ICS 35.040
L 80

中华人民共和国国家标准

GB/T 19715.1—2005/ISO/IEC TR 13335-1:1996

信息技术　信息技术安全管理指南 第1部分:信息技术安全概念和模型

Information technology—Guidelines for the management of IT security—Part 1:Concepts and models of IT security

(ISO/IEC TR 13335-1:1996,IDT)

2005-04-19 发布　　2005-10-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

前　言

GB/T 19715《信息技术　信息技术安全管理指南》分为五个部分：

——第1部分：信息技术安全概念和模型；

——第2部分：管理和规划信息技术安全；

——第3部分：信息技术安全管理技术；

——第4部分：防护措施的选择；

——第5部分：外部连接的防护措施。

本部分等同采用国际标准ISO/IEC TR 13335-1:1996《信息技术　信息技术安全管理指南　第1部分：信息技术安全概念和模型》。

本部分提出基本的管理概念和模型，将这些概念和模型引入信息技术安全管理是必要的。

本部分由中华人民共和国信息产业部提出。

本部分由全国信息安全标准化技术委员会归口。

本部分由中国电子技术标准化研究所(CESI)、中国电子科技集团第十五研究所、中国电子科技集团第三十研究所、上海三零卫士信息安全有限公司负责起草。

本部分主要起草人：安金海、林中、林望重、魏忠、罗锋盈、陈星。

引　言

GB/T 19715 的目的是提供关于 IT 安全管理方面的指南，而不是解决方案。那些在组织内负责 IT 安全的个人应该可以采用本标准中的资料来满足他们特定的需求。本标准的主要目标是：

a) 定义和描述与 IT 安全管理相关的概念；

b) 标识 IT 安全管理和一般的 IT 管理之间的关系；

c) 提出了几个可用来解释 IT 安全的模型；

d) 提供了关于 IT 安全管理的一般的指南。

GB/T 19715 由多个部分组成。本部分为第 1 部分，提供了描述 IT 安全管理用的基本概念和模型的概述。本部分适用于负责 IT 安全的管理者，及那些负责组织的总体安全大纲的管理者。

第 2 部分描述了管理和规划方面。它和负责组织的 IT 系统的管理者相关。他们可以是：

a) 负责监督 IT 系统的设计、实施、测试、采购或运行的 IT 管理者；

b) 负责制定 IT 系统的实际使用活动的管理者。

第 3 部分描述了在一个项目的生存周期(比如规划、设计、实施、测试、采办或运行)所涉及的管理活动中适于使用的安全技术。

第 4 部分提供了选择防护措施的指南，以及通过基线模型和控制的使用如何受到支持。它也描述了它如何补充了第 3 部分中描述的安全技术，如何使用附加的评估方法来选择防护措施。

第 5 部分为组织提供了将它的 IT 系统连接到外部网络的指南。该指南包含了提供连接安全的防护措施的选择、使用，那些连接所支持的服务，以及进行连接的 IT 系统的附加防护措施。

信息技术　信息技术安全管理指南
第1部分:信息技术安全概念和模型

1　范围

GB/T 19715包含IT安全管理的指南。本部分提出了基本的管理概念和模型,将这些概念和模型引入IT安全管理是必要的。在指南的其余部分还将进一步讨论和开发这些概念和模型以提供更详细的指南。为有助于标识和管理IT安全的各个方面可以同时使用本标准的各部分。本部分对全面理解本标准的后续各部分是必需的。

2　规范性引用文件

下列文件中的条款通过GB/T 19715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)

3　术语和定义

下列术语和定义适用于GB/T 19715的各个部分。

3.1

可核查性　accountability

确保可将一个实体的行动唯一地追踪到此实体的特性[GB/T 9387.2—1995]。

3.2

资产　asset

对组织具有价值的任何东西。

3.3

真实性　authenticity

确保主体或资源的身份是所声称身份的特性。真实性适用于诸如用户、过程、系统和信息这样的实体。

3.4

可用性　availability

已授权实体一旦需要就可访问和使用的特性[GB/T 9387.2—1995]。

3.5

基线控制　baseline controls

为一个系统或组织建立的防护措施的最小集合。

3.6

保密性　confidentiality

使信息不泄露给未授权的个人、实体、过程或不使信息为其利用的特性。

3.7

数据完整性 data integrity

数据未经未授权方式修改或破坏的特性[GB/T 9387.2—1995]。

3.8

影响 impact

不希望事故的后果。

3.9

完整性 integrity

见数据完整性和系统完整性。

3.10

IT 安全 IT security

与定义、获得和维护保密性、完整性、可用性、可核查性、真实性和可靠性有关的各个方面。

3.11

IT 安全策略 IT security policy

支持如何在一个组织或其 IT 系统中管理、保护和分布资产(包括敏感信息)的规则、指令和习惯做法。

3.12

可靠性 reliability

与预期行为和结果相一致的特性。

3.13

残留风险 residual risk

在已实现防护措施之后仍然存在的风险。

3.14

风险 risk

某种威胁会利用资产或若干资产的脆弱性使这些资产损失或破坏的可能性。

3.15

风险分析 risk analysis

标识安全风险、确定其大小和标识需要防护措施的区域的过程。

3.16

风险管理 risk management

标识、控制和消除可能影响 IT 系统资源的不确定事件或使这些事件降至最少的全部过程。

3.17

防护措施 safeguard

降低风险的习惯做法、规程或机制。

3.18

系统完整性 system integrity

系统以不受损害的方式执行其预定功能,避免对系统故意的或意外的未授权操纵的特性。

3.19

威胁 threat

可能导致对系统或组织危害的不希望事故潜在起因。

3.20

脆弱性 vulnerability

包括可能会被威胁所利用的资产或若干资产的弱点。

4 结构

本部分结构如下:第5章概述本部分的目的;第6章提供IT安全管理要求的背景信息;第7章提出IT安全概念和模型的综述;第8章研究IT安全的要素;第9章讨论IT安全管理所使用的过程;第10章提供出对若干模型的一般讨论,这些模型对理解本部分提出的概念是有用的;最后,在第11章中对整个第1部分予以小结。

