ICS 35.040
L 80

中华人民共和国国家标准

GB/T 19715.2—2005/ISO/IEC TR13335-2:1997

信息技术　信息技术安全管理指南 第2部分:管理和规划信息技术安全

Information technology—Guidelines for the management of IT security—Part 2:Managing and planning IT security

(ISO/IEC TR 13335-2:1997,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 13335-2:1997《信息技术　信息技术安全管理指南　第 2 部分：管理和规划信息技术安全》。

本部分中的指南提出 IT 安全管理的一些基本专题以及这些专题之间的关系。这些指南对标识和管理 IT 安全各个方面是有用的。

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。

本标准由多个部分组成。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。

本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；

c) 当然还有负责 IT 安全的管理者。

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2部分:管理和规划信息技术安全

1　范围

GB/T 19715的本部分提出IT安全管理的一些基本专题以及这些专题之间的关系。这些部分对标识和管理IT安全各个方面是有用的。

熟悉第1部分所介绍的概念和模型对全面理解本部分是重要的。

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 19715.1—2005　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(ISO/IEC TR 13335-1:1996,IDT)

3　术语和定义

GB/T 19715.1—2005确立的术语和定义适用于本部分,使用其下列术语:可核查性、资产、真实性、可用性、基线控制、保密性、数据完整性、影响、完整性、IT安全、IT安全策略、可靠性、残留风险、风险、风险分析、风险管理、防护措施、系统完整性、威胁、脆弱性。

4　结构

本部分有17章。第5章和第6章提供有关本文件目的和背景方面的信息。第7章提供成功的IT安全管理中所涉及的各种活动的概述。第8章到第16章详述这些活动。第17章提供小结。

5　目的

本部分的目的是要提出与IT安全管理和规划有关的各种活动,以及组织中有关的角色和职责。这一般与负责IT系统采购、设计、实现或运行的IT管理人员有关。除了IT安全管理人员外,还与负责使IT系统具体使用活动的管理人员有关。总之,本部分对与组织IT系统有关的负管理责任的任何人是有用的。

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过程的。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 资产的安全威胁和 IT 资产的脆弱性；

d) 标识和分析安全风险；

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规划不可分的组成部分并被集成到组织所有的职能过程中。因此，本部分所提出的若干安全专题具有广泛的管理内涵。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

7.1 规划和管理过程概述

IT 安全规划和管理是制订和维护组织内 IT 安全大纲的全面过程。图 1 示出此过程中的主要活动。由于管理风格、组织规模和结构不同，应对此过程予以剪裁，以适应使用此过程的环境。重要的是要根据组织的风格、规模和结构及其进行业务的方式采用图 1 所标识的各种活动和功能。这意味着进行管理评审是所有这些活动和功能的一部分。

起点是要制订组织 IT 安全目标的清晰视图。这些目标是根据更高层目标(例如，业务目标)得到的，然后依次产生组织的 IT 安全战略和总体 IT 安全策略，详见第 8 章。由此，部分总体 IT 安全策略创建合适的组织结构，保证能够实现所规定的目标。

