ICS 35.040
L 80

中华人民共和国国家标准

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

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

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

表 D.1　信息系统使命分类示例 …… 33
表 D.2　信息系统威胁分类示例 …… 33
表 D.3　信息系统安全保障级矩阵示例 …… 34
表 D.4　信息系统安全保障级要求示例 …… 34

前　言

GB/T 20274《信息安全技术　信息系统安全保障评估框架》分为四个部分：

——第1部分：简介和一般模型

——第2部分：技术保障

——第3部分：管理保障

——第4部分：工程保障

本部分的附录A和附录B为规范性附录，附录C和附录D为资料性附录。

本部分由全国信息安全标准化技术委员会提出并归口。

本部分起草单位：中国信息安全产品测评认证中心。

本标准主要起草人：吴世忠、王海生、陈晓桦、王贵驷、李守鹏、江常青、彭勇、张利、班晓芳、李静、王庆、邹琪、钱伟明、江典盛、陆丽、姚轶崭、孙成昊、门雪松、杜宇鸽、杨再山。

引　言

0.1　信息系统安全保障的含义

信息系统安全保障是在信息系统的整个生命周期中，通过对信息系统的风险分析，制定并执行相应的安全保障策略，从技术、管理、工程和人员等方面提出安全保障要求，确保信息系统的保密性、完整性和可用性，降低安全风险到可接受的程度，从而保障系统实现组织机构的使命。信息系统安全保障涵盖以下几个方面：

a) 信息系统安全保障应贯穿信息系统的整个生命周期，包括规划组织、开发采购、实施交付、运行维护和废弃5个阶段，以获得信息系统安全保障能力的持续性。

b) 信息系统安全保障不仅涉及安全技术，还应综合考虑安全管理、安全工程和人员安全等，以全面保障信息系统安全。在安全技术上，不仅要考虑具体的产品和技术，更要考虑信息系统的安全技术体系架构；在安全管理上，不仅要考虑基本安全管理实践，更要结合组织的特点建立相应的安全保障管理体系，形成长效和持续改进的安全管理机制；在安全工程上，不仅要考虑信息系统建设的最终结果，更要结合系统工程的方法，注重工程过程各个阶段的规范化实施；在人员安全上，要考虑与信息系统相关的所有人员包括规划者、设计者、管理者、运营维护者、评估者、使用者等的安全意识以及安全专业技能和能力等。

c) 信息系统安全保障是基于过程的保障。通过风险识别、风险分析、风险评估、风险控制等风险管理活动，降低信息系统的风险，从而实现信息系统安全保障。

d) 信息系统安全保障的目的不仅是保护信息和资产的安全，更重要是通过保障信息系统安全保障信息系统所支持的业务的安全，从而达到实现组织机构使命的目的。

e) 信息系统安全保障是主观和客观的结合。通过在技术、管理、工程和人员方面客观地评估安全保障措施，向信息系统的所有者提供其现有安全保障工作是否满足其安全保障目标的信心。因此，它是一种通过客观证据向信息系统所有者提供主观信心的活动，是主观和客观综合评估的结果。

f) 保障信息系统安全不仅是系统所有者自身的职责，而且需要社会各方参与，包括电信、电力、国家信息安全基础设施等提供的支撑。保障信息系统安全不仅要满足系统所有者自身的安全需求，而且要满足国家相关法律、政策的要求，包括为其他机构或个人提供保密、公共安全和国家安全等社会职责。

0.2　信息系统安全保障评估框架的编制目的和意义

本标准不仅可以作为信息系统安全保障评估的基础标准，也可以为从事信息系统安全保障工作的所有相关方（包括设计开发者、工程实施者、评估者、认证认可者等）提供一种标准化、规范化的通用描述语言、结构和方法。本标准是GB/T 18336—2001在信息系统领域的扩展和补充，它是以GB/T 18336—2001为基础，吸收其科学方法和结构，将GB/T 18336—2001从产品和产品系统扩展到信息技术系统，并进一步同其他国内外信息系统安全领域的标准和规范进行结合、扩展和补充，以形成描述和评估信息系统安全保障内容和能力的通用框架。在本标准中，信息系统作为评估对象，不仅涉及具体产品和产品系统，而且还包含信息系统运行环境的管理、工程等，是用于采集、处理、存储、传输、分发和部署信息的整个基础设施、组织结构、人员等的总和。

本标准属于信息系统安全保障的基础性和框架性标准，定义了信息系统安全保障的主要的通用要

求，制定此标准的意义在于：

a） 为信息系统安全的设计、实施、建设、测评、审核提供规范的、通用的描述语言。

b） 有利于信息系统所有者编制其信息系统的安全保障要求。

c） 有利于信息系统安全集成商和安全服务提供商提供更为科学规范化的设计和服务，促进信息安全市场的发展。

d） 有利于有关行政管理部门、执法机构、测评认证机构对信息系统进行安全检查、检测、审计、评估和认证。

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

1 范围

GB/T 20274 描述了信息系统安全保障的模型,建立了信息系统安全保障的框架,从信息系统安全技术、管理和工程三方面制定了信息系统的通用安全保障要求。

GB/T 20274 的本部分给出了信息系统安全保障的基本概念和模型,并建立了信息系统安全保障框架。

本部分适用于从事信息系统安全保障工作的所有相关方,包括设计开发者、工程实施者、评估者、认证认可者等。

本部分不适用于以下方面:

a) 人员技能和能力的评估,但对人员安全的要求在管理保障中体现;

b) 系统评估方法学;

c) 密码算法固有质量的评价。

2 规范性引用文件

下列文件中的条款通过 GB/T 20274 的本部分的引用而成为本部分的条款。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部分,然而,鼓励根据本部分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部分。

GB/T 9387.2—1995 信息处理系统 开放系统互连 基本参考模型 第2部分:安全体系结构(idt ISO 7498-2:1989)

GB/T 18336—2001 信息技术 安全技术 信息技术安全性评估准则(idt ISO/IEC 15408:1999)

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本部分。

3.1.1

访问控制 access control

防止对资源的未授权使用,包括防止以未授权方式使用某一资源。

[GB/T 9837.2—1995,3.3.1]

3.1.2

可追究性 accountability

这样一种性质,它确保一个实体的作用可以被独一无二地跟踪到该实体。

[GB/T 9837.2—1995,3.3.3]

3.1.3

资产 asset

信息系统安全策略中所保护的信息或资源。

[GB/T 18336.1—2001,3.3.1]

3.1.4

攻击　attack

在信息系统中一种绕过安全控制的行为。攻击成功与否取决于信息系统的脆弱性以及现有对策的有效性。

3.1.5

审计　audit

为了测试出系统的控制是否足够,为了保证与已建立的策略和操作堆积相符合,为了发现安全中的漏洞,以及为了建议在控制、策略和堆积中作任何指定的改变,而对系统记录与活动进行的独立观察和考核。

[GB/T 9837.2—1995,3.3.5]

3.1.6

鉴别　authentication

验证实体所声称的身份。

3.1.7

授权　authorization

授予权限,包括允许基于访问权的访问。

[GB/T 9837.2—1995,3.3.10]

3.1.8

授权用户　authorized user

依据安全策略可以执行某项操作的用户。

[GB/T 18336.1—2001,3.3.7]

3.1.9

可用性　availability

根据授权实体的请求可被访问与使用。

[GB/T 9387.2—1995,3.3.11]

3.1.10

计算环境　computing environment

整个信息系统、网络或组件运行的环境,包括物理环境、管理规则、人员工作程序以及与其他系统的通信和网络连接。

3.1.11

保密性　confidentiality

这一性质使信息不泄露给非授权的个人、实体或进程,不为其所用。

[GB/T 9837.2—1995,3.3.16]

3.1.12

配置管理　configuration management

在整个系统生命周期中通过控制硬件、软件、固件、文档、测试、测试设备和测试文档的变化来管理安全功能和保证措施。

3.1.13

信息系统安全保障　information systems security assurance;ISSA

在信息系统的整个生命周期中,通过对信息系统的风险分析,制定并执行相应的安全保障策略,从技术、管理、工程和人员等方面提出安全保障要求,确保信息系统的保密性、完整性和可用性,降低安全风险到可接受的程度,从而保障系统实现组织机构的使命。

3.1.14

信息系统　information systems;IS

用于采集、处理、存储、传输、分发和部署信息的整个基础设施、组织结构、人员和组件的总和。

3.1.15

信息系统安全　information systems security;INFOSEC

通过使用合理的安全控制措施保护在存储、处理或传输等过程中的信息不被未授权用户访问，并保证授权用户能够正常使用系统。

3.1.16

信息技术系统　information technology systems;IT Systems

用于采集、创建、通信、计算、分发、处理、存储和/或控制数据或信息的计算机硬件、软件和/或固件的任何组合，在信息系统中执行组织机构信息功能。

3.1.17

完整性　integrity

这一性质表明数据没有遭受以非授权方式所作的篡改或破坏。

[GB/T 9837.2—1995,3.3.31]

3.1.18

抗抵赖性　non-repudiation

证明一个行动或事件已经发生的能力，以便以后不能抵赖此事件或行动。

3.1.19

风险　risk

威胁利用资产或一组资产的脆弱性对组织机构造成伤害的潜在可能。

3.1.20

风险分析　risk analysis

估算风险大小的系统化的过程。

3.1.21

风险管理　risk management

以可接收的成本，标识、控制、减少或最小化那些可能影响信息系统的安全风险的过程。

3.1.22

安全　security

一种基于建立和保持保护措施的状态，以确保处于一种不被敌对行为或影响所侵犯的状态。

3.1.23

安全体系结构　security architecture

安全组件或部件之间如何构成一个相互协作的系统规则或方式。

3.1.24

安全域　security domain

遵守相同的安全策略的用户和系统的集合。

3.1.25

安全策略　security policy

组织机构为保障其运转而规定的若干安全规则、过程、规范和指南。

[GB/T 18336.1—2001,3.3.29]

注：安全策略使用 GB/T 18336.1—2001,3.3.29 中组织安全策略的定义。

3.1.26

信息系统安全保障级　information systems assurance level;ISAL

通过综合技术、管理和工程等安全机制所推荐的对抗各种安全威胁的保护组织机构信息和信息资产来保障组织机构使命的强度和保障度级别。

3.1.27

威胁　threat

能够通过未授权访问、毁坏、揭露、数据修改和/或拒绝服务对系统造成潜在危害的任何环境或事件。

3.1.28

脆弱性　vulnerability

在信息系统、系统安全程序、管理控制、物理设计、内部控制或实现中的，可能被攻击者利用来获得未授权的信息或破坏关键处理的弱点。

3.2　缩略语

下列缩略语适用于本标准。

CC：　通用准则(Common Criteria)

EAL：　评估保证级别(Evaluation Assurance Level)

IS：　信息系统(Information Systems)

ISAL　信息系统安全保障级(Information Systems Assurance Level)

TCML：安全技术能力成熟度级(Security Technique Capability Maturity Level)

MCML：安全管理能力成熟度级(Security Management Capability Maturity Level)

ECML：安全工程能力成熟度级(Security Engineering Capability Maturity Level)

ISPP：　信息系统保护轮廓(Information Systems Protection Profile)

ISST：　信息系统安全目标(Information Systems Security Target)

IT：　信息技术(Information Technology)

STR：　安全技术要求(Security Technique Requirements)

SMR：　安全管理要求(Security Management Requirements)

SER：　安全工程要求(Security Engineering Requirements)

SRL：　系统健壮性级别(System Robustness Level)

TOE：　评估对象(Target of Evaluation)

4　概述

本章介绍信息系统安全保障评估框架的主要概念，确定目标读者、评估环境和文档结构。

4.1　引言

信息安全的目标是为了保证信息的保密性、完整性和可用性。信息系统安全保障是在信息系统的整个生命周期中，通过对信息系统的风险分析，制定并执行相应的安全保障策略，从技术、管理、工程和人员等方面提出安全保障要求，确保信息系统的保密性、完整性和可用性，降低安全风险到可接受的程度，从而保障系统实现组织机构的使命。

4.2　信息系统安全保障评估框架的目标读者

4.2.1　概述

本标准的读者主要有三类，包括：信息系统的所有者或用户、信息系统的开发者和信息系统的评估者。本标准从内容和结构上支持所有三个方面的需求，他们是本标准的主要使用者。正如下文所述，他们都能从本标准中受益。

4.2.2 用户

用户可以参考本标准中给出的通用描述语言、方法和结构，从信息系统安全保障的技术、管理和工程领域来表达其信息系统安全保障要求，即信息系统安全保护轮廓(ISPP)。

用户可以使用本标准同信息系统的设计开发等相关人员进行更加有效的沟通和相互理解。

用户可根据信息系统安全保障的评估，了解其信息系统安全保障的现状，获得其信息系统安全保障的信心。同时，用户还可以根据评估结果，进一步完善和持续改进其信息系统的安全保障能力，以跟上外部和内在环境不断变化产生的安全保障要求。

4.2.3 开发者

开发者使用本标准能帮助客户更好的描述其信息系统安全需求，编制符合其运行环境要求的信息系统安全目标(ISST)和具体的信息系统安全保障方案和措施。

使用本标准还可以评估某个特定系统的信息系统安全目标(ISST)和特定的安全保护轮廓的符合性。通常，用户的需求由一个或多个信息系统保护轮廓(ISPP)提供。

开发者可以使用本标准来编制相应的安全保障证据的内容和表现形式，支持评估方的评估要求。

4.2.4 评估者

评估者可使用本标准来定义信息系统安全评估的内容。评估的内容包括安全技术、安全管理和安全工程等要求。

本标准并没有规定如何进行评估，具体的评估过程由信息系统安全保障评估方法、系统安全导出性测评指南、安全评估指南、操作手册等文档来描述。

4.2.5 其他读者

除上述人员之外，本标准还可以供以下人员参考使用：

a) 系统管理员和系统安全管理员：负责维护系统达到组织机构的信息系统安全保障策略和要求；

b) 内部和外部的审核员：负责评定信息系统安全保障是否恰当；

c) 安全规划和设计者：负责设计信息系统安全技术、工程和管理保障等规范；

d) 认可者：负责批准一个信息系统在特定环境中的使用；

e) 评估发起者：负责申请和支持一个信息系统安全评估活动；

f) 评估机构：负责管理和监督评估者实施信息系统安全保障评估。

4.3 评估上下文

为了使不同的评估机构和评估者得出的评估结果在技术上具有可比性，信息系统安全保障的评估应在国家权威的测评体系内执行，通过该体系所建立的严格、规范、科学的评估标准、评估质量的监督，以及评估机构和评估者遵循相关的国家法律和政策，确保了评估结果的权威性和客观性。

