ICS 35.040
L 80

中华人民共和国国家标准化指导性技术文件

GB/Z 30286—2013

信息安全技术 信息系统保护轮廓和信息系统安全目标产生指南

**Information security technology—
Guide for the production of information system
protect profile and information system security target**

2013-12-31 发布　　2014-07-15 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

本指导性技术文件按照 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。

本指导性技术文件由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本指导性技术文件主要起草单位:中国信息安全测评中心、中国信息安全测评中心华中测评中心、华北计算技术研究所。

本指导性技术文件主要起草人:江常青、张利、姚轶崭、佟鑫、彭勇、陆丽、胡卫华、付敏、周瑾。

引　言

本指导性技术文件是GB/T 20274《信息安全技术　信息系统安全保障评估框架》系列标准的配套指南文件，为信息系统保护轮廓(Information System Protect Profile，ISPP)和信息系统安全目标(Information System Security Target，ISST)的编制提供指导。

本指导性技术文件的使用者应熟悉GB/T 20274系列标准。

信息安全技术
信息系统保护轮廓和信息系统安全目标
产生指南

1 范围

本指导性技术文件给出了编制信息系统保护轮廓(ISPP)和信息系统安全目标(ISST)的过程,为编写 ISPP 和 ISST 提供指导。

本指导性技术文件适用于应用 GB/T 20274 系列标准进行信息系统安全性保障评估的评估者和确认评估者行为的认证者、系统开发者等。

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/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

GB/T 20274.2—2008 信息安全技术 信息系统安全保障评估框架 第 2 部分:技术保障

GB/T 20274.3—2008 信息安全技术 信息系统安全保障评估框架 第 3 部分:管理保障

GB/T 20274.4—2008 信息安全技术 信息系统安全保障评估框架 第 4 部分:工程保障

GB/T 20984—2007 信息安全技术 信息安全风险评估规范

3 术语和定义

GB/T 20274.1—2006、GB/T 20274.2—2008、GB/T 20274.3—2008、GB/T 20274.4—2008 界定的术语和定义适用于本文件。

4 ISPP 和 ISST 概述

4.1 ISPP 和 ISST 的用途

GB/T 20274 系列标准的主要用途是表达信息系统的安全保障要求。信息系统有许多不同的种类,每个信息系统运行于特定的现实环境中,受到来自于组织内部与外部环境的约束。因此对于不同的信息系统,通常有不同的安全保障要求。

GB/T 20274.1—2006 中用 ISPP 和 ISST 来表达某一类信息系统和某一个特定信息系统的安全保障要求。信息系统的所有者运用 ISPP 来描述某一类信息系统标准化、结构化和规范化的安全保障需求。信息系统的开发者依据 ISPP 针对特定的信息系统编制相应的 ISST,描述其特定用户系统的安全保障需求以及对 ISPP 的满足情况。

4.2 ISPP 和 ISST 的内容

GB/T 20274.1—2006 的图 A.1 描述了 ISPP 中所要求的内容条目。表 1 是推荐使用的 ISPP 样本

目录清单结构。GB/T 20274.1—2006 的图 B.1 中描述了 ISST 所要求的内容条目。表 2 是推荐使用的 ISST 样本目录清单结构。

表 1　安全保护轮廓样本目录清单

序号	目　录　结　构
1	ISPP 描述 1.1 ISPP 标识 1.2 ISPP 概述
2	信息系统描述 2.1 信息系统使命描述 2.2 信息系统概要描述 2.3 信息系统详细描述
3	安全保障需求 3.1 识别和说明假设 3.2 识别和说明威胁 3.3 识别和确定组织安全策略
4	安全保障目的 4.1 信息系统安全技术保障目的 4.2 信息系统安全管理保障目的 4.3 信息系统安全工程保障目的
5	安全保障要求 5.1 信息系统安全保障要求 5.2 信息系统安全技术保障要求 5.3 信息系统安全管理保障要求 5.4 信息系统安全工程保障要求
6	ISPP 应用注解
7	符合性声明 7.1 安全目的符合性声明 7.2 安全要求符合性声明

表 2　安全目标样本目录清单

序　　号	目　录　结　构
1	ISST 描述 1.1 ISST 标识 1.2 ISST 概述
2	信息系统描述 2.1 信息系统使命描述 2.2 信息系统概要描述 2.3 信息系统详细描述

表 2（续）

序　号	目　录　结　构
3	安全保障需求 3.1 识别和说明假设 3.2 识别和说明威胁 3.3 识别和确定组织安全策略
4	安全保障目的 4.1 信息系统安全技术保障目的 4.2 信息系统安全管理保障目的 4.3 信息系统安全工程保障目的
5	安全保障要求 5.1 信息系统安全保障要求 5.2 信息系统安全技术保障要求 5.3 信息系统安全管理保障要求 5.4 信息系统安全工程保障要求
6	信息系统概要规范 6.1 信息系统安全保障要求 6.2 信息系统安全技术保障 6.3 信息系统安全管理保障 6.4 信息系统安全工程保障
7	ISPP 声明 7.1 ISPP 引用 7.2 ISPP 剪裁 7.3 ISPP 附加项
8	符合性声明 8.1 安全目的符合性声明 8.2 安全要求符合性声明

ISPP 或 ISST 的描述部分标识了 ISPP 或 ISST 的信息系统，并概要描述了 ISPP 或 ISST。ISPP 概述可以被 ISPP 文档的编目和注册引用。

信息系统描述提供了信息系统（或信息系统类型）的一般信息，帮助目标读者理解信息系统的安全要求和信息系统的预期使用方法。ISST 的信息系统描述应该包括信息系统使命描述、信息系统概要描述和信息系统详细描述。

安全保障需求是信息系统所处环境的安全保障需求，即信息系统的预期使用方式、预期使用的环境范围和特征。安全环境详细描述了用于定义安全保障需求的假设、预期使用的范围、资产所面临的已知威胁以及信息系统必须遵从的组织安全策略。

安全保障目的提供与安全保障需求相对应的符合性声明。详尽说明见第 9 章。

安全保障要求包括信息系统的安全技术保障要求、安全管理保障要求和安全工程保障要求，分别使用 GB/T 20274.2—2008、GB/T 20274.3—2008 和 GB/T 20274.4—2008 中的功能组件和保证组件来描述。详尽说明见第 10 章。

ISPP 应用注解是 ISPP 的可选部分，它提供了 ISPP 有用的附加信息。

信息系统概要规范包括由信息系统提供的用于满足特定安全保障要求的安全功能，以及所有声明满足特定安全保障要求的安全保障措施。详尽说明见第 11 章。

ISPP 声明是 ISST 的可选部分，用于声明 ISST 遵从和满足的所有 ISPP，以及对 ISPP 内容的补充或裁减。详尽说明见第 12 章。

4.3 ISPP 和 ISST 的目标读者

ISPP 和 ISST 的目标读者主要包括：

a) 用户：用户需要了解遵从 ISPP 的信息系统应该采取哪些安全保障措施；

b) 开发者：开发者需要获得清晰的安全保障要求，以便去构建符合 ISPP 的信息系统；

c) 信息系统使用者：信息系统使用者（包括安装人员、管理员和运维人员）需要获得信息系统安全需求；

d) 评估者：ISPP 或 ISST 评估者需要获得相关的证实 ISPP 或 ISST 技术正确性和有效性的信息。

ISPP 或 ISST 的描述、信息系统描述、安全保障需求以及安全保障目的等部分主要针对用户和系统使用者。同时，信息系统开发者也应该认真了解安全保障需求和安全保障目的。

ISPP 中的安全保障要求部分、ISST 中的信息系统概要规范部分主要针对信息系统的开发者、系统使用者和评估者。

5 ISPP 和 ISST 的产生过程

信息系统安全保障要求根本上来源于对信息系统的目的、环境及其本身的考虑。图 1 阐明了 ISPP 和 ISST 的产生过程。

在 GB/T 20274.1—2006 附录 A 和附录 B 中，要求 ISPP 与 ISST 的编制应按逻辑顺序以“自上而下”的方式进行。例如，ISPP 的编制顺序是：

a) 定义安全保障需求；

b) 确认与安全保障需求对应的安全保障目的；

c) 定义满足安全保障目的的安全保障要求。

ISPP 与 ISST 的编制可能需要多次迭代，从而反映信息系统内部或外部环境的产生的新需求。例如：

a) 出现新的威胁；

b) 组织安全策略发生变化；

c) 信息系统的使命发生变化。

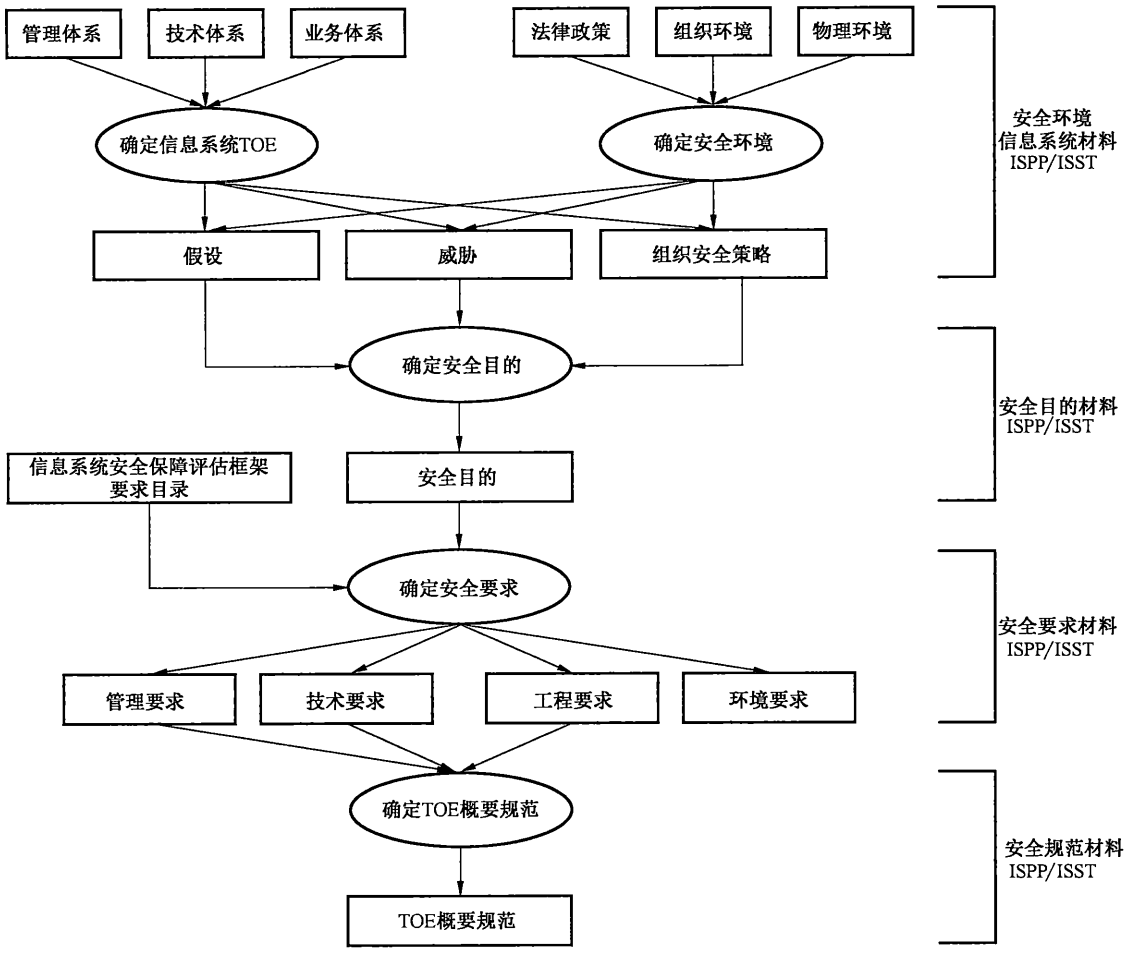

图 1　ISPP 和 ISST 的产生过程

6　ISPP 和 ISST 的描述部分

6.1　概述

本章为规范 ISPP 和 ISST 的描述部分提供指南，即：

a)　ISPP 和 ISST 标识；

b)　ISPP 和 ISST 概述；

c)　ISPP 应用注解。

6.2　ISPP 和 ISST 标识

ISPP 或 ISST 标识部分应能提供足够的信息，唯一标识出 ISPP 或 ISST。ISPP 或 ISST 标识部分至少包括具有唯一版本的 ISPP 或 ISST 名称，以及用于标识信息系统的内容(例如，信息系统的名称和版本号)。标识部分还需包括用于编制 ISPP 或 ISST 的 GB/T 20274.1—2006 的版本信息，以便于版本控制。

6.3　ISPP 和 ISST 概述

根据 GB/T 20274.1—2006 的要求，概述部分应概要性描述 ISPP 或 ISST。该部分应包括 ISPP 或

ISST 所关注的、最主要的安全问题，作为编制者判断 ISPP 或 ISST 是否适合的依据。

6.4 ISPP 应用注解

ISPP 应用注解是 ISPP 中的可选项，可以自成一节，也可以将特定注释内容分散到 ISPP 的相应部分，例如与安全保障要求一起描述。ISPP 应用注释的一个典型应用是提供如何在信息系统上下文中解释特定安全保障要求的说明，或 ISST 编制者的操作建议。如果 ISPP 应用注解被整合到整个 ISPP 中，建议清楚地标识出该应用注解，以使读者能够清楚地知道它是说明性的文本。