5 目的

GB/T 19715是为各种读者编写的。本部分的目的是要描述IT安全管理范围内的各种专题,并简略介绍基本IT安全概念模型。为提供高层管理综述,本资料力求简洁。本部分适用于组织内负责安全的资深管理者,且为对GB/T 19715其余部分感兴趣的人员提供IT安全简介。第2部分和第3部分为直接负责IT安全实现和监督的个人提供适宜的更为广泛的信息和资料。这是以本部分中提出的概念和模型为基础的。

GB/T 19715并不打算建议一种具体的IT安全管理方法。而是,本部分首先对有用的概念和模型进行一般讨论,最后讨论IT安全管理有效的专门技术和工具。本资料是通用的并适用于许多不同管理风格的管理和组织环境。本部分以允许剪裁本资料的方式编排,以满足一个组织及其特定的管理风格的需要。

6 背景

为进行业务活动,政府和商业组织极其依赖信息的使用。信息和服务的保密性、完整性、可用性、可核查性、真实性和可靠性的损失会给组织带来负面影响。因此,在组织中对保护信息和管理信息技术(IT)的安全有着重要的需求。在现今环境中,保护信息的这一要求尤为重要,因为许多组织通过IT系统的网络进行内部和外部的连接。

IT安全管理是用来实现和维护保密性、完整性、可用性、可核查性、真实性和可靠性相应等级的过程。IT安全管理功能包括:

a) 确定组织IT安全目标、战略和策略;
b) 确定组织IT安全要求;
c) 标识和分析对组织内IT资产的安全威胁;
d) 标识和分析风险;
e) 规定合适的防护措施;
f) 监督防护措施的实现和运作,使费用花在有效保护组织内的信息和服务所必需的防护措施上;
g) 制订和实施安全意识大纲;
h) 对事故的检测和反应。

为了履行IT系统的这些管理职责,安全必须是组织的整个管理计划不可分的组成部分。因此,本部分所提出的若干安全专题有广泛的管理内涵。本部分将不关注广泛的管理问题,而是这些专题的安全方面以及它们与管理的关系如何。

7 IT安全管理概念

采用下列概念需要考虑到组织运行的文化和环境,因为这些因素对实现安全的整个方法会有重要的影响。此外,它们对负责保护组织中特定部分的部门或人会有影响。在某些情况下,认为由政府负责,并通过颁布和执行法律履行此职责。在另一些情况下,而是认为由拥有者或管理者负责。这些问题对所采用的方法有相当大的影响。

7.1 方法

系统方法对标识组织中IT安全要求是必需的。这也是实现IT安全及其业务管理部门的实际情况。此过程称之为IT安全管理并包括如下活动：

a) 制订IT安全策略；
b) 标识在组织中的角色和职责；
c) 风险管理，包括下列内容的标识和评估：
   1) 受保护的资产；
   2) 威胁；
   3) 脆弱性；
   4) 影响；
   5) 风险；
   6) 防护措施；
   7) 残留风险；
   8) 约束。
d) 配置管理；
e) 变更管理；
f) 应急计划和灾难恢复计划；
g) 防护措施的选择和实施；
h) 安全意识；
i) 直至，包括：
   1) 维护；
   2) 安全审核；
   3) 监督；
   4) 评审；
   5) 事故处理。

7.2 目标、战略和策略

需形成总体安全目标、战略和策略(见图1)以作为组织有效IT安全的基础。它们支持组织的业务并保证各种防护措施之间的相容性。目标标识出应实现什么，战略标识出如何实现这些目标，而策略标识出需要做什么。

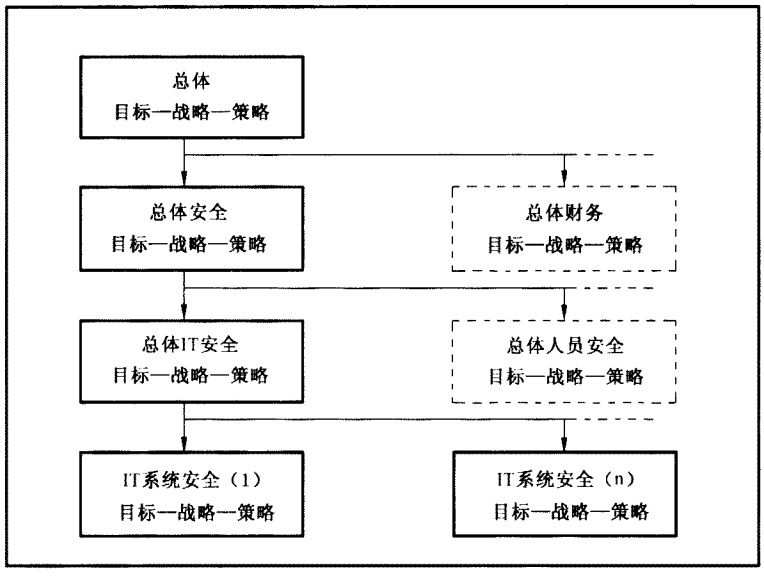

图1 目标，战略和策略层次结构

可从组织的最高层到运行层分层制订目标、战略和策略。它们要反映组织的要求并考虑组织的任何约束，它们要保证在每一层，直至所有层保持相容性。安全是组织中各管理层的职责并在系统生存周期各个阶段予以重视。应根据定期安全评审(例如，风险分析、安全审核)的结果维护和更新目标、战略和策略，并对业务目标进行更改。