图1描述了形成评估上下文的主要部分。

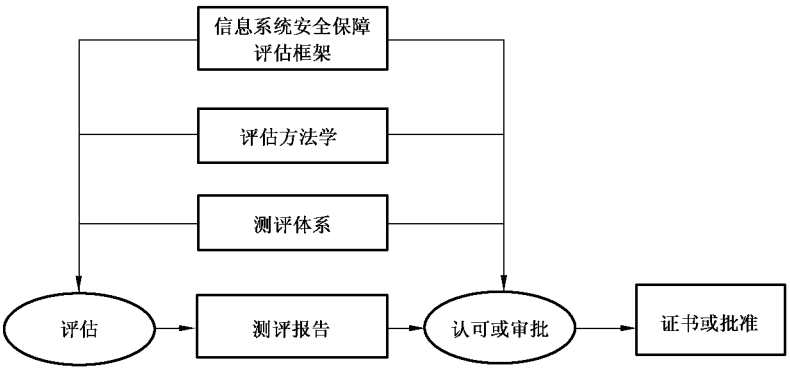

图1 评估上下文

在评估上下文中，信息系统安全保障通用评估方法学（SCEM）有助于保证评估结果的可重复性和客观性，但仅靠 SCEM 本身是不充分的。本标准的许多条款需要专业判断和一定的背景知识，而这些是很难达到一致的。为了增强评估结果的一致性，评估机构须在权威的测评体系内，不同评估机构须遵循相同的评估机构认可准则，同时评估机构之间要增加评估基准的对比测试。此外，评估的结果即测评报告可以进入认可或审批过程，并生成最终的评定证书或正式批准文件。这些证书或文件通常是公开的。

对于测评体系、评估方法学和评估过程的监督和管理是认证监督管理机构的责任，不属于本标准的范围；对评估结果的认可或审批是信息系统所有者或其主管机构的责任，也不属于本标准的范围。

4.4 信息系统安全保障评估框架的文档结构

本标准由以下相互关联的 4 个部分组成：

a) 第 1 部分：简介和一般模型。该部分定义了信息系统安全保障评估框架的一般概念和原理，并在信息安全的基础上提出了信息系统安全保障的模型。它也详细解释了信息系统安全保障模型的概念和关系以及信息系统安全保障评估的整体框架和应用。在该部分的附录中，给出了信息系统保护轮廓（ISPP）和信息系统安全目标（ISST）的描述规范；

b) 第 2 部分：技术保障。该部分描述了信息系统安全保障框架中的技术保障方面的内容，定义了一系列信息系统安全技术保障组件，定义了反映信息系统安全技术保障能力的成熟度模型和级别；

c) 第 3 部分：管理保障。该部分描述了信息系统安全保障框架中的管理保障方面的内容，定义了一系列信息系统安全管理保障组件，定义了反映信息系统安全管理保障能力的成熟度模型和级别；

d) 第 4 部分：工程保障。该部分描述了信息系统安全保障框架中的工程保障方面的内容，定义了一系列信息系统安全工程保障组件，定义了反映信息系统安全工程保障能力的成熟度模型和级别。

表 1 列出了主要的三方面读者及其可能感兴趣的信息系统安全保障评估框架内容：

表 1 信息系统安全保障评估框架使用指南

内　　容	用　　户	开发者	评估者
第 1 部分	理解和建立信息系统安全保障的整体概念和背景知识，帮助建立信息系统安全保障工作的整体规划和开发信息系统保护轮廓（ISPP）。	理解和建立信息系统安全保障的整体概念和背景知识，根据信息系统保护轮廓（ISPP）编制信息系统安全目标（ISST）。	理解和建立信息系统安全保障的整体概念和背景知识，评估信息系统保护轮廓（ISPP）和信息系统安全目标（ISST）。
第 2 部分	作为建立信息系统安全技术保障体系的指导和参考。用户可以选择合适的信息系统安全技术架构能力级，制定相应的安全技术控制措施以形成信息系统安全技术体系和信息系统保护轮廓。	用于理解信息系统安全技术控制措施并作为生成技术方案的参考。	作为系统评估、保护轮廓评估和安全目标评估的依据之一，信息系统安全技术控制措施是信息系统保护轮廓和信息系统安全目标的组成部分。

表 1（续）

内　　容	用　　户	开发者	评估者
第 3 部分	作为建立信息系统安全管理保障体系的指导和参考。用户可以选择合适的信息系统安全管理能力级，制定相应的安全管理控制措施以形成信息系统安全管理体系和信息系统保护轮廓。	用于理解信息系统安全管理控制措施并作为生成管理策略与制度的参考。	作为系统评估、保护轮廓评估和安全目标评估的依据之一，信息系统安全管理控制措施是信息系统保护轮廓和信息系统安全目标的组成部分。
第 4 部分	作为建立信息系统安全工程保障体系的指导和参考。用户可以选择合适的信息系统安全工程能力级，制定相应的安全工程控制措施以形成信息系统安全工程体系和信息系统保护轮廓。	用于理解信息系统安全工程控制措施和生成安全工程规范的参考。	作为系统评估、保护轮廓评估和安全目标评估的依据之一，信息系统安全工程控制措施是信息系统保护轮廓和信息系统安全目标的组成部分。

5　一般模型

5.1　概述

本章提出了信息系统安全保障评估框架的一般概念，其中也包括使用这些概念的上下文，以及使用这些概念的方法。本标准的其他部分在这些概念的基础上进一步展开，并使用了本章描述的方法。

本部分使用一系列安全保障概念和术语讨论信息系统安全保障。对这些概念和术语的理解是有效运用本标准的前提条件。这些概念和术语是相当通用的，不限于在本标准的应用，可以在其他标准中使用。

5.2　安全保障上下文

5.2.1　安全保障概念

随着组织机构的使命越来越依赖于信息系统，信息系统也越来越成为组织机构生存和发展的关键因素。信息系统的安全风险也成为组织风险的一部分。为了保障组织机构完成其使命，必须针对信息系统面临的各种各样的风险，制定相应的策略来抵抗这些风险。图 2 说明了信息系统安全保障中的这些高层概念的关系。

信息系统是用于采集、处理、存储、传输、分发和部署信息的整个基础设施、组织结构、机构人员和组件的总和。每个信息系统总是运行于特定的现实环境中，它从属某个组织机构，受来自组织内部与外部环境的约束，因此，信息系统的安全保障除了要在充分分析信息系统本身的技术、业务、管理等特性基础上提出相应的要求外，还要考虑这些约束条件产生的要求。

信息系统安全风险是具体的风险，各个风险是针对某一特定对象的风险。产生风险的因素主要有信息系统自身存在的脆弱性和来自系统外部的威胁。信息系统运行环境存在着怀有特定威胁动机的威胁源，它会使用各种攻击方法，利用信息系统运行环境中的各种脆弱性，对信息系统造成相应的风险，由此才产生信息安全事件和问题。

信息系统安全保障工作就是针对信息系统在运行环境中所面临的各种风险，制定信息安全保障策略体系，在它的指导下，设计并实现信息安全保障架构或模型，采取技术、管理等安全保障措施，将风险减少至预定可接受的程度，从而保障其使命要求。策略体系是组织机构在对风险、资产和使命综合理解的基础上所作出的指导文件。策略体系的制定，反映了组织机构对信息系统安全保障及其目标的理解，它的制定和贯彻执行对组织机构信息系统安全保障起着纲领性的指导作用。

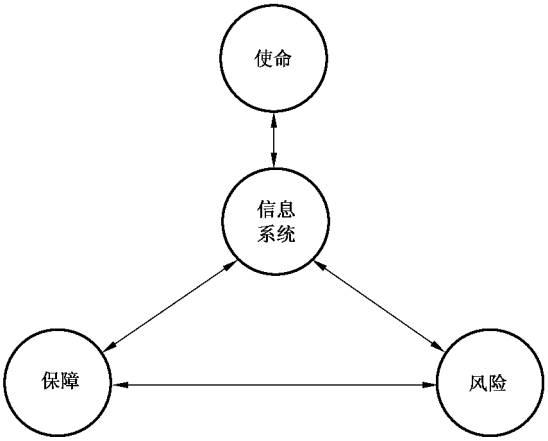

图 2　信息系统安全概念和关系

5.2.2　信息系统安全保障模型

5.2.2.1　信息系统安全保障模型

在 5.2.1 的内容中，给出了信息系统安全保障涉及的高层概念关系。这个高层概念是本标准的基础，本标准在此基础上提出了信息系统安全保障模型。

信息系统安全保障模型的主要内容是：以风险和策略为基础和出发点（即从信息系统所面临的风险和信息系统所处的环境出发），制定组织机构信息系统安全保障策略体系，通过在信息系统生命周期中在技术、管理、工程和人员等方面实施保障措施，确保信息的保密性、完整性和可用性特征，从而实现和贯彻组织机构策略并将风险降低到可接受的程度，达到保护组织机构信息和信息系统资产，从而保障组织机构实现其使命的最终目的。

图 3 描述了信息系统安全保障模型。

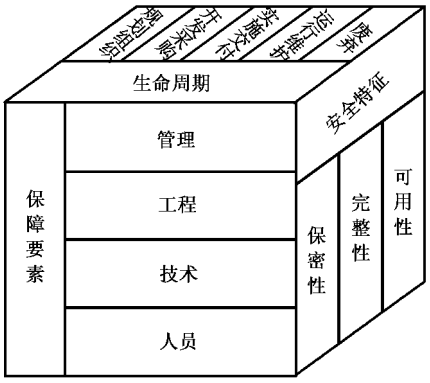

图 3　信息系统安全保障模型

整个信息系统安全保障模型包含保障要素、生命周期和安全特征三方面。

本模型主要特点为：

a）　以安全概念和关系为基础，将风险和策略作为信息系统安全保障的基础和核心；

b）　强调信息系统安全保障持续发展的动态安全模型，即强调信息系统安全保障应贯穿于整个信息系统生命周期的全过程中；

c）　强调信息系统安全保障的概念，信息系统的安全保障是通过综合技术、管理、工程和人员的安全保障要求来实施和实现信息系统的安全保障目标，通过对信息系统的技术、管理、工程和人员要求的评估，提供了对信息系统安全保障的信心；

d）　通过以风险和策略为基础，在整个信息系统的生命周期中实施技术、管理、工程和人员保障要素，从而使信息系统安全保障实现信息安全的安全特征：信息的保密性、完整性和可用性特征，

从而达到保障组织机构执行其使命的根本目的。

本标准更强调信息系统所处的运行环境、信息系统的生命周期和信息系统安全保障的概念。信息系统生命周期有各种各样的模型，在本标准中的信息系统生命周期模型是基于这些模型的一个简单、抽象的概念性说明模型，它的主要用途在于对信息系统生命周期模型进行示例说明。在进行信息系统安全保障具体操作时，可根据实际环境和要求，在信息系统生命周期内进行改动和细化。在这里，强调信息系统生命周期的意义是强调信息系统安全保障并不是仅在某个时间点下的安全，而是在信息系统的整个生命周期中通过对技术、管理、工程和人员这些方面建立信息系统安全保障，来保证信息系统整个生命周期的、动态持续的、长效的安全。

5.2.2.2 在信息系统生命周期中的安全保障

在信息系统安全保障模型中，信息系统的生命周期层面和保障要素层面不是相互孤立的，而是相互关联、密不可分的。图4示例化地描述了它们之间的关系。

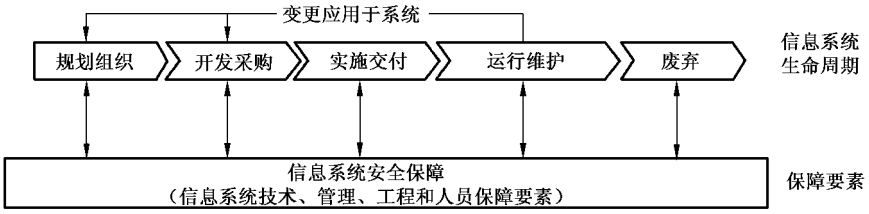

图4 信息系统安全保障生命周期的安全保障要素

在信息系统生命周期模型中，将信息系统的整个生命周期抽象成规划组织、开发采购、实施交付、运行维护和废弃五个阶段以及在运行维护阶段的变更产生的反馈，形成信息系统生命周期完整的闭环结构。在信息系统的生命周期中的任何时间点上，都需要综合信息系统安全保障的技术、管理、工程和人员保障要素对信息系统进行安全保障。

a) 规划组织阶段：由于组织机构的使命要求和业务要求产生了信息系统安全保障建设和使用的需求。在此阶段，信息系统的风险及策略应加入至信息系统建设和使用的决策中，从信息系统建设的开始就应该综合考虑系统的安全保障要求，使信息系统的建设和信息系统安全保障的建设同步规划、同步实施。

b) 开发采购阶段：此阶段是规划组织阶段的细化、深入和具体体现，在此阶段中，进行系统需求分析、考虑系统运行的需求、进行系统体系的设计以及相关的预算申请和项目准备等管理活动。在此阶段，应克服传统的基于具体技术或产品的片面性，要基于系统需求和风险、策略将信息系统安全保障作为一个整体进行系统体系的设计和建设，以建立信息系统安全保障整体规划和全局视野。组织机构可根据具体要求，对系统整体的技术、管理安全保障规划或设计进行评估，以保证对信息系统的整体规划满足组织机构的建设要求和相关国家、行业和组织机构的其他要求。

c) 实施交付阶段：在此阶段，组织机构可通过对承建方进行安全服务资格要求和信息安全专业人员资格要求以确保施工组织的服务能力；组织机构还可通过信息系统安全保障的工程保障对实施施工过程进行监理和评估，最终确保所交付系统的安全性。

d) 运行维护阶段：信息系统进入运行维护阶段后，对信息系统的管理、运行维护和使用人员的能力等方面进行综合保障，是信息系统得以安全正常运行的根本保证。

e) 变更和反馈：信息系统投入运行后并不是一成不变的，它随着业务和需求的变更、外界环境的变更产生新的要求或增强原有的要求，重新进入信息系统的规划阶段。

f) 废弃阶段：当信息系统的保障不能满足现有要求时，信息系统进入废弃阶段。

这样，通过在信息系统生命周期的所有阶段融入信息系统安全保障概念，确保了信息系统的持续动态安全保障。

5.3 信息系统安全保障评估

5.3.1 概述

信息系统安全保障评估，就是在信息系统所处的运行环境中对信息系统安全保障的具体工作和活动进行客观的评估，通过信息系统安全保障评估所搜集的客观证据，向信息系统的所有相关方提供信息系统的安全保障工作能够实现其安全保障策略，能够将其所面临的风险降低到其可接受的程度的主观信心。信息系统安全保障评估的评估对象是信息系统，信息系统是用于采集、处理、存储、传输、分发和部署信息的整个基础设施、组织结构、人员等的总和，因此信息系统不仅包含了仅讨论技术的信息技术系统，还包括同信息系统所处的运行环境相关的人和管理等领域。信息系统安全保障是一个动态持续的过程，涉及信息系统整个生命周期，因此信息系统安全保障的评估也应该提供一种动态持续的信心。