7 信息系统描述

7.1 概述

本章为描述一个完整的信息系统提供指南。一个完整的信息系统描述应包括信息系统使命描述、信息系统概要描述和信息系统详细描述三部分。

7.2 信息系统使命描述

信息系统使命描述，即从目的和意义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。

7.3 信息系统概要描述

信息系统概要描述是对信息系统进行概括性说明和描述，内容如下：

a) 信息系统：包括信息系统名称、所属的组织机构及其地点和最终用户及其地点等相关信息；

b) 信息系统环境：描述信息系统的运行、开发、集成和维护的环境；

c) 信息系统评估边界和接口：描述信息系统的边界和相应的外部接口，此描述建议采用图表和文字相结合的方式，清晰地描述和界定信息系统部件和边界；

d) 信息系统安全域：根据信息系统的重要性（描述信息系统的重要程度以及可接受的风险级别）、数据的分类和密级（描述信息系统所处理的数据类型和机密级别），以及系统用户（描述使用系统的用户）等方面划分系统的安全域。

7.4 信息系统详细描述

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组织结构、所使用的规章制度和所涉及的重要资产进行描述。

   1) 组织机构：描述同信息系统相关的管理/使用/开发/集成/支持等组织机构，特别是与安全保障管理相关的组织机构的描述；

   2) 规章制度：列出目前使用的、同信息系统管理相关的规章制度；

   3) 资产：描述了信息系统的物理资产（信息系统中的各种硬件、软件和物理设施）和信息资产（在信息系统计划组织、开发采购、实施交付、运行维护和废弃生命周期过程中产生的、有价值的信息以及信息系统所存储、处理和传输的各种办公、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核心，对信息系统的应用、网络基础设施和技术标准进行描述。技术体系的描述为业务体系的描述提供支持。

   1) 网络基础设施：描述信息系统的网络层次等网络体系结构；

   2) 应用：描述信息系统应用的技术架构；

   3) 技术标准：描述应用所采用的技术标准。

c) 业务体系：基于技术体系，业务体系对组织机构的主要业务进行分类和描述，并通过业务流程

和业务信息流来进一步解释。

1） 主要业务：列出组织机构的主要业务并进行描述；

2） 业务流程：基于组织机构对主要业务的流程进行描述；

3） 业务信息流：描述主要业务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方式。

8 安全保障需求

8.1 概述

本章为定义在 ISPP 或 ISST 中描述信息系统的安全保障需求提供指南，这一部分内容的要求见 GB/T 20274.1—2006 的 A.2.4 和 B.2.4。

定义安全保障需求首先应识别信息系统的安全环境，根据安全环境定义信息系统的安全保障需求。安全环境应描述信息系统的预期使用方式以及使用的环境范围和特征。安全环境描述应包括假设、威胁和组织安全策略，如图 2 所示。

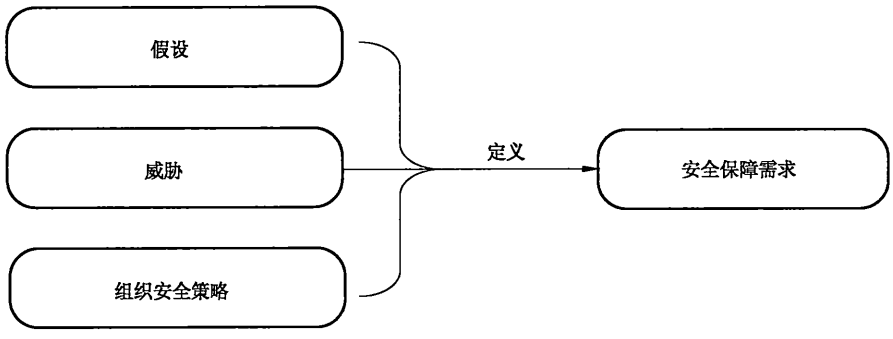

图 2 定义安全保障需求的过程

本章包括以下内容：

a） 依据信息系统安全环境的假设，定义出“安全保障需求”的范围；

b） 依据需要保护的系统资产，包括信息系统环境或信息系统本身典型的资产，以及已知的威胁主体和对系统资产的威胁；

c） 在处理安全保障需求时，必须服从的所有组织安全策略。

8.2 识别和说明假设

GB/T 20274.1—2006 要求 ISPP 或 ISST 的信息系统安全环境部分包括安全环境的假设或信息系统的预期用途。首先需要回答下面的问题：

对于信息系统安全环境和安全保障需求范围，应做出什么假设？

例如，可能需要给出几个假设来保证某个系统的潜在威胁实际上是与信息系统环境无关的。

常用的假设类型：

a） 有关信息系统预期用途的假设；

b） 信息系统任一部分的环境（例如，物理的）保护假设；

c） 连通性假设，例如信息系统与其他系统之间的网络连接点；

d） 人员方面的假设，例如预期的用户权限类型，他们的一般责任以及假设给予这些用户的信任度等。

e） 通常情况下，不太可能一次就完全识别出所有假设，而应在 ISPP 或 ISST 的整个编制过程中

不断识别出更多的假设。特别是在编制 ISPP 或 ISST 符合性声明时，例如在阐明安全保障目的适于对抗已知的威胁时，应考虑该威胁是否包含在 ISPP 或 ISST 的陈述中。

为方便引用，建议对每个假设设定唯一的名称或编号。

8.3 识别和说明威胁

8.3.1 概述

GB/T 20274.1—2006 要求 ISPP 或 ISST 包括所有对要保护资产的威胁的描述(见 GB/T 20274.1—2006 的 A.2.4)，但 GB/T 20274.1—2006 还指出：如果安全保障目的仅源于组织安全策略，也就是“安全保障需求”完全由组织的安全策略和假设来定义，那么就可以不需要进行威胁分析。例如，在回应招标书或投标邀请书给出的组织安全策略就属于这种情况。

在 ISPP 或 ISST 中安全需求被陈述为“威胁”会比陈述为相应的“组织安全策略”要好，因为这有助于对安全需求的理解。另外，如果只使用组织安全策略陈述安全需求，那么可能出现不能及时更新当前威胁的风险。风险分析的重要意义在于正确地识别资产以及对于资产的威胁，不应低估风险分析的重要性。

如果风险分析做不好，可能出现下列情况：

a) 信息系统可能会提供不充分的保护，那么组织的资产就可能面临不可接受的风险；

b) 可能过高估计威胁，从而提高了实现成本及保障要求，并限制了潜在解决方案。

GB/T 20274 系列标准没有提供风险分析的框架和组织规范，识别资产威胁的详细讨论也超出了本指导性技术文件的范围，为了保持本指导性技术文件内容的完整性，下面将陈述有关的一般性原理，另见 GB/T 20274.1—2006 的第 5 章。有关这一主题的详细说明，见 GB/T 20984—2007 等。

8.3.2 识别威胁

威胁是指那些不希望发生的事件，可能由已知的威胁主体引起，而使资产面临风险，注意：对组织安全策略和假设的违背不应算作风险。要识别风险是什么，应回答下列问题：

a) 需要保护的资产是什么？

b) 威胁主体是什么？

c) 需要保护资产免于什么攻击方法或事件造成的损害？

8.3.3 识别资产

在一个组织中，资产有多种表现形式，同样的两个资产也因属于不同的信息系统而重要性不同，而且对于提供多种业务的组织，其支持业务持续运行的系统数量可能更多。这时首先需要将信息系统及相关的资产进行恰当的分类，然后对资产进行识别，以此为基础进行下一步的风险评估。在实际工作中，具体的资产分类方法可以根据具体的评估对象和要求，由评估者灵活把握。例如根据资产的表现形式进行分类，可将资产分为数据、软件、硬件、文档、服务、人员等类型，如表 3 所示(另见 GB/T 20984—2007)。识别资产的描述应包括资产的价值、资产所有者、责任人等。

表 3 资产分类

分类	示　例
数据	保存在信息媒介上的各种数据资料，包括源代码、数据库数据、系统文档、运行管理规程、计划、报告、用户手册等
软件	系统软件：操作系统、语句包、工具软件、各种库等； 应用软件：外部购买的应用软件，外包开发的应用软件等； 源程序：各种共享源代码、自行或合作开发的各种代码等

表 3（续）

分类	示　例
硬件	网络设备：路由器、网关、交换机等； 计算机设备：大型机、小型机、服务器、工作站、台式计算机、移动计算机等； 存储设备：磁带机、磁盘阵列、磁带、光盘、软盘、移动硬盘等； 传输线路：光纤、双绞线等； 保障设备：动力保障设备（UPS、变电设备等）、空调、保险柜、文件柜、门禁、消防设施等； 安全保障设备：防火墙、入侵检测系统、身份验证等； 其他：打印机、复印机、扫描仪、传真机等
服务	办公服务：为提高效率而开发的管理信息系统（MIS），包括各种内部配置管理、文件流转管理等服务； 网络服务：各种网络设备、设施提供的网络连接服务； 信息服务：对外依赖该系统开展的各类服务
文档	纸质的各种文件，如传真、电报、财务报告、发展计划等
人员	掌握重要信息和核心业务的人员，如主机维护主管、网络维护主管及应用项目经理等
其他	企业形象、客户关系等

8.3.4　识别攻击方法

在确定要保护的资产和威胁主体之后，下一步就是识别可能导致资产受损的攻击方法，应基于对信息系统环境的了解来确认攻击方法，如：

a）　内部人员攻击；

b）　被动攻击；

c）　主动攻击；

d）　物理临近攻击；

e）　分发攻击。

各种攻击方式具体解释如下：

a）　内部人员攻击

1）　内部人员威胁通常由内部合法人员造成，他们具有对信息系统的合法访问权限。威胁分为恶意和非恶意两种，即恶意攻击和非恶意威胁。

2）　恶意攻击是内部人员出于各种目的，对所使用的信息系统实施攻击。

3）　非恶意威胁是由于合法用户的无意行为造成了对系统的攻击，他们并非故意要破坏信息和系统，但由于误操作、经验不足、培训不足而导致一些特殊的行为，对系统造成了无意的破坏。

4）　典型的内部人员攻击：

——　恶意修改数据和安全机制配置参数；

——　恶意建立未授权的网络连接，如拨号连接；

——　恶意的物理损坏和破坏；

——　无意的数据损坏和破坏，如误删除。

b）　被动攻击

被动攻击主要包括被动监视开放的通信信道（如无线电、卫星、微波和公共通信网络）上的传

送信息。被动攻击主要是了解所传送的信息，一般不易被发现。典型例子如下：

1） 监视通信数据；

2） 解密加密不当的通信数据；

3） 口令截获；

4） 通信量分析。

c） 主动攻击

主动攻击是攻击者主动对信息系统实施攻击，包括企图避开安全保护，引入恶意代码，以及破坏数据和系统的完整性。典型的例子有：

1） 修改传输中的数据；

2） 重放所截获的数据；

3） 插入数据；

4） 盗取合法建立的会话；

5） 伪装；

6） 越权访问；

7） 利用缓存区溢出(BOF)漏洞执行代码；

8） 插入和利用恶意代码(如特洛依木马、后门、病毒等)；

9） 利用协议、软件、系统故障和后门；

10） 拒绝服务攻击。

d） 邻近攻击(接近攻击)

此类攻击的攻击者试图在地理上尽可能接近被攻击的网络、系统和设备，目的是修改、收集信息，或者破坏系统。这种接近可以是公开的和秘密进入的，也可以是两种都有，典型案例有：

1） 修改数据；

2） 收集信息；

3） 偷窃；

4） 物理破坏。

e） 分发攻击

分发攻击是指在系统软件和硬件的开发、生产、运输、安装阶段，攻击者恶意修改设计、配置等行为。例如：

1） 利用开发制造商的设备上修改软硬件配置；

2） 在产品分发、安装时修改软硬件配置。

8.3.5 说明威胁

识别出信息系统或环境所处理的威胁之后，下一步就是将它们列入 ISPP 或 ISST 中。如前所述，信息系统安全环境部分应清晰简明地陈述安全保障需求。

为了提供清晰的威胁说明，威胁说明应包括以下细节：

a） 威胁主体(例如，信息系统的授权用户)；

b） 受威胁控制的资产(例如，敏感数据)；

c） 使用的攻击方法(例如，假冒的信息系统授权用户)。

陈述威胁的具体示例如下：

1） 攻击者可能通过假冒信息系统的授权用户，未经授权访问信息或资源；

2） 信息系统的授权用户可能假冒其他信息系统的授权用户，未经授权地访问信息或资源。

如果将威胁描述与描述项的解释、资产受到的威胁范围、以及威胁主体可能使用的攻击方法一起综合陈述，那么读者就比较容易理解威胁描述。例如，上面陈述的威胁示例中，处于风险中的资产是用户