总体安全策略基本上由看作整体的组织安全原则和指令组成。总体安全策略必须反映更广的共同策略，包括致力个人权利、法律要求和标准的策略。

总体IT安全策略必须反映适用于总体安全策略和组织中普遍使用的IT系统的基本安全原则和方针。

IT系统安全策略必须反映总体IT安全策略中所包含的安全原则和指令。它还应包含详细的具体安全要求、要实现的防护措施以及如何正确使用它们以保证充分的安全。在各种情况中，重要的是所采用的方法对组织的业务需求而言必须是有效的。

IT系统安全目标、战略和策略，就安全而言，是对IT系统的要求。通常使用自然语言表示它们，但有可能要求使用某种机器语言的更为正式的方法表示它们。它们应给出IT安全事项，例如：

a) 保密性；

b) 完整性；

c) 可用性；

d) 可核查性；

e) 真实性；

f) 可靠性。

目标、战略和策略要规定组织的安全等级、接受风险的限值和组织的应急要求。

8 安全要素

下列各条从高层描述了在安全管理过程中所涉及的重要要素。将介绍每个要素和所标识的重要影响因素。这些要素的更详细描述和讨论以及它们的关系包含在本标准的其他部分。

8.1 资产

妥善管理资产是组织成功不可或缺的因素，也是所有管理层的重要职责。组织的资产包括：

a) 物理资产(例如，计算机硬件，通信设施，建筑物)；

b) 信息/数据(例如，文档，数据库)；

c) 软件；

d) 生产某种产品或提供服务的能力；

e) 人员；

f) 无形资产(例如，信誉、形象)。

对大部分或全部资产保证有某种程度的保护是值得的。即使这些资产未受保护，对要被接受的风险进行评估亦是必要的。

从安全观点来看，如果组织的资产未予以标识，则不可能实现和维护成功的安全大纲。在许多情况中，标识资产和确定价值的过程可在最高层完成并可以不要求费用高、详细和费时的分析。这种分析的详细程度必须根据时间和成本与资产价值加以衡量。不管在什么情况下，详细规程要根据安全目标加以确定。在许多情况，将资产分组是有帮助的。

待考虑的资产特性包括其价值和/或敏感度，以及特有的防护措施。资产的保护要求受到存在特定威胁时其脆弱性影响。如果资产的拥有者明白这些方面，则应在此阶段予以专门的关注。组织运行的环境和文化影响资产及其特性。例如，某些文化认为保护个人信息是非常重要的，而另一些文化则不太注意这个问题。这些环境和文化差异对国际组织和垮境使用IT系统可能要特别重视。

8.2 威胁

资产可能经受多种威胁。威胁可能引起不希望事故，导致系统或组织及其资产的损害。这种损害可能由对 IT 系统处理的信息或服务的直接或间接攻击产生，例如，信息未经批准的销毁、泄露、修改、损坏和不可用或丢弃。威胁要利用资产存在的脆弱性才能成功地使资产受到损害。威胁可能源于自然或人为因素，可能是意外的或故意的。要标识意外和故意的威胁，要评估其程度和可能性。

威胁的例子有：

人为的		环境的
故意的	意外的	
窃听	疏忽和差错	地震
信息修改	文件删除	雷击
系统被黑客攻击	不正确的路由选择	水灾
恶意代码	物理事故	火灾
盗窃		

可以利用有关多种环境威胁的统计数据。在威胁评估过程期间，组织应获得并使用这些数据。威胁可以影响一个组织的特殊部分，例如，破坏个人计算机。有些威胁对系统或组织所处的特定位置的周围环境造成普遍的影响，例如，飓风或雷电对建筑物的破坏。威胁可能来自组织内部（例如员工的破坏活动）或外部（例如，恶意的黑客或工业间谍）。不希望事故引起的损害可能是暂时性的或是永久性的（如资产毁坏的情况）。

当威胁每次出现时，由此造成的损害程度可能很不相同。例如：

a) 软件病毒可能引起不同的损害程度，视其机能而定；

b) 某个特定地区的地震每次发生时可能有不同的强度。

这些威胁经常用与它们有关的严重程度描述。例如：

a) 病毒可以描述成破坏性的或非破坏性的；

b) 地震强度可用里氏等级来描述。

某些威胁可能影响一个以上的资产。在此情况时，它们可引起不同的影响，这视受影响的资产而定。例如，个人计算机上的软件病毒只具有限的或局部的影响。然而，在一个基于网络的文件服务器上的相同软件病毒可能具有广泛的影响。不同的威胁或不同地方的相同威胁，它们引起的损害程度可能是一致的。如果这种威胁引起的损害是一致的，则可以采取共同的方法。如果，损害很不相同，则应对此种威胁的每次出现采用更为专门的方法方才合适。

威胁具有一些特征，这些特征中可以提供有关威胁自身的有用信息。这种信息的例子有：

a) 来源，即内部人员和外部人员；

b) 动机，例如财务赢利，竞争利益；

c) 出现频次；

d) 威胁严重程度。

组织所处于的环境和文化对如何处理对组织的威胁具有重要意义和影响。在极个别情况下，有些威胁在某些文化下不认为有害。当讨论威胁时必须考虑环境和文化的方方面面。

8.3 脆弱性

与资产相关的脆弱性包括物理布局、组织、规程、人员、管理、行政部门、硬件、软件或信息方面的弱点。这些弱点可能会被威胁利用，引起 IT 系统或业务目标的损害。脆弱性本身不会引起损害；脆弱性只是一种条件或一组条件。这些条件会使威胁影响资产。需要考虑不同源引起的脆弱性，例如，资产内在的脆弱性。除非资产本身改变以致脆弱性不再适用，否则脆弱性可能依然存在。

脆弱性包括系统中可能被利用并可导致不希望后果的弱点。它们是使威胁产生损坏的机会。例如，缺乏访问控制机制是可能发生入侵威胁，并使资产丢失这一类的脆弱性。在一特定的系统或组织

