**信息安全技术 网络安全等级保护测评要求**

**第1部分：安全通用要求**

**编制说明**

# 概述

## 任务来源

《信息安全技术 信息系统安全等级保护测评要求》于2012年成为国家标准，标准号为GB/T 28448-2012，被广泛应用于各个行业的开展等级保护对象安全等级保护的检测评估工作。但是随着信息技术的发展，尤其云计算、移动互联网、物联网和大数据等新技术的发展，该标准在时效性、易用性、可操作性上还需进一步提高，2013年公安部第三研究所联合中国电子技术标准化研究院和北京神州绿盟科技有限公司向安标委申请对GB/T 28448-2012进行修订。

根据全国信息安全标准化技术委员会2013年下达的国家标准制修订计划，国家标准《信息安全技术 信息系统安全等级保护测评要求》修订任务由公安部第三研究所负责主办，项目编号为2013bzxd-WG5-006。

## 制定本标准的目的和意义

《信息安全等级保护管理办法》（公通字[2007]43号）明确指出信息系统运营、使用单位应当接受公安机关、国家指定的专门部门的安全监督、检查、指导，而且等级测评的技术测评报告是其检查内容之一。这就要求等级测评过程规范、测评结论准确、公正及可重现。

《信息安全技术 信息系统安全等级保护基本要求》（GB/T22239-2008）（简称《基本要求》）和《信息安全技术 信息系统安全等级保护测评要求》（GB/T28448-2012）（简称《测评要求》）等标准对近几年来全国信息安全等级保护工作的推动起到了重要的作用。

伴随着IT技术的发展，《基本要求》中的一些内容需要结合我国信息安全等级保护工作的特点，结合信息技术发展尤其是信息安全技术发展的特点，比如无线网络的大量使用，数据大集中、云计算等应用方式的普及等，需要针对各等级系统应当对抗的安全威胁和应具有的恢复能力，提出新的各等级的安全保护目标。

作为《基本要求》的姊妹标准，《测评要求》需要同步修订，依据《基本要求》的更新内容对应修订相关的单元测评章节。

此外，《测评要求》还需要吸收近年来的测评实践，更新整体测评方法和测评结论形成方法。

## 与其他标准的关系



**图1 等级保护标准相互关系**

从上图可以看出，在等级保护对象实施安全保护过程中，首先利用《信息安全技术 信息系统安全等级保护定级指南》（GB/T 22240-2008）（简称“《定级指南》”）确定等级保护对象的安全保护等级，然后根据《信息安全技术 网络安全等级保护基本要求》系列标准选择安全控制措施，随后利用《信息安全技术 信息系统安全等级保护实施指南》（简称“《实施指南》”）或其他相关标准确定其特殊安全需求，进行等级保护对象的安全规划和建设工作，此后利用《信息安全技术 网络安全等级保护测评过程指南》（GB/T 28449-20XX）（简称“《测评过程指南》”）来规范测评过程和各项活动，利用《信息安全技术 网络安全等级保护测评要求》系列标准来判断安全控制措施的有效性。同时，等级保护整个实施过程又是由《实施指南》来指导的。

在等级保护的相关标准中，《测评要求》系列标准是《基本要求》系列标准的姊妹篇，《测评要求》针对《基本要求》中各要求项，提供了具体测评方法、步骤和判断依据等，是为了确认等级保护对象是否按照《基本要求》中的不同等级的技术和管理要求实施的，而《测评过程指南》则是规定了开展这些测评活动的基本过程，包括过程、任务及产品等，以指导用户对《测评要求》的正确使用。

## 标准组成

为了适应移动互联、虚拟计算、云计算、物联网、工控系统和大数据等新技术、新应用情况下网络安全等级保护测评工作的开展，需对GB/T 28448-2012进行修订，修订的思路和方法是针对移动互联、虚拟计算、云计算、物联网、工控系统和大数据等新技术、新应用领域提出扩展的测评要求。