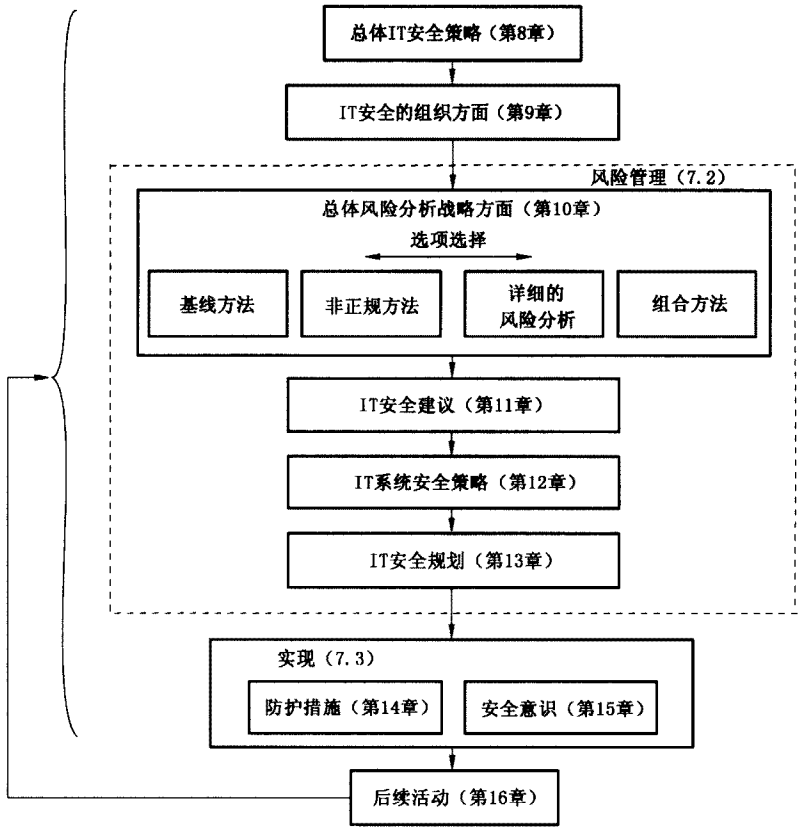

图 1 IT 安全规划和管理概述

7.2 风险管理概述

风险管理包括四种不同的活动：

a) 在总体 IT 安全策略上下文内确定适合于组织的全面风险管理战略；

b) 作为风险分析活动的结果或按照基线控制，选用适用于各个 IT 系统的防护措施；

c) 根据安全建议形成 IT 系统安全策略，以及在必要时更新总体 IT 安全策略（和合适时更新部门 IT 安全策略）；

d) 根据批准的 IT 系统安全策略，制订 IT 安全计划以实现防护措施。

7.3 实现概述

应按 IT 安全计划实现每个 IT 系统所必须的防护措施。全面改善 IT 安全意识（虽然常被忽视），对防护措施的有效性而言，是个重要方面。图 1 清楚地表明两项工作，即防护措施实现和安全意识大纲，应并行运作，这是因为用户行为不可能很快改变，需要在一个较长的时期内不断提高安全意识。

7.4 后续活动概述

第 16 章中提出的“后续”活动包括：

a) 维护防护措施，以保证其连续而有效地运行；

b) 检查，以保证防护措施符合已批准的策略和计划；

c) 监督资产、威胁、脆弱性和防护措施的变异以检测可能影响风险的变化；

d) 事故处理以保证对不希望事件的合适反应。

后续活动是项持续的工作，它应包括早期决定的重新评估。

7.5 结合 IT 安全

如果在组织内全面开展 IT 安全活动并且从系统生存周期开始，那么这些活动就能发挥最大效用。IT 安全过程本身就是一个主要的活动周期并应与系统生存周期的各个阶段相结合。虽然在新系统一开始就结合，安全才会最有效，但是传统系统和业务活动也会因为在任何阶段及时结合安全而受益。

IT 系统生存周期可划分为三个基本阶段。每个阶段通过以下途径与 IT 安全联系：

a) 计划：在做出活动计划和决定期间应处理 IT 安全要求；

b) 获得：IT 安全要求应与系统设计、开发、采购、升级或另行构建的过程相结合。安全要求与这些活动相结合保证在合适的时间将成本有效安全特性加入系统而不滞后；

c) 运行：IT 安全应与运行环境相结合。当用 IT 系统执行其预期任务时，一般要经历一系列升级，包括采购新的硬件或修改或增加软件。除此之外，运行环境经常改变。环境的这些变化可能产生新的系统脆弱性，对此应予以分析和评估，要么想法减轻，要么接受。同等重要的是系统的安全处置或重新指派。

IT 安全应是在 IT 系统生存周期阶段内和之间的具有许多反馈的持续过程。在图 1 中仅示出了总的反馈通路。在大部分情况中，反馈还会出现在 IT 安全过程各主要活动内和之间。这提供有关 IT 系统脆弱性、威胁和防护措施，贯穿 IT 系统生存周期三个阶段的持续信息流。

还值得注意的是每个组织业务范围可以标识独特的 IT 安全要求。这些范围应相互支持并通过分享能用来支持管理决策形成过程的安全方面的信息支持整个 IT 安全过程。

8 总体 IT 安全策略

8.1 目标

可以为组织的每个层次和每个业务单位或部门定义目标（要实现什么）、战略（如何实现这些目标）和策略（实现这些目标的规则）。为了实现有效的 IT 安全，调整每个组织层次和业务单位的各个目标、战略和策略是必要的。虽然相应文件受不同观点影响，但是相应文件之间的一致性是重要的，因为许多威胁（例如系统被黑客攻击，文件删除和火灾）是共同的业务问题。

8.2 管理承诺

高层管理对IT安全的承诺是重要的，并应产生正式协议，并记录总体IT安全策略。总体IT安全策略应根据总体安全策略派生出来。

8.3 策略关系

若合适，总体IT安全策略可以包含在总体技术和管理的范围内，共同形成总体IT安全战略报告的基础。此报告应对安全重要性，特别是安全对符合战略是否必要，作出有说服力的表述。图2示出了各种策略之间的关系。没有考虑组织使用的文件和组织结构，重要的是提供所述策略的不同消息(message)和维护一致性。