或假冒的用户有权访问或获取这些假冒的一系列的信息和资源。

为有助于确保简明描述威胁，威胁描述应尽可能独立，即不同威胁之间应尽可能不重叠。这样既有助于避免使 ISPP 或 ISST 读者产生混淆，也可以通过避免不必要的重复来简化 ISPP 或 ISST 符合性声明。

如果以同样详细程度陈述所有威胁，那么威胁之间的重叠就容易避免。例如，如果特定攻击情节与在 ISPP 或 ISST 的其他部分陈述的一般威胁有关，那么就不要陈述这样的威胁，因为它描述的是已详细说明了的对特定资产的攻击方法。

每个威胁都应唯一标识以方便引用，标识方式有：

a) 采用连续的编号进行标识（例如 T1、T2、T3 等）；

b) 采用简短而有意义的名称进行标识。

第一种方法的优点是，编号通常很短，并易于参考。第二种方法的优点是，使用名称作为标识，名称具有充分的含义并且容易记忆。然而，在使用第二种标识方法时，由于实际中限制名称中字符数量，并且名称还要含义准确和易于记忆，因此，不可能在所有情况下都分配一个完整定义的标识。

威胁描述不应仅涉及那些直接危害被保护资产的事件，还应要考虑对资产的间接威胁，即针对威胁的措施间接导致资产损失的攻击，例如对信息系统安全功能的旁路或篡改攻击。针对间接威胁，要特别注意以下几点：

a) 不要将间接威胁作为信息系统安全环境，否则会使读者过早涉及信息系统的实现细节，从而产生困惑；

b) 不要将间接威胁纳入已有的威胁范围之内。

例如，如果威胁 X 可能损害资产 Y，则任何旁路对抗威胁 X 的措施也可能导致资产 Y 的损害。由于这种旁路威胁是一种已经隐含在威胁 X 内的攻击方法，不应再将它作为单独的威胁陈述出来。

还应注意到，当需要选择 GB/T 20274.1—2006 中有依赖关系的组件形成安全保障要求时，必须考虑对信息系统安全措施的攻击方法，比如旁路或篡改攻击。任何对信息系统安全功能的可行攻击都应在信息系统评估期间被全部罗列出来。

8.4 识别和确定组织安全策略

GB/T 20274.1—2006 的 A.2.4 要求信息系统安全环境部分包括信息系统必须服从的所有组织安全策略的描述，但 GB/T 20274.1—2006 又指出：如果安全保障目的仅源于威胁，也就是“安全保障需求”完全由威胁来定义，那么就可以忽略组织安全策略的陈述。

组织安全策略是指组织机构为保障其运转而规定的若干安全规则、程序、规范和指南。组织安全策略可能需要由信息系统或其环境或由两者一起实施。

如果 ISPP 或 ISST 指定了组织安全策略及威胁，那么就应在信息系统安全环境部分给出安全保障需求的简明陈述。仅以不同形式简单重述某个威胁的组织安全策略，通常是无用的。该现象仅出现在组织强制要求对某个组织安全策略进行声明的情况，实际上这个组织安全策略是对一个已存在的威胁的重新声明。

例如，如果已经识别出一个威胁“非授权者可能获得对信息系统的逻辑访问”，再给出如下陈述的组织安全策略“必须在信息系统访问被接纳之前鉴别信息系统的合法用户”，并不会赋予更多信息。这个组织安全策略不仅以不同方式重述这个威胁，而且也重复了安全保障目的的定义。如果只陈述一次，ISPP 或 ISST 将更清晰易懂。

一般的规则是：信息系统预期由特定组织或一类组织使用，或信息系统需要实现一组明显不包含或仅隐含在威胁描述中的规则时，制定出组织安全策略才是适当的。例如：

a) 标识所使用的信息流控制规则；

b) 标识所使用的访问控制规则；

c) 定义有关安全审计的组织策略；

d) 强制性要求，例如使用特别批准的密码算法，或使用与认定的指南相一致的密码算法。应唯一标识每个组织安全策略以便于引用。

8.5 明确安全保障需求定义

定义安全保障需求的最后一个阶段是完成安全保障需求定义详述，包括两件工作：

a) 准备假设、威胁、组织安全策略的列表；

b) 执行一致性和完整性检查，确定安全保障需求。

9 安全保障目的

9.1 概述

本章提供在 ISPP 或 ISST 中识别和制定安全保障目的的指南，这方面要求见 GB/T 20274.1—2006 的 A.2.5 和 GB/T 20274.1—2006 的 B.2.5 的描述。

安全保障目的是对安全保障需求预期响应的简明陈述，换言之，如果在安全环境中已经陈述了安全保障需求，那么就必须在安全保障目的的陈述中明确地界定出安全保障需求是由信息系统还是由环境来满足或实现的。如图 3 所示。

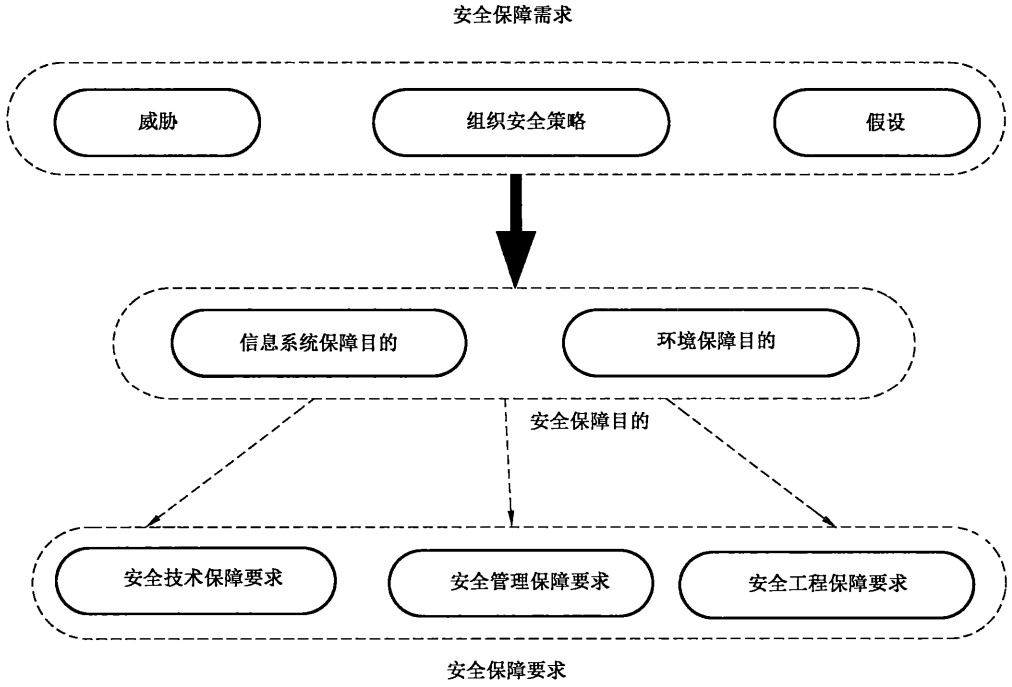

图 3 安全保障目的的作用

图 3 中明确标识出 GB/T 20274.1—2006 要求的两种类型的安全保障目的，它们在 ISPP 或 ISST 中是明确分开的：

a) 信息系统安全保障目的，由信息系统的安全保障措施来满足；

b) 环境安全保障目的，由信息系统外部环境来满足，例如国家或行业的政策与法律法规。

信息系统的安全保障目的包括由信息系统安全保障控制措施和信息系统安全保障能力级别。

信息系统安全保障目的基于下面一系列的步骤产生：

a) 安全保障目的要覆盖所有威胁、组织安全策略和假设；
b) 识别信息系统安全保障目的；
c) 识别环境安全保障目的；
d) 关联威胁、组织安全策略和假设的安全保障目的的符合性声明。

9.2 威胁、假设和组织安全策略的列表

首先，从安全保障需求定义中裁减所有适用的威胁、组织安全策略和假设的列表。特别是由于假设不会产生安全保障目的的威胁，这些威胁应被裁减。

保留下的威胁、组织安全策略和假设应按照以下类型区分：

a) 与信息系统环境有关的；
b) 与信息系统有关的。

9.3 信息系统环境保障目的

环境安全保障目的使用唯一性标识以便于引用，采用的标识方法最好能区别环境安全保障目的和信息系统安全保障目的。如果采用序列编号，应为两类安全保障目的分别编号（如对环境安全保障目的使用 OE1、OE2、OE3 等）。

9.4 信息系统安全保障目的

信息系统安全保障目的可进一步细分为安全技术保障目的、安全管理保障目的和安全工程保障目的。

安全技术保障目的，是从信息系统安全角度达到信息系统安全保障目标。可将安全技术保障目的进一步分解为对网络基础设施的目的、对边界安全的目的、对计算环境的目的和对支撑性安全基础设施的目的以及端到端的安全技术保障目的。

安全管理保障目的，是根据通过覆盖信息系统生命周期的各阶段的管理域来标准化建立完善的信息安全保障管理体系，从而在实现信息能够充分共享的基础上，同时保障信息和其他资产，保证业务的持续性并使业务的损失最小化。可将安全管理保障目的进一步分解为安全风险管理、安全策略管理和安全运行等。

安全工程保障目的，是对信息系统工程过程进行标准化。依据信息系统的安全工程过程生命周期，可将安全工程保障目的进一步分解为挖掘安全需求、定义安全保障要求、设计体系结构、详细安全设计、实现系统安全和有效性评估等。

GB/T 20274.1—2006 的 A.2.5 要求信息系统安全保障目的可明确映射到相关威胁或组织安全策略，因此需要确保：

a) 每个已知的、由信息系统完全或部分对抗的威胁，至少被一个安全保障目的所覆盖；
b) 每个已知的、由信息系统完全或部分符合的组织安全策略，至少被一个安全保障目的所覆盖。

这一映射可以通过交叉引用或用表格形式提供。要求的信息在符合性声明中提供。在安全保障目的部分提供映射对 ISPP 或 ISST 读者来讲更有帮助。描述遵从组织安全策略的安全保障目的时，引用组织安全策略比重述完整的实现规则更适用。

唯一标识信息系统安全保障目的以便于引用，标识方法可采用序列编号（如 O1、O2、O3 等），也可采用简短而有意义的名称。

10 安全保障要求

10.1 概述

本章提供有关 ISPP 与 ISST 中的信息系统安全保障的编制指导，此指导不仅适用于信息系统安全

保障要求而且适用于环境的安全保障要求。

在 ISPP 与 ISST 中说明了下列类型的信息系统安全保障要求，如图 4 所示：

a) 信息系统的安全保障技术要求(STR)，标识出确保达到信息系统安全保障目的的安全技术保障要求；

b) 信息系统的安全保障管理要求(SMR)，标识出确保达到信息系统安全保障目的的安全管理保障要求；

c) 信息系统的安全保障工程要求(SER)，标识出确保达到信息系统安全保障目的的安全工程保障要求；

d) 信息系统的环境安全保障要求(这些在 ISPP 或 ISST 是可选的)。

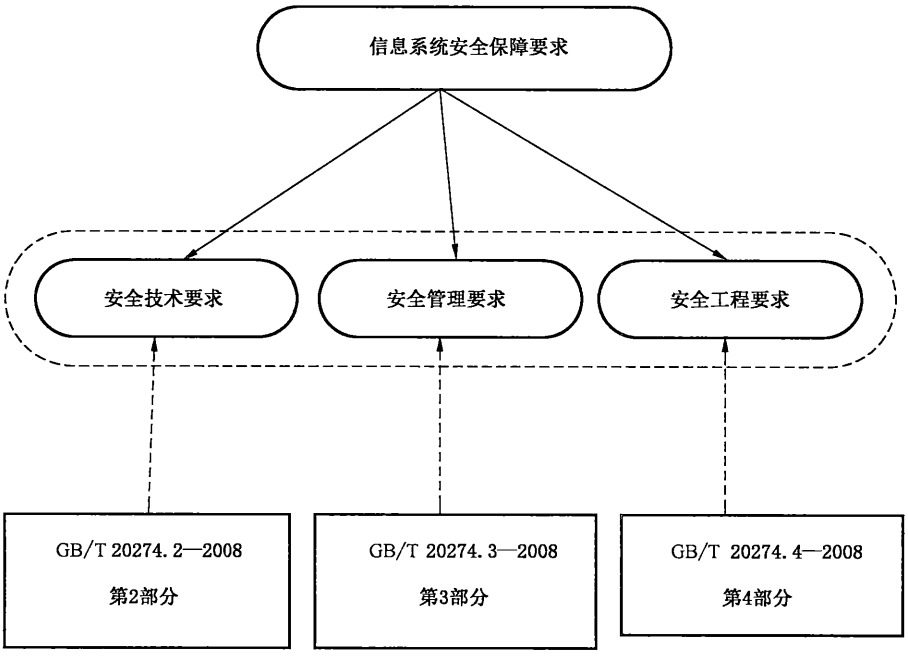

图 4 信息系统安全保障要求

除信息系统安全技术、管理和工程要求组件外，对 ISPP 与 ISST 的信息系统安全保障要求部分需要说明信息系统安全技术强度的最低级别，并在相关地方对强度进行明确声明(见 GB/T 20274.1—2006 的 A.2.6 和 GB/T 20274.1—2006 的 B.2.6)。

