

ICS 35.020
L 09



中华人民共和国国家标准

GB/T 20282—2006

信息安全技术 信息系统安全工程管理要求

Information security technology—
Information system security engineering management requirements

2006-05-31 发布

2006-12-01 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 工 程 管 理 要 求
GB/T 20282—2006

*

中国标准出版社出版发行
北京西城区复兴门外三里河北街16号
邮政编码:100045

<http://www.spc.net.cn>
电话:(010)51299090、68522006
2006年9月第一版

*

书号:155066·1-27972

版权专有 侵权必究
举报电话:(010)68522006

目 次

前言	III
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 安全工程体系	2
4.1 概述	2
4.2 安全工程目标	2
4.3 基本关系	2
5 资格保证要求	2
5.1 系统集成资质要求	2
5.2 人员资质要求	2
5.3 第三方服务要求	2
5.4 安全产品要求	2
5.5 工程监理要求	2
5.6 法律、法规、政策符合性要求	3
6 组织保证要求	3
6.1 定义组织的系统工程过程	3
6.2 改进组织的系统工程过程	3
6.3 管理系列产品演化	3
6.4 管理系统工程支持环境	4
6.5 培训	5
6.6 与供应商协调	5
7 工程实施要求	6
7.1 管理安全控制	6
7.2 评估影响	6
7.3 评估安全风险	7
7.4 评估威胁	7
7.5 评估脆弱性	8
7.6 建立保证论据	8
7.7 协调安全	9
7.8 监视安全态势	9
7.9 提供安全输入	10
7.10 指定安全要求	11
7.11 验证和确认安全性	11
8 项目实施要求	12
8.1 质量保证	12
8.2 管理配置	13
8.3 管理项目风险	13

8.4	监视技术活动	14
8.5	计划技术活动	15
9	安全工程管理分等级要求	16
9.1	第一级:用户自主保护级	16
9.2	第二级:系统审计保护级	17
9.3	第三级:安全标记保护级	19
9.4	第四级:结构化保护级	20
9.5	第五级:访问验证保护级	22
9.6	安全保护等级划分与安全工程要求对照表	23
10	安全工程流程与安全工程要求	23
10.1	安全工程流程	23
10.2	安全工程流程各阶段的安全工程要求	26
附录 A (资料性附录) 安全工程要求与安全保护等级、安全工程流程的对应关系		27
参考文献		34

前 言

本标准的附录 A 是资料性附录。

本标准由信息安全标准化技术委员会提出并归口。

本标准起草单位：中国电子科技集团第三十研究所、上海二零卫士信息安全有限公司、上海标准化研究院。

本标准主要起草人：张建军、魏忠、叶铭、陈长松、孔一童。

信息安全技术

信息系统安全工程管理要求

1 范围

本标准规定了信息系统安全工程(以下简称安全工程)的管理要求,是对信息系统安全工程中所涉及到的需求方、实施方与第三方工程实施的指导,各方可以此为依据建立安全工程管理体系。

本标准按照 GB 17859—1999 划分的五个安全保护等级,规定了信息系统安全工程管理的不同要求。

本标准适用于信息系统的需求方和实施方的安全工程管理,其他有关各方也可参照使用。

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

GB/T 20271—2006 信息安全技术 信息系统通用安全技术要求

3 术语和定义

下列术语和定义适用于本标准。

3.1

安全工程 security engineering

为确保信息系统的保密性、完整性、可用性等目标而进行的系统工程过程。

3.2

安全工程的生存周期 security engineering lifecycle

在整个信息系统生存周期中执行的安全工程活动包括:概念形成、概念开发和定义、验证与确认、工程实施开发与制造、生产与部署、运行与支持 and 终止。

3.3

安全工程指南 security engineering guide

由工程组做出的有关如何选择工程体系结构、设计与实现的指导性信息。

3.4

脆弱性 vulnerability

能够被某种威胁利用的某个或某组资产的弱点。

3.5

风险 risk

某种威胁会利用一种资产或若干资产的脆弱性使这些资产损失或破坏的可能性。

3.6

需求方 owner

信息系统安全工程建设的拥有者或组织者。