

ICS 35.040
L 80



中华人民共和国国家标准

GB/T 20274.1—2006

GB/T 20274.1—2006

信息安全技术 信息系统安全保障评估框架 第 1 部分：简介和一般模型

Information security technology—
Evaluation framework for information systems security assurance—
Part 1: Introduction and general model

中华人民共和国
国家标准
信息安全技术
信息系统安全保障评估框架
第 1 部分：简介和一般模型
GB/T 20274.1—2006

*
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.bzcs.com
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 3 字数 81 千字
2006 年 10 月第一版 2006 年 10 月第一次印刷

*
书号：155066·1-28089 定价 20.00 元

如有印装差错 由本社发行中心调换
版权专有 侵权必究
举报电话：(010)68533533



GB/T 20274.1—2006

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

参 考 文 献

- [1] GB/T 19000—2000 质量管理体系 基础和术语(idt ISO 9000:2000)
- [2] GB/T 19001—2000 质量管理体系 要求(idt ISO 9001:2000)
- [3] GB/T 19004—2000 质量管理体系 业绩改进指南(idt ISO 9004:2000)
- [4] ISO/IEC TR 15443-1: 2005, A framework for IT Security assurance—Part 1: Overview and framework
- [5] ISO/IEC TR 15443-2:2005, A framework for IT Security assurance—Part 2: Assurance methods
- [6] ISO/IEC WD 15443-3, A framework for IT security assurance—Part 3: Analysis of assurance methods
- [7] ISO/IEC PDTR 19791: 2004, Information technology—Security techniques—Security assessment of operational systems
- [8] Information Assurance Technical Framework, Release 3.1, National Security Agency Information Assurance Solutions Technical, September 2002
- [9] ISO/IEC 17799:2005 Information technology—Security techniques—Code of practice for information security management
- [10] ISO/IEC 13335-1: 2004 Information technology—Security techniques—Management of information and communications technology security (MICTS)—Part 1: Concepts and models for information and communications technology security management
- [11] ISO/IEC 4th WD 13335-2: 2004, Management of information and communications technology security (MICTS)—Part 2: Techniques for information and communications technology security risk management
- [12] ISO/IEC 1st CD 18028-1: 2004, Information technology—Security techniques—IT network security—Part 1: Network security management
- [13] ISO/IEC FCD 18028-2: 2004, Information technology—Security techniques—IT network security—Part 2: Network security architecture
- [14] ISO/IEC FCD 18028-3: 2004, Information technology—Security techniques—IT network security—Part 3: Securing communications between networks using security gateways
- [15] ISO/IEC 18028-4:2005, Information technology—Security techniques—IT network security—Part 4: Remote access
- [16] ISO/IEC 1st CD 18028-5: 2004, Information technology—Security techniques—IT network security—Part 5: Securing communications across networks using Virtual Private Networks
- [17] NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems, November 2001
- [18] NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems, January 2002
- [19] NIST Special Publication 800-34 Continuity Planning Guide for Information Technology System, June 2002
- [20] NIST Special Publication 800-50, Building an Information Security Awareness and Training Program, October 2003
- [21] NIST Special Publication 800-64, Security Considerations in the Information System Devel-

目 次

前言	V
引言	VI
0.1 信息系统安全保障的含义	VI
0.2 信息系统安全保障评估框架的编制目的和意义	VI
1 范围	1
2 规范性引用文件	1
3 术语、定义和缩略语	1
3.1 术语和定义	1
3.2 缩略语	4
4 概述	4
4.1 引言	4
4.2 信息系统安全保障评估框架的目标读者	4
4.3 评估上下文	5
4.4 信息系统安全保障评估框架的文档结构	6
5 一般模型	7
5.1 概述	7
5.2 安全保障上下文	7
5.3 信息系统安全保障评估	10
5.4 ISPP 和 ISST 的生成	12
5.5 信息系统安全保障描述材料	14
6 信息系统安全保障评估和评估结果	17
6.1 介绍	17
6.2 ISPP(信息系统保护轮廓)和 ISST(信息系统安全目标)的要求	18
6.3 TOE 的要求	18
6.4 评估结果的声明	19
6.5 TOE 评估结果的应用	19
附录 A (规范性附录) 信息系统保护轮廓	20
A.1 概述	20
A.2 信息系统保护轮廓内容	20
A.2.1 内容和表述	20
A.2.2 ISPP 引言	20
A.2.3 TOE 描述	20
A.2.4 TOE 安全环境	21
A.2.5 安全保障目的	21
A.2.6 信息系统安全保障要求	22
A.2.7 ISPP 应用注解	22
A.2.8 符合性声明	22
附录 B (规范性附录) 信息系统安全目标规范	24