图 4 表明，信息系统安全保障要求的显著特点是，尽可能用 GB/T 20274.2—2008、GB/T 20274.3—2008、GB/T 20274.4—2008 中定义的保障组件来构建。GB/T 20274.1—2006 的意图是确保安全保障要求以标准化的方式提出。使用 GB/T 20274.2—2008、GB/T 20274.3—2008、GB/T 20274.4—2008 表达信息系统安全保障要求更有利于 ISPP 与 ISST 之间的对比。

在有些情况下允许不用 GB/T 20274.2—2008、GB/T 20274.3—2008、GB/T 20274.4—2008 的组件来陈述安全保障要求，但这些要求必须是明确的、可评估的，并且采用与 GB/T 20274.2—2008、GB/T 20274.3—2008、GB/T 20274.4—2008 相同的风格描述组件。

GB/T 20274.2—2008、GB/T 20274.3—2008、GB/T 20274.4—2008 允许 STR、SMR 和 SER 有一定程度的灵活性，允许通过实施一系列的操作以满足相应的安全保障要求。这些操作包括赋值、反复、选择和细化，用于特殊数据项的显示和(或)修改。

10.2 提供了对 GB/T 20274.2—2008 技术组件进行操作的指导，10.3 提供了对 GB/T 20274.3—2008 管理组件的操作指导，10.4 提供了对 GB/T 20274.4—2008 工程组件的操作指导。每个安全保障

要求组件都有唯一的基于分类标准的参考名。例如：

a) GB/T 20274.2—2008 中的组件 FAU_GEN.1.2 具有如下含义：
   1) “F”表示它是技术(功能)组件；
   2) “AU”表示它属于 STR 的安全审计类；
   3) “GEN”表示它属于该类中安全审计数据产生子类；
   4) “1”表示它属于该子类中审计数据产生组件；
   5) “2”表示它是该组件中的第二个元素。
b) GB/T 20274.3—2008 中的组件 MPS_SAT.2 具有如下含义：
   1) “M”表明它是管理组件；
   2) “PS”表明它属于 SMR 的“人员安全”类；
   3) “SAT”表明它属于“安全意识和培训”子类；
   4) “2”表明它属于该子类中的“安全培训”组件。
c) GB/T 20274.4—2008 中的 PEN_SEE.2 具有如下含义：
   1) “P”表示它是工程组件；
   2) “EN”表示属于 SER 的“工程过程”类；
   3) “SEE”表示它属于该类中的“安全工程实施”子类；
   4) “2”表示它属于该子类中的“系统试运行”组件。

STR、SMR 和 SER 的选择以组件为单位。如果在 ISPP 与 ISST 中包括某个组件，则组件中所有已定义的元素都应包括进来。要注意组件间有两种关联类型，它会影响信息系统安全保障要求的选择：

a) 子类内组件可能有层次关系，表明一个组件包括在子类内其他组件中规定的全部要求元素。例如，FAU_SAA.4 是 FAU_SAA.3 的从属组件，因为前者中包含了所有在后者中定义的功能元素。但 FAU_SAA.4 不是 FAU_SAA.1 的从属组件，因此可以在同一个 ISPP 与 ISST 中同时包括这两个组件；
b) 已经定义的组件可能与其他子类中的组件有依赖关系。例如，FAU_SAA.1(潜在侵害分析)依赖于 FAU_GEN.1(审计数据产生)。这些组件也必须包括在 ISPP 与 ISST 中，除非依赖性可以表明与威胁和安全保障目的无关。

10.2 安全技术保障要求

10.2.1 安全技术保障要求的选择

在定义了安全保障需求并以安全技术保障目的的形式对应了这些需求之后，现在需要详细阐述安全技术要求将如何满足这些安全保障目的。首先，选择一组适当的 STR 组件，如果预先定义与信息系统的安全保障目的相关的技术组件包，将简化 STR 的选择过程。本指导性技术文件的附录 A 提供了信息系统安全技术要求从 GB/T 20274.2—2008 中定义的安全技术要求(STR)组件中选取。

为 ISPP 或 ISST 选择 STR 的过程分几个阶段，在选择过程中要注意区别以下两种类型的 STR：

a) 主要的 STR，它直接满足信息系统安全保障目的；
b) 支持性的 STR，它不直接满足信息系统安全保障目的，但对主要的 STR 提供支持，从而间接支持相应信息系统安全保障目的。

GB/T 20274.2—2008 没有明确区别这两种类型的 STR，但其差别暗含在功能组件间的依赖性或 STR 间的相互支持中。因此，没有必要在 ISPP 或 ISST 中明确区分这两类 STR，但在编写安全保障目的符合性声明时，认识到存在这两类 STR 是非常有益的。

在选择 STR 时，首先识别出能够满足信息系统一个安全保障目的的一组主要的 STR，再识别出一组完整的支持性 STR。如前所述，所有 STR(不论主要的或支持性的)应该用适当的 GB/T 20274.2—

2008 中的技术保障组件来表达。当从 GB/T 20274.2—2008 中选择组件时，应参考在 GB/T 20274.2—2008 的附录中技术保障组件依赖关系表。

两种类型 STR 之间的关系如图 5 所示，注意这种关系与 ISPP 或 ISST 符合性声明相关，要求表现 STR 之间的相互支持。它包含了对支持性 STR 提供支持的性质的解释，从而保证了信息系统安全技术保障目的得到满足。

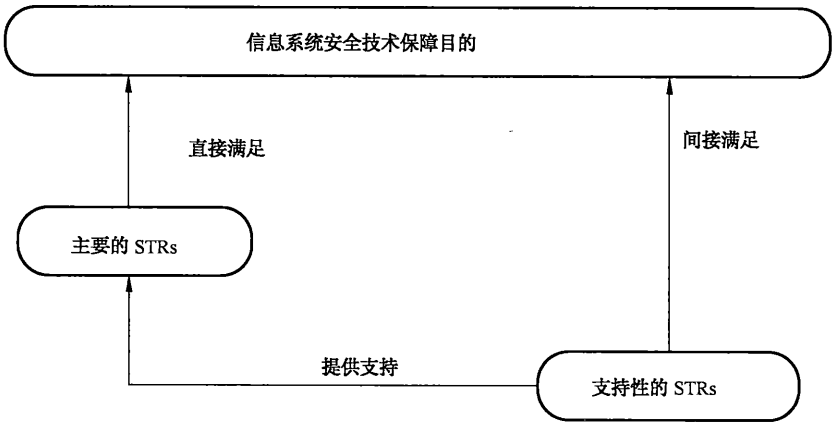

图 5　主要的 STRs 和支持性的 STRs 的关系

识别完整的支持性 STR 的过程分 3 个阶段：

a) 识别出所需的用于满足(认为它适用的话)所有主要 STR 依赖性的 STR(像 GB/T 20274.2—2008 中定义相关技术组件一样)。它包括本阶段识别的支持性 STR 的所有依赖性；

b) 识别为确保达到信息系统安全保障目的补充 STR。它包括用来抵抗组合攻击的 STR；

c) 识别补充 STR 的支持性 STR(认为它适用的话)，以满足那些在 a)和 b)这两个阶段中选择的 STR 的依赖关系。

支持性 STR 满足 GB/T 20274.2—2008 中给出的依赖关系的识别过程，可能需要多次反复，例如：

a) 假设 ISPP 或 ISST 要包括的安全保障目的要求信息系统在检测到即将发生安全事故时做出响应，这会导致将基于 FAU_ARP.1 组件(安全警告)作为主要 STR 包含进来；

b) 根据 GB/T 20274.2—2008，FAU_ARP.1 依赖于 FAU_SAA.1(潜在侵害分析)，这样该组件要作为支持性 STR 应被包含进来；

c) FAU_SAA.1 依赖于 FAU_GEN.1(审计数据产生)，该组件也要作为支持性 STR 应被包含进来；

d) FAU_GEN.1 依赖于 FPT_STM.1(可信时间戳)，该组件也要作为支持性 STR 应被包含进来；

e) FPT_STM.1 则不需要引入别的功能组件。

GB/T 20274.1—2006 允许部分有依赖关系产生的 STR 不满足安全保障目的，但需要作者对此进行合理的解释。

依赖性应以一致的方式被使用，例如，对于 FAU_ARP.1 而言，其符合性是由该组件的性质决定的(即 FAU_ARP.1 依赖于对可能发生的安全违规的预测，这种违规是用 FAU_SAA.1.2 来定义的)。

对另外一些组件来说，保证符合性可能比较困难。例如，对于组件 FDP_ACC.1，ISPP 或 ISST 将识别出与之相关的特殊访问控制 SFP，为满足 FDP_ACC.1 对 FDP_ACF.1 的依赖性，必须确保相同的访问控制 SFP 作用于 FDP_ACF.1 和 FDP_ACC.1。如果针对不同访问控制 SFP，对组件 FDP_ACC.1 施行“反复操作”，那么对每个访问控制 SFP，都需要满足对 FDP_ACF.1 的依赖性。

对额外的支持性 STR 的识别(例如在 GB/T 20274.2—2008 中未被识别的依赖性)包括 GB/T 20274.2—2008 中未提及的 STR 的识别对支持达到信息系统安全保障目的是必须的。这类的

STR 一般通过减少攻击者可利用的选择或机会提供支持，或增加攻击者要实现成功攻击所需达到的专业知识水平或资源。应根据安全保障需求和安全保障目的考虑下述问题：

a) 基于 GB/T 20274.2—2008 中同类相关组件的 STR。比如，如果包括组件 FAU_GEN.1(审计数据产生)，那么就隐含着一个产生和维护存储所产生数据(需要一个或多个来自 FAU_STG 子类的功能组件)的安全审计踪迹的组件，以及利用工具审查所产生的审计数据(需要一个或多个来自 FAU_SAR 子类的功能组件)的组件。或者将所产生的审计数据输出到其他系统去审查；

b) 基于 FPT 类相关组件的 STR。这类 STR 一般保护其他 STR 所依赖的 TSF 或 TSF 数据的完整性和可用性。以 FPT_AMT.1(抽象机测试)和 FPT_SEP(域分离)子类的组件为例，当有确定的需求要保护 TSF 使之不出故障、不被中断或不被(可能是恶意的)修改时，可能需要上述组件支持相应的安全保障目的；

c) 基于 FMT 类相关组件的 STR。这些组件用于规定所有需要支持的安全管理 STR，以处理取消安全属性的 FMT_REV.1 组件为例，在含有处理安全属性(如访问控制)的 STR 时，可以考虑使用这类相关组件。

应根据安全保障目的选择支持性的 STR，尤其要考虑 STR 应该是相互支持的、紧密结合的、有效的整体。构建 ISPP 符合性声明的过程会影响那些支持性 STR 的选择，因为符合性声明需要证明 STR 是相互支持的、完整的、有效的整体。强烈建议不要选取与安全保障目的无关的支持性 STR，因为这样会让 ISPP 或 ISST 不易被接受，其原因是：

a) STR 不适用某些信息系统；

b) 增加 STR 的数量会增加成本及对不必要需求的维护。

如果 ISPP 以相关 ISPP 为基础编写，那么选择 STR 的过程会大大简化。相同的，如果 ISST 以相关 ISST 为基础编写，那么选择 STR 的过程也会大大简化。ISPP 和 ISST 应包括不同的 STR，并考虑信息系统中的安全环境和(或)安全保障目的之间的差异。

10.2.2 安全技术保障要求的操作

根据 GB/T 20274.2—2008，安全技术控制组件可以依据本指导性技术文件中定义的操作使用，也可以通过使用安全保障控制组件允许的操作，对安全技术控制组件进行裁剪，以满足特定的安全策略或应对特定的威胁。安全技术控制组件标识并定义了组件是否允许“赋值”“选择”和“细化”等操作，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结果。允许的操作如下所述：

a) 反复：采用不同的操作多次使用同一组件；

b) 赋值：对指定参数的详述；

c) 选择：对列表中的一个或多个元素的选择；

d) 细化：对安全保障要求组件增加细节，细化了可能接受的解决办法，但不引入任何新的 STR 的依赖性。

10.2.3 GB/T 20274.2—2008 中未包含的 STR 的说明

如果 ISPP 或 ISST 增加 GB/T 20274.2—2008 中未定义的保障要求时，应按 GB/T 20274.2—2008 中组件的表达模式构建 STR。

可以通过恰当应用细化、赋值、选择等操作构建新的 STR。一般情况下，建议 ISPP 中不要轻易添加保障组件，因为这样会使安全保障要求的含义或意图变得模糊，进而增加对其他不适于包括在 ISPP 中的组件的依赖性。