5.3.2 信息系统安全保障评估概念和关系

评估是信息系统安全保障的一个重要概念，系统所有者可以根据评估所得到的客观评估结果建立其主观的信心。图5描述了信息系统安全保障评估的概念和关系。

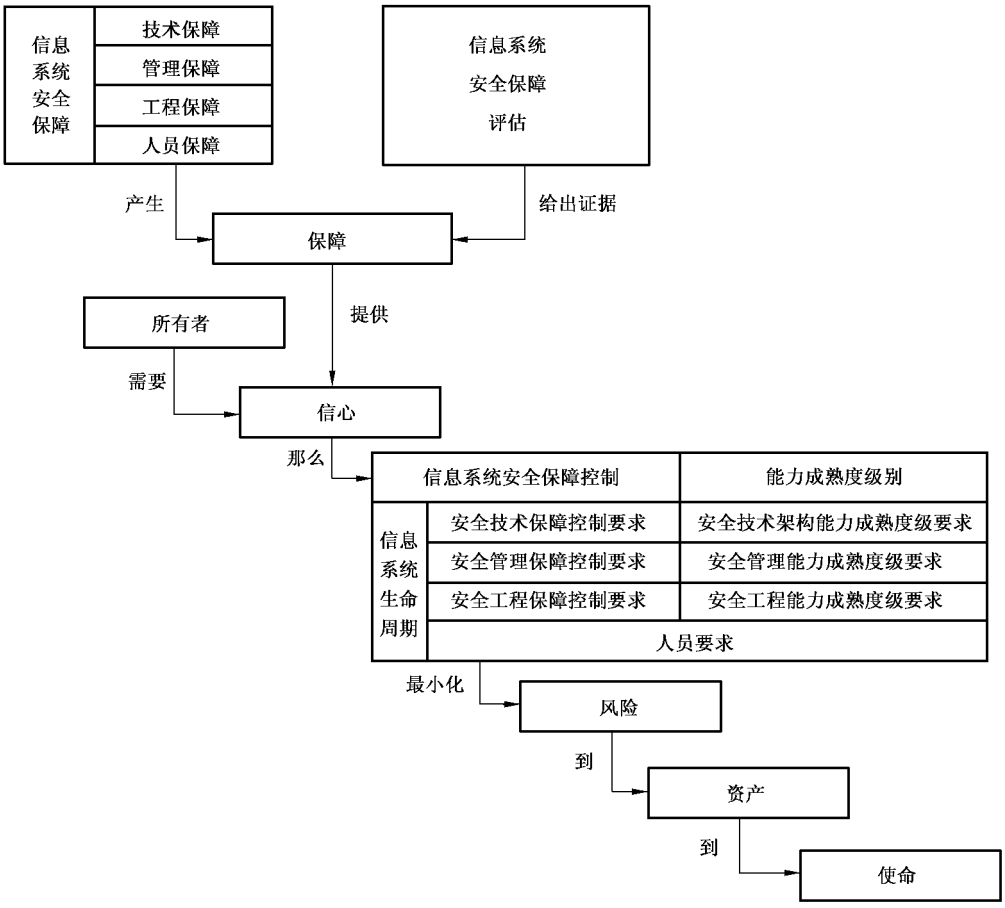

图5 信息系统安全保障评估概念和关系

5.3.3 信息系统安全保障评估内容

5.3.3.1 概述

信息系统安全保障的评估，是从信息系统安全保障的概念出发，在信息系统的生命周期内，根据组织机构的要求，在信息系统的安全技术、安全管理和安全工程领域内对信息系统的安全技术控制措施和技术架构能力、安全管理控制和管理能力以及安全工程实施控制措施和工程实施能力进行评估综合，从而最终得出信息系统在其运行环境中安全保障措施满足其安全保障要求的符合性以及信息系统安全保

障能力的评估。图 6 给出信息系统安全保障评估的描述。

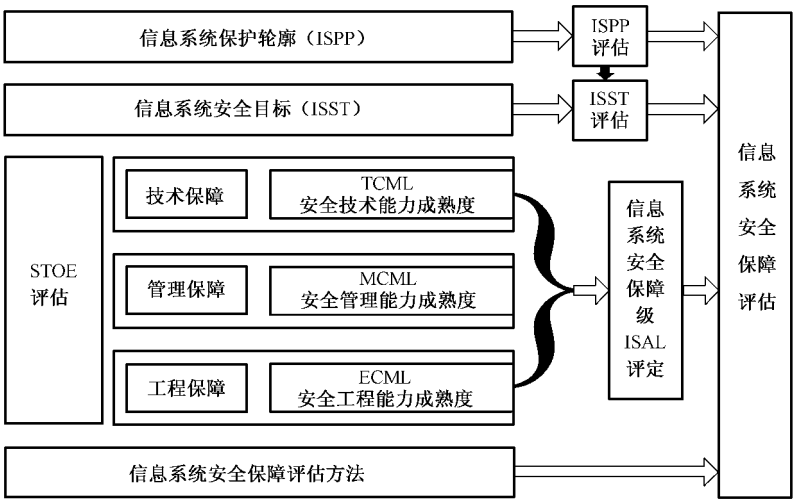

图 6　信息系统安全保障评估说明

信息系统安全保障评估主要包括两方面的评估：信息系统在其运行环境中其具体的安全保障控制相对于安全保障要求的符合性的评估以及信息系统安全保障级的评估。

a）　信息系统在其运行环境中其安全保障控制对安全保障要求的符合性（即信息系统的技术体系、管理控制和工程实施相对于信息系统在其运行环境下的符合性），是同信息系统保护轮廓（ISPP）和信息系统安全目标（ISST）相关的内容。信息系统保护轮廓（ISPP）是从信息系统的所有者角度来描述的信息系统安全保障的规范化需求描述。对信息系统保护轮廓（ISPP）的评估就是评估所编制的信息系统保护轮廓（ISPP）是否符合 ISPP 规范化描述的要求以及评估它是否真正反应了信息系统所有者的真实的安全保障要求。信息系统安全目标（ISST）是从信息系统安全保障的建设方角度来描述的信息系统安全保障方案。信息系统安全目标（ISST）的评估就是评估所编制的信息系统安全目标（ISST）是否符合 ISST 规范化描述的要求以及它是否能够真正解决和满足信息系统保护轮廓（ISPP）的信息系统安全保障要求。

b）　信息系统安全保障级（ISAL）是信息系统所提供的各项安全技术保障、安全管理保障、安全工程保障的实施、正确性、质量和能力进行保障（或信心）的强度和程度的特征，是对信息系统安全保障持续改进的能力特征的描述。信息系统安全保障级（ISAL）是信息系统在其运行环境中，实施信息系统安全保障方案（即实施信息系统安全目标（ISST））的具体实施情况和实施能力的反应。

5.3.4　信息安全整体和应用

本标准是建立在 GB/T 18336 信息技术安全性评估准则的基础之上的综合安全技术、安全管理、安全工程等要求的综合评估。图 7 描述了包含 GB/T 18336 和本标准的信息系统安全保障评估的整体和应用。

在信息系统安全保障评估的整体中，信息技术安全性评估准则是本标准的基础，本标准是信息技术安全性评估准则的扩展和补充。信息系统安全保障评估整体和应用的含义如下：

a）　GB/T 18336 是本标准的基石，它为本标准提供了本质的信息技术安全性评估的准则，为信息系统安全保障评估引入了科学、严格的方法论。在信息技术安全性评估准则之上，是相应的功能/保证类扩展，这些功能/保证类扩展的标准化，方便了进一步建立相关产品保护轮廓等。

b) 本标准是基于信息技术安全性评估准则的扩展，它在吸取了信息技术安全性评估准则的方法和原则之上，根据信息系统的特点，分别建立了安全技术、安全管理和安全工程的保障框架，完善了信息技术安全性评估准则在信息系统领域的应用。

c) 其他相关辅助资料包括信息技术安全性评估方法、信息系统安全保障评估方法等资料。

d) 特定领域信息系统安全保障要求是本标准在特定领域和行业的深化。

e) 信息系统保护轮廓(ISPP)是根据组织机构使命和所处的运行环境，从组织机构的策略和风险的实际情况出发对具体信息系统安全保障要求和能力的具体描述。

f) 信息系统安全目标(ISST)是针对信息系统保护轮廓(ISPP)所编制的满足信息系统所处的运行环境中的信息系统安全保障方案。

g) 以上各个层次的标准、准则、框架、保护轮廓、安全目标等，构成了对信息系统进行安全性评估的整体体系。其中，GB/T 18336 主要是对产品和产品系统进行评估，本标准主要是对信息系统的安全工程、安全管理和安全技术分别或信息系统整体进行评估。

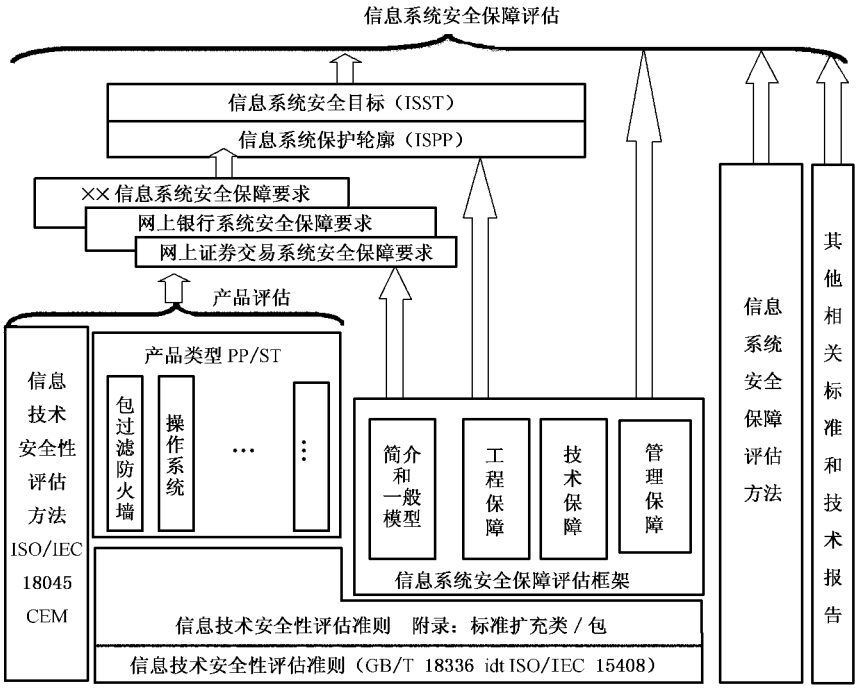

图 7 信息系统安全保障评估整体和应用

5.4 ISPP 和 ISST 的生成

5.4.1 概述

本条仅提供例证和指导，并不限制生成 ISPP、ISST 的具体的分析过程、开发方法、评估体制。

本标准只有在针对某类或特定的信息系统，采用合适的信息系统安全技术保障控制组件、安全管理保障控制组件、安全工程保障控制组件和相应的能力成熟度级别，生成相应的 ISPP、ISST 时，才是可操作的。

如图 8 描述，本标准将表述分成不同的层次，它阐明了一种方法，通过它当开发一种 ISPP 或 ISST 时，就能引申出安全保障要求和规范。所有的信息系统安全保障要求根本上均来源于对 TOE 的目的、环境和信息系统本身的考虑。这个图表不打算限制 ISPP 和 ISST 开发的方法，而在于阐明一些分析方法的结果是怎么与 ISPP 和 ISST 的内容相联系的。

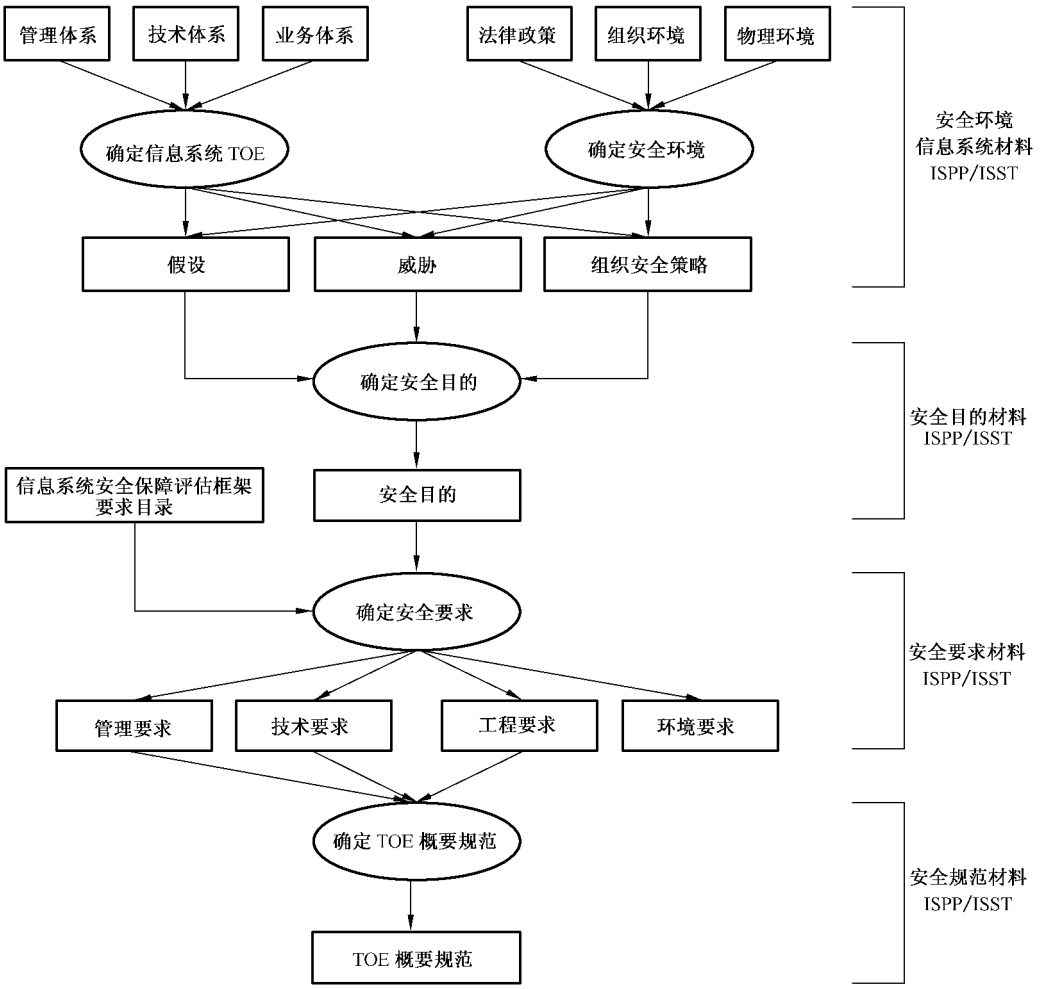

图 8　ISPP 和 ISST 的生成过程

5.4.2　安全环境

安全环境包括所有的明确相关的法律政策、组织机构的策略、物理环境，它定义了信息系统的运行环境。

为建立安全环境，ISPP 或 ISST 的作者必须考虑以下几点：

a）　信息系统的物理环境，指所有的与信息系统安全相关的运行环境，如已知的物理部署、自然条件、建筑物等；

b）　组织机构内部相关的组织、业务、管理策略；

c）　法律政策，包括国家的法律法规、行业的政策、制度规范等。

关于假设、安全威胁、组织安全策略的描述应注意以下内容：

a）　对假设的陈述。如果环境满足该假定，信息系统可以被认为是安全的。对信息系统的评估而言，该陈述可以作为公理而接受。

b）　安全威胁的陈述。本陈述应指明信息系统相关的安全分析中发现的所有威胁。本标准使用威胁动机、假定的攻击方法、作为攻击基础的任何弱点和被攻击的资产名称等词汇描述一个威胁。对安全风险的评估是通过给出每一种威胁实际发生的可能性、该威胁成功实施的可能性以及可能造成的被破坏后果来实现的。

c）　组织安全策略的陈述将阐明相关的策略和规则。对特定的信息系统，可能明确提及这样的策略，然而对一般的信息系统，可能需要假设出组织机构的安全策略。

5.4.3 安全保障目的

环境安全性分析结果被用来阐明安全保障目的，对抗其所面临的威胁，并说明被认定的组织化的安全策略和假设。安全保障目的应和已说明的信息系统运行的法律法规要求、组织机构环境要求和物理环境一致。

