美国商业部
技术局
国家标准和技术学会

华安信达

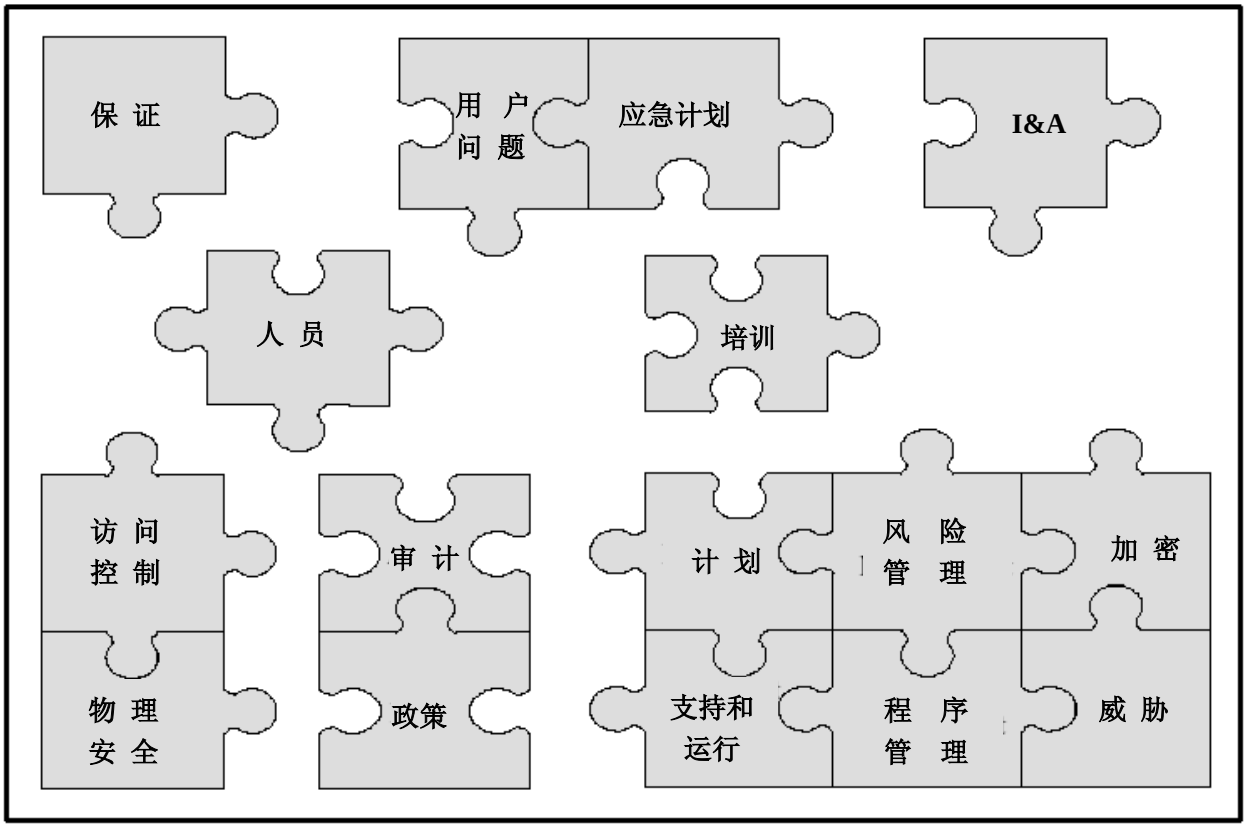
特别报告书 800-12

计算机安全介绍：NIST 手册

第二部分：管理控制

（中文版v1.00）

翻译：陈海燕，CISSP（phrackchen@hotmail.com）



目录

II. 管理控制

第五章

计算机安全的政策

第六章

计算机安全的项目管理

第七章

计算机安全的风险管理

第八章

计算机系统生命周期中的安全和计划

第九章

保证

II. 管理控制

第五章

计算机安全政策

在讨论计算机安全的过程中，**政策**这一术语具有多种含义[45]。**政策**是高级管理层对建立计算机安全项目的指导，确立其目标并设定相关责任。**政策**这一术语也被用于表示特定系统的特定安全规则[46]。另外，**政策**还可以表示完全不同的事物，如对于设定机构电子邮件隐私政策或传真安全政策的特定管理决策。