使用 GB/T 20274.2—2008 保障组件的表达模式，构建新的 STR，具体表达模式如下：

a) 使用与 GB/T 20274.2—2008 组件相同的抽象程度；

b) 使用与 GB/T 20274.2—2008 组件相似的风格和措辞；

c) 使用 GB/T 20274.2—2008 组件采用的拓扑和逻辑。

新构建的 STR 具有与类或子类中其他组件相似的性质，使用整个类或子类通用概念的特定用词，有助于减少对它的陌生感。

GB/T 20274.2—2008 中的组件表现风格的独特性包括：

a) 多数安全保障要求组件是以短语“TSF 将”或“TSF 将能够”开始的，后面跟着这样的动词：检测、执行、确保、限制、监视、防止、保护、提供或限制；

b) 使用标准术语，如：安全属性、授权管理员等；

c) 每个元素往往各自独立并无须引用以前元素即可理解。

d) 每个安全保障要求必须是可评估的，即必须是可以判定它是否被信息系统实现。

当形成符合上述风格的 STR 后，还应考虑是否：

a) 允许 ISST 作者对该 STR 实施赋值或选择操作；

b) 有依赖关系的其他 STR 必须包括在 ISPP 或 ISST 中；

c) STR 描述应审计的所有事件，以及应记录这些事件的那些信息；

d) STR 有安全管理的含义，如依赖需要管理的安全属性。

如果构建了一个比 GB/T 20274.2—2008 中已有的功能组件更好的 STR，可以考虑在标准下一次修改时提交这个 STR。

GB/T 20274.1—2006 允许 ISST 引用 GB/T 20274.2—2008 中未定义的 STR，如果这个 STR 只是用于自身的 ISST，并不准备复用于其他的 ISPP、ISST 或功能包，那么，不要求为这些 STR 指定 GB/T 20274.1—2006 规定的诸如赋值、选择等操作。

命名 GB/T 20274.2—2008 中未定义的 STR，建议采用与标准相同的结构和习惯，该类新增组件是 GB/T 20274.2—2008 的扩展组件。扩展组件应该用“T”表示技术，然后是相应的类、子类和组件编号。如果是在已有的类之上扩展组件，那么应将其置于相应的位置。如果扩展的组件与已有的类没有关联，那么组件的类名要清楚地表明它是扩展的安全保障要求，例如，可以在组件类名前或后加上“EX”字样。扩展组件的含义在 ISPP 或 ISST 应用解释中要加以说明，还要注意命名的习惯不能与 GB/T 20274.2—2008 的习惯相冲突。

10.2.4 安全技术能力级的确定

安全技术能力级通过对组织机构执行安全技术每个过程域能力反映了组织机构在执行信息安全技术达到预定的成本、功能和质量目标上的度量。一个组织机构一般可随意以他们所选择的方式和次序来计划、跟踪、定义、控制和改进他们的系统安全技术架构构建过程。然而，由于一些较高级别的通用实践依赖于较低级别的实践，因此组织机构应在试图达到较高级别的系统安全技术体系架构之前，应首先实现较低级别的系统安全技术体系架构的构建实践过程。

安全技术能力级的实施划分为如下的能力级别：

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：计划和跟踪；

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。

安全技术能力级别的确定见 GB/T 20274.2—2008 的第 18 章。

10.3 安全管理保障要求

10.3.1 安全管理保障要求的选择

在定义了安全保障需求并以安全管理保障目的的形式对应了这些需求之后，现在需要详细阐述安全管理要求将如何满足这些安全保障目的。首先，在组件级选择一组适当的 SMR，当然，如果可以预先定义与信息系统的安全保障目的相关的管理组件包，SMR 选择过程就会非常容易。附录 B 提供了信息系统安全技术要求从 GB/T 20274.3—2008 中定义的安全管理要求(SMR)组件中选取。

在进行信息系统安全管理要求的选择时，应考虑以下方面的问题：

a) 应以风险和策略为核心，因此应适当选择信息安全策略(MSP)和风险管理(MRM)安全保障控制类中的组件，并将其作为所有其他安全管理控制措施的核心；

b) 从信息系统安全管理的角度来看，组织机构的信息系统安全组织机构(MSO)、人员安全(MPS)、资产管理(MAM)、物理和环境安全(MPE)以及符合性管理(MCM)是所有信息系统安全管理保障活动所必须依赖的基础；

c) 信息系统安全管理保障应覆盖信息系统整个生命周期。信息系统典型的生命周期模型分为规划组织、开发采购、实施交付、运行维护、废弃五个阶段应用于系统产生的闭合循环周期结构。因此，与之对应并结合了组织机构信息系统的特殊要求，在必要时，安全保障要求的选择应覆盖信息系统安全规划管理(MIP)、系统开发管理(MSD)、运行管理(MOP)、应急响应管理(MER)以及业务持续和灾难恢复管理(MBD)信息系统安全管理控制类。

信息系统安全管理要求是通过不同的信息安全管理控制类中的组件来体现的。

10.3.2 安全管理保障要求的操作

根据 GB/T 20274.3—2008，安全管理控制组件可以依据本指导性技术文件中定义的操作使用，也可以通过使用安全保障控制组件允许的操作，对安全管理控制组件进行裁剪，以满足特定的安全策略或应对特定的威胁。安全管理控制组件标识并定义了组件是否允许“赋值”、“选择”和“细化”等操作，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结果。允许的操作如下所述：

a) 赋值：当组件被应用时，允许填入所规定的参数；

b) 选择：允许从组件表中选定若干项；

c) 反复：允许一个组件与不同的操作一起多次使用；

d) 细化：允许增加细节。

10.3.3 GB/T 20274.3—2008 中未包含的 SMR 的说明

如果 ISPP 或 ISST 增加 GB/T 20274.3—2008 中未定义的保障要求时，应按 GB/T 20274.3—2008 中组件的表达模式构建 SMR。

可以通过恰当应用细化或赋值等操作构建 SMR、选择操作来得到。一般情况下，建议 ISPP 中不要轻易添加保障组件，因为这可能使安全保障要求的含义或意图变得模糊，进而增加对其他不适于包括在 ISPP 中的组件的依赖性。

使用 GB/T 20274.3—2008 保障组件的表达模式，构建新的 SMR，具体表达模式如下：

a) 使用与 GB/T 20274.3—2008 组件相同的抽象程度；

b) 使用与 GB/T 20274.3—2008 组件相似的风格和措辞；

c) 使用 GB/T 20274.3—2008 组件采用的拓扑和逻辑。

新构建的 SMR 具有与类或子类中其他组件相似的性质，使用整个类或子类通用概念的特定用词，有助于减少对它的陌生感。

GB/T 20274.3—2008 中的组件表现风格的独特性包括：

a) 使用标准术语，如：控制、信息处理设施等；

b) 每个元素往往各自独立并无须引用以前元素即可理解；

c) 每个安全保障要求必须是可评估的，即必须是可以判定它是否被信息系统满足。

当形成符合上述风格的 SMR 时，还应考虑是否：

a) 允许 ISST 作者对该 SMR 实施赋值或选择操作；

b) SMR 描述应审计的所有事件，以及应记录这些事件的那些信息。

如果构造了一个比 GB/T 20274.3—2008 中已有的功能组件更好的 SMR，可以考虑在标准下一次修改时提交这个 SMR。

GB/T 20274.1—2006 允许 ISST 引用 GB/T 20274.3—2008 中未定义的 SMR，如果这个 SMR 只是用于自身的 ISST，并不准备复用于其他的 ISPP、ISST 或功能包，那么，不要求为这些 SMR 指定 GB/T 20274.3—2008 规定的诸如赋值、选择等操作。

命名 GB/T 20274.3—2008 中未定义的 SMR，建议采用与标准相同的结构和习惯，该类新增组件是 GB/T 20274.3—2008 的扩展组件。扩展组件应该用“M”表示管理，然后是相应的类、子类和组件编号。如果是在已有的类之上扩展组件，那么应将其置于相应的位置。扩展组件的含义在 ISPP 或 ISST 应用解释中要加以说明，还要注意命名的习惯不能与 GB/T 20274.3—2008 的习惯相冲突。

10.3.4 安全管理能力级的确定

安全管理能力级通过对组织机构执行安全管理每个过程域能力反映了组织机构在执行信息安全管理达到预定的成本、功能和质量目标上的度量。一个组织机构一般可随意以他们所选择的方式和次序来计划、跟踪、定义、控制和改进他们的系统安全管理架构构建过程。然而，由于一些较高级别的通用实践依赖于较低级别的实践，因此组织机构应在试图达到较高级别的系统安全管理体系架构之前，应首先实现较低级别的系统安全管理体系架构的构建实践过程。

安全管理能力级的实施划分为如下的能力级别：

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：计划和跟踪；

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。

安全管理能力级别的确定见 GB/T 20274.3—2008 的第 19 章。

10.4 ISPP 或 ISST 中的安全工程保障要求

10.4.1 安全工程保障要求的选择

定义了安全保障需求并以安全工程保障目的的形式对应了这些需求之后，现在需要详细阐述安全工程要求将如何满足这些安全保障目的。首先，在组件级选择一组适当的 SER，当然，如果可以预先定义与信息系统的安全保障目的相关的工程组件包，SER 选择过程就会非常容易。本指导性技术文件的附录 C 提供了信息系统安全技术要求从 GB/T 20274.4—2008 中定义的安全工程要求(SER)组件中选取。

根据 GB/T 20274.4—2008，信息系统安全工程可划分为三个基本的过程域(即信息系统安全工程控制类)：风险、工程和保障。虽然这些域不是互相独立的，但在进行安全保障要求的选择时，可以分开考虑它们。在最简单的级别中，风险过程识别是按优先级排序对开发出的信息系统的内在危险进行识

别。安全工程过程与其他工程学科共同作用来决定和实施危险所引起问题的解决方案。最后，保障过程建立对安全解决方案的信心并将这种信心传递给用户。

在对风险过程域的安全保障要求进行选择时要考虑：安全工程的一个主要目标是降低风险。风险评估是识别尚未发生的问题的过程。通过针对威胁、脆弱性、影响或者风险本身实施保护措施来降低风险。然而，降低所有风险或完全根除任一特定风险都是不可能的。这主要是因为风险降低的成本，以及相关的不确定性。因此，总是必须接受一些残余风险。在不确定性很高的情况下，由于不能精确地描述风险，接受风险会有很大问题。信息系统安全工程保障的过程域包括确保服务提供方组织机构进行了威胁、脆弱性和影响分析，并综合这些活动所得到的威胁、脆弱性和影响信息进行风险分析，然后得到风险信息。

在对工程过程域的安全保障要求进行选择时要考虑：安全工程和其他工程学科一样，是一个贯穿概念、设计、实施、测试、验收、运行、维护和废弃的过程。在整个过程中，安全工程师必须与系统工程组的其他部分密切工作。信息系统安全工程保障强调安全工程师是大团队的一部分，而且需与其他学科的工程师协作他们的活动。这有助于确保安全是较大过程的重要组成部分，而不是分离、独立的活动。

在对工程过程域的安全保障要求进行选择时要考虑：保障是指安全保障需求得到满足的信心度。它是安全工程的重要产物。保障有很多形式。安全工程的过程保障提供了一个方面：安全工程的过程结果可重复性的信心。这种信心的基础是一个成熟的组织比一个不成熟的组织更可能重复结果。不同形式的保障之间的详细关系是研究中的主题。保障不增加任何附加控制措施对抗安全风险，但它提供这样的信心：已经实施的控制措施将减少已预料到的风险。

10.4.2 安全工程保障要求的操作

根据 GB/T 20274.4—2008，安全工程控制组件可以依据本指导性技术文件中定义的操作使用，也可以通过使用安全保障控制组件允许的操作，对安全工程控制组件进行裁剪，以满足特定的安全策略或应对特定的威胁。安全工程控制组件标识并定义了组件是否允许“赋值”“选择”和“细化”等操作，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结果。允许的操作如下所述：

a) 赋值：当组件被应用时，允许填入所规定的参数；

b) 选择：允许从组件表中选定若干项；

c) 反复：允许一个组件与不同的操作一起多次使用；

d) 细化：允许增加细节。

10.4.3 GB/T 20274.4—2008 中未包含的 SER 的说明

如果 ISPP 或 ISST 增加 GB/T 20274.4—2008 中未定义的保障要求时，应按 GB/T 20274.4—2006 中组件的表达模式构建 SER。

一般情况下，建议 ISPP 作者不要轻易添加保障组件，因为这可能使安全保障要求的含义或意图变得模糊，进而增加对其他不适于包括在 ISPP 中的组件的依赖性。

使用 GB/T 20274.4—2008 保障组件作为表达模式，构建新的 SER，应包括：

a) 使用与 GB/T 20274.4—2008 组件相同的抽象程度；

b) 使用与 GB/T 20274.4—2008 组件相似的风格和措辞；

c) 使用 GB/T 20274.4—2008 组件采用的拓扑和逻辑。

新构建的 SER 具有与类或子类中其他组件相似的性质，使用整个类或子类通用概念的特定用词，有助于减少对它的陌生感。

GB/T 20274.4—2008 中的组件表现风格的独特性包括：

a) 使用标准术语，如：确认、验证等；

b) 每个元素往往各自独立并无须引用以前元素即可理解；

c) 每个安全保障要求必须是可评估的，即必须是可以判定它是否被信息系统满足。

当形成符合上述风格的 SMR 时，还应考虑是否：

a) 允许 ISST 作者对该要求实施赋值或选择操作；

b) SER 描述应审计的所有事件，以及应记录这些事件的那些信息。

如果构造了一个比 GB/T 20274.4—2008 中已有的功能组件更好的 SER，可以考虑在标准下一次修改时提交这个 SER。

GB/T 20274.1—2006 允许 ISST 引用 GB/T 20274.4—2008 中未定义的 SER，如果这个 SER 只是用于自身的 ISST，并不准备复用于其他的 ISPP、ISST 或功能包，那么，不要求为这些 SMR 指定 GB/T 20274.4—2008 规定的诸如赋值、选择等操作。