确定安全保障目的的意图是为了阐明所有的安全考虑并指出哪些安全方面的问题是直接由信息系统来处理，哪些由其环境来处理。这种归类基于工程判断、安全政策、经济因素和可接受的风险决策相结合的过程。

环境的安全保障目的将在信息系统领域内用非技术、管理、工程的手段来实现。

5.4.4 安全保障要求

安全保障要求是将安全目的细化为一系列信息系统及其环境的安全保障要求，一旦这些要求得到满足，就可以保证信息系统达到它的安全目的。

本标准分别从安全技术领域的技术保障控制要求和技术架构能力成熟度级要求、安全管理领域的管理保障控制要求和管理能力成熟度级要求以及安全工程领域的工程保障控制要求和工程能力成熟度级要求来提出安全保障要求。安全保障要求的组成如下：

a) 安全技术保障要求。技术保障要求来自于支持信息系统安全保障的那些技术领域中期望的安全行为。本标准第2部分定义了安全技术保障控制要求和技术架构能力成熟度级。

b) 安全管理保障要求。管理保障要求来自于支持信息系统安全保障的那些管理领域中期望的安全行为。本标准第3部分定义了安全管理保障控制要求和管理能力成熟度级。

c) 安全工程保障要求。工程保障要求来自于支持信息系统安全保障的那些工程领域中期望的安全行为。本标准第4部分定义了安全工程保障控制要求和工程能力成熟度级。

通过合理选择的安全技术、管理和工程保障控制要求及其能力成熟度级，可以确保达到一定的安全保障目的，这种保证来源于以下两个因素：

a) 对安全保障控制（包括安全技术保障控制、管理保障控制和工程保障控制）正确实现的信任，也就是评估实现的正确性。

b) 对安全保障控制实现的有效性和长效性的信任，也就是评估组织机构实现安全保障控制的能力级别（包括安全技术架构能力成熟度级别、管理能力成熟度级别和工程能力成熟度级别）。

5.4.5 TOE概要规范

在安全保障目标（ISST）中提供的TOE概要规范定义了TOE安全保障要求的实例。它提供了高层设计的描述，分别满足安全控制措施的要求以及能力成熟度的要求。

5.4.6 TOE实现

TOE实现是基于TOE的安全技术、管理和工程保障要求和ISST中的TOE概要规范的具体实现。TOE的实现就是完成一个应用安全和信息系统工程技巧、知识的整合过程。如果正确有效地实现了ISST中包含的所有的安全保障要求，TOE将达到其安全目的。

5.5 信息系统安全保障描述材料

5.5.1 概述

本标准提出了信息系统安全保障的框架。通过对证明和分析提出要求，可以得到更为客观、有用的评估结果。本标准为信息系统安全保障提供了一种标准化、规范化的公共描述语言、结构和方法，这将帮助信息系统安全保障工作的所有相关方（包括设计开发人员、评估人员等）描述和沟通其信息系统安全保障的要求。

5.5.2 安全保障要求的表达

5.5.2.1 概述

本标准定义了一系列表达信息系统安全保障要求的组件的集合，通过将各种组件组合起来，就形成了信息系统安全保障要求。

信息系统安全保障要求根据安全技术、安全管理和安全工程领域的不同，分为安全技术保障要求、安全管理保障要求和安全工程保障要求。每种安全保障要求又分为安全保障控制要求和能力成熟度要求。安全保障控制要求包括安全技术保障控制、安全管理保障控制和安全工程保障控制。它们都使用“类—子类—组件”层次化的结构。能力成熟度要求使用六级能力成熟度级别的结构。这六级能力成熟度级别是：能力级别 0——未实施、能力级别 1——基本执行、能力级别 2——计划跟踪、能力级别 3——充分定义、能力级别 4——量化控制和能力级别 5——持续改进，具体详见 5.5.2.3。

图 9 描述了表达安全保障控制要求的不同结构之间的关系，其不同结构之间的关系将在后面描述。

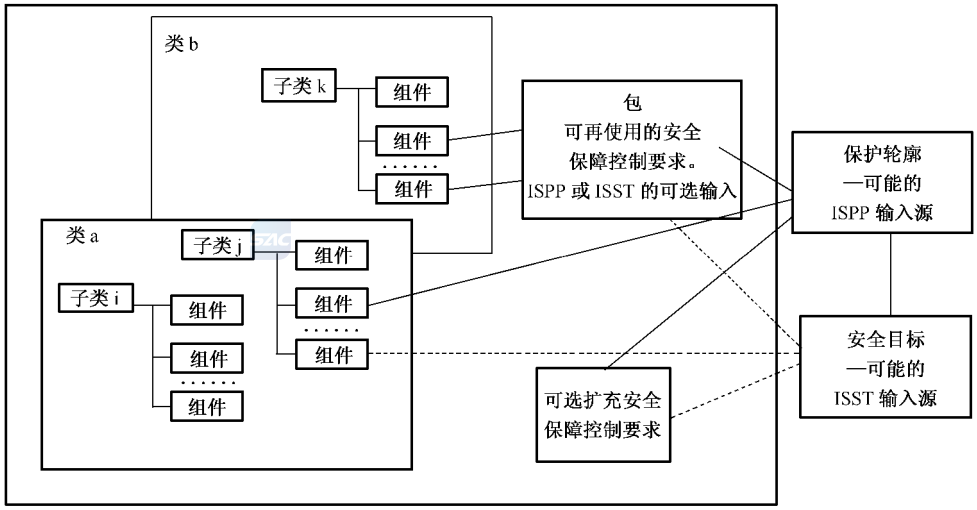

图 9　安全保障控制要求的组织和结构

用户可根据需要选择特定的安全保障控制和能力成熟度级别要求。

5.5.2.2　安全保障控制要求的结构

本标准的安全保障控制要求，包括安全技术保障控制要求、安全管理保障控制要求和安全工程保障控制要求，它们都使用类—子类—组件这种层次化的组织结构，以帮助用户选择特定的安全保障控制要求。

a）　安全保障控制类。安全保障控制类是最通用的一组安全保障控制要求的组合。类的所有成员关注同一个安全问题，区别在于覆盖不同的安全保障目的。在本标准中，根据安全保障控制要求所属领域的不同，分为安全技术保障类、安全管理保障类和安全工程保障类。类的成员被称为子类。

b）　安全保障控制子类。安全保障控制子类是若干组安全保障控制要求的组合，这些要求针对同一个安全保障目的，但在强度和程度上有所区别。在本标准中，安全技术保障类、安全管理保障类和安全工程保障类的子类分别为安全技术保障子类、安全管理保障子类和安全工程保障子类。子类的成员被称为安全保障控制组件，简称组件。每个安全保障控制子类由一个安全保障目的和一个或多个实现此安全保障目的的安全保障控制组件组成。

c）　安全保障控制组件。安全保障控制组件描述一个明确的安全保障控制要求集合，并且它是本标准定义的结构中所包含可选的最小安全保障要求集合。安全保障控制组件是实现其安全保障控制子类的安全保障控制目的的信息安全保障具体控制措施。在本标准中，根据安全保障控制要求所属领域的不同，分为安全技术保障控制组件、安全管理保障控制组件和安全工程保障控制组件。安全保障控制组件由可选的安全保障控制元素组成。

安全保障控制组件是实现安全保障控制目的的信息安全保障具体控制措施，在本标准中，为安全按保障控制组件提供了组件间的依赖和组件允许的操作以提供组织机构使用安全保障控制组件的灵活性。安全保障控制组件间的依赖和安全保障控制组件允许的操作说明如下：

a) 安全保障控制组件间的依赖：

安全保障控制组件间可能存在依赖关系。当一个安全保障控制组件无法充分表达安全保障控制要求并且依赖于另一个安全保障控制组件的存在时，依赖关系就产生了。依赖关系可以存在于安全技术保障控制、安全管理保障控制和安全工程保障控制各自内部的组件之间，也可以存在于安全技术保障控制、安全管理保障控制和安全工程保障控制的组件之间。

安全保障控制组件间依赖关系描述是本标准安全保障控制组件定义的一部分。为了保证达到TOE要求的完备性，当把组件加入到适当的ISPP和ISST中时，应满足相应的依赖关系。

b) 安全保障控制组件允许的操作：

安全保障控制组件可以像在本标准中定义的那样使用，或者通过使用安全保障控制组件允许的操作对安全保障控制组件进行裁剪，以满足特定的安全策略或对抗特定的威胁。安全保障控制组件说明并定义了组件是否允许“赋值”和“选择”操作、在哪些情况下可对组件使用这些操作以及使用这些操作的后果。任何安全保障控制组件都允许“反复”和“细化”操作。这四个操作如下所述：

1) 反复：在不同操作时，允许组件多次使用；
2) 赋值：当组件被应用时，允许规定所填入的参数；
3) 选择：允许从组件表中选定若干项；
4) 细化：当组件被应用时，对组件增加细节。

5.5.2.3 安全保障能力成熟度级要求的结构

本标准的安全保障能力成熟度级要求，包括安全技术架构能力成熟度级要求、安全管理能力成熟度级要求和安全工程能力成熟度级要求。这三种能力成熟度级要求都分别用所对应的能力成熟度级别要求来表达。

本标准采用六级能力成熟度级别要求，分别为：

a) 能力级别0：未实施；
b) 能力级别1：基本执行；
c) 能力级别2：计划跟踪；
d) 能力级别3：充分定义；
e) 能力级别4：量化控制；
f) 能力级别5：持续改进。

每种能力成熟度级别的具体要求将在本标准的第2、第3和第4部分中详细介绍。

5.5.3 安全保障要求的使用

5.5.3.1 概述

本标准定义了三种类型的安全保障控制要求结构：包、ISPP和ISST。开发这些结构的中心观念是尽可能使用本标准所定义的安全保障要求组件，这些组件都代表众所周知、易于理解的领域。图10表明了这些不同结构间的关系。

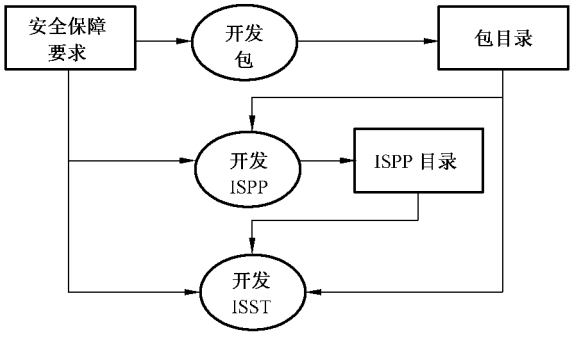

图10 安全保障要求的应用

5.5.3.2 包

组件的中间组合被称为包。包允许描述安全保障控制要求和安全保障能力成熟度级要求的一个集合，满足指定安全保障目的的子集。包可重复使用，可用来定义那些公认有用的、对满足特定安全目的有效的要求。包可用在构造更大的包、ISPP 和 ISST 中。

5.5.3.3 信息系统保护轮廓

信息系统保护轮廓(ISPP)包含信息系统安全保障评估框架中的或明确阐述的安全保障要求。ISPP 可以描述与实现无关的一系列 TOE 的安全保障要求，这些要求与安全目的完全一致。ISPP 可以反复使用，还可用来定义公认有用的、有效并达到特定安全目的的 TOE 要求。ISPP 也包括安全目的和安全保障要求的基本原理。

ISPP 的开发者可以是用户团体、信息系统开发者或其他对定义这样一系列通用要求有兴趣的团体。ISPP 为消费者提供了一套方法，有关一组特定安全保障要求以及有助于将来对这些要求进行评估。

5.5.3.4 信息系统安全目标

信息系统安全目标(ISST)包括一系列安全保障要求，这些要求可以引用 ISPP，也可以直接引用信息系统安全保障评估框架中的技术、工程和管理组件，或明确阐述。ISST 允许对特定 TOE 的安全保障要求进行描述，通过评估可以证明该 TOE 有用和有效的满足指定目的。

ISST 包含 TOE 的概要规范，同时还包括安全保障要求和目的，以及它们的基本原理。ISST 是各个相关方对 TOE 提供什么样的安全性达成一致的基础。

5.5.4 安全保障要求的来源

TOE 安全保障要求可以通过使用下列输入来构造：

a) 已存在的 ISPP：

1) ISST 中 TOE 的安全保障要求可使用或完全遵从已存在的 ISPP 中的要求来充分地表达；

2) 已有的 ISPP 可以作为新 ISPP 的基础。

b) 已存在的包：

ISPP 或 ISST 中的部分 TOE 安全保障要求可能已在包中表述。

c) 已存在的安全技术保障控制、安全管理保障控制和安全工程保障控制要求组件：

ISPP 或 ISST 中的 TOE 安全技术保障控制、安全管理保障控制和安全工程保障控制要求可以通过使用本标准的第 2、第 3 或第 4 部分的安全保障控制组件直接表达。

d) 扩展的要求：

不包括在本标准的第 2、第 3 和第 4 部分的附加的技术、管理和工程要求也可在 ISPP 或 ISST 中使用。

应尽可能使用来自本标准的第 2、第 3 和第 4 部分已存在的安全保障控制要求。使用已存在的 ISPP 有助于保证 TOE 满足一组公认的已知功用的要求，进而有利于 TOE 被广泛地认可。