对GB/T 28448-2012的修订完成后，测评要求标准成为由多个部分组成的系列标准，目前主要有六个部分：

——GB/T 28448.1-20XX 信息安全技术 网络安全等级保护测评要求 第1部分：安全通用要求；

——GB/T 28448.2-20XX 信息安全技术 网络安全等级保护测评要求 第2部分：云计算安全扩展要求；

——GB/T 28448.3-20XX 信息安全技术 网络安全等级保护测评要求 第3部分：移动互联安全扩展要求；

——GB/T 28448.4-20XX 信息安全技术 网络安全等级保护测评要求 第4部分：物联网安全扩展要求；

——GB/T 28448.5-20XX 信息安全技术 网络安全等级保护测评要求 第5部分：工控控制安全扩展要求；

——GB/T 28448.6-20XX 信息安全技术 网络安全等级保护测评要求 第6部分：大数据安全扩展测评要求。

# 编制过程

1）2013年12月，公安部第三研究所、中国电子技术标准化研究院和北京神州绿盟科技有限公司成立了《信息安全技术 信息安全等级保护测评要求》标准编制组。

2）2014年1月至5月，标准编制组按照计划调研了国际和国内无线接入、虚拟计算、云计算平台、大数据应用和工控系统应用等新技术、新应用的情况，分析并总结了新技术和新应用中的安全关注点和要素；同时标准编制组调研了与《信息安全技术 信息系统安全等级保护测评要求》(GB/T 28448-2012)相关的其他国家标准和行业标准，分析了《信息安全技术 信息系统安全等级保护基本要求》(GB/T 22239-2008)的修订可能对其产生的影响。

3）2014年5月，为适应无线移动接入、虚拟计算环境、云计算平台应用、大数据应用和工控系统应用等新技术、新应用的情况下等级保护工作开展，公安部十一局牵头会同有关部门组织2014年新领域的国家标准立项，根据新标准立项结果确定《基本要求》修订思路发生重大变化，为适应《基本要求》修订思路的变化在《信息安全技术 信息系统安全等级保护测评要求》（GB/T 28448-2012）的基础上，针对无线移动接入、虚拟计算环境、云计算平台应用、大数据应用和工控系统应用等新领域形成“测评要求”的分册，如《信息安全技术 网络安全等级保护测评要求 第2部分： 云计算安全扩展要求》、《信息安全技术 网络安全等级保护测评要求 第3部分：移动互联安全扩展要求》、《信息安全技术 网络安全等级保护测评要求 第4部分：物联网安全扩展要求》、《信息安全技术 网络安全等级保护测评要求 第5部分：工控控制安全扩展要求》和《信息安全技术 网络安全等级保护测评要求 第6部分：大数据安全扩展要求》。构成GB/T 28448.1、GB/T 28448.2、……等测评要求系列标准，上述思路的变化直接影响了国家标准GB/T 28448-2012的修订思路和内容。

5）2014年7月至2015年5月，标准编制组根据新修订《基本要求》草案第一稿编制了《信息安全技术 网络安全等级保护测评要求 第1部分：安全通用要求》草案第一稿。

6）2015年5月至2015年12月，标准编制组根据新修订《基本要求》草案第三稿编制了《信息安全技术 网络安全等级保护测评要求 第1部分：安全通用要求》草案第二稿。

7）2016年5月至2016年6月，标准编制组根据新修订《基本要求》草案第五稿编制了《信息安全技术 网络安全等级保护测评要求 第1部分：安全通用要求》草案第三稿。

8）2016年5月23日，在评估中心针对《信息安全技术 网络安全等级保护测评要求 第1部分：安全通用要求》草案第三稿进行行业内专家评审会。

9）2016年7月，标准编制组根据新修订《基本要求》草案第六稿和第七稿编制了《信息安全技术 网络安全等级保护测评要求 第1部分：安全通用要求》草案第四稿。

9）2016年7月-8月，将《信息安全技术 网络安全等级保护测评要求 第1部分：安全通用要求》草案第四稿发送11家等级测评机构和WG5工作组成员单位征求意见。

10）2016年8月12日，在北京瑞安宾馆第五会议室召开WG5工作组部分专家评审会，针对《信息安全技术 网络安全等级保护测评要求 第1部分：安全通用要求》草案第四稿征求意见。

11）2016年8月25日，在北京瑞安宾馆第二会议室参加WG5工作组在研标准推进会，在会上征求所有WG5工作组成员单位意见。

12）根据专家意见已经修订完成，形成《信息安全技术 网络安全等级保护测评要求 第1部分：安全通用要求》草案第五稿。

13）根据测评机构反馈意见修订完成，形成《信息安全技术 网络安全等级保护测评要求 第1部分：安全通用要求》草案第六稿。

14）前正在推进《测评要求》后续专标准修订工作。

# 标准编制的技术路线

安全等级保护测评（以下简称等级测评）的概念性描述框架由两部分构成：单项测评和整体测评，图1给出了等级测评框架。



**图1 等级测评描述框架**

针对基本要求各安全要求项的测评称为单项测评，单项测评是等级测评工作的基本活动，支持测评结果的可重复性和可再现性。单项测评是由测评指标、测评对象、测评实施和单元判定构成。

本部分的测评指标包括《信息安全技术 网络安全等级保护基本要求 第1部分：安全通用要求》第四级目录下的要求项。

测评对象是指测评实施的对象，即测评过程中涉及到的制度文档、各类设备及其安全配置和相关人员等。对于框架来说，每一个被测安全要求项（不同级别）均有一组与之相关的预先定义的测评对象（如制度文档、各类设备设施及相关人员等）。

