ICS 35.020
L 80

中华人民共和国国家标准

GB/T 28448—2012

信息安全技术
信息系统安全等级保护测评要求

Information security technology—
Testing and evaluation requirement for classified protection of information system

2012-06-29 发布　　2012-10-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

中 华 人 民 共 和 国
国 家 标 准
信息安全技术
信息系统安全等级保护测评要求
GB/T 28448—2012
*
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(100013)
北京市西城区三里河北街 16 号(100045)
网址:www.gb168.cn
服务热线:010-68522006
2012 年 10 月第一版
*
书号:155066·1-45598

版权专有 侵权必究

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由全国信息安全标准化技术委员会提出并归口(SAC/TC 260)。

本标准起草单位:公安部信息安全等级保护评估中心。

本标准主要起草人:朱建平、马力、黄洪、毕马宁、任卫红、谢朝海、李升、袁静、曲洁、刘静、尚旭光、张振峰、李明、陈雪秀。

引　言

依据《中华人民共和国计算机信息系统安全保护条例》(国务院147号令)、《国家信息化领导小组关于加强信息安全保障工作的意见》(中办发[2003]27号)、《关于信息安全等级保护工作的实施意见》(公通字[2004]66号)和《信息安全等级保护管理办法》(公通字[2007]43号)等有关文件要求,制定本标准。

本标准是信息安全等级保护相关系列标准之一。

与本标准相关的系列标准包括:

——GB/T 22239—2008　信息安全技术　信息系统安全等级保护基本要求;

——GB/T 22240—2008　信息安全技术　信息系统安全等级保护定级指南;

——GB/T 28449—2012　信息安全技术　信息系统安全等级保护测评过程指南。

《信息安全技术　信息系统安全等级保护测评过程指南》就有关信息系统安全等级保护测评工作的组织、实施和过程控制方面提供指导。本标准对信息系统进行安全等级保护测试评估的技术活动提出要求,为评价信息系统是否符合GB/T 22239—2008提供了获取证据的途径和方法,用以指导测评人员从信息安全等级保护的角度对信息系统进行测试评估。

本标准中的信息系统指计算机信息系统。

在本标准文本中,黑体字的测评要求表示该要求出现在当前等级而在低于当前等级信息系统的测评要求中没有出现过。

信息安全技术
信息系统安全等级保护测评要求

1 范围

本标准规定了对实现的信息系统是否符合 GB/T 22239—2008 所进行的测试评估活动的要求，包括对第一级信息系统、第二级信息系统、第三级信息系统和第四级信息系统进行测试评估的要求。本标准略去对第五级信息系统进行测评的要求。

本标准适用于信息安全测评服务机构、信息系统的主管部门及运营使用单位对信息系统安全等级保护状况进行的安全测试评估。信息安全监管职能部门依法进行的信息安全等级保护监督检查可以参考使用。

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/T 5271.8 信息技术 词汇 第 8 部分：安全

GB/T 22239—2008 信息安全技术 信息系统安全等级保护基本要求

3 术语和定义

GB/T 5271.8 和 GB/T 22239—2008 界定的以及下列术语和定义适用于本文件。

3.1

访谈 interview

访谈是指测评人员通过引导信息系统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

检查 examination

检查是指测评人员通过对测评对象(如制度文档、各类设备、安全配置等)进行观察、查验、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 testing

测试是指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，将运行结果与预期的结果进行比对的过程。

4 概述

4.1 测评框架

信息系统安全等级保护测评(以下简称等级测评)的概念性框架由三部分构成：测评输入、测评过程