6 信息系统安全保障评估和评估结果

6.1 介绍

本章给出 ISPP 和 TOE 评估的预期结果。ISPP 或者 TOE 评估将分别得到经评估的 ISPP 或 TOE 的目录。ISST 评估的结果是 TOE 评估框架中使用的中间结果。见图 11。

不管有没有绝对客观的尺度描述信息系统安全保障评估结果，评估过程都应能产生出客观的、可重复的可作为证据的结果。评估标准是评估结果有意义的必要前提，同时也是不同评估机构之间评估结果互认的技术基础。但标准的应用包含了主观和客观的因素，这也是不可能精确且通用评定信息系统安全保障级别的原因。

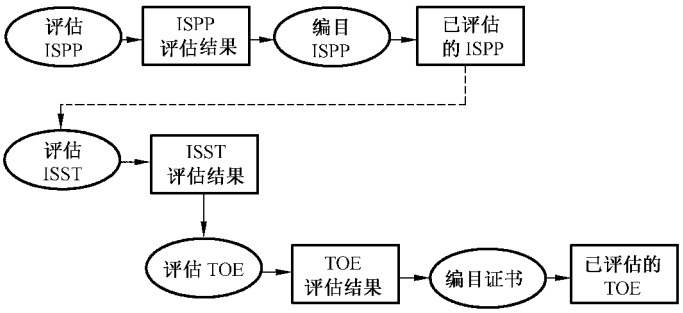

图 11　评估结果

本标准中的级别评定是对某一 TOE 的安全性质进行专门研究的结果。这种级别评定并不保证适用于任何特定的应用环境。在特定应用环境下决定是否让 TOE 投入使用，应考虑包括评估结果在内的多个安全因素。

6.2　ISPP(信息系统保护轮廓)和 ISST(信息系统安全目标)的要求

6.2.1　概述

本标准定义了一套能满足大多数组织需求的安全保障控制要求和能力成熟度级要求。本标准是围绕这样一个中心思想展开的，即在 ISPP 和 ISST 中描述 TOE 的安全保障要求时，尽可能使用本标准的第 2 部分的安全技术保障控制要求组件和安全技术架构能力成熟度级要求、本标准的第 3 部分的安全管理保障控制要求组件和安全管理能力成熟度级以及本标准的第 4 部分的安全工程保障控制要求组件和安全工程能力成熟度级，因为它们已被公认和理解。

也可能需要本标准中未列出的安全技术保障控制要求、安全管理保障控制要求和安全工程保障控制要求，以完整表达对信息系统安全保障的要求。以下内容适用于包容这些扩展的安全保障控制要求：

a)　ISPP 和 ISST 中包容的任何扩展的安全保障控制要求必须清晰和明确地表达，以便评估和证实。可以参照已经存在的信息系统安全技术保障控制、安全管理保障控制和安全工程保障控制要求组件描述的详细程度和方式。

b)　应声明评估结果是通过使用扩展的安全保障控制要求得到的。

6.2.2　ISPP 评估结果

本标准可帮助评估者说明一个 ISPP 是否完备、一致和正确，并可用于描述一个可评估 TOE 的安全保障要求。

ISPP 的评估结果为“通过”或“失败”。评估结果为“通过”的 ISPP 才可以注册登记。

6.3　TOE 的要求

6.3.1　概述

本标准可帮助评估者判定 TOE 是否满足了 ISST 中描述的安全保障要求。在 TOE 的评估中使用本标准，评估者应能够说明：

a)　TOE 的指定安全保障控制是否满足安全保障控制要求，进而有效地达到 TOE 的安全目的。

b)　TOE 的指定能力成熟度级是否正确地实现。

在本标准中的技术保障、工程保障和管理保障要求定义了公认的信息系统安全保障评估标准适用的工作领域。一个 TOE 的安全保障要求只有使用本标准中的安全保障控制要求和能力成熟度级别要求术语进行描述，该 TOE 才可以按照本标准进行评估。

不过，也存在这样的可能，无法直接使用本标准描述 TOE 的安全保障要求。本标准也考虑到了评估这种 TOE 的必要性，但是，因为附加要求属于本标准的公认的适用领域之外，因此，这种评估的结果应作相应声明。这种声明可能会使评估结果不为相关评估机构广泛接受。

TOE 的评估结果应包括与本标准一致性的陈述。运用本标准的术语来描述 TOE 的安全，使不同 TOE 的安全特性可以进行比较。

6.3.2 TOE 评估结果

TOE 评估结果应说明 TOE 满足指定要求的可信程度。

TOE 的评估结果为“通过”或“失败”。评估结果为“通过”的 TOE 才可以注册登记。

6.4 评估结果的声明

评估的“通过”结果应说明对 ISPP 或 TOE 满足指定要求的可信程度。

评估结果应分别针对本标准的第 2 部分、第 3 部分、第 4 部分或直接针对 ISPP 按下列进行说明：

a) 本标准第 2 部分一致——当安全技术保障要求只建立在第 2 部分的安全技术保障控制组件上，并且只使用第 2 部分的安全技术能力成熟度级要求时，ISPP 或 TOE 是第 2 部分一致的。

b) 本标准第 2 部分外扩——如果安全技术保障要求包含有第 2 部分中没有的安全技术保障控制组件，并且只使用第 2 部分的安全技术能力成熟度级要求时，ISPP 或 TOE 是第 2 部分外扩的。

c) 本标准第 3 部分一致——当安全管理保障要求只建立在第 3 部分的安全管理保障控制组件上，并且只使用第 3 部分的安全管理能力成熟度级要求时，ISPP 或 TOE 是第 3 部分一致的。

d) 本标准第 3 部分外扩——如果安全管理保障要求包含有第 3 部分中没有的安全管理保障控制组件，并且只使用第 3 部分的安全管理能力成熟度级要求时，ISPP 或 TOE 是第 3 部分外扩的。

e) 本标准第 4 部分一致——当安全工程保障要求只建立在第 4 部分的安全工程保障控制组件上，并且只使用第 4 部分的安全工程能力成熟度级要求时，ISPP 或 TOE 是第 4 部分一致的。

f) 本标准第 4 部分外扩——如果安全工程保障要求包含有第 4 部分中没有的安全工程保障控制组件，并且只使用第 4 部分的安全工程能力成熟度级要求时，ISPP 或 TOE 是第 4 部分外扩的。

g) ISPP 一致——只有当 TOE 与 ISPP 的所有部分一致时它才是 ISPP 一致的。

6.5 TOE 评估结果的应用

本标准可分别用于工程、技术和管理的评估，也可以用于对信息系统整体进行评估。

TOE 的建设要求需要考虑已评估的工程、技术、管理和系统，以及所引用 ISPP 的安全性质，随后的 TOE 评估会产生一系列文档化的评价结果。

当所评估的 TOE 是或将是一个实际环境中运行的信息系统，评估结果对系统认可者才是有效的。当认可者使用组织专用的认可准则，而认可准则要求进行信息系统安全保障评估时，应考虑信息系统安全保障评估框架的评估结果。

附 录 A
（规范性附录）
信息系统保护轮廓

A.1 概述

一个信息系统保护轮廓(ISPP)定义了某种类型信息系统的与实现无关的一组系统级安全保障要求。这些类型的信息系统是用来满足用户对信息系统安全保障的需求，因而用户可以不必参考特定的信息系统就能建立或引用信息系统保护轮廓来表达他们对信息系统安全的要求。

信息系统保护轮廓中，信息系统安全保障的评估对象可包括信息系统整体、信息系统安全管理、信息系统安全技术或信息系统安全工程这几方面。由此产生的信息系统保护轮廓也分别应用于信息系统整体、信息系统安全管理、信息系统安全技术和信息系统安全工程的评估。本附录中所描述的信息系统保护轮廓是将信息系统整体作为评估对象的内容和格式，在将此信息系统保护轮廓格式应用于安全管理保障、安全技术和信息系统安全工程这些方面的评估时，需要将部分内容进行裁减(在信息系统保护轮廓中将详细指出)。

A.2 信息系统保护轮廓内容

A.2.1 内容和表述

信息系统保护轮廓同信息技术安全保障要求略有不同，它是信息技术安全性评估准则安全保障要求在信息系统中的扩展。

信息系统保护轮廓应满足本附录内容的要求。信息系统保护轮廓以面向用户文档的形式给出，它应尽量少地引用用户不易得到的材料。必要时，应单独提供符合性声明。

图 A.1 描述了信息系统保护轮廓的内容，应按其建立信息系统保护轮廓文档大纲。

需要指出的是，当将信息系统安全管理保障、信息系统安全技术保障架构和信息系统安全工程保障作为评估对象时，信息系统保护轮廓中可只出现对应的安全保障要求子项(例如：如将信息系统安全技术保障架构作为评估对象，那么在信息系统保护轮廓部分可只包含信息系统安全技术保障要求)。

A.2.2 ISPP 引言

信息系统保护轮廓引言将包括文档管理和进行信息系统保护轮廓注册所必要的信息，如下所述：

a) 信息系统保护轮廓标识：应提供信息系统保护轮廓的标记和描述的必要信息，供标识、编目、注册和交叉引用；

b) 信息系统保护轮廓概述：以叙述形式描述信息系统保护轮廓。概述应足够详细，使一个潜在用户可以据此确定信息系统保护轮廓是否有价值。概述作为一个独立摘要也可用于信息系统保护轮廓编目和注册。

A.2.3 TOE 描述

信息系统保护轮廓的这部分应描述评估对象，以帮助了解评估对象的安全保障要求。在信息系统安全保障评估框架中，评估对象是信息系统整体或其技术、工程和管理方面的某一局部领域。无论是信息系统整体还是某一领域，在评估对象描述中都必须先给出整个信息系统的完整描述，然后再对确切的评估对象作进一步描述。

评估对象描述提供了用于评估的上下文。在评估对象描述中给出的信息将用于在评估过程中识别不一致的地方。由于信息系统保护轮廓一般不指明特定的实现，因此描述的评估对象特性可能是假设的。评估对象描述的具体内容可参考安全保障目标对 TOE 描述的具体要求，抽象提炼出所评估信息系统类的共同特征。

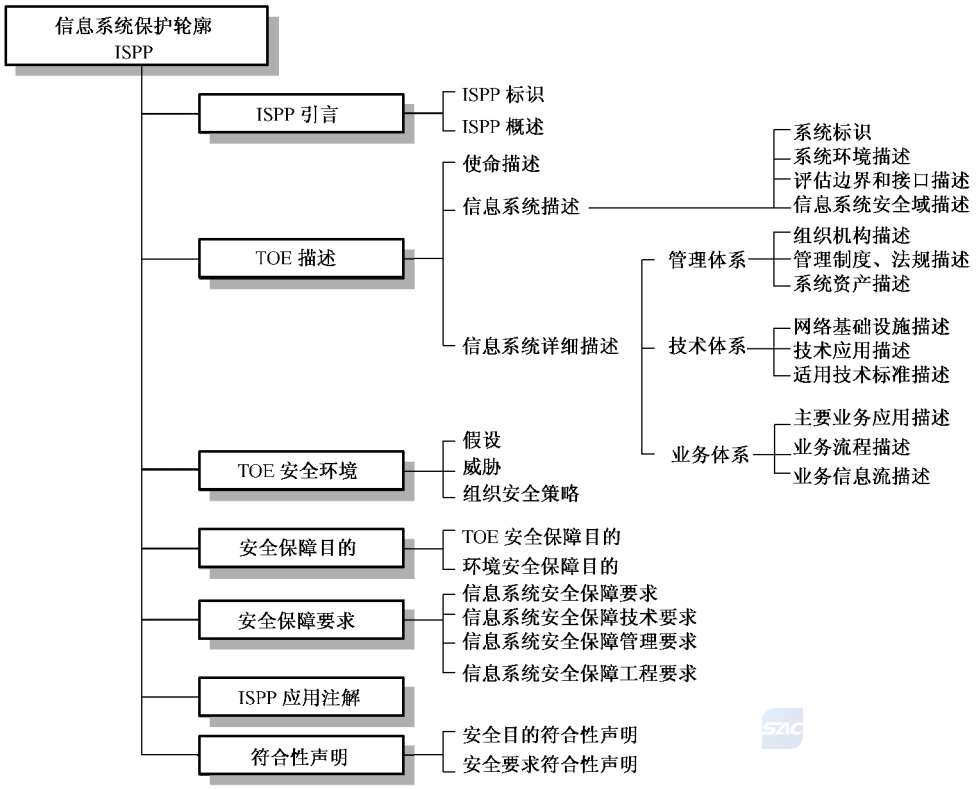

图 A.1　信息系统保护轮廓内容

A.2.4　TOE 安全环境

信息系统安全环境的陈述应描述信息系统所处环境的安全问题和信息系统使用环境的方式。该陈述包括以下几点：

a）　假设的描述应描述信息系统将在或拟在使用的环境的安全问题，它将包括以下两点：

1）　关于信息系统预期使用方式的信息，如：预期的应用、潜在的资产价值、可能的使用限制；

2）　有关信息系统使用环境的信息，如：在物理的、人员的和连通性方面。

b）　威胁的描述将描述对资产的所有威胁，这些资产是在信息系统或其环境内需要特定保护的。值得注意的是，并非所有的在环境中可能遇到的威胁都必须列出，只有那些与信息系统的安全运行相关的威胁才需要列出。威胁应通过已确定的威胁主体、攻击和作为攻击对象的资产进行描述。威胁主体应通过注入专门技术、可用资源和动机等来描述。攻击应通过诸如攻击方法、可利用的脆弱性和时机等来描述。如果安全保障目的仅仅来源于组织性安全策略和假设，可以省略对威胁的描述。

c）　组织安全策略的描述应确定信息系统必须遵守的所有组织安全策略陈述或规则，必要时还应加以说明。如果使用某个策略来建立清晰的安全保障目的，就必须对策略陈述进行说明和解释。如果安全保障目的仅仅来自威胁和假设，可以略去组织安全策略。

