ICS 35.020
L 09

GA

中华人民共和国公共安全行业标准

GA/T 713—2007

信息安全技术
信息系统安全管理测评

Information security technology—
Information system security management testing and evaluation

2007-08-13 发布　　2007-10-01 实施

中华人民共和国公安部　　发布

中华人民共和国公共安全
行业标准
信息安全技术
信息系统安全管理测评
GA/T 713—2007
*
中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045
网址 www.spc.net.cn
电话:68523946 68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 2 字数 52 千字
2007年11月第一版 2007年11月第一次印刷
*
书号:155066·2-18283

目　　次

前　言

本标准的附录A为资料性附录。

本标准由公安部信息系统安全标准化技术委员会提出并归口。

本标准起草单位：北京江南天安科技有限公司，北京思源新创信息安全资讯有限公司。

本标准主要起草人：陈冠直、王志强、吉增瑞、景乾元、宋建平。

引　言

本标准用于在实施信息系统安全等级保护时，根据 GB/T 20269—2006《信息安全技术　信息系统安全管理要求》对安全管理体系各等级安全管理要求的落实情况进行评估，规定了评估的主要内容和原则，明确了评估过程和方法。对于涉及国家秘密的信息和信息系统的保密管理，应按照国家有关保密管理规定和相关测评标准执行。

信息系统安全管理评估的主体包括信息系统的主管领导部门、信息安全监管机构、第三方评估机构、信息系统的管理者等，对应的评估可以是检查评估、第三方评估或自评估，本标准中统称评估。

本标准第 4 章（管理评估的基本原则）、第 5 章（评估方法）、第 6 章（评估实施）给出了每一安全保护等级的评估需要执行的统一要求和评估方法，在第 7 章分等级描述了 GB/T 20269—2006 规定的评估要求。本标准中有关信息系统安全管理评估项见附录 A。

信息安全技术
信息系统安全管理测评

1 范围

本标准规定了按照 GB 17859—1999 等级划分的要求对信息系统实施安全管理评估的原则和方法。

本标准适用于相关组织机构(部门)对信息系统实施安全等级保护所进行的安全管理评估与自评估。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准,然而,鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本标准。

GB 17859—1999 计算机信息系统 安全保护等级划分准则

GB/T 20269—2006 信息安全技术 信息系统安全管理要求

3 术语和定义

GB 17859—1999、GB/T 20269—2006 确立的以及下列术语和定义适用于本标准。

3.1

安全审计 security audit

对信息系统记录与活动的独立的审查和检查,以测试系统控制的充分程度,确保符合已建立的安全策略和操作过程,检测出安全违规,并对在控制、安全策略和过程中指示的变化提出建议。

3.2

风险评估 risk assessment

风险识别、分析、估值的全过程,其目标是确定和估算风险值。

3.3

安全策略 security policy

一个组织为其运转而规定的一个或多个安全规则、规程、惯例和指南。

3.4

监测验证 validate by inspect and test

通过对与安全管理有关的监测信息(包括审计信息以及各种监测、监控机制收集的信息)的分析,对安全管理实施的有效性进行验证的过程。

4 管理评估的基本原则

对信息系统安全管理的评估应坚持科学性、有效性、公正性等基本原则,即评估的原理、方法、流程、具体要求是科学的、正确的;评估的方法、流程等是可操作的,成本和效率等方面可接受;评估结果是客观公正的,评估机构是中立权威的。还应遵循以下原则:

——有效性原则:根据 GB/T 20269—2006 充分考虑信息系统功能,信息资产的重要性,可能受到的威胁及面临的风险,评估整个安全管理体系的有效性;