命名 GB/T 20274.4—2008 中未定义的 SER，建议采用与标准相同的结构和习惯，该类新增组件是 GB/T 20274.4—2008 的扩展组件。扩展组件应该用“P”表示工程，然后是相应的类、子类和组件编号。如果是在已有的类之上扩展组件，那么应将其置于相应的位置。扩展组件的含义在 ISPP 或 ISST 应用解释中要加以说明，还要注意命名的习惯不能与 GB/T 20274.4—2008 的习惯相冲突。

10.4.4 安全工程能力级的确定

安全工程能力级通过对组织机构执行安全工程每个过程域能力反映了组织机构在执行信息安全工程达到预定的成本、功能和质量目标上的度量。一个组织机构一般可随意以他们所选择的方式和次序来计划、跟踪、定义、控制和改进他们的系统安全工程架构构建过程。然而，由于一些较高级别的通用实践依赖于较低级别的实践，因此组织机构应在试图达到较高级别的系统安全工程体系架构之前，应首先实现较低级别的系统安全工程体系架构的构建实践过程。

安全工程能力级的实施划分为如下的能力级别：

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：计划和跟踪；

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。

安全工程能力级别的确定见 GB/T 20274.4—2008 的第 10 章。

11 信息系统概要规范

11.1 概述

信息系统概要规范的目的是让读者了解：STR 如何适用于信息系统的安全技术保障；SMR 如何适用于信息系统的安全管理保障；SER 如何适用于信息系统的安全工程保障。

11.2 信息系统概要规范概述

构成信息系统概要规范的一个好方法是要以概述开始，概述表明信息系统的结构和如何保护自身不被干扰和旁路。然后，安全技术保障应该被描述为基于 STR 的模型；安全管理保障应该被描述为基于 SMR 的模型；安全工程保障应该被描述为基于 SER 的模型。GB/T 20274.1—2006 的 ISST 中对信息系统概要规范有介绍，而在 ISPP 中没有对应的内容。在 GB/T 20274.1—2006 中对信息系统概要规范的定义为在 ISST 中提供的信息系统概要规范定义了信息系统安全保障要求的实例化。它提供了高层设计的描述，分别满足安全保障控制的要求以及相应能力级的要求。信息系统概要规范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

能力级要求。GB/T 20274.1—2006 的 B.2.7 对信息系统概要规范有如下要求：

a) 定义满足已知安全技术保障要求的安全技术保障措施；

b) 定义满足已知安全管理保障要求的安全管理保障措施；

c) 定义满足已知安全工程保障要求的安全工程保障措施；

d) 定义系统的安全保障能力级。

信息系统概要规范的主要组成如图 6 所示。

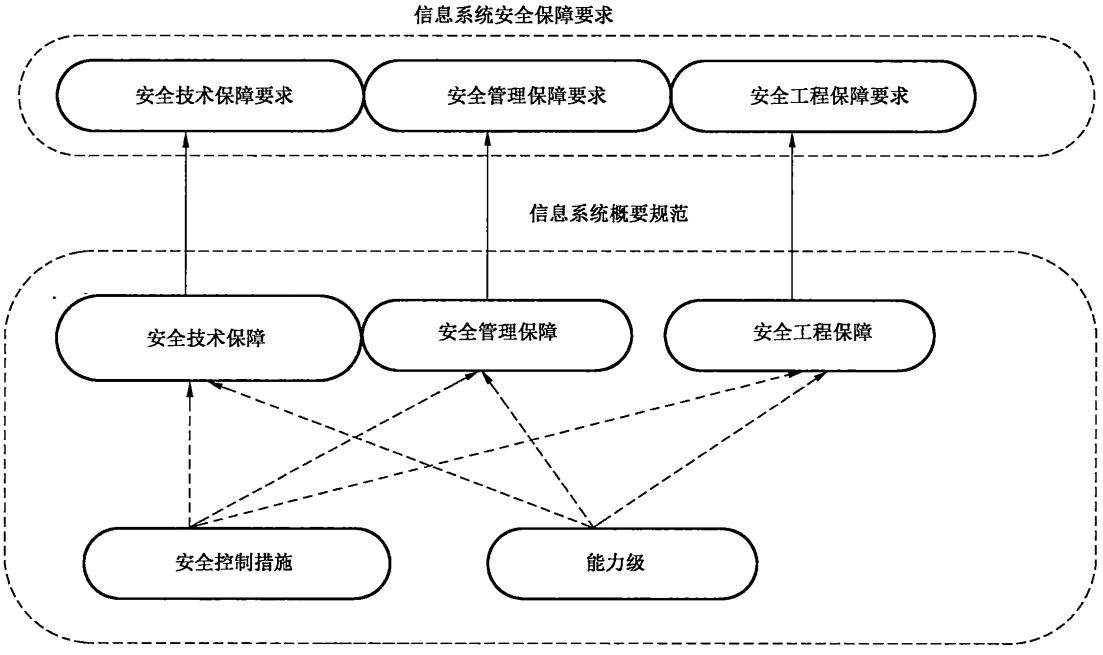

图 6 信息系统概要规范的组成

11.3 安全保障措施的选择

本条针对已知的安全保障需求，确定特定信息系统解决方案，即为满足前面定义的安全保障要求，信息系统应提供哪些安全保障控制措施，以及应达到的信息系统安全保障级。因此信息系统概要规范应定义信息系统为满足安全保障要求而提供的方法和内容。

本条为 ISST 读者提供了确定安全保障技术、管理、工程控制措施的指南，与安全保障要求相比，安全保障控制措施应通过一种易于 ISST 读者理解的方式来编写。特别是：

a) 为满足安全保障需求，安全保障控制措施可以表述成强调信息系统实际操作的形式；

b) 安全保障控制措施可以组织成更密切反映信息系统文档内容的形式。除安全保障要求外，提供比安全保障要求更适于评估的控制措施，会提高信息系统评估的效率，使得 ISST 到安全控制措施表述(如信息系统设计文档)、ISST 到开发者的测试计划和规范的映射更容易。如果已知信息系统设计和实现的同一底层机制能满足几个安全保障要求，那么可以规定一项安全保障控制措施满足这一组安全保障要求，在组织文档时可采用这种方法。这样做可以在不损失严格性的情况下，减少开发者必须提供的对应性证据陈述量，并从中受益；

c) 包含信息系统特定术语可以使安全保障控制措施更容易与设计、用户或管理员手册建立联系。此外，还应包含通用术语(如主题、目的和管理员职责)的详细定义。

因此，信息系统概要规范应详细描述信息系统以表明其满足信息系统特定要求，但不必提供信息系统实现及其结构或设计原理的详细内容，也不需要详细介绍开发者是如何实施、测试安全保障控制措施。

如上所述，GB/T 20274.1—2006 要求 ISST 中的信息系统概要规范包含由信息系统提供的安全保障控制措施规范，信息系统的评估将以此为依据。但是，ISST 必须表明安全保障控制措施满足了所有的安全保障要求，而且每个安全保障控制措施至少映射到一个安全保障要求。

总之，在概要规范中，信息系统的安全保障控制措施至少应包括下列内容：

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安全目标的完整描述；

b) 信息系统安全技术保障：陈述应包含信息系统安全技术控制要求和安全技术能力级要求，并说明这些要求是如何满足信息系统安全目标的。该陈述将包括一个在安全技术控制和安全技术控制要求间的映射，清楚表示哪个安全技术控制满足哪个安全技术控制要求，并表明所有的要求都达到。每一个安全技术控制至少要满足一个安全技术控制要求；

c) 信息系统安全管理保障：陈述应包含信息系统安全管理控制要求和安全管理能力要求，并说明这些要求是如何满足信息系统安全目标的。该陈述将包括一个在安全管理控制和安全管理控制要求间的映射，清楚表示哪个安全管理控制满足哪个安全管理控制要求，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安全管理控制要求；

d) 信息系统安全工程保障：陈述应包含信息系统安全工程控制要求和安全工程能力要求，并说明这些要求是如何满足信息系统安全目标的。该陈述将包括一个在安全工程控制和安全工程控制要求间的映射，清楚表示哪个安全工程控制满足哪个安全工程控制要求，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安全工程控制要求。

12 ISPP 声明

12.1 概述

本章为如何构建 ISST 中声明的 ISPP 提供指导。GB/T 20274.1—2006 的 B.2.8 要求在 ISPP 的符合性声明中包含如下信息：

a) ISPP 引用；

b) ISPP 裁减；

c) ISPP 附加项。

注意，声明不能部分满足 ISPP，必须满足 ISPP 的所有要求。当然，对于一些 ISPP 安全目的和安全要求不在 ISST 评估范围之内的情况，必须在 ISST 符合性声明中表明信息系统和环境安全特征完全被信息系统或环境安全所涵盖，并在符合性说明中清楚的说明这种依赖关系。

如果没有 ISPP 符合性声明，在 ISST 的这节中就要明确声明这种影响。

12.2 ISPP 引用

ISPP 必须以某种方式进行标识，以使得 ISST 的读者在有疑问时能方便地查到 ISPP 的内容，建议使用包和 ISPP 的 ISO 注册索引形式，还要注意确保标识出特定版本和 ISPP 引用源。

12.3 ISPP 裁剪

如果 ISPP 在安全保障要求声明中包含额外许可的操作，需要在此处添加详细的替代部分。如果需要替代的要求，最好在 ISST 内重述完整的 ISPP 内容。

12.4 ISPP 附加项

如果 ISPP 开发者不满足 ISPP 的安全保障目的，需要增加附加的威胁、策略、目的，并在 ISST 符合性声明中覆盖这些附加项。

13 符合性声明

13.1 概述

本章为如何编写 ISPP 或 ISST 的符合性声明提供指导。符合性声明包括安全保障目的符合性声明和安全保障要求的符合性声明。

13.2 安全保障目的的符合性声明

本条为如何构建 ISPP 和 ISST 中的符合性声明提供指导。

ISPP 和 ISST 的安全保障目的符合性声明是为了说明信息系统在安全环境下提供了一套有效的安全措施。尤其是要说明信息系统安全保障要求适当的满足了安全保障目的，安全保障目的也适当的满足了信息系统安全环境(它定义了安全保障需求)的所有方面。

图 7 说明 ISPP 符合性声明的主要组成部分。

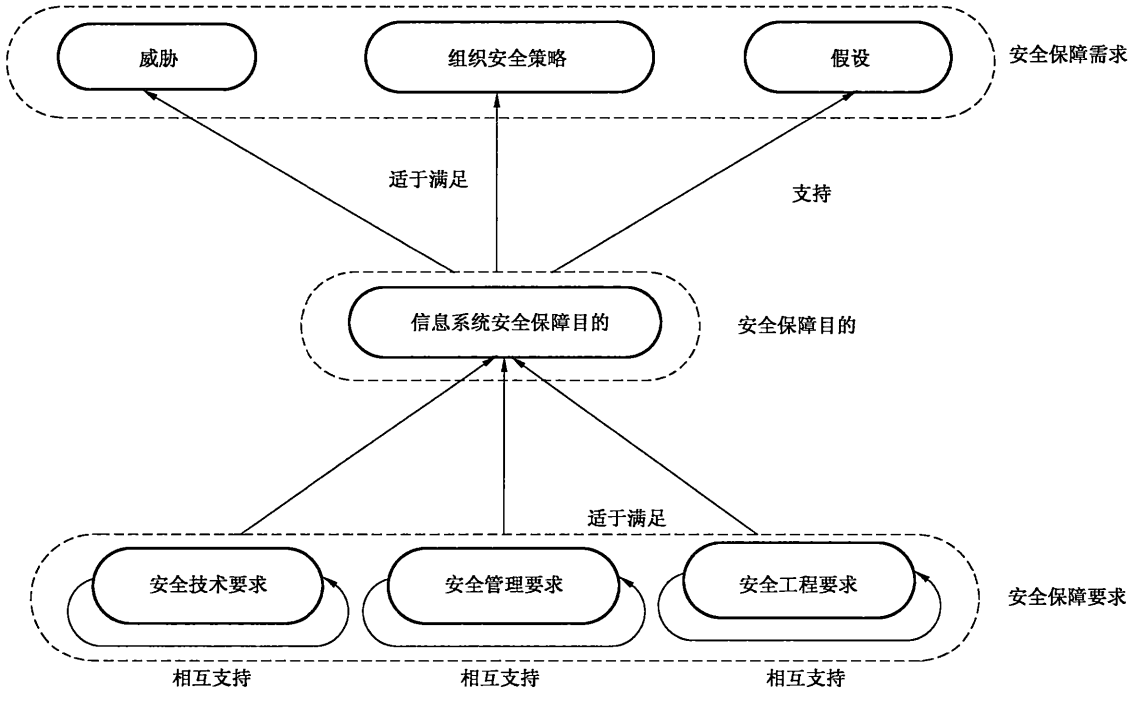

图 7 ISPP 的符合性声明

对于所有安全保障要求已完成的操作，应在安全保障要求部分进行标识，而不是作为 ISPP 符合性声明的一部分。这种方法的主要优点在于：避免在 ISPP 符合性声明中重复安全保障要求，从而减少了 ISPP 及其符合性声明之间存在不一致的可能。