B.1 概述 24

B.2 信息系统安全目标内容 24

B.2.1 内容和形式 24

B.2.2 ISST 引言 24

B.2.3 TOE 描述 25

B.2.4 TOE 安全环境 26

B.2.5 安全保障目的 26

B.2.6 安全保障要求 27

B.2.7 TOE 概要规范 27

B.2.8 ISPP 声明 28

B.2.9 符合性声明 28

附录 C (资料性附录) 信息系统描述 30

C.1 概述 30

C.2 信息系统描述规范 30

C.3 信息系统描述说明 31

附录 D (资料性附录) 信息系统安全保障级说明 33

D.1 概述 33

D.2 信息系统使命分类 33

D.3 信息系统威胁分级 33

D.4 信息系统安全保障级 (ISAL) 矩阵 34

D.5 信息系统安全保障级 (ISAL) 分级要求 34

参考文献 36

图 1 评估上下文 5

图 2 信息系统安全概念和关系 8

图 3 信息系统安全保障模型 8

图 4 信息系统安全保障生命周期的安全保障要素 9

图 5 信息系统安全保障评估概念和关系 10

图 6 信息系统安全保障评估说明 11

图 7 信息系统安全保障评估整体和应用 12

图 8 ISPP 和 ISST 的生成过程 13

图 9 安全保障控制要求的组织和结构 15

图 10 安全保障要求的应用 16

图 11 评估结果 18

图 A.1 信息系统保护轮廓内容 21

图 B.1 信息系统安全目标内容 25

图 C.1 信息系统安全保障评估的信息系统描述规范 30

图 C.2 信息系统技术参考模型 32

图 D.1 信息系统安全管理能力成熟度级要求示例图 35

图 D.2 某信息系统安全工程能力成熟度级要求示例图 35

表 1 信息系统安全保障评估框架使用指南 6

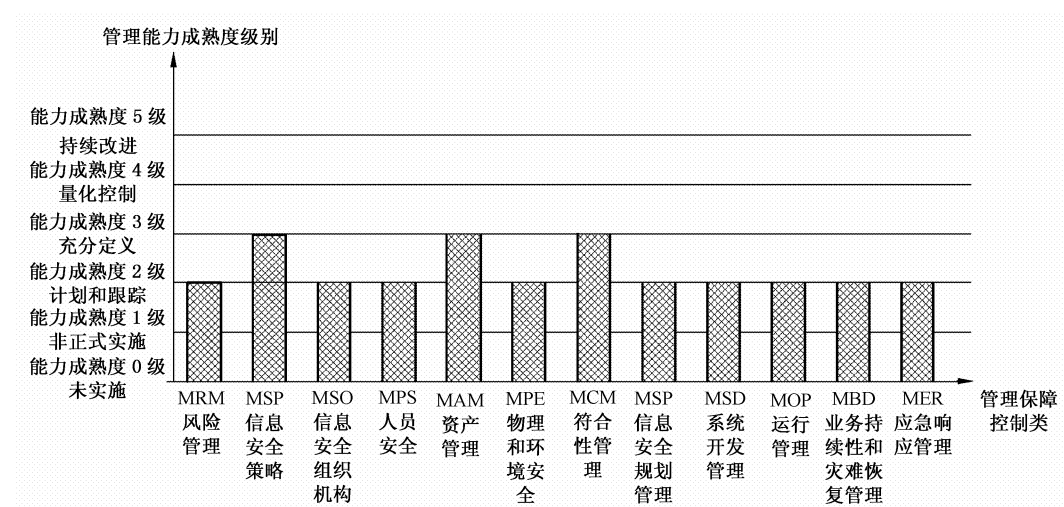


图 D.1 信息系统安全管理能力成熟度级要求示例图

图 D.2 描述了某信息系统安全工程能力成熟度级的要求示例。

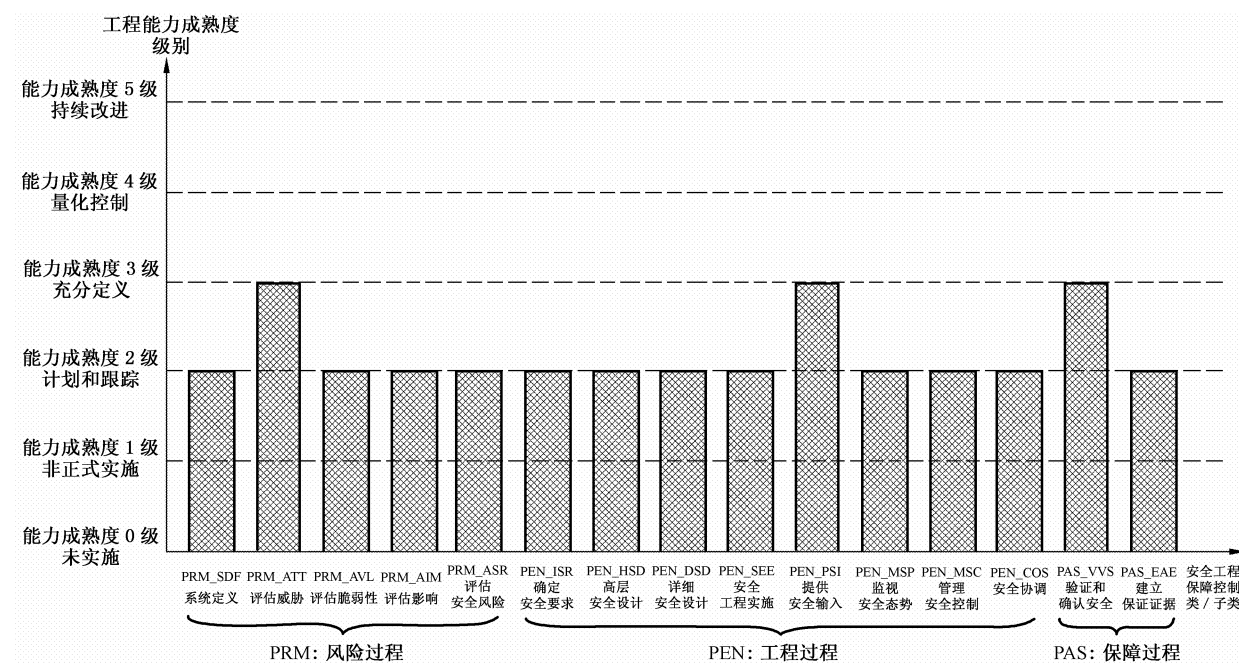


图 D.2 某信息系统安全工程能力成熟度级要求示例图