另外，特定系统和服务，或一组IT系统和服务要求更详细的IT安全策略。这些通常称之为IT系统安全策略。它是重要的管理方面，其范围和界限是清晰地定义并且以业务和技术理由为基础的。

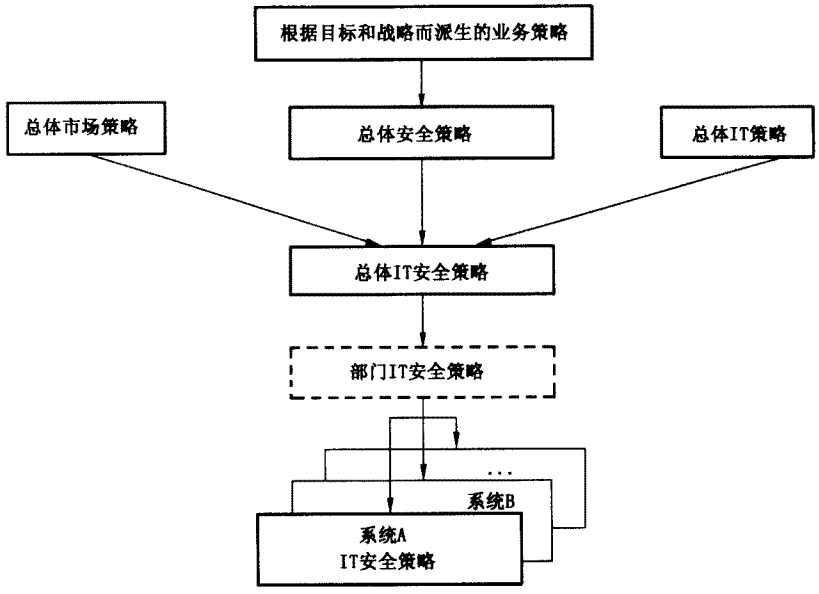

图2 策略关系

8.4 总体IT安全策略要素

总体IT安全策略至少应包括下列专题：

a) IT安全要求，例如，在保密性、完整性、可用性、真实性、可核查性和可靠性方面，特别是与资产拥有者意图有关方面；

b) 组织基础设施和职责的分配；

c) 安全与系统开发和采购的结合；

d) 指令和规程；

e) 信息分类的级别定义；

f) 风险管理战略；

g) 应急计划；

h) 人员问题(对要求信赖的岗位上的人员应予以特别注意，例如，维护人员和系统管理人员)；

i) 意识和培训；

j) 法律和规章责任；

k) 外包管理；

l) 事故处理。

9 IT 安全的组织方面

9.1 角色和职责

IT 安全是一项跨学科的课题并与组织内的 IT 项目、系统和所有 IT 用户有关。职责的合理分配和划分应保证完成所有重要工作任务和有效的方法履行这些职责。

虽然可根据组织的规模和结构，通过不同的组织方案达到此目的，但在每个组织中需要包含下列角色：

a) IT 安全管理协调小组，它一般解决跨学科问题并审批指令和标准；

b) 高层 IT 安全官员，他起到组织内所有 IT 安全方面的聚集点的作用。

IT 安全管理协调小组和高层 IT 安全官员应具有明确规定的职责并是足够资深的人以保证对总体 IT 安全策略的承诺。组织应为高层 IT 安全官员提供清晰的通信线路、角色和职权，责任应由 IT 安全管理协调小组审批。可通过使用外部顾问补充完成这些责任。

图 3 示出了一个典型的高层 IT 安全官员，IT 安全管理协调小组和代表之间关系的例子。其中代表来自组织其他方面，例如：其他的安全职能、用户委员会和 IT 人员。这些关系可以是分层管理或功能管理的。图 3 所述的 IT 安全组织的例子使用三个组织层。分层管理是便于组织采纳的，它可以根据自己的需求增加或删除层次。对于小的媒体组织可以选择只有一名高层 IT 安全官员承担所有安全角色的职责。当将这些功能组合在一起时，重要的是要保证维护合适的检查和平衡以避免没有施加影响或控制的可能，而将太大的权力集中在一个人手中。

