.tc260.org.cn/, 2018–10–31.
全国信息安全标准化技术委员会 . 信息安全技术网络安全等级保护测评要求（征求意见稿）[EB/OL]. https://www.tc260.org.cn/, 2018–10–31.