图 8 说明了 ISST 符合性声明的主要部分。

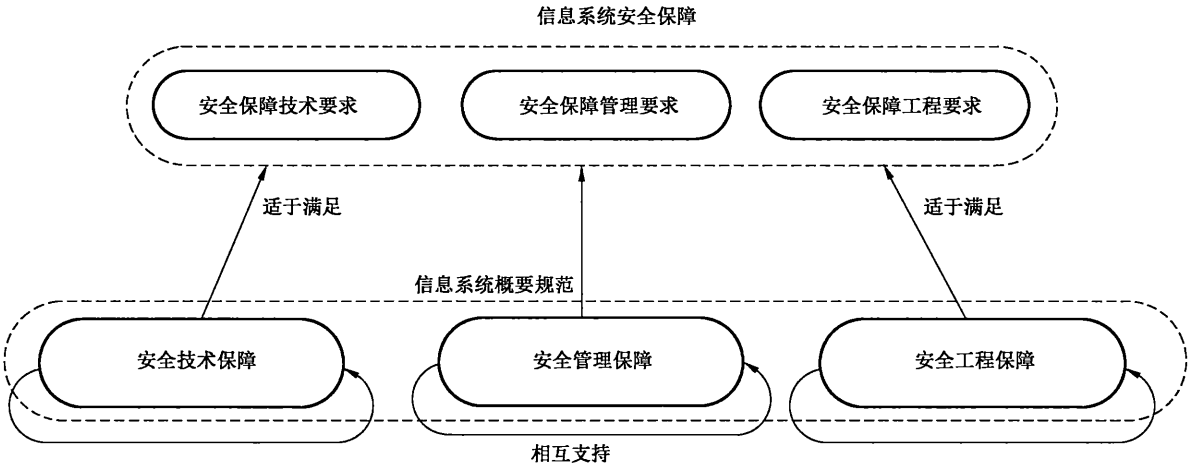

图 8　ISST 的符合性声明

此外，ISST 符合性声明必须表明所有和 ISPP 一致的声明都经过证明。

ISPP 和 ISST 的符合性声明用于表明已知的安全保障要求适于满足已知的安全保障目的，涵盖了 ISPP 和 ISST 的信息系统安全环境部分涉及的所有安全保障需求。它不仅显示安全保障目的与所关注的安全保障需求充分对应的，而且是必须的。建议采纳下面的方法：

首先，应有交叉引用的表格来将威胁、组织安全策略和假设与安全保障目的映射起来。从表格中，可以获取如下评估证据：

a）　每个安全保障目的至少映射到一项威胁、组织安全策略或假设；

b）　每一项威胁、组织安全策略和假设至少被一个安全保障目的所涵盖。

满足第一条就证明每一安全保障目的都是必须的（即不存在冗余的安全保障目的）。

其次，通过引用表格提供的非形式化的交叉引用关系信息来表明安全保障目的是充分满足安全保障需求的。这些论证应围绕信息系统安全保障目的展开。

a）　对每一项威胁，应提供充分的非形式化的论证来说明这些安全保障目的是如何有效的对抗威胁的，即安全保障目的表明在威胁说明中标识的事件可以是：

1）　被检测或恢复（从资产的有限破坏状态）；

2）　被阻止或降低危害（到可接受水平）。

b）　同样，对每一标识的组织安全策略或假设，应提供非形式化的论证说明标识出的安全保障目的是如何充分的与组织安全策略和假设对应的。

论证集中在信息系统的安全保障目的对应的威胁和组织安全策略。这些论证应该包括：

a）　讨论每一个安全保障目的的地位，这些被标识的安全保障目的用于对应威胁或组织安全策略；

b）　描述有多少个相关的环境安全保障目的支持信息系统要达到的安全保障目的。

本条只判定与安全环境对应的安全保障目的，不是对所有威胁进行评估，即使其中包含有与风险评估相似的陈述。应由各组织来定义哪些风险是可接受的，并在定义其安全策略时完成风险分析。基于一个好的评估基础上的 ISPP 或 ISST，用户可以选择其中的符合性声明作为组织的风险分析过程中论据的基础。

如果 ISST 中有 ISPP 符合性声明，那么 ISST 的符合性声明部分应简单说明与 ISPP 不一致的地方，如：

a）　所有补充的由安全保障目的应对的威胁；

b）　所有补充的由安全保障目的满足的组织安全策略；

c）　所有附加的安全保障目的及其如何处理相关威胁和（或）组织安全策略。

13.3 安全保障要求的符合性声明

13.3.1 安全保障要求的适当性

ISPP 的符合性声明用于展示信息系统安全保障要求满足其安全保障目的。对安全保障目的，要说明这些信息系统安全保障要求不仅是必须的而且是充分的。推荐采用下面的方法。

首先要提供安全保障目的与安全保障要求对应的交叉引用表。该表要提供如下信息：

a) 每一个安全保障要求至少对应一个安全保障目的；

b) 每一个安全保障目的也至少要对应一个安全保障要求。

前一条要充分说明每一个安全保障要求是必须的(即不存在冗余的安全保障要求)。

其次是通过交叉引用表中以非形式化的方式论证安全保障要求的充分性。这些非形式化的论证应围绕信息系统安全保障目的展开。对于每个安全保障目的，在显示的需求和导出的需求都满足的情况下，都应提供非形式化的论证证明安全保障要求是充分满足安全保障目的的。这些论证应涵盖 ISPP 中的所有安全保障要求，这些安全保障要求不仅直接满足安全保障需求，还起到支持作用。在讨论时，应考虑以下方面：

a) 为什么以及如何应用 GB/T 20274.2—2008、GB/T 20274.3—2008、GB/T 20274.4—2008 中的操作；

b) 信息系统安全保障要求如何与环境安全保障要求相适应。

如果 ISST 有 ISPP 符合性声明，在 ISST 的符合性声明部分要简要说明与 ISPP 不同的地方：

a) 所有附加的安全保障目的如何与安全保障要求相对应；

b) 所有附加的安全保障要求如何与安全保障目的相对应。

13.3.2 安全保障要求的相互支持

13.3.2.1 概要

在 ISPP 符合性声明中，本节通过展示安全保障要求的相互支持及其具有的完备、有效和整体性来说明安全保障控制措施是完整的、内部一致的。建议采纳如下方法：

a) 提供安全保障要求之间内部一致性的说明；

b) 表明支持性安全保障要求已包括在内，这些安全保障要求适合于保护其他安全保障要求免受诸如旁路或篡改之类的攻击。

分析方式应与安全保障要求是相互支持的分析方式一样。因为安全保障要求的相互支持性已经在安全保障要求中说明了，这部分的分析应关注安全保障要求之外引入的额外细节部分所产生的影响。对任何由额外细节部分引入的安全保障控制措施之间的相互支持或关联的实例都要进行分析。然而，由于信息系统概要规范是从信息系统的角度对安全保障要求的再次解释，因此，对安全保障要求分析结果的复用应说明结果的不同视角来源。

13.3.2.2 组件依赖性分析

不管组件依赖性分析使用什么表达方式，都应具有如下的能力：

a) 能够展示安全保障要求组件在相应级别的依赖性是如何得到满足；

b) 能够标识出所有未满足的依赖，并解释不需要满足的原因。

信息系统也可能不需要去满足某个依赖关系，原因是它可能与信息系统无关或没必要由安全保障目的来陈述，依赖关系可能是由环境的手段来满足。

如上所述，表示依赖关系的一种方法是构建一张对应表，例如：

a) 用一行表示包含在 ISPP 中的一个组件，多行表示该组件出现多次；

b) 每个识别出的组件和在 GB/T 20274.2—2008、GB/T 20274.3—2008、GB/T 20274.4—2008 中定义的其他依赖组件都要列出；

c) 对于每个识别出的依赖关系，给出满足依赖关系的行号，或说明不需满足依赖关系的理由。

组件依赖性分析也应能证明安全保障要求是相互支持的。换言之，如果组件 A 依赖于组件 B，那么，就可以说 B 是 A 的支持。

如果 ISST 声明与某个 ISPP 保持一致，那么这部分只需要反映出与该 ISPP 的不同之处，即表明所有补充的安全保障要求是满足依赖关系的。

13.3.2.3 内部一致性

作为证明相互支持的第二个方面，在所有组件间的依赖关系都已满足的情况下，必须提供安全保障要求内部一致性的证据。在满足安全保障要求方面，应针对不同安全保障要求应用于同一类型的事件、操作或数据的不同场合，分别考虑其内部一致性。例如，ISPP 不仅包括用户匿名要求，还包括用户单独可审计性要求，那么就必须证明这些要求之间是不冲突的，也就是说不需要产生那些操作与用户账户相关联的匿名用户的审计事件。

如果 ISST 声明与某个 ISPP 保持一致，那么 ISST 的符合性声明部分只要反映与 ISPP 不同之处，并展示附加部分的安全保障要求是一致的，包括：

a) 被其他安全保障要求支持；

b) 提供对其他安全保障要求的支持；

c) 与其他安全保障要求是一致的。

13.3.3 ISST 与 ISPP 的一致性

在 ISST 符合性声明中，需确认 ISST 与 ISPP 是一致的，并表明在 ISST 中：

a) 包括了 ISPP 的所有安全保障目的，且这些目的的任何细化操作都是有效的；

b) 包括了 ISPP 的所有安全保障要求，且这些要求的任何细化操作或其他操作都是有效的；

c) 所有安全保障要求没有与 ISPP 中的安全保障要求发生冲突。

如果 ISST 精确地包括了 ISPP 安全保障目的和安全保障要求，就不需要进行 ISST 与 ISPP 的一致性分析。只有在 ISST 包括附加细节时，该分析才会有意义。当 ISPP 安全保障目的和安全保障要求中有附加的细节时，必须说明这些内容与 ISPP 中的任何内容不冲突。

另外，ISPP 安全保障要求中的未完成的操作如赋值、选择操作都应由 ISST 的作者去完成，必须在 ISST 中证明完成了所有 ISPP 未完成的操作。

13.3.4 安全保障控制措施满足安全保障要求

在 ISST 符合性声明中，这部分用来确定安全保障控制措施适当地满足 ISST 中包括的所有安全保障要求。建议采用表格的方式，将安全保障控制措施映射到安全保障要求上。表格应该是这样的：

a) 每个安全保障要求至少映射到一个安全保障控制措施；

b) 每个安全保障控制措施至少映射到一个安全保障要求。

除此之外，必须对特殊的安全保障要求是如何被满足的给出必要的解释。例如，当多个安全保障控制措施映射到一个安全保障要求时候，应作出适当的解释。

附 录 A
（资料性附录）
从 GB/T 20274.2—2008 选取 STRs

本附录的表格提供了信息系统安全技术要求从 GB/T 20274.2—2008 中定义的安全技术要求(STR)组件中选取。一些组件可能仅仅覆盖了范例的一个方面，因此，在表中也对应了多个组件。

表 A.1～表 A.11 用于帮助识别和确定适当的 STR 组件。ISST 或 ISPP 作者要选取和使用这些组件表达安全保障模式的各方面和允许的操作。同时，对于体系架构要求，表 A.1～表 A.11 提供了架构问题的列表，用于指导 GB/T 20274.2—2008 中相关问题 STR 组件的选择。

表 A.1 安全审计相关 STR

信息系统安全技术要求	STR 组件
安全审计自动应答	FAU_ARP.1
安全审计数据产生	FAU_GEN.1，FAU_GEN.2
安全审计分析	FAU_SAA.1，FAU_SAA.2，FAU_SAA.3，FAU_SAA.4
安全审计查阅	FAU_SAR.1，FAU_SAR.2，FAU_SAR.3
安全审计事件选择	FAU_SEL.1
安全审计事件存储	FAU_STG.1，FAU_STG.2，FAU_STG.3，FAU_STG.4

表 A.2 通信相关 STR

信息系统安全技术要求	STR 组件
原发抗抵赖	FCO_NRO.1，FCO_NRO.2
接收抗抵赖	FCO_NRR.1，FCO_NRR.2

表 A.3 密码支持相关 STR

信息系统安全技术要求	STR 组件
密钥管理	FCS_CKM.1，FCS_CKM.2，FCS_CKM.3，FCS_CKM.4
密码运算	FCS_COP.1

表 A.4 用户数据保护相关 STR

信息系统安全技术要求	STR 组件
访问控制策略	FDP_ACC.1，FDP_ACC.2
访问控制功能	FDP_ACF.1
数据鉴别	FDP_DAU.1，FDP_DAU.2
输出到 TSF 控制之外	FDP_ETC.1，FDP_ETC.2
信息流控制策略	FDP_IFC.1，FDP_IFC.2