A.2.5　安全保障目的

安全保障目的的陈述定义信息系统及其环境的安全保障目的。安全保障目的应涉及已确定安全环境的所有方面。安全保障目的应反映被陈述的意图，并应适用于所有已知的组织安全策略和假设。应指明以下两类安全保障目的。（注意：当威胁或组织安全策略部分被 TOE 所覆盖并部分被它的环境所覆盖，那么相关的安全保障目的应在每一个种类中重复。）

a）　应明确说明信息系统安全保障目的，并且可追溯到信息系统所对抗的已知威胁或信息系统可满足的组织安全策略；

b） 应明确说明环境安全保障目的，并且可追溯到已知的信息系统无法完全对抗的威胁或信息系统无法完全满足的组织安全策略及假设。

注意环境安全保障目的可以是全部或部分的信息系统安全环境陈述的假设部分的重述。

A.2.6 信息系统安全保障要求

这部分详细定义信息系统及其环境应满足的信息系统安全保障要求。信息系统安全保障要求应按下列方式描述：

a） 信息系统安全保障要求的陈述应定义信息系统的技术、管理和工程的安全保障要求或综合这些领域的信息系统整体的安全保障要求。根据评估对象类型的不同，信息系统安全保障要求包括以下全部或部分内容：

1） 信息系统整体安全保障要求的陈述应能给出信息系统整体的安全保障要求的概要性描述；

2） 信息系统技术安全保障要求的陈述应把评估对象的技术安全保障要求定义为从本标准的第2部分中提取的技术安全保障控制组件和安全技术架构能力成熟度要求；

3） 信息系统管理安全保障要求的陈述应把评估对象的管理安全保障要求定义为从本标准的第3部分中提取的管理安全保障控制组件和安全管理能力成熟度要求；

4） 信息系统工程安全保障要求的陈述应把评估对象的工程安全保障要求定义为从本标准的第4部分中提取的工程安全保障控制组件和安全工程能力成熟度要求。

b） 要注意的是非信息系统环境的安全保障要求，尽管在实际中常常是有用的，但因它们与TOE实现没有直接关系，不要求它们成为ISST的正式部分。

c） 下列通用条件应同样适用于信息系统及其环境的安全保障要求的表达：

1） 所有信息系统的安全技术保障控制要求都应引用本标准第2部分的安全技术保障控制要求组件，所有信息系统的安全管理保障控制要求都应引用本标准第3部分的安全管理保障控制要求组件，所有信息系统的安全工程保障控制要求都应引用本标准第4部分的安全工程保障控制要求组件。如果对所有或部分安全保障控制要求而言，没有打算使用本标准第2、第3和第4部分的安全保障控制组件，ISST应明确说明这些要求没有引用本标准；

2） 所有信息系统的安全技术架构能力成熟度要求、安全管理能力成熟度要求和安全工程能力成熟度要求都应引用本标准第2、第3和第4部分中的能力成熟度要求；

3） 任何一个信息系统安全保障要求均应准确、无歧义地表达，才能进行一致性评估和论证。现有的信息系统安全保障评估框架的技术、管理和工程要求的详细程度和表达方式应当作一个典范来使用。

所有信息系统安全保障要求之间的依赖关系都应满足。依赖关系可以通过在信息系统安全保障要求内包含相关的要求或对环境提出要求而满足。

A.2.7 ISPP应用注解

这个可选的部分可能包括额外的支持信息，该信息对构造、评估或使用信息系统是相关或有用的。

A.2.8 符合性声明

这部分提出用于ISPP评估的依据。这些依据将支持：ISPP是一个完整的、紧密结合的安全保障要求集合，满足该ISPP的信息系统应在安全环境内提供一组有效的信息系统安全模型。符合性声明应包括以下内容：

a） 安全保障目的符合性声明应阐明安全保障目的可追溯到在信息系统安全环境里指明的所有方面，并且能覆盖所有的这些方面。

b） 安全保障要求符合性声明应阐明系列安全保障要求（信息系统和环境）是适合于满足，并可追溯到安全保障目的。应阐明以下几点：

1） 将信息系统及其安全环境的技术、管理和工程要求相组合，能满足所述的安全保障目的；

2） 该组安全保障要求一起构成一个互相支持且内在一致的整体；

3） 安全保障要求的选择应说明理由，所有下列情况都应当专门说明：

——选择本标准的第2、第3和第4部分中没有的要求；

——不满足依赖关系。

这部分材料可能篇幅太大，不一定对所有ISST用户都适合和有用，因此可以单独发行。

附 录 B
（规范性附录）
信息系统安全目标规范

B.1 概述

一个信息系统安全目标包括信息系统安全保障的技术要求、管理要求、工程要求和它们的综合要求以及信息系统所要达到的保证目标。

信息系统安全目标是基于 GB/T 18336 中的安全保障目标在信息系统领域的扩展，两者的格式和内容不完全等同。在本附录中将介绍信息系统安全目标的内容和表述。

信息系统安全目标中，评估对象可包括信息系统整体、信息系统安全管理、信息系统安全技术或信息系统安全工程这几个方面；由此产生的信息系统安全目标也分别应用于信息系统整体、信息系统安全管理、信息系统安全技术或信息系统安全工程的评估。本附录中所描述的信息系统安全目标是将信息系统整体作为评估对象的内容和格式，在将此信息系统保护轮廓格式应用于安全管理保障、安全技术和信息系统安全工程这些方面的评估时，需要将部分内容进行裁减（在信息系统安全中将详细指出）。

对信息系统而言，信息系统安全目标是开发者、评估者、用户在信息系统安全特性和评估范围之间达成一致的基础。对于信息系统安全保障评估框架而言，一个信息系统安全目标（ISST）的编制者不限于对信息系统的制造和评估负有责任，他同时也对信息系统整个生命周期中管理、营销、购买、安装、配置、操作和使用信息系统等负有安全责任。

信息系统安全目标可能包含或宣称符合一个或多个信息系统保护轮廓的要求。最初在 B.2 中定义所要求的 ISST 内容时，并未考虑到 ISPP 的这类一致性声明的影响。B.2.8 中涉及了 ISPP 一致性声明与 ISST 所需内容的影响。

本附录以描述的方式说明了信息系统安全目标的各种要求。

B.2 信息系统安全目标内容

B.2.1 内容和形式

信息系统安全目标同信息技术安全保障目标略有不同，它是信息技术安全性评估准则安全保障要求在信息系统中的扩展。

信息系统安全目标应满足本附录内容的要求。信息系统安全目标应是一个面向用户使用的文档，它应尽量少地引用用户不易得到的材料。必要时，应单独提供符合性声明。

图 B.1 描述了信息系统安全目标的内容，应按其建立信息系统安全目标文档大纲。

需要指出的是，当将信息系统安全技术保障架构、信息系统安全工程保障和信息系统安全管理保障作为评估对象时，信息系统安全目标中可只出现对应的安全保障要求子项（例如：如将信息系统安全技术保障架构作为评估对象，那么在信息系统保护轮廓部分可只包含信息系统安全技术保障要求）。

B.2.2 ISST 引言

信息系统安全目标引言将包括文档管理和概述信息，如下所述：

a) ISST 标识：应提供必要的标记和描述信息，以控制和标识 ISST 和它所指的 TOE；

b) ISST 概述：以叙述形式概述 ISST。概述应有足够的细节提供给 TOE 的潜在用户，以便他们决定对该 TOE 是否有兴趣。概述也可作为一个单独的摘要，包含在已评估产品一览表中；

c) 符合性声明：应说明 TOE 与信息系统安全保障评估框架的符合性声明。

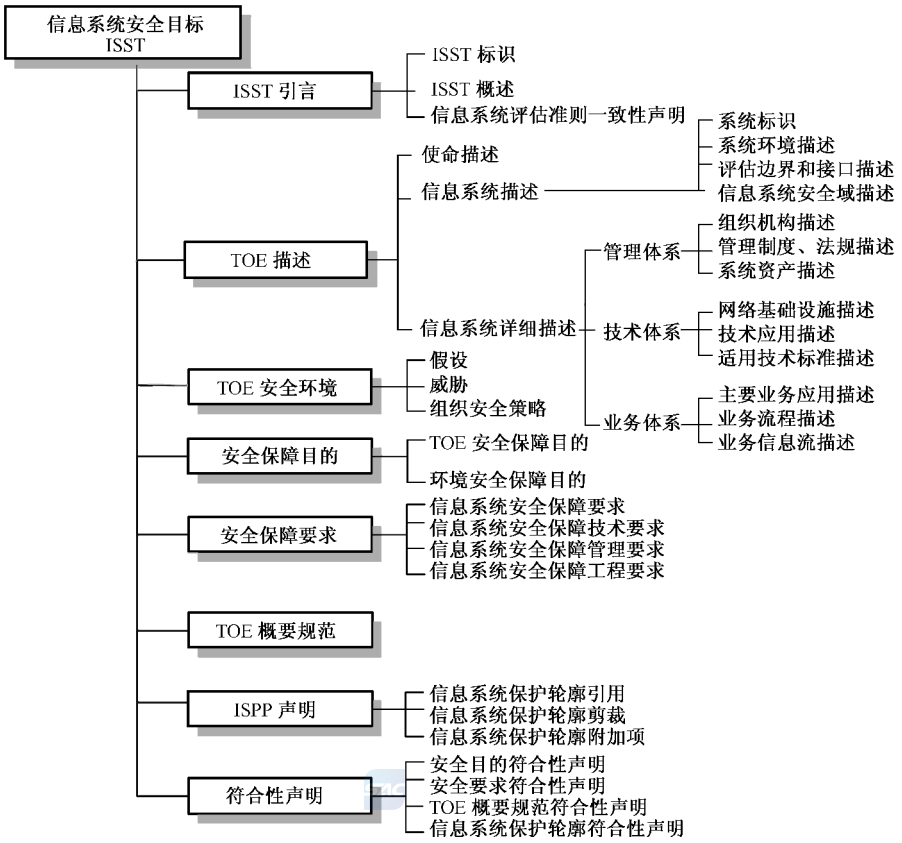

图 B.1　信息系统安全目标内容

B.2.3　TOE 描述

信息系统安全目标的这部分应描述评估对象，以帮助了解它的安全保障要求，并对所评估的信息系统进行详细完整地说明。在信息系统安全保障评估框架中，评估对象可以是信息系统整体或信息系统技术、工程或管理某一局部领域。无论是信息系统整体还是信息系统某一领域，在评估对象描述中都必须先给出整个信息系统的完整描述，然后再对确切的评估对象作进一步描述。

评估对象描述提供了用于评估的上下文。在评估对象描述中给出的信息将用于在评估过程中识别不一致的地方。

在信息系统安全目标中，必须详尽完整地给出信息系统的描述，整个信息系统描述主要包括三个大类：信息系统使命、信息系统概述和信息系统详细描述。

B.2.3.1　信息系统使命描述

信息系统的使命，即从目的和意义的角度对信息系统进行高层描述，它是信息系统根本和本质的要求。通常，信息系统使命描述了信息系统的高层要求。

B.2.3.2　信息系统概述

信息系统概述：对所要评估的信息系统进行概括性说明和描述。

a)　信息系统标识：应给出系统的正式名称和标识，系统标识包括其名称、所属的组织机构及其地点和包含最终用户的组织机构及其地点等相关信息；

b)　信息系统环境描述：描述的运行环境以及系统开发、集成和维护的环境；

c)　信息系统评估边界和接口描述：描述所要评估系统的边界和相应的外部接口，此描述必须用图表或文字清晰地描述和界定所要评估的系统部件和边界；

d)　信息系统安全域描述：根据系统的重要性（描述系统的重要性以及系统的可接受的风险级别）、数据的分类和密级（描述系统所处理的数据类型和机密级别）和系统用户（描述使用系统

的用户描述)等方面划分系统的安全域。

B.2.3.3 信息系统详细描述

信息系统详细描述:此部分从管理体系、技术体系和业务体系分别对信息系统进行详细描述。

a) 管理体系:在管理体系中,需要对信息系统现有的管理组织结构、所使用的相应规章制度和所涉及的重要资产进行描述:
   1) 组织机构描述:包含同信息系统相关的管理、使用、开发、集成和支持组织机构的描述,特别是相关安全管理保障的组织机构的描述;
   2) 管理制度、法规描述:列出同信息系统安全管理相关的目前使用的相应规章制度和相关法规;
   3) 资产描述:描述信息系统的物理资产(指信息系统中的各种硬件、软件和物理设施)和信息资产(指在信息系统计划组织、开发采购、实施交付、运行维护和废弃这一信息系统生命周期过程中产生的同信息系统本身相关的有价值的信息以及信息系统所存储、处理和传输的各种相关的办公、管理和业务等信息)。

b) 技术体系:技术体系是信息系统描述的基础,需要对现有的各种应用、相应的网络基础设施和所使用的技术标准进行描述,这些描述将帮助了解用户的信息系统并为进一步描述业务系统提供基础和支持:
   1) 基础设施描述:描述系统的网络层次等网络体系结构说明;
   2) 应用描述:描述用户信息系统的各种应用说明;
   3) 技术标准描述:列出相关技术应用等所适用的技术标准。

c) 业务体系:业务体系从业务角度和应用角度出发,基于技术体系,对组织机构的主要业务应用进行分类和描述,并通过业务流程和业务信息流来进一步解释:
   1) 业务应用描述:列出组织机构的主要业务应用并进行描述;
   2) 流程描述:基于组织机构的管理结构等,描述业务的流程;
   3) 信息流描述:描述主要业务应用的接口和相应数据流,数据流描述应包括数据的类型以及数据传送的一般方式。

B.2.4 TOE 安全环境

信息系统安全环境的陈述应描述信息系统所处环境的安全问题和信息系统使用环境的方式。该陈述包括以下几点:

a) 假设的描述应描述信息系统将在或拟在使用的环境的安全问题,它将包括以下两点:
   1) 关于信息系统预期使用方式的信息,如:预期的应用、潜在的资产价值、可能的使用限制;
   2) 有关信息系统使用环境的信息,如:在物理的、人员的和连通性方面。

b) 威胁的描述将描述对资产的所有威胁,这些资产是在信息系统或其环境内需要特定保护的。值得注意的是,并非所有的在环境中可能遇到的威胁都必须列出,只有那些与信息系统的安全运行相关的威胁才需要列出。威胁应通过已确定的威胁主体、攻击和作为攻击对象的资产进行描述。威胁主体应通过注入专门技术、可用资源和动机等来描述。攻击应通过诸如攻击方法、可利用的脆弱性和时机等来描述。如果安全保障目的仅仅来源于组织性安全策略和假设,可以省略对威胁的描述。

c) 组织安全策略的描述应确定信息系统必须遵守的所有组织安全策略陈述或规则,必要时还应加以说明。如果使用某个策略来建立清晰的安全保障目的,就必须对策略陈述进行说明和解释。如果安全保障目的仅仅来自威胁和假设,可以略去组织安全策略。