内，不是所有的脆弱性都会对一种威胁敏感。具有相对应威胁的脆弱性才需要立即关注。然而，因为环境是动态变化的，应监督所有脆弱性以识别已暴露于新老威胁的那些脆弱性。

脆弱性分析是指对被已标识的威胁利用的弱点的分析。这种分析必须考虑环境和现有的防护措施。特定系统或资产相对某种威胁而言，脆弱性是此系统或资产易受损害的容易程度的说明。

8.4 影响

影响是故意或意外引起的、影响资产的不希望事故的后果。此后果可能是某些资产的毁坏、IT 系统的损坏和保密性、完整性、可用性、可核查性、真实性或可靠性的丧失。可能的间接后果包括财务损失以及市场份额或组织形象的丧失。影响的度量可以在不希望事故的结果和防止这种不希望事故的防护措施的费用之间作出平衡。不希望事故发生的频度需予以考虑。当每次出现所引起的损害程度虽不大，但多次发生的聚集效应可能是有害的时候，这一点特别重要。影响的评估是风险评估和选用防护措施的一个重要的要素。

可用多种方法实现对影响的定性和定量的度量，例如：

a) 制订财务费用；

b) 规定严重程度经验等级，例如，1 到 10；

c) 从预定表中选用修饰词，例如，高、中、低。

8.5 风险

风险是某种威胁将利用脆弱性直接或间接引起组织资产或若干资产丢失或损坏的可能性。单个或多个威胁可能利用单个或多个脆弱性。

风险说明描述一特定威胁或若干威胁可能如何利用特定的脆弱性或若干脆弱性使资产受到损坏。风险由两个因素组合予以表征：不希望事故发生的概率及其影响。对资产、威胁、脆弱性和防护措施的任何改变对风险会有重要的影响。早期检测或知道环境和系统的变化将增加采取合适行动降低风险的机会。

8.6 防护措施

防护措施是习惯做法、规程或机制，它们可以防止威胁，减少脆弱性，约束不希望事故的影响，检测不希望事故和促使恢复。有效的安全通常要求不同防护措施的组合以提供资产的多种安全层次。例如，审核控制、人员规程、培训和物理安全要支持应用于计算机的访问控制机制。某些防护措施可能已经作为环境的一部分或作为资产的内在方式存在，或可能已经在系统或组织中实施了。

防护措施可以看成执行下列一种或多种功能：检测、威慑、防护、约束、纠正、恢复、监督和了解。适当选用防护措施对正确实现安全大纲是重要的。许多防护措施能起多种功能的作用。选用能满足多种功能需要的防护措施，费用上是更为经济的。能够使用防护措施的方面的例子有：

a) 物理环境；

b) 技术环境(硬件、软件和通信)；

c) 人员；

d) 行政管理。

安全意识是种防护措施并与人员方面有关。然而由于它的重要性，我们将在 9.6 中讨论。组织运行的环境和文化对所选用的防护措施和组织的安全意识具有影响。有些防护措施表达了组织对安全的态度的有力而清晰的信息。就此而言，重要的是不要选用违背组织运行的文化和/或社会的防护措施。

防护措施的例子有：

a) 网络防火墙；

b) 网络监督和分析；

c) 用于保密性的加密；

d) 数字签名；

e) 防病毒软件；

f) 信息备份；

g) 备用电源；

h) 访问控制机制。

8.7 残留风险

风险通常只能通过防护措施部分减轻。部分减轻是通常可能达到的全部，并且达到越多，花费也越多。这意味着通常存在着残留风险。判断安全是否适于组织需要的要素是接受残留风险。此过程称为风险接受。

管理部门应利用一次事件发生的影响和可能性了解所有的残留风险。必须由负责接受不希望事故的影响后果和如果残留风险不能接受，可以授权实施附加防护措施的人做出是否可接受残留风险的判定。

8.8 约束

通常组织管理部门要设立或考虑一些约束，而这些约束会受到组织运行的环境影响。要考虑的一些约束例子有：

a) 组织的；

b) 财务的；

c) 环境的；

d) 人员；

e) 时间；

f) 法律；

g) 技术；

h) 文化/社会。

在选用和实施防护措施时，必须要考虑所有这些因素。必须定期评审既有的和新的约束，任何改变应予以标识。还要注意这些约束可以随时间、区域和社会发展，以及组织文化的变化而变化。组织运行的环境和文化可能对若干安全要素，特别是威胁、风险和防护措施有影响。

9 IT安全管理过程

IT安全管理是由若干其他过程组成的不断前进的过程。一些过程，例如配置管理和变更管理，对纪律而不是对安全具有适用性。经验表明在IT安全管理中非常有用的一个过程是风险管理及其子过程的风险分析。IT安全管理的若干方面，包括风险管理、风险分析、变更管理和配置管理，示于图2。

9.1 配置管理

配置管理是保持跟踪系统变更的过程，可以正式或非正式进行。配置管理的主要安全目的是保证系统变更不降低防护措施和组织总的安全的有效性。

配置管理的安全目的是要知道已经发生哪些变更，而不是将安全用作阻止对系统变更的手段。在某些情况中，作出会降低安全的一些变更可能是有原因的。在这些情况时，应对安全的降低进行评估并根据所有相关因素作出管理决策。换句话说，对系统的变更必须充分考虑安全问题。配置管理的另一个目的是保证系统的变更要在其他文件(灾难恢复和应急计划)中予以反映。如果是重要的变更，则可能需要重新分析部分或全部系统防护措施。

9.2 变更管理

变更管理是当IT系统发生变更时协助标识新的安全要求的过程。

IT系统以及它们运行的环境在不断变更。这些变更是有了新的IT特性和服务可用性，或显露新的威胁和脆弱性的一个后果。IT系统变更包括：

a) 新规程；

b) 新特性；

c) 软件更新；

d) 硬件更换；

e) 新用户，包括外部组或匿名组；

f) 附加网络和互连。

当IT系统发生变更或计划要变更时，重要的是要确定这种变更将会对系统的安全产生什么影响（如果有的话）。如果系统有一个配置控制部门或其他组织机构管理技术系统变更，那么，应向此部门指派IT安全官员并负责作出这种变更是否会影响安全的判定，如果有影响将作出如何影响的判定。对重要的涉及新硬件、软件或服务采购的变更，要求作出分析以确定新的安全要求。另一方面，对系统作出的若干次要变更并不要求进行像重要变更那样的广泛分析。对这两种类型的变更，应进行估量利益和成本的风险评估。对次要更改，一般可在会议上非正式进行，但是结果和管理决定应形成文件。

