ICS 35.040
L 80

中华人民共和国国家标准

GB/T 28453—2012

信息安全技术
信息系统安全管理评估要求

Information security technology—
Information system security management assessment requirements

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

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:北京江南天安科技有限公司。

本标准主要起草人:陈冠直、吉增瑞、陈硕、景乾元、王志强。

引　言

本标准依据国家有关信息安全等级保护的政策法规，提出了用于规范信息系统安全管理评估的要求。主要包括信息系统安全管理评估的原则和模式、组织和活动、方法工具和实施等要求，以及在信息系统生存周期各个阶段，针对第一级到第五级信息系统安全管理评估的要求。

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、信息系统的管理者、第三方评估机构等，对应的评估可以是检查评估、自评估或第三方评估。本标准中对三种评估模式提出共同要求时统称评估。信息系统安全管理评估以信息安全管理体系为主线进行评估，必要时采集信息安全技术测评结果进行综合分析。信息系统安全管理评估可以是独立的评估，也可以与信息安全技术测评联合进行综合评估。信息系统安全管理评估贯穿于信息系统的整个生存周期，各阶段管理评估的原则和方法是一致的，各阶段安全管理的内容、对象、安全需求存在一定不同，使得安全管理评估的目的、要求等各方面也有所不同。信息系统安全管理评估针对信息安全保护各个等级的信息系统，安全管理评估的要求随着保护等级的提高而增强。

本标准第4章阐述管理评估的原则和模式；第5章阐述管理评估的组织、评估目标范围和依据、管理活动的内容；第6章阐述管理评估方法、管理评估工具、管理评估实施，给出了各个安全保护等级的安全管理评估需要执行的共同要求和评估方法；第7章分等级评估，以GB/T 20269—2006规定的信息系统安全管理要求为基本依据，从信息系统生存周期的规划立项阶段、设计实施阶段、运行维护阶段、终止处置阶段，对五个安全保护等级的安全管理评估要求分别进行描述。附录A中提供的信息系统安全管理评估参照表，描述了本标准中有关各等级信息系统安全管理评估要求的具体评估内容要点。

本标准仍沿用GB/T 20269—2006中的称谓，对于信息系统的所有者可包括国家机关、事业单位、厂矿企业、公司、集团等各种类型和不同规模的组织机构，统称为“组织机构”。

信息安全技术
信息系统安全管理评估要求

1 范围

本标准依据 GB/T 20269—2006 规定的信息系统分等级安全管理要求，从信息系统生存周期的不同阶段，规定了对信息系统进行安全管理评估的原则和模式、组织和活动、方法和实施，提出了信息安全等级保护第一级到第五级的信息系统安全管理评估的要求。

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，以及评估者和被评估者对评估的管理。

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 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

GB/T 20282—2006 信息安全技术 信息系统安全工程管理要求

GB/T 25070—2010 信息安全技术 信息系统等级保护安全设计技术要求

3 术语和定义

GB 17859—1999、GB/T 20269—2006 中界定的以及下列术语和定义适用于本文件。

3.1

安全评估 security assessment

依照国家有关法规与标准，对信息系统的安全保障程度进行评估的活动，包括安全技术评估和安全管理评估。本标准所述评估是指信息系统安全管理评估。

3.2

自评估 self-assessment

由信息系统所有者自身发起，组成组织机构内部的评估机构，依据国家有关法规与标准，对信息系统安全管理进行的评估活动。

3.3

检查评估 inspection assessment

由被评估信息系统所有者的上级主管部门、业务主管部门或国家相关监管部门发起的，依据国家有关法规与标准，对信息系统安全管理进行的评估活动。

3.4

第三方评估 third party assessment

由信息系统所有者委托商业评估机构或其他评估机构，依据国家有关法规与标准，对信息系统安全管理进行的评估活动。