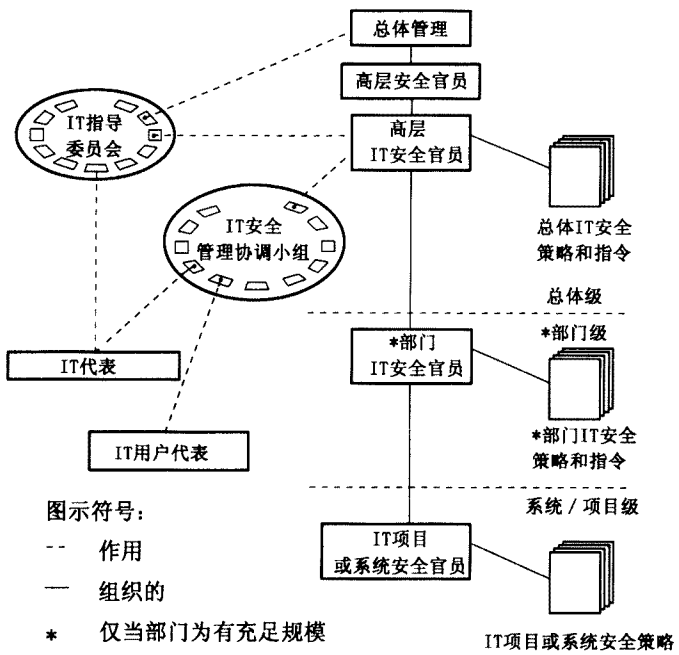

图 3 IT 安全组织的例子

9.1.1 IT 安全管理协调小组

这个管理协调小组应由具有标识要求、制订策略、起草安全大纲、评审成果以及指导高层 IT 安全官员必要技能的人员组成。可以用已经有的合适管理协调小组或独立的 IT 安全管理协调小组。这种管理协调小组或委员会的任务是：

a) 向 IT 指导委员会提供有关战略性安全计划的建议；

b) 制订总体 IT 安全策略以支持 IT 战略并获得 IT 指导委员会的批准；

c) 将总体 IT 安全策略转化为 IT 安全大纲；

d) 监督 IT 安全大纲的实施；

e) 评审总体 IT 安全策略的有效性；

f) 提高对 IT 安全问题的意识；

g) 提出关于支持计划过程和 IT 安全大纲实现所需资源方面(人力、财力、知识等)的建议。

为了有效起见，此管理协调小组应包括具有 IT 系统安全和技术背景的成员，以及 IT 系统提供者和用户的代表。需要这些领域的知识和技能制订实用的总体 IT 安全策略。

9.1.2 高层 IT 安全官员

因为共同承担 IT 安全责任，结果会发生没有一个人感到有责任的风险。为了避免这种风险，应指定专人负责，高层 IT 安全官员应起到组织内所有 IT 安全方面的聚焦点作用。可能已经有一个合适的人能担任附加职责，但是仍建议设立专门的岗位。优先选用具有安全和 IT 背景的人作为高层 IT 安全官员。主要职责是：

a) 监视 IT 安全大纲的实施；

b) 与 IT 安全管理协调小组和高层安全官员联络并向他们报告；

c) 维护总体安全策略和指令；

d) 协助事故调查；

e) 管理全组织安全意识大纲；

f) 确定 IT 项目和系统安全官员(以及相关部门 IT 安全官员)职责范围条款。

9.1.3 IT 项目安全官员和 IT 系统安全官员

各个项目和系统应有人负责安全，通常称作 IT 安全官员。在某些情况下，可以不是全职角色。对这些人的功能管理将是高层 IT 安全官员的责任(或合适时，是部门 IT 安全官员的责任)。此安全官员起到项目、系统或一组系统所有安全方面的聚焦点作用。此岗位的主要职责是：

a) 与高层 IT 安全官员(或若合适，部门 IT 安全官员)联络并向他报告；

b) 颁发和维护 IT 项目或系统安全策略；

c) 制订和实施安全计划；

d) 对 IT 防护措施的实施和使用进行日常监督；

e) 启动和协助事故调查。

9.2 承诺

对有效的 IT 安全极其重要的是各个层次的管理要支持每个人所作的努力。业务对 IT 安全目的的全面承诺包括：

a) 理解组织的全局需求；

b) 理解组织对 IT 安全的需求；

c) 表明对 IT 安全的承诺；

d) 愿意解决 IT 安全需求的意愿；

e) 愿意将资源配给 IT 安全；

f) 意识到，在最高层，IT 安全意味着什么，或由什么组成(范围、程度)。

9.3 一致的方法

与 IT 安全一致的方法应用于各种开发、维护和运行活动。在信息和 IT 系统整个生存周期，从计划到处置，应保证受到保护。

组织结构(如图 3 所示)能够在整个组织内支持与 IT 安全相协调的方法。这需要通过承诺到标准予以支持。标准可以包括国际、国家、区域、工业部门和组织标准或规则，选用和应用应视组织的 IT 安全需求。技术标准需由与其实现、使用和管理有关的规则和指南加以补充。

使用标准的好处有：

a) 综合性安全；
b) 互操作性；
c) 一致性；
d) 可移植性；
e) 规模经济性；
f) 组织间互通(interworking)。

10 总体风险分析战略选项

希望加强安全的任一个组织应以适当方法提出合适其环境并包含用有效的方式避免风险的手段的风险管理战略。所要求的战略能在需要安全的地方集中安全力量并启用一种成本和时间有效的方法。