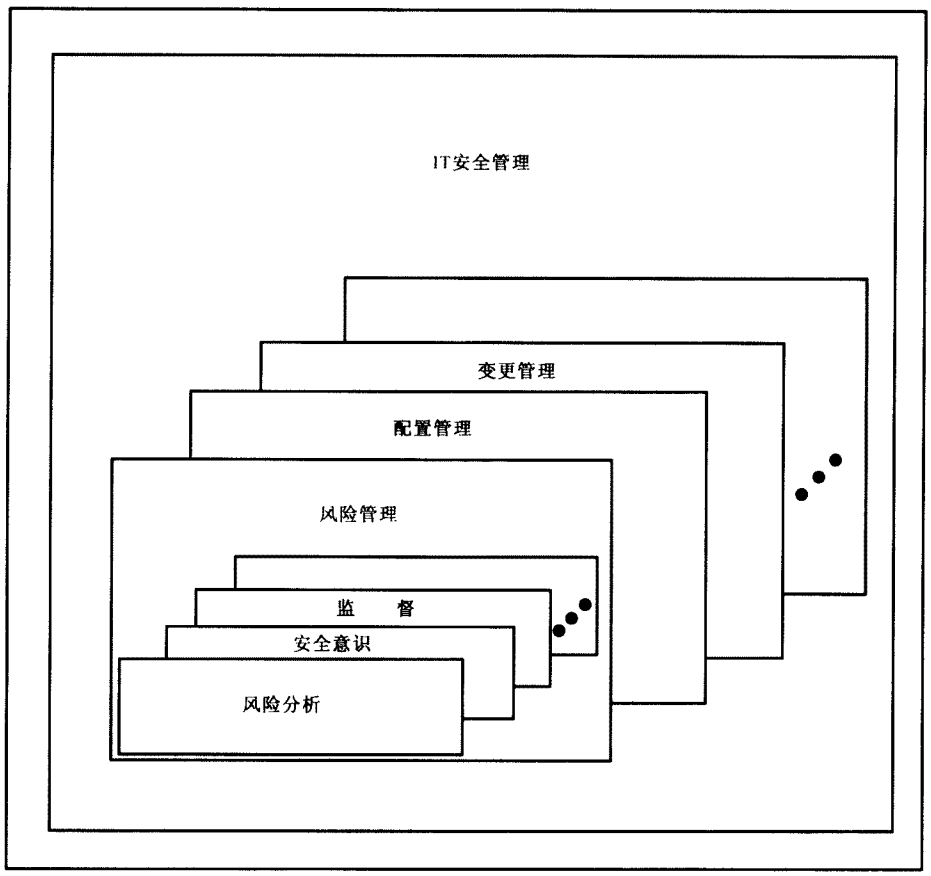

图 2　IT 安全管理的各方面

9.3　风险管理

如果在整个系统生存周期中存在风险，那么风险管理活动是最有效的。风险管理过程本身是个主要的活动周期。当对一个新系统可以采用完整的周期时，在传统系统情况中，可在系统生存周期中任何一个时刻启动它。此战略可以规定在系统生存周期的某些时刻进行评审，或以预先规定的次数进行评审。在上一次评审之后，会有一些后续活动，其目的是检查实现防护措施的过程。可要求在系统设计和开发期间进行风险管理，因而保证以最低成本的有效时间设计和实现安全。在计划对系统作重要变更时，也应启动风险管理。第10章，图4表示了在风险管理中所涉及的要素。

不管使用什么风险管理方法或技术，重要的是要在花费在标识和实现防护措施上的时间和资源最小和仍保证所有系统受到合适保护之间提供良好的平衡。

风险管理是将所评估的风险与防护措施带来的好处和/或成本进行比较并得出实现战略和系统安

全策略与总体IT策略和业务目标相一致结论的过程。要考虑不同类型的防护措施，要进行成本和/或利益分析。要选用与风险和潜在影响有关的防护措施。还必须考虑可接受残留风险的级别。

应予以注意的是防护措施本身也可能包含脆弱性，因而产生新的风险。因此，在选用合适的防护措施时必须小心，既要降低风险还要不引入潜在的新风险。

下列各条将提供有关风险管理过程的若干细节。

9.4 风险分析

风险分析标识需要受控或面对的风险。在IT安全的上下文中，对IT系统的安全分析包括资产价值、威胁和脆弱性的分析。要根据可能由于保密性、完整性、可用性、可核查性、真实性或可靠性的违规产生的潜在影响评估风险。风险分析评审的结果是对资产的可能风险的表述。

风险分析是风险管理的一部分，不必花费时间和资源投入调查，只需对所有系统进行初始的简略分析既可完成。风险分析将确定哪些系统受到规则或基线控制的充分保护，哪些系统将会从详细的风险分析评审中收益。规则由一组指南和基线控制组成，它们可用作协议的公共基础和满足基线保护要求的最佳习惯做法。

9.5 可核查性

有效的安全要求可核查性以及安全职责的明确分派和确认。须向资产的拥有者，提供者和IT系统用户分派职责和可核查性。因此，资产所有权和有关的安全职责以及安全性能的审核对有效的安全是重要的。