表 A.4（续）

信息系统安全技术要求	STR 组件
信息流控制功能	FDP_IFF.1,FDP_IFF.2,FDP_IFF.3,FDP_IFF.4,FDP_IFF.5,FDP_IFF.6
从 TSF 控制之外输入	FDP_ITC.1,FDP_ITC.2
信息系统内部传输	FDP_ITT.1,FDP_ITT.2,FDP_ITT.3,FDP_ITT.4
残余信息保护	FDP_RIP.1,FDP_RIP.2
反转	FDP_ROL.1,FDP_ROL.2
存储数据的完整性	FDP_SDI.1,FDP_SDI.2
TSF 间用户数据传输的保密性保护	FDP_UCT.1
TSF 间用户数据传输的完整性保护	FDP_UIT.1,FDP_ UIT.2,FDP_ UIT.3

表 A.5　标识和鉴别相关 STR

信息系统安全技术要求	STR 组件
鉴别失败	FIA_AFL.1
用户属性定义	FIA_ATD.1
秘密的规范	FIA_SOS.1,FIA_SOS.2
用户鉴别	FIA_UAU.1,FIA_UAU.2,FIA_UAU.3,FIA_UAU.4,FIA_UAU.5,FIA_UAU.6,FIA_UAU.7
用户标识	FIA_UID.1,FIA_UID.2
用户-主体绑定	FIA_USB.1

表 A.6　安全管理相关 STR

信息系统安全技术要求	STR 组件
TSF 中功能的管理	FMT_MOF.1
安全属性的管理	FMT_MSA.1,FMT_MSA.2,FMT_MSA.3
TSF 数据管理	FMT_MTD.1,FMT_MTD.2,FMT_MTD.3
撤消	FMT_REV.1
安全属性到期	FMT_SAE.1
安全管理角色	FMT_SMR.1,FMT_SMR.2,FMT_SMR.3

表 A.7　隐秘相关 STR

信息系统安全技术要求	STR 组件
匿名	FPR_ANO.1,FPR_ANO.2
假名	FPR_PSE.1,FPR_PSE.2,FPR_PSE.3
不可关联性	FPR_UNL.1
不可观察性	FPR_UNO.1,FPR_UNO.2,FPR_UNO.3,FPR_UNO.4

表 A.8　TSF 保护相关 STR

信息系统安全技术要求	STR 组件
根本抽象机测试	FPT_AIM.1
失败保护	FPT_FLS.1
输出 TSF 数据的可用性	FPT_ITA.1
输出 TSF 数据的保密性	FPT_ITC.1
输出 TSF 数据的完整性	FPT_ITI.1,FPT_ITI.2
信息系统内 TSF 数据的传输	FPT_ITT.1,FPT_ITT.2,FPT_ITT.3
TSF 物理保护	FPT_PHP.1,FPT_PHP.2,FPT_PHP.3
可信恢复	FPT_RCV.1,FPT_ RCV.2,FPT_ RCV.3,FPT_ RCV.4
重放检测	FPT_RPL.1
参照仲裁	FPT_RVM.1
域分离	FPT_SEP.1,FPT_SEP.2,FPT_SEP.3
状态同步协议	FPT_SSP.1,FPT_SSP.2
时间戳	FPT_STM.1
TSF 间 TSF 数据的一致性	FPT_TDC.1
信息系统内 TSF 数据复制的一致性	FPT_TRC.1
TSF 自检	FPT_TST.1

表 A.9　资源利用相关 STR

信息系统安全技术要求	STR 组件
容错	FRU_FLT.1,FRU_FLT.2
服务优先级	FRU_PRS.1,FRU_PRS.2
资源分配	FRU_RSA.1,FRU_RSA.2

表 A.10　信息系统访问相关 STR

信息系统安全技术要求	STR 组件
可选属性范围限定	FTA_LSA.1
多重并发会话限定	FTA_MCS.1,FTA_MCS.2
会话锁定	FTA_SSL.1,FTA_SSL.2,FTA_SSL.3
信息系统访问旗标	FTA_TAB.1
信息系统访问历史	FTA_TAH.1
信息系统会话建立	FTA_TSE.1

表 A.11　可信路径/信道相关 STR

信息系统安全技术要求	STR 组件
TSF 间可信信道	FTP_ITC.1
可信路径	FTP_TRP.1

附 录 B
（资料性附录）
从 GB/T 20274.3—2008 选取 SMRs

本附录的表格提供了信息系统安全管理要求从 GB/T 20274.3—2008 中定义的安全管理要求(SMR)组件中选取。一些组件可能仅仅覆盖了范例的一个方面，因此，在表中也对应了不止一个组件。

表 B.1～表 B.12 用于帮助识别和确定适当的 SMR 组件。ISST 或 ISPP 作者要选取和使用这些组件表达安全保障模式的各方面和允许的操作。同时，对于体系架构要求，表 B.1～表 B.12 提供了架构问题的列表，用于指导 GB/T 20274.3—2008 中相关问题 SMR 组件的选择。

表 B.1 风险管理相关 SMR

信息系统安全管理要求	SMR 组件
对象确立	MRM_TEM.1，MRM_TEM.2，MRM_TEM.3
风险评估	MRM_RAM.1，MRM_RAM.2，MRM_ RAM.3
风险控制	MRM_RCT.1，MRM_RCT.2，MRM_RCT.3
沟通与监控	MRM_CAM.1，MRM_CAM.2

表 B.2 信息安全策略相关 SMR

信息系统安全管理要求	SMR 组件
信息安全策略	MSP_SPL.1，MSP_SPL.2，MSP_SPL.3，MSP_SPL.4

表 B.3 信息安全组织机构 SMR

信息系统安全管理要求	SMR 组件
信息安全的管理支持	MSO_IOA.1
信息安全组织架构	MSO_ORG.1
信息安全职责	MSO_RES.1，MSO_RES.2，MSO_RES.3
沟通协作	MSO_CAC.1，MSO_CAC.2

表 B.4 人员安全相关 SMR

信息系统安全管理要求	SMR 组件
人员审查	MPS_PEC.1，MPS_PEC.2，MPS_PEC.3
安全意识和培训	MPS_SAT.1，MPS_SAT.2
考核和奖惩	MPS_CRP.1
人事变更	MPS_PCM.1，MPS_PCM.2

表 B.5　资产管理相关 SMR

信息系统安全管理要求	SMR 组件
资产登记管理	MAM_ARM.1
资产管理职责	MAM_AMR.1,MAM_AMR.2
资产分类管理	MAM_ACM.1,MAM_ACM.2

表 B.6　物理和环境安全相关 SMR

信息系统安全管理要求	SMR 组件
物理安全区域管理	MPE_PSA.1,MPE_PSA.2,MPE_PSA.3,MPE_PSA.4,MPE_PSA.5,MPE_PSA.6
支撑基础设施安全	MPE_SIS.1,MPE_SIS.2,MPE_SIS.3, MPE_SIS.4
设备安全	MPE_EMS.1,MPE_EMS.2,MPE_EMS.3

表 B.7　符合性管理相关 SMR

信息系统安全管理要求	SMR 组件
法律法规和政策符合性	MCM_LCP.1,MCM_LCP.2,MCM_LCP.3
标准符合性	MCM_STP.1,MCM_STP.2
安全策略符合性	MCM_PSP.1, MCM_PSP.2

表 B.8　信息安全规划管理相关 SMR

信息系统安全管理要求	SMR 组件
信息安全规划	MSP_ISP.1,MSP_ISP.2,MSP_ISP.3
投资和预算	MSP_IAB.1,MSP_IAB.2

表 B.9　系统开发管理相关 SMR

信息系统安全管理要求	SMR 组件
安全需求管理	MSD_SRM.1
系统设计管理	MSD_SDM.1
工程实施管理	MSD_ENM.1,MSD_ENM.2
交付管理	MSD_IRM.1,MSD_IRM.2

表 B.10　运行管理相关 SMR

信息系统安全管理要求	SMR 组件
系统漏洞管理	MOP_TVM.1，MOP_TVM.2，MOP_TVM.3，MOP_TVM.4
逻辑访问控制管理	MOP_LAC.1，MOP_LAC.2，MOP_LAC.3，MOP_LAC.4，MOP_LAC.5，MOP_LAC.6
审计和监控管理	MOP_AMM.1，MOP_AMM.2，MOP_AMM.3，MOP_AMM.4
安全配置管理	MOP_NSM.1，MOP_ NSM.2，MOP_ NSM.3，MOP_ NSM.4
系统变更管理	MOP_SCM.1
运行管理	MOP_ITM.1，MOP_ITM.2，MOP_ITM.3，MOP_ITM.4，MOP_ITM.5，MOP_ITM.6，MOP_ITM.7，MOP_ITM.8
信息传输安全	MOP_IEX.1，MOP_IEX.2，MOP_IEX.3

表 B.11　业务持续性和灾难恢复管理相关 SMR

信息系统安全管理要求	SMR 组件
业务持续性管理	MBD_BCM.1，MBD_BCM.2，MBD_BCM.3，MBD_BCM.4，MBD_BCM.5，MBD_BCM.6

表 B.12　应急响应管理相关 SMR

信息系统安全管理要求	SMR 组件
汇报安全事件和安全漏洞	MER_REW.1，MER_REW.2
应急响应管理	MER_IMI.1，MER_IMI.2，MER_IMI.3

附 录 C
（资料性附录）
从 GB/T 20274.4—2008 选取 SERs

本附录的表格提供了信息系统安全工程要求与 GB/T 20274.4—2008 中定义的安全工程要求(SER)组件中选取。一些组件可能仅仅覆盖了范例的一个方面，因此，在表中也对应了不止一个组件。

表 C.1～表 C.3 用于帮助识别和确定适当的 SER 组件。ISST 或 ISPP 要选取和使用这些组件表达安全保障模式的各方面和允许的操作。同时，对于体系架构要求，表 C.1～表 C.3 提供了架构问题的列表，用于指导 GB/T 20274.4—2008 中相关问题 SER 组件的选择。

表 C.1 风险过程相关 SER

信息系统安全工程要求	SER 组件
系统定义	PRM_SDF.1
评估威胁	PRM_ATT.1，PRM_ATT.2，PRM_ATT.3，PRM_ATT.4，PRM_ATT.5，PRM_ATT.6
评估脆弱性	PRM_AVL.1，PRM_AVL.2，PRM_AVL.3，PRM_AVL.4，PRM_AVL.5
评估影响	PRM_AIM.1，PRM_AIM.2，PRM_AIM.3，PRM_AIM.4，PRM_AIM.5，PRM_AIM.6
评估安全风险	PRM_ASR.1，PRM_ ASR.2，PRM_ ASR.3，PRM_ ASR.4，PRM_ ASR.5，PRM_ ASR.6

表 C.2 工程过程相关 SER

信息系统安全工程要求	SER 组件
确定安全要求	PEN_ISR.1，PRM_ ISR.2，PRM_ ISR.3，PEN_ISR.4，PRM_ ISR.5，PRM_ ISR.6，PEN_ISR.7
高层安全设计	PEN_HSD.1，PEN_HSD.2
详细安全设计	PEN_DSD.1，PEN_DSD.2，PEN_DSD.3，PEN_DSD.4
安全工程实施	PEN_SEE.1，PEN_ SEE.2，PEN_ SEE.3，PEN_SEE.4，PEN_ SEE.5，PEN_ SEE.6
提供安全输入	PEN_PSI.1，PEN_PSI.2，PEN_PSI.3，PEN_PSI.4，PEN_PSI.5，PEN_PSI.6
监视安全态势	PEN_MSP.1，PEN_ MSP.2，PEN_ MSP.3，PEN_ MSP.4，PEN_ MSP.5，PEN_ MSP.6，PEN_ MSP.7
管理安全控制	PEN_MSC.1，PEN_MSC.2，PEN_MSC.3，PEN_MSC.4
协调安全	PEN_COS.1，PEN_ COS.2，PEN_ COS.3，PEN_ COS.4

表 C.3 保障过程相关 SER

信息系统安全工程要求	SER 组件
验证和确认安全	PAS_VVS.1，PAS_VVS.2，PAS_VVS.3 ，PAS_VVS.4，PAS_VVS.5
建立保证证据	PAS_EAE.1，PAS_ EAE.2，PAS_ EAE.3，PAS_ EAE.4，PAS_ EAE.5

参 考 文 献

[1] GB/Z 20283—2006 信息安全技术 保护轮廓和安全目标产生指南

[2] ISO/IEC 15292 Protection profile registration procedures

[3] ISO/IEC 13335 Information technology—Security techniques—Management of information and communications technology security

[4] ISO/IEC 14516 Information technology—Security techniques—Guidelines on the use and management of Trusted Third Parties services

中 华 人 民 共 和 国
国家标准化指导性技术文件
信息安全技术
信息系统保护轮廓和信息系统安全目标
产生指南
GB/Z 30286—2013
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)64275323 发行中心:(010)51780235
读者服务部:(010)68523946
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 2.75 字数 74 千字
2014年5月第一版 2014年5月第一次印刷
*
书号:155066·1-49173 定价 39.00元

GB/Z 30286-2013