无论是对所有系统进行详细评审还是不找出严重风险都不能有效利用资源或时间。在这两种极端之间提供平衡的方法包括进行高层评审以确定对系统的IT安全需求，同时研究这些需求的深层一致性。组织的安全需求将取决于其规模、进行的业务类型及其环境和文化。要选用的总体风险分析战略选项应与这些因素直接有关。

在某些情况中，组织可以决定什么也不做或推迟实现防护措施。这种管理决定只应在组织高层完成评审之后作出。然而，如果作这种决定，管理部门应全面了解风险和为此易受到的负面影响，以及发生不希望事故的可能性。没有这些知识，组织可能无意中违背法律或规章并可能使其业务受到潜在的损失。只有对这些和其他可能的有害影响作出严肃的考虑之后才应采纳什么也不做或推迟实现防护措施的决定和判断。

根据高层评审结果，可使用下面叙述的四个选项之一选用减缓风险的防护措施。下列各条提供每种选择的优缺点说明。

10.1 基线方法

第一种选项是要为所有系统选择一组防护措施，使系统保护达到基线水平。要在基线文件和实用规则中建议各种标准防护措施，在检验这些基本需求之后，也可从其他组织，例如，国际和国家标准组织、工业部门标准或建议或具有合适相似性(例如，业务目标、规模、IT系统和应用)的其他公司吸纳这些防护措施。

这种方法有若干优点，例如：

a) 详细风险分析不需要资源，并减少花在防护措施选择上的时间和精力。通常，标识基线防护措施不需要显著的资源；
b) 不必花费巨大精力，许多系统可以采用相同或类似的基线防护措施。如果大量的组织系统运行一个通用的环境并且业务需求也相近，则基线防护措施可以提供经济有效的解决方案。

这种选项的缺点是：

a) 如果基线水平设置得太高，则对某些系统可能是过于昂贵或过于严格限制的安全，如果基线水平过低，则对某些系统可能是没有足够的安全；
b) 在管理与安全有关的变化方面可能会有困难。例如，系统升级，则可能难以评估原先基线防护措施是否仍然足够。

10.2 非正规方法

第二种选项是对所有系统进行非正规的、注重实效的风险分析。非正规方法不是以结构法为基础，而是利用个人的知识和经验。如果在内部没有可用的安全专家，可请外部顾问进行分析。

这种选项的优点如下：

a) 进行非正规分析无须学习另外的技能，并且比详细风险分析要快。因此这种方法可能经济有效并适合小型组织。

存在的若干缺点如下：

a) 没使用结构化方法，遗漏某些风险和关注范围的可能性增加；

b) 由于这种方法的不正规性，其结果可能受到评审者主观看法和偏见的影响；

c) 对所选用的防护措施几乎没有什么正当理由，因此用于防护措施的费用难以判定；

d) 随着时间的流逝，没有再评审，可能难以管理与安全相关的变化。

10.3 详细的风险分析

第三种选项是对所有系统进行详细的风险分析。详细的风险分析包括资产的标识和估价，对这些资产威胁程度和这些资产的脆弱性的评估。使用这些作为输入以评估风险。通过这些工作，风险分析支持标识、选择和采用根据所标识的资产风险认为正确的防护措施并支持将这些风险降低到由管理部门定义的可接受程度。详细的风险分析可能是一个非常耗费资源的过程，因此，需要认真建立边界，也需要管理上的经常关注。

这种选项的优点是：

a) 为每个系统的安全需要定义合适的安全级别；

b) 管理与安全有关的变化会从详细的风险分析所获得的附加信息中获益。

这种选项的主要缺点是：

a) 为获得可行的结果要用大量的时间、精力和专家。

10.4 组合方法

第四种选项使用高层风险分析方法首先标识高风险或对业务运行重要的那些系统。根据这些结果，将系统分类：为达到合适的保护哪些系统需要详细的风险分析；哪些系统基线保护足够了。

这种选项是10.1基线方法和10.3详细风险分析方法所述选项最佳要点的组合。因此，它在使标识防护措施方面使花费的时间和精力最小和同时仍保证所有系统受到合适保护之间提供了良好的平衡。

这种选项的优点是：

a) 在花费大量资源之前，使用简单的高层方法收集必要的信息更可能得到可接受的风险管理大纲；

b) 绘制组织安全大纲直接战略图成为可能，这种图可用作规划的良好辅助手段；

c) 使资源和钱用在最值得的地方，以及处于高风险的系统得到更早的处理。

这种选项的缺点是：

a) 如果高层风险分析导致不准确的结果，则有些需要详细风险分析的系统则可能未被处理。如果合适地检查高层风险分析的结果则多半不会发生此事，而且无论如何这些系统们都会受到基线防护措施的保护。