9.6 安全意识

安全意识是有效安全的基本要素。由于组织中人员缺乏安全意识和不良的安全习惯做法可能明显地降低防护措施的有效性。一般认为组织中的人员是最薄弱的安全链之一。为了保证组织中有足够的安全意识级别，重要的是编制和维护有效的安全意识大纲。安全意识大纲的目的是向员工、合作方和供应商说明：

a) 安全目标、战略和策略；

b) 安全及其有关角色和职责的需求。

除此之外，此大纲应促使员工、合作方和供应商保证承担安全责任。

应在组织的不同层次上，从最高管理层到负责日常活动的个人实现安全意识大纲，针对组织的不同部分、不同角色和责任的人员编制不同的意识材料并分发给他们常常是必要的。要分期制订并分发综合性的安全意识大纲。每一期建立在上一期的基础上，从安全概念开始，直到实施和监督安全的责任为止。

组织的安全意识大纲包括各种各样的活动。活动之一是安全意识材料(例如告示、期刊、小册子或简报)的编制和分发。这些材料的用途是要增加员工和合同商的普通安全意识。另一项活动是提供训练特定员工进行正确安全操作的教程。最后，需要一个在特定安全领域提供专业级培训的课程。

在某些情况中，将安全信息编入其他培训大纲是很有效的。这种方法应当作独立的安全意识大纲的补充，或用这种方法替代独立的安全意识大纲。为了编制与某个组织的文化和管理要求相融合的安全意识大纲，需要考虑下列方面：

a) 需求分析；

b) 大纲交付；

c) 监督；

d) 意识大纲内容。

9.7 监督

对防护措施的使用应予以监督以保证这些防护措施正确地运行，环境的变化没有使它们失效以及

可核查性被增强。系统日志的自动化评审和分析是一种有效的工具，这有助于保证所预期的性能。这些工具还可用来检测不希望事故并且它们的使用可具有威慑作用。

应定期检验安全防护措施的有效性。通过监督和一致性检查可实现这种有效性检验，从而保证防护措施以预期的方式在运行和使用。许多防护措施产生输出，例如日志、告警报告。应检查这些输出以发现重要安全事件。从安全角度来看，普通的系统审核工作能提供有用的信息，并可用于这方面。

9.8 应急计划和灾难恢复

应急计划包含当支持过程(包括 IT 系统)，被降级或不可用时如何运行业务的信息。这些计划应着手解决下列若干情况可能的组合：

a) 不同长度的中断；

b) 不同类型设施的损失；

c) 对建筑物的物理访问全部损失；

d) 返回破坏未发生时已存在状态的需求。

灾难恢复计划描述如何恢复运行受不希望事故影响的 IT 系统。灾难恢复计划包括：

a) 构成灾难的准则；

b) 启动恢复计划的职责；

c) 各种恢复活动的职责；

d) 恢复活动的描述。

10 模型

对 IT 安全管理而言有若干种模型。但是本部分所描述的模型提供理解 IT 安全管理问题所必须的一些概念。要描述的模型如下：

a) 安全要素关系；

b) 风险管理关系；

c) IT 安全过程管理。

前面所引入的概念和组织业务目标共同构成组织 IT 安全的计划、战略和策略。最重要的目的是要保证当风险处于可接受级别时，组织具有运行其业务的能力。没有一项安全能全面有效，重要的是要计划从不希望事故中恢复和构建安全来约束损害的程度。

IT 系统的安全是能从不同角度审视的多维问题。因此，为了确定和实现总的、一致的 IT 安全战略和策略，组织应考虑各个有关方面。图 3 表示资产怎样潜在经受若干威胁。威胁的汇集不断随时间改变并且只知道了其中一部分。

此模型表示：

a) 包含威胁的环境，而这些威胁不断改变并且只知道了其中一部分；

b) 组织的资产；

c) 资产的脆弱性；

d) 保护资产、降低威胁后果所选用的防护措施；

e) 修改风险的防护措施；

f) 组织可接受的残留风险。

如图 3 中所示，某些防护措施在降低与多种威胁和/或多种脆弱性有关的风险方面可以是有效的。有时，需要几种防护措施使残留风险降低到可接受的级别。在某些情况中，当认为风险是可接受时，即使存在威胁也不实现防护措施。在其他一些情况中，要是没有已知的威胁利用脆弱性，可以存在这种脆弱性。可以实现一些防护措施监督威胁环境以保证威胁不至演变成能利用这种脆弱性。约束(图 3 中没有显示)影响防护措施的选择。