B.2.5 安全保障目的

安全保障目的的陈述定义信息系统及其环境的安全保障目的。安全保障目的应涉及已确定安全环境的所有方面。安全保障目的应反映被陈述的意图,并应适用于所有已知的组织安全策略和假设。应

指明以下两类安全保障目的。(注意:当威胁或组织安全策略部分被 TOE 所覆盖并部分被它的环境所覆盖,那么相关的安全保障目的应在每一个种类中重复。)

a) 应明确说明信息系统安全保障目的,并且可追溯到信息系统所对抗的已知威胁或信息系统可满足的组织安全策略;

b) 应明确说明环境安全保障目的,并且可追溯到已知的信息系统无法完全对抗的威胁或信息系统无法完全满足的组织安全策略及假设。

注意环境安全保障目的可以是全部或部分的信息系统安全环境陈述的假设部分的重述。

B.2.6 安全保障要求

这部分定义信息系统应满足的安全保障要求。安全保障要求应按下列方式描述:

a) 安全保障要求的陈述应定义信息系统的技术、管理和工程的安全保障要求或综合这些领域的信息系统整体的安全保障要求。根据评估对象类型的不同,安全保障要求包括以下全部或部分内容:

1) 信息系统整体安全保障要求的陈述应能给出信息系统整体安全保障要求的概要性描述;

2) 信息系统技术安全保障要求的陈述应把信息系统的技术安全保障要求定义为从本标准第 2 部分中提取的安全技术保障控制组件和安全技术架构能力成熟度要求;

3) 信息系统管理安全保障要求的陈述应把评估对象的管理安全保障要求定义为从本标准第 3 部分中提取的安全管理保障控制组件和安全管理能力成熟度要求;

4) 信息系统工程安全保障要求的陈述应把评估对象的工程安全保障要求定义为从本标准第 4 部分中提取的安全工程保障控制组件和安全工程能力成熟度要求。

b) 下列通用条件应同样适用于信息系统及其环境的安全保障要求的表达:

1) 所有信息系统的安全技术保障控制要求都应引用本标准第 2 部分的安全技术保障控制要求组件,所有信息系统的安全管理保障控制要求都应引用本标准第 3 部分的安全管理保障控制要求组件,所有信息系统的安全工程保障控制要求都应引用本标准第 4 部分的安全工程保障控制要求组件。如果对所有或部分安全保障控制要求而言,没有打算使用本标准第 2、第 3 和第 4 部分的安全保障控制组件,ISST 应明确说明这些要求没有引用本标准;

2) 所有信息系统的安全技术架构能力成熟度要求、安全管理能力成熟度要求和安全工程能力成熟度要求都应引用本标准第 2、第 3 和第 4 部分中的能力成熟度要求;

3) 任何一个信息系统安全保障要求均应准确、无歧义地表达,才能进行一致性评估和论证。现有的信息系统安全保障评估框架的技术、管理和工程要求的详细程度和表达方式应当作一个典范来使用;

4) 所有安全保障要求之间的依赖关系都应满足。依赖关系可以通过在信息系统安全保障要求内包含相关的要求或对环境提出要求而满足。

B.2.7 TOE 概要规范

信息系统概要规范将定义信息系统安全保障要求的实现方法,该规范描述符合信息系统安全保障要求的信息系统安全保障控制要求和能力成熟度要求。

信息系统概要规范包括下列内容:

a) 信息系统整体安全保障要求陈述应包含对信息系统整体保护轮廓的完整描述。

b) 信息系统安全技术保障陈述应包含信息系统安全技术保障控制要求和安全技术架构能力成熟度要求,并说明这些要求是如何满足信息系统保护轮廓的。该陈述将包括一个在技术控制和技术控制要求间的双向映射,清楚表示哪个控制满足哪个要求,并表明所有的要求都达到。每一个安全控制至少要满足一个信息系统安全技术保障控制要求。

c) 信息系统安全管理保障陈述应包含信息系统安全管理保障控制要求和安全管理能力成熟度要

求，并说明这些要求是如何满足信息系统保护轮廓的。该陈述将包括一个在管理控制和管理控制要求间的双向映射，清楚表示哪个管理控制满足哪个管理控制要求，并表明所有的要求都达到。每一个安全管理控制至少要满足一个信息系统安全管理保障控制要求。

d) 信息系统安全工程保障陈述应包含信息系统安全工程保障控制要求和安全工程能力成熟度要求，并说明这些要求是如何满足信息系统保护轮廓的。该陈述将包括一个在工程控制和工程控制要求间的双向映射，清楚表示哪个工程控制满足哪个工程控制要求，并表明所有的要求都达到。每一个安全工程控制至少要满足一个信息系统安全工程保障控制要求。

B.2.8 ISPP 声明

ISST 可以根据情况做 TOE 与 ISPP(一个或多个 ISPP)的一致性声明。如果作出了任何 ISPP 一致性声明，ISST 就应包括 ISPP 声明陈述，其中包括：解释、理由和其他支持材料，以证实该声明。

对 TOE 目的和要求的 ISST 陈述，其内容和表达会受 TOE 的 ISPP 声明的影响。通过对每一个所声明的 ISPP 考察以下情况后来概括对 ISST 的影响：

a) 如果没有 ISPP 一致性声明，那么 TOE 目的和要求的完整表达应按本附录的规定来完成，也不需要任何 ISPP 的声明；

b) 如果 ISST 的声明仅符合 ISPP 的要求，没有更进一步的限制，那么对 ISPP 的引用就足以确定和证明 TOE 目的和要求。重述 ISPP 的内容是不必要的；

c) 如果 ISST 声明符合 ISPP 要求，并且对 ISPP 要求进一步的限制，那么 ISST 应表明 ISPP 对限制的要求已经满足。例如在 ISPP 包括不完整操作的情况下，ISST 可引用特定的要求，但应在 ISST 内完成该操作。在某些情况下，完成操作的要求是重要的，此时最好在 ISST 中重述 ISPP的内容，以便描述得更清楚；

d) 尽管 ISPP 的引用已经足够充分定义 ISPP 的目的和要求，如果 ISST 的声明不仅与 ISPP 的目的和要求一致，而且还通过增添目的和要求来扩展 ISPP，那么 ISST 应定义这些增添的内容。在某些情况下，增添是重要的，此时最好在 ISST 中重述 ISPP 的内容，以便描述得更清楚；

e) 信息系统安全保障评估框架不允许 ISST 声明与 ISPP 部分一致。

信息系统安全保障评估框架并不规定是重述还是引用 ISPP 的目的和要求。对 ISST 内容的基本要求是必须完备、清楚、无歧义，这样 ISST 的评估才是可能的，ISST 是 TOE 评估可接受的基础，并且应能清楚地追溯到所有所声明的 ISPP。

要作出任何一个 ISPP 一致性声明，该声明应包括以下内容的陈述：

a) ISPP 引用的陈述应指出与哪个 ISPP 一致，并包括任何与此相关的详细内容。一个有效的声明意味着 TOE 满足该 ISPP 所有的要求；

b) ISPP 裁减的陈述应指出那些满足 ISPP 操作的信息系统保护轮廓，否则对 ISPP 要求进一步限制；

c) ISPP 附加项的陈述应指出那些作为 ISPP 目的和要求增添的 TOE 目的和要求。

B.2.9 符合性声明

这部分提出用于 ISST 评估的依据。这些依据将支持：ISST 是一个完整的、紧密结合的要求集合，满足该 ISST 的 TOE 应在安全环境内提供一组有效的信息系统安全模型，并且 TOE 概要规范已经说明这些要求。符合性声明应包括以下内容：

a) 安全保障目的符合性声明应阐明安全保障目的可追溯到在信息系统安全环境里指明的所有方面，并且能覆盖所有的这些方面。

b) 安全保障要求符合性声明应阐明系列安全保障要求(信息系统和环境)是适合于满足，并可追溯到安全保障目的。应阐明以下几点：

1) 将信息系统及其安全环境的技术、管理和工程要求相组合，能满足所述的安全保障目的；

2) 该组安全保障要求一起构成一个互相支持且内在一致的整体；

3） 安全保障要求的选择应说明理由，所有下列情况都应当专门说明：

——选择本标准的第2、第3和第4部分中没有的要求；

——不满足依赖关系。

c） 信息系统概述规范符合性声明应说明信息系统安全技术保障、管理和工程将适合于满足信息系统安全保障要求。

d） 信息系统保护轮廓符合性声明的陈述应解释ISST信息系统安全保障目的与所有声明一致的ISPP之间的区别。如果没有ISPP符合性声明或者ISST安全保障目的和要求与任何声明的ISPP是等同的，这部分可以忽略。

这部分材料可能篇幅太大，不一定对所有ISST用户都适合和有用，因此可以单独发行。

附 录 C
（资料性附录）
信息系统描述

C.1 概述

在本标准中，首先需要对信息系统（信息系统是用于采集、处理、存储、传输、分发和部署信息的整个基础设施、组织结构、人员和组件的总和）的各个方面进行深入全面的了解，只有对所评估的信息系统本身有深刻认识才能进一步进行假设、威胁和组织安全策略的分析。

本附录是资料性附录，它为本标准的用户提供了一种信息系统描述的参考。

C.2 信息系统描述规范

在本标准中，根据信息系统安全保障评估的角度，提出了信息系统描述规范。图 C.1 描述了信息系统安全保障评估的信息系统描述规范。

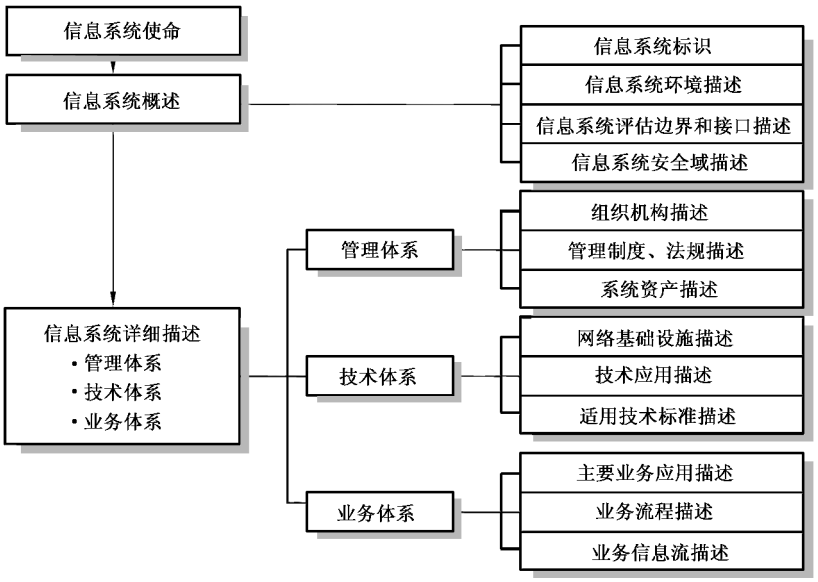

图 C.1 信息系统安全保障评估的信息系统描述规范

整个信息系统描述主要包括三个大类：信息系统使命、信息系统概述和信息系统详细描述，相应的具体描述内容包括：

a) 信息系统使命描述：信息系统的使命，即从目的和意义方面对信息系统进行高层描述，它是信息系统根本和本质的要求。

b) 信息系统概述：对所要评估的信息系统进行概括性说明和描述：

1) 信息系统标识：应给出系统的正式名称和标识。系统标识包括其名称、所属的组织机构及其地点和包含最终用户的组织机构及其地点等相关信息；

2) 信息系统环境描述：描述的运行环境以及系统开发、集成和维护的环境；

3) 信息系统评估边界和接口描述：描述所要评估系统的边界和相应的外部接口，此描述必须用图表或文字清晰地描述和界定所要评估的系统部件和边界；

4) 信息系统安全保障域描述：根据系统的关键性（描述系统的关键性以及系统的可接受的

风险级别)、数据的分类和密级(描述系统所处理的数据类型和机密级别)和系统用户(描述使用系统的用户描述)等方面划分系统的安全域。

c) 信息系统详细描述:此部分从管理体系、技术体系和业务体系分别对信息系统进行详细描述:

1) 管理体系:在管理体系中,需要对信息系统现有的管理组织结构、所使用的相应规章制度和所涉及的重要资产进行描述:

——组织机构描述:描述管理、使用、开发、集成、支持信息系统的相关组织机构,特别是安全管理保障相关的组织机构的描述;

——管理制度、法规描述:列出同信息系统安全管理相关的目前使用的相应规章制度和相关法规;

——系统资产描述:描述信息系统的物理资产(指信息系统中的各种硬件、软件和物理设施)和信息资产(指在信息系统计划组织、开发采购、实施交付、运行维护和废弃这一信息系统生命周期过程中产生的同信息系统本身相关的有价值的信息以及信息系统所存储、处理和传输的各种相关的办公、管理和业务等信息)。

2) 技术体系:技术体系是信息系统描述的基础,需要对现有的各种应用、相应的网络基础设施和所使用的技术标准进行描述,这些描述将帮助了解用户的信息系统并为进一步描述业务系统提供基础和支持:

——网络基础设施描述:描述系统的网络层次等网络体系结构说明;

——技术应用描述:描述用户信息系统的各种应用说明;

——适用技术标准描述:列出相关技术应用等所适用的技术标准。

3) 业务体系:业务体系从业务角度和应用角度出发,基于技术体系,对组织机构的主要业务应用进行分类和描述,并通过业务流程和业务信息流来进一步解释:

——主要业务应用描述:列出组织机构的主要业务应用并进行描述;

——业务流程描述:基于组织机构的管理结构等,描述业务的流程;

——业务信息流描述:描述主要业务应用的接口和相应数据流,数据流描述应包括数据的类型以及数据传送的一般方式。

C.3 信息系统描述说明

为了更好地帮助理解和规范化信息系统描述,图 C.2 描述了信息系统技术参考模型示例。

信息系统技术参考模型是为了建立一个描述和理解信息技术系统的公共词汇表,并定义了信息技术系统通用的服务和接口集合。通过公共词汇表和服务、接口集合的定义,帮助用户以通用、标准化和提高互操作的方式建设、分析和描述信息技术系统。

信息系统技术参考模型主要涉及信息系统描述中的技术体系和业务体系。整个信息系统技术参考模型分为三层:外部环境(其中主要涉及通信基础设施)、应用平台和应用软件。这三层分别提供其特定的服务,三层之间建立两个接口:外部环境接口(其中主要涉及通信基础设施接口)和应用程序接口 API。

