



中华人民共和国国家标准

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

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

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

目 次

前言	V
引言	VI
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 符号和缩略语	1
5 等级测评概述	1
5.1 等级测评的作用	1
5.2 等级测评风险	2
5.2.1 可能影响系统正常运行	2
5.2.2 可能泄漏敏感信息	2
5.3 等级测评风险的规避	2
5.4 等级测评过程概述	3
6 测评准备活动	3
6.1 测评准备活动的工作流程	3
6.2 测评准备活动的主要任务	4
6.2.1 项目启动	4
6.2.2 信息收集和分析	4
6.2.3 工具和表单准备	5
6.3 测评准备活动的输出文档	5
6.4 测评准备活动中双方的职责	5
7 方案编制活动	6
7.1 方案编制活动的工作流程	6
7.2 方案编制活动的主要任务	6
7.2.1 测评对象确定	6
7.2.2 测评指标确定	7
7.2.3 测评内容确定	8
7.2.4 工具测试方法确定	8
7.2.5 测评指导书开发	9
7.2.6 测评方案编制	10
7.3 方案编制活动的输出文档	11
7.4 方案编制活动中双方的职责	11
8 现场测评活动	11
8.1 现场测评活动的工作流程	11
8.2 现场测评活动的主要任务	12
8.2.1 现场测评准备	12

8.2.2	现场测评和结果记录	12
8.2.2.1	访谈	12
8.2.2.2	检查	13
8.2.2.3	测试	14
8.2.3	结果确认和资料归还	14
8.3	现场测评活动的输出文档	14
8.4	现场测评活动中双方的职责	15
9	报告编制活动	15
9.1	报告编制活动的工作流程	15
9.2	报告编制活动的主要任务	16
9.2.1	单项测评结果判定	16
9.2.2	单元测评结果判定	16
9.2.3	整体测评	17
9.2.4	风险分析	18
9.2.5	等级测评结论形成	18
9.2.6	测评报告编制	19
9.3	报告编制活动的输出文档	19
9.4	报告编制活动中双方的职责	20
附录 A (资料性附录)	等级测评工作流程	21
附录 B (资料性附录)	测评对象确定准则和样例	23
B.1	测评对象确定准则	23
B.2	测评对象确定样例	23
B.2.1	第一级信息系统	23
B.2.2	第二级信息系统	23
B.2.3	第三级信息系统	24
B.2.4	第四级信息系统	25
附录 C (资料性附录)	等级测评工作要求	26
C.1	依据标准,遵循原则	26
C.2	恰当选取,保证强度	26
C.3	规范行为,规避风险	26
附录 D (资料性附录)	测评方案与测评报告编制示例	27
D.1	测评方案编制示例	27
D.1.1	系统描述	27
D.1.2	测评对象	28
D.1.3	测评指标	30
D.1.4	测评工具和接入点	30
D.1.5	测评内容	32
D.1.6	测评指导书	35
D.2	测评报告编制示例	39
D.2.1	整体测评	39
D.2.2	安全建设整改建议	40

附录 E (资料性附录) 信息系统基本情况调查表模版	42
E.1 说明	42
E.2 单位基本情况	42
E.3 参与人员名单	43
E.4 物理环境情况	43
E.5 信息系统基本情况	43
E.6 信息系统承载业务(服务)情况	44
E.7 信息系统网络结构(环境)情况	44
E.8 外联线路及设备端口(网络边界)情况	45
E.9 网络设备情况	45
E.10 安全设备情况	46
E.11 服务器设备情况	46
E.12 终端设备情况	47
E.13 系统软件情况	47
E.14 应用系统软件情况	47
E.15 业务数据情况	48
E.16 数据备份情况	48
E.17 应用系统软件处理流程(多表)	49
E.18 业务数据流程(多表)	49
E.19 管理文档情况	50
E.20 安全威胁情况	52
附录 F (资料性附录) 信息系统安全等级测评报告模版(试行)	54
参考文献	70

前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

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:公安部信息安全等级保护评估中心。

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

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),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 28448—2012 信息安全技术 信息系统安全等级保护测评要求。

信息安全技术

信息系统安全等级保护测评过程指南

1 范围

本标准规定了信息系统安全等级保护测评(以下简称“等级测评”)工作的测评过程,对等级测评的活动、工作任务以及每项任务的输入/输出产品等提出指导性建议。

本标准适用于测评机构、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价。

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 17859—1999 计算机信息系统 安全保护等级划分准则

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 28448—2012 信息安全技术 信息系统安全等级保护测评要求
《信息安全等级保护管理办法》(公通字[2007]43号)

3 术语和定义

GB/T 5271.8、GB 17859—1999 和 GB/T 28448—2012 界定的以及下列的术语和定义适用于本文件。

3.1

优势证据 superior evidence

测评结果显现的凭据强于其他测评结果的那个/些测评结果视为优势证据。它可用于平衡实施等级测评过程中获得的多个测评结果之间的矛盾。

4 符号和缩略语

DDN:数字数据网 (Digital Data Network)

PSTN:公共交换电话网络 (Public Switched Telephone Network)

SDH:同步数字体系 (Synchronous Digital Hierarchy)

5 等级测评概述

5.1 等级测评的作用

依据《信息安全等级保护管理办法》(公通字[2007]43号),信息系统运营、使用单位在进行信息系