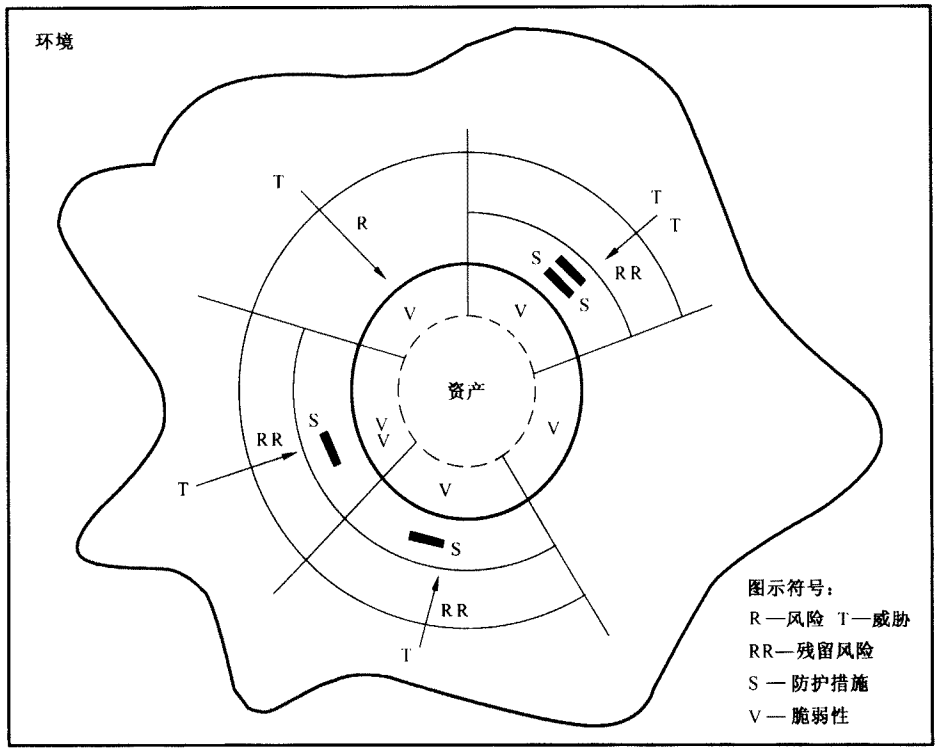

图 3 安全要素关系

图 4 表示常与风险管理有关的安全要素之间的关系。为清晰起见，仅表示了主要的关系。

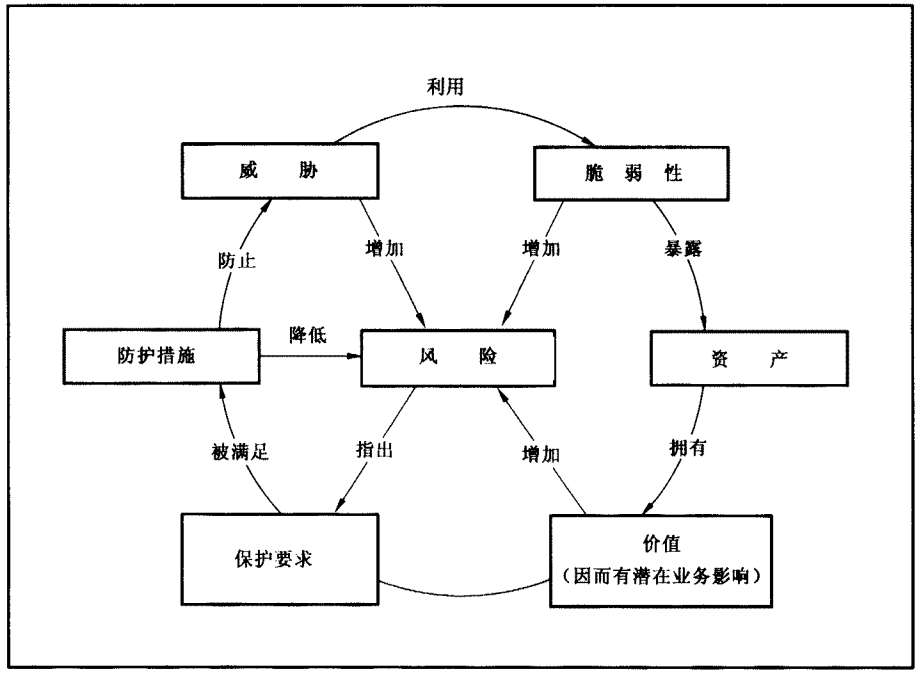

图 4 风险管理中的关系

注：任何二个方块之间箭头上的标记描述了这些方块之间的关系。

图 5、图 6 和图 7 分别示出保护要求和威胁、脆弱性及资产价值之间的关系。一些 IT 安全管理方法可能强调这些图所示观点之一。然而这些方法可能忽视一些重要方面。因此，图 4 提供较为通用的方法并可用作 GB/T 19715 的第 2 和第 3 部分的基础。

IT 安全管理是必须考虑安全生存周期的前进过程。这些方面在 GB/T 19715 的第 2 部分予以研究。GB/T 19715 的第 3 部分提出安全管理的技术。图 8 所示过程模型将与 IT 安全管理有关的安全要素联系起来。图 8 将在 GB/T 19715 的第 2 部分详细研究。