为了更加强调业务应用为中心的信息系统描述和评估原则,在此参考模型中将应用软件分为支持应用和业务应用子层并在信息系统描述规范中将两者分离。在具体规范化描述中,技术参考模型的其他部分(即信息系统描述规范中的技术体系部分)建立信息系统技术描述的基础,而技术参考模型中业务应用子层(即信息系统描述规范中的业务体系部分),从业务和信息流出发、综合信息系统业务管理流程对业务应用进行描述。

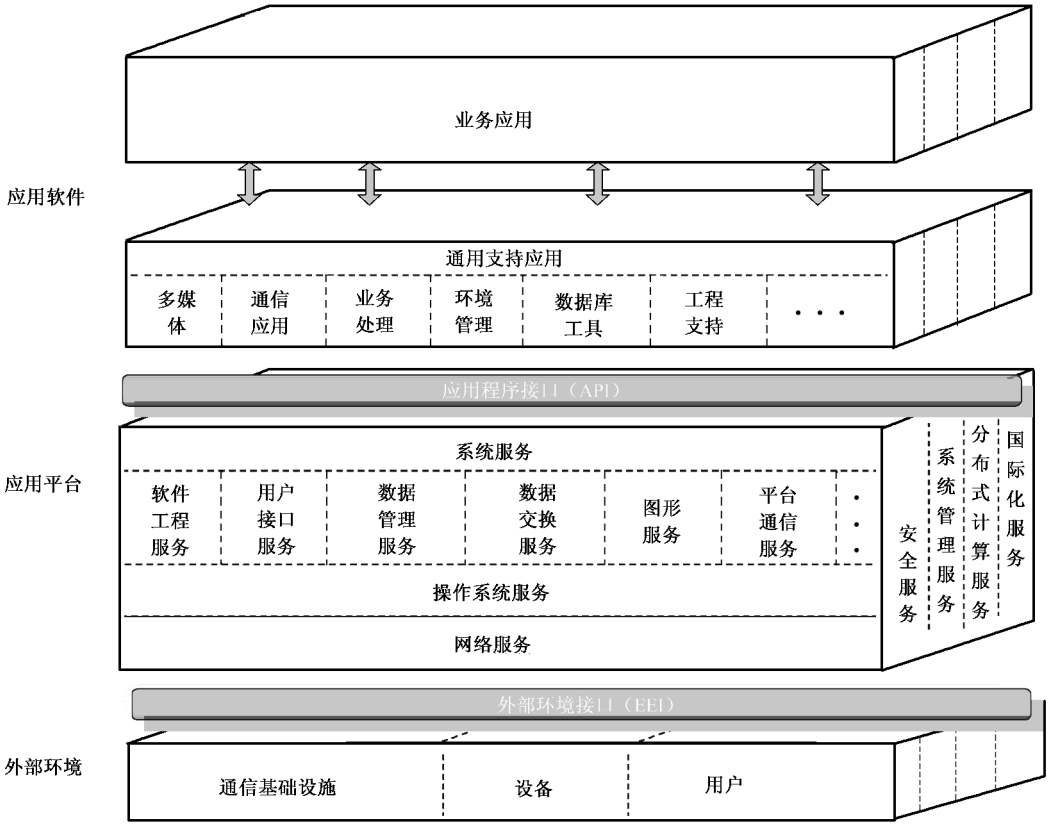

图 C.2　信息系统技术参考模型

附 录 D
（资料性附录）
信息系统安全保障级说明

D.1 概述

组织机构应根据其信息系统的具体要求选择对应的信息系统安全保障级。在确定所需的信息系统安全保障级时，组织机构应首先根据其信息系统使命、所对抗的威胁等确定其信息系统的分类和分级，然后将信息系统的分类和分级同信息系统安全保障级进行对应，确定每个分类分级的系统有合适的信息系统安全保障级。

本附录中所提供的信息系统使命分类和信息系统威胁分级只是一种分类分级的示例说明，信息系统分级分类的标准和规范不在本标准的讨论范围之内，组织机构可应根据信息系统安全保障工作的具体要求选择和定义自己的分级分类标准。

D.2 信息系统使命分类

在本章中，根据保密性、完整性和可用性特征以及信息和信息系统价值将信息系统划分为5类，见表D.1。

表 D.1 信息系统使命分类示例

信息系统使命类	信息特征			信息和信息系统价值
	保密性	完整性	可用性	
Ⅰ	B	B	B	对信息系统安全保障策略的违反造成的负面影响和结果可以忽略
Ⅱ	B	M	M	对信息系统安全保障策略的违反会对安全、保险、金融状况、组织机构的基础设施造成不良影响和/或小的破坏
Ⅲ	B	M	H	对信息系统安全保障策略的违反会产生一定破坏
Ⅳ	B	H	H	对信息系统安全保障策略的违反会严重的破坏安全、保险、金融状况、组织机构的基础设施
Ⅴ	M	H	H	对信息系统安全保障策略的违反会造成异常严重的破坏
注1：信息特征的保密性、完整性和可用性根据要求分为B(基本-Basic)、M(中等-Middle)和H(高-High)。 注2：本表只是作为概念说明，并没有讨论特定的信息系统(例如：高保密性的特定信息系统等)。				

D.3 信息系统威胁分级

在本章中，将信息系统的威胁分为7级，见表D.2。

表 D.2 信息系统威胁分类示例

威胁级别	威胁说明
T1	无意的或意外的事件
T2	被动的、无意识的占有很少资源并且愿意冒少量风险的对手
T3	占有少量资源但是愿意冒很大风险的对手

表 D.2（续）

威胁级别	威胁说明
T4	占有中等程度资源的熟练的对手，愿意冒少量风险
T5	占有中等程度资源的熟练的对手，愿意冒较大风险
T6	占有丰富程度资源的特别熟练的对手，愿意冒少量风险
T7	占有丰富程度资源的特别熟练的对手，愿意冒较大风险

D.4 信息系统安全保障级（ISAL）矩阵

得到了信息系统的使命类和信息系统威胁的分级，就可以利用表 D.3 对信息系统的安全保障级作出要求。

表 D.3 信息系统安全保障级矩阵示例

使命类	威胁级别					
	T1	T2	T3	T4	T5	T6
Ⅰ	ISAL1	ISAL1	ISAL1	ISAL2	ISAL2	ISAL2
Ⅱ	ISAL1	ISAL1	ISAL1	ISAL2	ISAL3	ISAL3
Ⅲ	ISAL1	ISAL2	ISAL2	ISAL3	ISAL3	ISAL4
Ⅳ	ISAL2	ISAL3	ISAL4	ISAL4	ISAL4	ISAL5
Ⅴ	ISAL3	ISAL3	ISAL4	ISAL4	ISAL5	ISAL5

D.5 信息系统安全保障级（ISAL）分级要求

信息系统安全保障级（ISAL）是信息系统技术、管理、工程的分类分级的综合评定。信息系统安全保障级（ISAL）需要根据相关国家、政府部门、行业等的法律、法规、规范和要求来具体制定并最终反映在相关的信息系统安全保障评估框架之中，根据具体要求的不同，安全管理能力成熟度级和安全工程能力成熟度级的具体要求也随之不同，因此此处所列出的信息系统安全保障级（ISAL）及相应安全管理能力成熟度级要求及描述和安全工程能力成熟度级要求及描述仅作为原理性概念参考说明。

表 D.4 描述了不同信息系统安全保障级别的技术、管理和工程要求的对应表。

表 D.4 信息系统安全保障级要求示例

信息系统安全保障级	安全技术架构能力成熟度级	安全管理能力成熟度级	安全工程能力成熟度级
ISAL1	TCML1	MCML1	ECML1
ISAL2	TCML2	MCML2	ECML2
ISAL3	TCML3	MCML3	ECML3
ISAL4	TCML4	MCML4	ECML4
ISAL5	TCML5	MCML5	ECML5

在本标准中，所要指出的是，信息系统安全保障级是一个循序渐进、不断完善和深入的发展级别，高安全保障级必须建立在完成低安全保障级别完成实现的基础上，高等级的安全保障级是低等级保障级的基础上不断能力成熟、完善和发展的结果。

为了更完整地描述信息系统安全保障级的内容，下面列出信息系统安全管理保障能力成熟度级别和信息系统安全工程保障能力成熟度级别评估的示例，具体内容参见本标准的第 2、第 3 和第 4 部分。

图 D.1 描述了某信息系统安全管理能力成熟度级的要求示例。

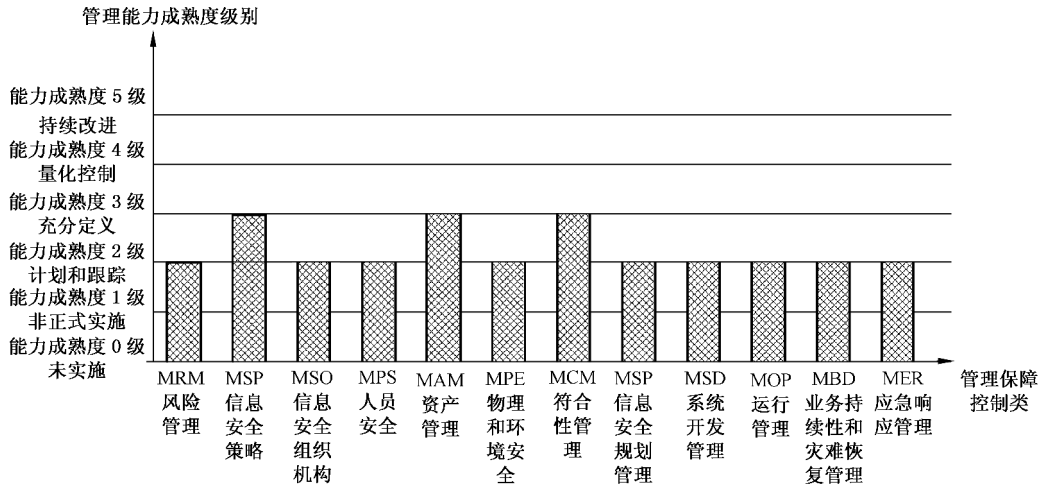

图 D.1　信息系统安全管理能力成熟度级要求示例图

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。

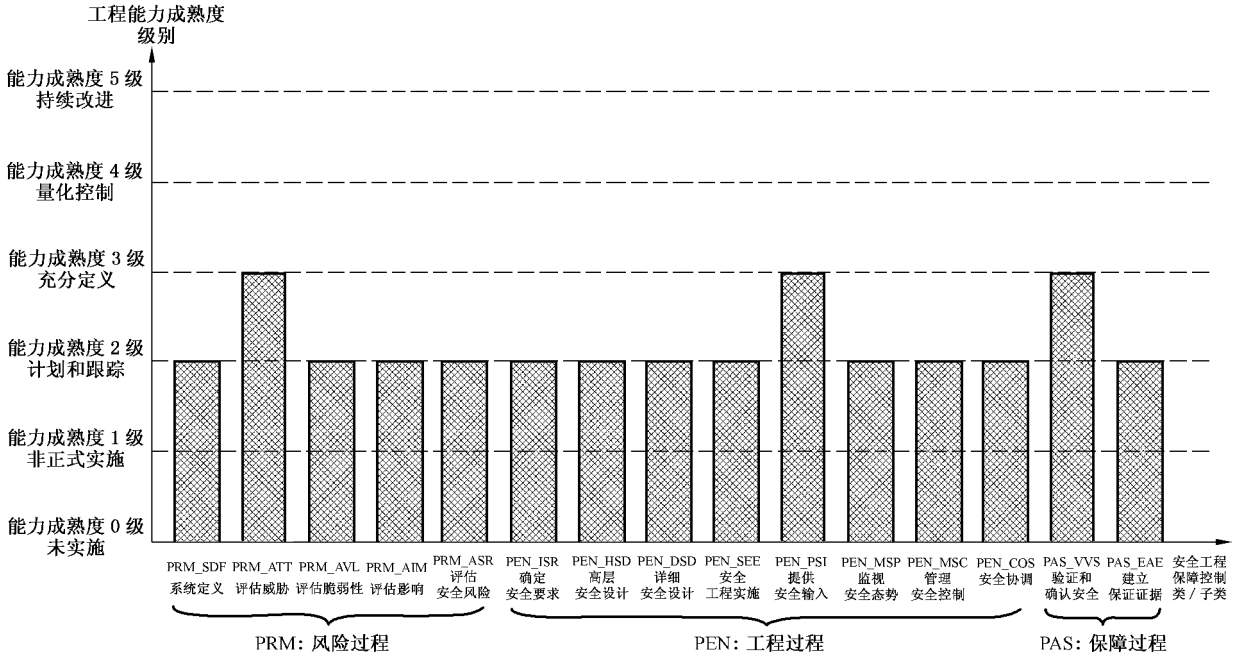

图 D.2　某信息系统安全工程能力成熟度级要求示例图

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-

opment Life Cycle,October 2003

[22] NIST Special Publication 800-53,Recommended Security Controls for Federal Information Systems,Feberuary 2005

[23] OECD Guidelines for Security of Information Systems and Networks:'Toward a Culture of Security',2002

[24] NSTISSI No. 4009 National Information Systems Security (INFOSEC) Glossary

[25] Carnegie Mellon University/Software Engineering Institute,CMU/SEI-2002-TR-011,CMMI℠ for Systems Engineering,Software Engineering,Integrated Product and Process Development, and Supplier Sourcing(CMMI-SE/SW/IPPD/SS,V1.1) Continuous Representation,CMMI Product Team,March 2002

[26] Carnegie Mellon University/Software Engineering Institute,CMU/SEI-2002-TR-012,CMMI℠ for Systems Engineering,Software Engineering,Integrated Product and Process Development, and Supplier Sourcing (CMMI-SE/SW/IPPD/SS, V1.1) Staged Representation, CMMI Product Team,March 2002

[27] System Security Engineering Capability Maturity Model (SSE-CMM) Model Descritpion Document,Version 3.0,June 15,2003

[28] System Security Engineering Capability Maturity Model (SSE-CMM) Appraisal Method, Version 2.0,April 16,1999

[29] CoBIT ,3rd Edition,Management Guidelines,COBIT Steering Committee and the IT Governance Institute™,July 2000

[30] CoBIT ,3rd Edition,Audit Guidelines,COBIT Steering Committee and the IT Governance Institute™,July 2000

[31] CoBIT ,3rd Edition,Control Objectives,COBIT Steering Committee and the IT Governance Institute™,July 2000

[32] Department of Defense Technical Reference Model,Version 2.0,9 April 2001

[33] Department of Defense Technical Architecture Framework for Information Management, Volume 1: Overview,Version 3.0,30 April 1996

[34] DoD Architecture Framework, Version 1.0, DoD Architecture Framework Working Group,August 2003

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 10 月第一版
*
书号:155066·1-28089

GB/T 20274.1-2006