制度文档是指针对等级保护对象所制定的相关联的文件（如：政策、程序、计划、系统安全需求、功能规格及建筑设计）。各类设备是指安装在等级保护对象之内或边界，能起到特定保护作用的相关部件（如：硬件、软件、固件或物理设施）。相关人员或部门，是指应用上述制度、设备及安全配置的人。

测评实施是一组针对特定测评对象，采用相关测评方法，遵从一定的测评规程所形成的，用于测评人员使用的确定该要求项有效性的程序化陈述。测评实施主要由测评方法和测评规程构成。其中测评方法包括：访谈、检查和测试（说明见术语），测评人员通过这些方法试图获取证据。上述的评估方法都由一组相关属性来规范测评方法的测评力度。这些属性是：广度（覆盖面）和深度。对于每一种测评方法都标识(定义）了唯一属性，深度特性适用于访谈和检查，而覆盖面特性则适用于全部三种测评方法。上述三种测评方法（访谈、检查和测评）的测评结果都用以对安全控制的有效性进行评估。测评规程是各类测评方法操作使用的过程、步骤，测评规程实施完成后，可以获得相应的证据。

结果判定描述测评人员执行测评实施并产生各种测评输出数据后，如何依据这些测评输出数据来判定被测系统是否满足测评指标要求的原则和方法。通过测评实施所获得的所有证据都满足要求则为符合，不全满足要求则该单项要求不符合。

整体测评是在单项测评基础上，分别从安全控制点测评，安全控制点间和层面间三个角度分别进行测评。

# 标准总体框架

本标准共分为11章，4个附录，每章内容如下：

第1、2、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，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组成；

第5、6、7、8章，分别描述了第一、二、三、四级测评要求，每级分别遵从《基本要求》的框架从安全技术和安全管理两大方面描述如何实施测评工作，其中技术方面分别从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全四个层面展开；而管理方面则分别从安全策略和管理制度、安全管理机构和人员、安全建设管理和安全系统运维管理四个方面展开，与《基本要求》形成了相互对照、和谐统一的标准体系。

第9章，略掉第五级的测评要求。

第10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、安全控制点间及层面间测评三方面进行描述，分析了在进行系统测评时所需考虑的方向和指导思想。

第11章，概要说明了给出测评结论的方法，测评结论主要应该包括哪些方面的内容等。

附录A，描述了各种测评方法的测评强度，并具体描述针对不同等级保护对象的测评强度。

附录B，描述了测评指标编码规则及专用缩略语。

附录C，描述了设计要求测评验证内容。

附录D，为基本要求的要求项和测评要求的测评单元索引表。

# 主要章节的编写方法

第5、6、7、8章分别描述了第一级、第二级、第三级和第四级所有测评要求的内容，在章节上分别对应国标GB/T 22239.1-2XXX的第5章到第8章。在国标GB/T 22239.1-20XX第5章到第8章中，各章的二级目录都分为安全技术和安全管理两部分，三级目录从安全层面（如物理和环境安全、网络和通信安全、设备和计算安全等）进行划分和描述，四级目录按照安全控制点进行划分和描述（如设备和计算安全层面下分为身份鉴别、访问控制、安全审计等），第五级目录是每一个安全控制点下面包括的具体安全要求项。具体编制案例如下。

*案例：*

*7 第三级测评要求*

*7.1 安全技术单项测评*

*7.1.1 物理和环境安全*

*7.1.1.1 物理位置的选择*

*7.1.1.1.1 测评单元（L3-PES1-01）*

*a) 测评指标*

*机房场地应选择在具有防震、防风和防雨等能力的建筑内；（本条款引用自GB/T 22239.1-20XX 7.1.1.1 a））*

*b) 测评对象*

*记录类文档、机房。*

*c) 测评实施*

*1) 应核查所在建筑物是否具有建筑物抗震设防审批文档；*

*2) 应核查机房是否不存在雨水渗漏；*

*3) 应核查门窗是否不存在因风导致的尘土严重；*

*4) 应核查屋顶、墙体、门窗和地面等是否不存在破损开裂。*

*d) 单元判定*

*如果1）-4）均为肯定，则等级保护对象符合本测评单元指标要求，否则，等级保护对象不符合或部分符合本测评单元指标要求。*

*7.1.1.1.2 测评单元（L3-PES1-02）*

*a) 测评指标*

*机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。（本条款引用自GB/T 22239.1-20XX 7.1.1.1 b））*

*b) 测评对象*

*机房。*

*c) 测评实施*

*1) 应核查是否不位于所在建筑物的顶层或地下室，如果否，则核查是否采取了防水和防潮措施。*

*d) 单元判定*

*如果以上测评实施内容为肯定，则等级保护对象符合本测评单元指标要求，否则，等级保护对象不符合本测评单元指标要求。*

**信息安全技术 网络系统安全等级保护测评要求**

**第1部分：安全通用要求编写组**

**2016年10月**