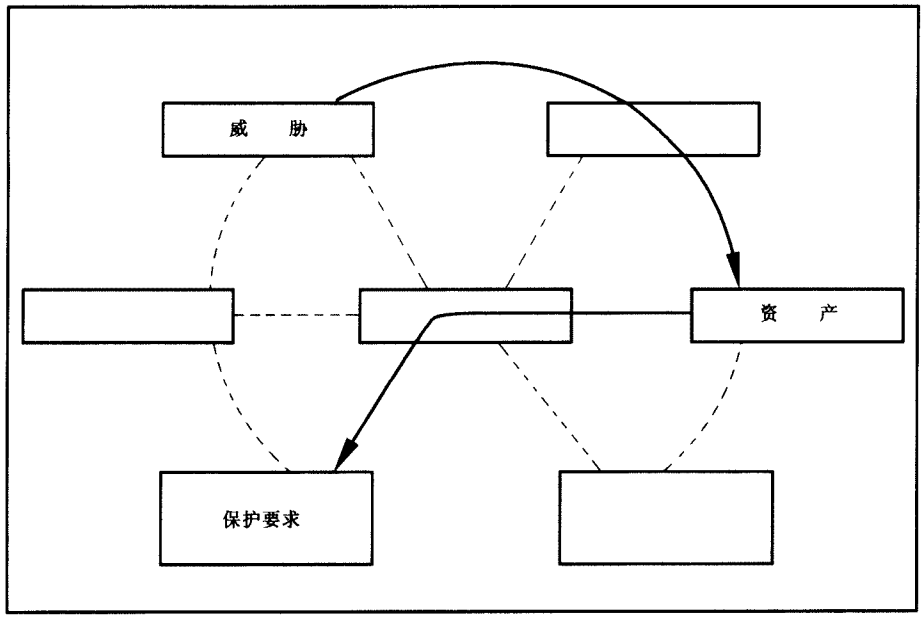

图 5　威胁视图

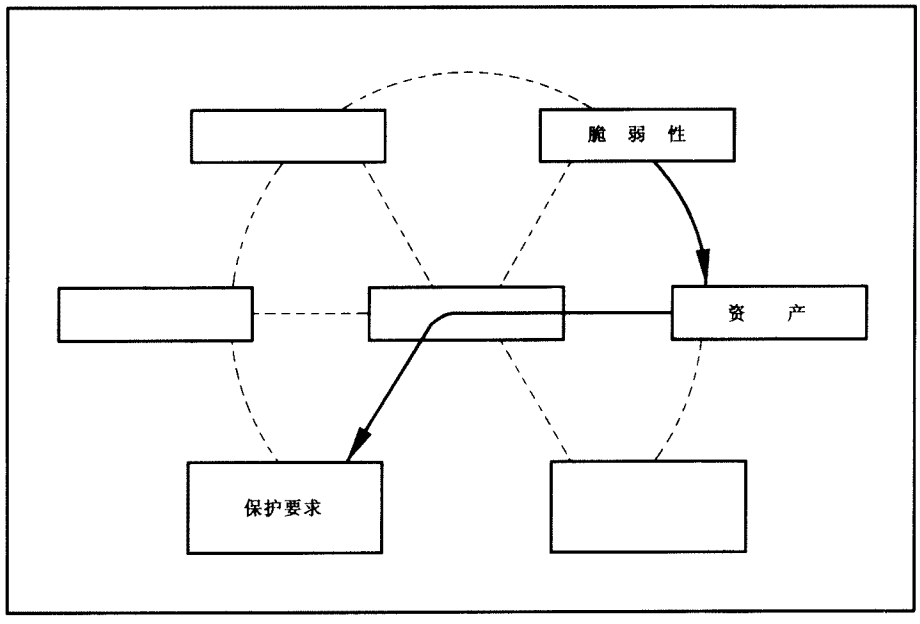

图 6　脆弱性视图

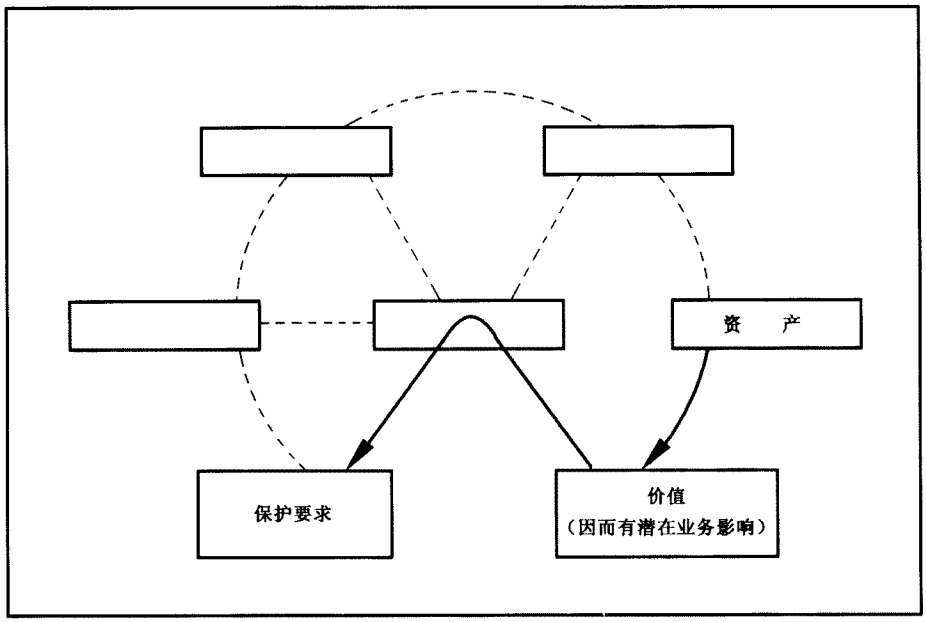

图 7　影响视图

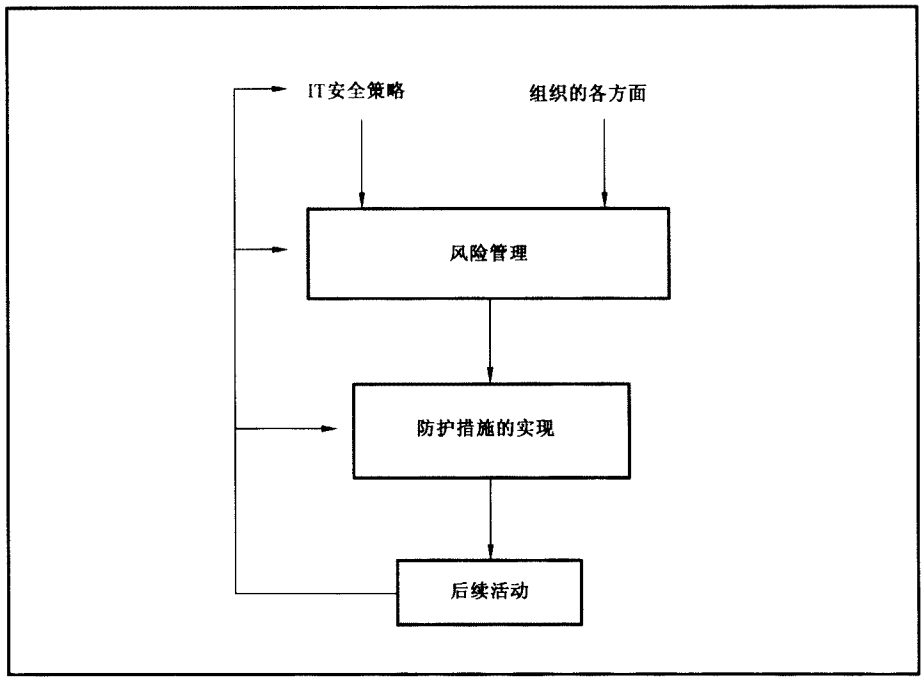

图 8　IT 安全过程管理

11　小结

本部分所讨论的概念和模型可用来制订保护组织 IT 资产的战略。此战略和有关的策略需在组织内不断地予以评审，考虑到技术以及信息服务的开发和使用的迅速发展。GB/T 19715 的其他部分将进一步描述在组织中如何有效使用这些概念和模型。