在大多数情况，这种选项提供使花费最有效的方法，并向多数组织强力推荐这种风险分析选项。

11 IT安全建议

第10章中的任一方法应提供使安全风险降到可接受水平的若干建议。这些建议应由管理部门批准，并应包括：

a) 确定被考虑系统可接受风险水平的准则；

b) 选择使风险降低到可接受水平的防护措施；

c) 关于实现这些防护措施的好处以及这些保护所能达到的风险降低；

d) 所有这些防护措施已被实现时仍存在的可接受的残留风险。

11.1 防护措施的选择

有若干防护措施类型：防止、减少、监督、检测或排除不希望事故和从不希望事故中恢复等类型。防止可以包括阻止提高安全意识的不希望行动和活动。适用防护措施的主要范畴和每种范畴的一些例子有：

a) 硬件(备份、钥匙);

b) 软件(电子签名、记录、抗病毒工具);

c) 通信(防火墙、数据加密);

d) 物理环境(围墙、标记);

e) 人员(工作人员意识,解除员工的规程);

f) 管理(授权、硬件处置、特许控制)。

防护措施不是彼此独立的,并且经常是以组合方法工作。选择过程必须考虑防护措施相互依赖关系。在防护措施选择期间,必须检查是否仍留有缺口。这种缺口使避开现有的防护措施成为可能并能使偶然的威胁造成损坏。

对新系统,或对现有系统作出重大改变时,防护措施可以包括一种安全体系结构。安全体系结构描述如何满足IT系统的安全要求并是整个系统体系结构的一部分。它解决技术防护措施,同时考虑非技术方面。

所有防护措施需要管理以保证有效地运行,许多防护措施将要求对维护过程的管理支持。这些因素应在防护措施选择过程期予以考虑。

有效地实施防护措施并且不引起用户或管理的过分负担是重要的。如果防护措施引起重要的变化,那么其实现应与安全意识大纲、变更管理和配置管理相结合。

11.2 风险接受

在实现所选择的防护措施之后,总是会有残留风险的。这是因为不可能使系统绝对安全,以及因为某些资产可能有意未加以保护(例如,由于设定低风险或相对被保护资产的评估价值而言建议的防护措施费用过高)。

风险接受过程的第一步是要审查所选的防护措施,标识并评估所有的残留风险。下一步是对残留风险分类,对组织而言,哪些被认为"可接受的"和哪些是"不可接受的"。

显然不能容许不可接受的风险,因此,应考虑限制这些风险影响或后果的附加防护措施。不管哪种情况,必须作出业务决定。风险被判定为"可接受的"或将风险降到可接受水平的附加防护措施的费用必须予以审批。

12 IT系统安全策略

IT系统的安全策略应根据总体和部门的安全策略制订。这些系统的安全策略由一组保护系统和服务的原则和规则组成。必须通过对系统和服务适合的防护措施的应用实施这些策略以保证达到足够的保护水平。

IT系统安全策略必须由上级管理部门批准作为强制的n组原则和规则以保证调拨财务和人力资源用于其应用和执行。

在决定每个IT系统安全策略时要考虑的关键问题:

a) 确定所考虑IT系统及其边界;

b) 确定此系统要达到的业务目标,因为这些目标可能对此系统的安全策略以及防护措施的选择和实现有影响;

c) 潜在有害的业务影响来自:

   1) 服务或资产,包括信息的不可利用性、拒绝或破坏;

   2) 信息或软件的未授权修改;

   3) 信息未授权的泄露;

   具有定量的影响,例如,直接或间接地损失钱财,以及定性的影响,例如,失去信誉,失去生命或生命危险、侵犯个人隐私;

d) 在IT方面的投资水平;

e) 对此 IT 系统和所处理的信息的重要威胁；

f) 脆弱性，包括使 IT 系统遭受已标识威胁危险的缺点；

g) 所要求的防护措施，它们与所标识的风险是相称的；

h) IT 安全成本，即保护 IT 资产的费用(应将 IT 安全成本看成 IT 系统拥有权成本的一部分)；

i) 与外部资源提供者(例如，计算中心，PC 支持)的关系和选用外部资源提供者的原则。

IT 安全需要一种已计划的方法并且不应孤立地予以考虑。它在战略计划过程中起重要作用，从而，保证一开始就在系统中计划和设计安全。在大多数情况中，后来再增加防护措施，费用将更昂贵或甚至是不切实际的。

13 IT 安全计划

IT 安全计划是一份定义实现 IT 系统安全策略要承担的协调活动的文件。根据投入、运行成本、工作负荷等，这份计划应包括短期、中期和长期范围要承担的主要活动和相关成本以及实现时间表。它应包括：

a) 全面的安全体系结构和设计；

b) 对 IT 系统符合组织安全目的的简短评论，用最大财务损失、困难、公司形象等反映；

c) 标识与管理部门所评估、支持和证实的风险相适应的防护措施；

d) 对防护措施实际置信水平的评估，包括其有效性的决定；

e) 就指定系统或应用中而言，残留风险评估概述；

f) 标识和定义实现防护措施具有其相应优先权的活动；

g) 实现防护措施的详细工作计划，包括优先权、预算和时间表；

h) 项目控制活动，包括：

   1) 资源调拨和职责分配；

   2) 进度报告规定的定义；

i) 对 IT 工作人员和末端用户的安全意识和培训要求；

j) 对编制安全操作和管理规程的要求。

此外，此计划应包括定义证实上述每一要点的条件和活动的规程，包括计划本身修改的规程。

14 实施防护措施

在制订 IT 安全计划之后，必须实施它。通常，IT 系统安全官员负责此项工作。在安全实施期间应关注下列目标。应保证：

a) 防护措施成本保持在已批准的范围内；

b) 按照 IT 安全计划要求正确实施防护措施；

c) 按照 IT 安全计划要求运行和管理防护措施。

大部分技术防护措施需根据操作和管理规程来实施并且不能用纯粹的技术手段来实施。因此，这些规程应由各方面管理支持和实施。

安全意识和培训也应看作一项防护措施，由于其重要性，在第 15 章将单独讨论意识。

安全意识适用于所有人员，对下列人员要给以特别的安全培训：

a) 负责开发 IT 系统的人员；

b) 负责 IT 系统运行的人员；

c) IT 项目和系统安全官员；

d) 负责安全管理(例如访问控制)的人员。

在完成 IT 安全计划实施时，应产生批准实施 IT 系统安全计划所规定的防护措施的正式过程。当获得批准时，才授权 IT 系统或服务投入运行。这种批准过程称之为认可。

对 IT 系统或服务的任何重大修改应导致对此 IT 系统或服务的重新检查，重新测试和重新批准。

15 安全意识

应在组织所有层面上，从最高管理层到用户，实施安全意识大纲。没有用户层人员的接受和参与，安全意识大纲就不可能成功。用户需要理解安全意识对大纲成功的重要性。

意识大纲应传递总体 IT 安全策略的知识并保证对安全指南和合适行动的全面理解。此外，安全意识大纲应包括系统安全计划的目标。此大纲至少应提出下列专题：

a) 对信息保护的基本需求；

b) 对用户和组织而言，安全事故含意；

c) 目标背景和总体 IT 安全策略和风险管理战略的说明，这有助于对风险和防护措施的了解；

d) 实施和检查防护措施的 IT 安全计划；

e) 信息分类；

f) 数据拥有者的职责；

g) 职责、岗位描述和规程；

h) 需要报告和调查安全违规或试图攻击；

i) 没按授权方式行动(包括纪律活动)的后果；

j) 安全符合性检查；

k) 变更和配置管理。

有效的安全意识大纲要使用各种媒体，例如，小册子、手册、告示、电视、简讯、动手实习、专题研究会、报告会和讲座。重要的是安全大纲的实施要考虑社会、文化和心理方面，发展充分认识安全重要性的文化。

安全意识应涉及组织内的每个人，要影响其行为，提高所有人的责任感。重要因素是要使管理部门了解安全需求。保证其工作人员的安全意识是所有管理者工作的一部分。因此，他们必须计划相应的预算。在大组织中，高层 IT 安全官员应担负 IT 安全意识职责。安全大纲的目的是要使有关人员认识到 IT 系统存在重大风险和信息丢失，或未授权修改，或泄露对组织及其员工可能具有严重影响。

更为可取的是组织与组织环境有关的意识会议。结合公司案例介绍有关例子，这更易于理解也比新闻媒体报道的案例影响更大。这种会议还向员工提供与教师交流的机会。应监督员工对防护措施的服从性以衡量安全意识会议的影响和评价会议内容。如果其结果不令人满意，那么安全意识会议的内容应作相应修改。

安全意识会议应定期召开，以更新现有工作人员的知识和使新人员获得知识。此外，应对每位新员工、每位最近转岗人员和每位最近提升的人员，结合其新的职责予以教育。将 IT 安全方面与其他教材相结合也是一种合理选择。需要强调的是安全意识是个不断前进的过程，决不会一劳永逸。

16 后续活动

所有防护措施需要维护以保证它们以预期的、合适的方式起作用。安全的这一方面工作是一项重要的工作，但是，一般未引起注意。最常见的是，系统或服务已经存在，当想到时就添加安全，然后又忘掉安全。趋势是忽视已经实现的防护措施，充其量，对维护或加强安全只给予一点点关注。因此，应通过计划活动而不是心血来潮发现防护措施的过时。此外，安全符合检查、运行环境的监督、日志记录审查和事故处理也是必需的，这才能保证安全深入和加强。

16.1 维护

维护防护措施(包括行政管理)是组织安全大纲的一部分。它是各个管理层的职责，要保证：

a) 将组织资源分配给防护措施的维护；

b) 定期复验防护措施，保证它们按预期的方式运行；

c) 当发现新的要求时,升级防护措施;

d) 明确建立维护防护措施的职责;

e) 对 IT 系统硬件、软件的修改和升级不改变现有防护措施的预期性能;

f) 技术上的进步不引入新的威胁或脆弱性。

完成上述维护活动,现有的防护措施将继续按预期的方式运行,将会避免不利的、代价很高的影响。

16.2 安全符合性

安全符合性检查(也称做安全审核或安全评审)是保证与 IT 系统安全计划一致和符合的十分重要的活动。

为了保证 IT 安全的合适水平保持有效,重要的是所实施的防护措施与 IT 项目或系统安全计划所规定的防护措施一致并且继续保持一致。对所有 IT 项目和系统,在下列期间它必须是确实的:

a) 设计和开发;

b) 运行生命期;

c) 取代或处置。

安全符合性检查可使用外部或内部人员(例如,审核员)进行,并基本按照与 IT 项目或系统安全策略有关的检查单进行。

安全符合性检查应有计划并与其他计划活动相结合。在确定运行支持工作人员和用户是否符合具体防护措施和规程时,现场检查特别有帮助。

应使这种检查保证实现,正确地实施,正确地使用,具有正确的安全防护措施,若合适,还应测试。当发现有些防护措施与安全不符合,则应制订、启动纠正活动计划并评审结果。

16.3 监督

监督是 IT 安全周期的重要部分。如果予以合适地进行,会给管理部门提供下列情况的清晰看法:

a) 与所提出的目标和最终期限相比较,已经实现了什么;

b) 成果是否令人满意,规定的主动措施在哪些地方已经起作用或在哪些地方没有起作用。

资产、威胁、脆弱性和防护措施的所有改变可能对风险具有潜在的重大影响,尽早检测到这些变更以便采取预防行动。

许多防护措施输出安全相关事件的日志。至少,应对这些日志进行定期评审以及如果可能,使用统计技术予以分析,从而能早期检测倾向性变化和检测重复的有害事故。利用日志仅仅作为事后分析忽视了潜在的非常强有力的防护措施机制。监督还应包括定期向有关 IT 安全官员和管理部门报告的规程。

16.4 事故处理

发生安全事故是不可避免的。应对每次事故做出与此事故所引起的危害相适应的深度调查。事故处理提供对正常 IT 系统运行的偶然或蓄意破坏进行反应的能力。因此,应制订适合于整个组织 IT 系统和服务的事故报告和调查方案。此外,应考虑与组织内其他报告方案相结合以获得出现 IT 安全事故和有关威胁,及其对 IT 资产和业务运行相关影响的更广宽的视野。

在 IT 安全事故调查期间,基本目标要:

a) 以敏感和有效的方式对事故作出反应;

b) 从事故中学习,因此可以预防今后类似有害事故的发生。

所制订的行动计划和预先的决定会使组织在合理时间内作出反应以减少进一步的危险以及与此相关的用辅助手段恢复已减少的业务。事故处理计划必须包括对按时间编排的所有事件和行动的文件的要求;这将标识事故的源头。这是达到第二个目的前提,即通过对防护措施的改进,进一步减少风险。事故的正面影响是它增加投资防护措施的意愿。

进行事故分析并写成文件是重要的,要解决下列问题:

a) 在什么时间发生什么?

b) 工作人员遵从计划么?

c) 工作人员按时得到所要求的信息?

d) 工作人员建议下一步做什么?

回答这些问题有助于了解事故,通过改进有关的 IT 安全策略和计划(例如,改善防护措施,减少脆弱性和修改安全意识大纲)还可减少风险。

17 小结

本部分讨论了与有效 IT 安全大纲有关的管理过程和职责。这种讨论的目的是给在 IT 安全管理中担任角色的管理者熟悉主要的过程和功能。本部分所提供的信息不可直接应用于所有组织。特别是,小型组织不可能有用来全面执行所述某些功能的各种资源。在此情况中,重要的是用合适的方式向组织解决基本概念和功能。即使在一些大组织,本部分所讨论的一些功能也不可能按所述准确完成。第 3 部分将探讨能用来完成本部分所述功能的某些技术。其后续部分将提供防护措施的选择和适于外部连接的特别防护措施。