本章中，**计算机安全政策**这一术语被定义为包含上述所有类型政策的“计算机安全决策的文档”。在制定决策时[47]，管理人面临艰难抉择，这些抉择与资源分配、相互竞争的目标以及机构政策有关，涉及到技术和信息资源、指导员工行为的机构政策。所有级别的管理人作出的决策都可以成为政策，政策的适用范围因管理人的权限范围不同而各不相同。在本章中，我们在比较宽泛的含义上使用**政策**这一术语，它包括上面描述的所有政策类型，包括所有级别的管理人作出的特定政策。

> **政策**对于不同的人有不同的含义。本章中使用的“政策”这一术语含义比较宽泛，是指与计算机安全相关的重要决策。

计算机安全方面的管理决策有各种各样。为了区别不同类型的政策，本章将其分为三个基本类：

- 项目政策建立机构的计算机安全项目。
- 专题政策涉及到机构所关心的特定问题。
- 特定系统政策关注于管理层为了保护特定系统[48]所作出的决定。

规程、标准和指导方针被用于描述机构如何执行这些政策。（参见下页文字框中的内容）

---

[45] **政策**这一术语的使用存在很多变化，在 1994 年技术评估办公室的报告《网络环境中的信息安全和隐私》中提到，“这里所说的**安全政策**是机构、公司、部门发布的确立整体信息访问和防护政策的声明。另一种含义来自国防领域，是指关于用户访问机密信息的许可规则。在另一种用法中，**安全政策**被用于泛指广泛的机构安全政策…”

[46] 这是计算机安全专家用来特指系统的技术、管理和操作控制所**执行**的政策类型。

[47] 通常，政策由管理人制定。但是，在有些情况下可能由一个团队（如机构内的政策委员会）制定。

[48] 系统是指处理的整体集合，既包括人工执行部分也包括使用计算机的部分（如人工的数据采集以及随后的计算机处理），也就是功能部分。这既包括应用系统和包括支持系统，如网络。

执行政策的工具：规程、标准和指导方针

由于政策是在比较宽泛层面上制定的，所以机构还制定了标准、指导方针和规程，这些内容为用户、管理人和其他人员提供了执行政策和满足机构目标的清晰的方法。标准和指导方针为保护系统设定了技术和方法。规程是完成特定安全相关任务所要遵行的详细步骤。标准、指导方针和规程可以通过手册、规章或指南的方式在机构范围内传播。

机构的标准（不要同美国国家标准、FIPS、联邦标准或其它国家或国际标准相混淆）要求统一使用的对机构有益的统一技术、参数或规程。在机构范围内使用标准化的识别证件就是一个典型的例子，这使员工可以更方便、更灵活、更自动化地出入系统。通常，标准在机构中被强制执行。

指导方针协助用户、系统人员和其他人有效地保护系统。由于系统的多样性，所以有时强制执行统一的标准可能办不到、不适宜或不经济，这时候就需要指导方针了。例如，机构的指导方针可以被用来帮助制定针对系统的标准规程。通常可以使用指导方针协助确保特定的安全措施不会被忽略，正确地执行该措施可以有多种方式。

规程通常对于所遵循的安全政策、标准和指导方针进行协助。它们是用户、系统操作人员或其他人员完成特定任务（如准备新的用户帐户和设定适当的特权）所需遵循的详细步骤。

有些机构发布整体的计算机安全指南、规章、手册或类似的文件。由于政策、指导方针、标准和规程是相互关联的，所以这些文件可能同时包含这几个内容。指南和规章做为重要的工具通常与政策及其实施有明显的不同，应该加以区分。这样可以为达到政策目标提供多种方法以提高其灵活性和成本效益。

熟悉各种政策类型和部件可以帮助管理人处理对机构重要的计算机安全问题。有效的政策是制定和实施良好的计算机安全项目、保护系统和信息的基础。

对这些类型的描述有利于读者的理解[49]。将机构具体的政策归于三种类别的哪一种并不重要，重要的是要透彻理解其功能。

5.1 项目政策

管理官员，通常是机构的领导或高级管理人员发布的、确立机构计算机安全项目及其基本架构的项目政策。这种高级政策定义了项目的目的，及其在机构中的范围；设定了直接进行系统实施的责任（对于计算机安全机构），以及其它相关部门的责任（如信息资源管理［IRM］）；并涉及到政策的执行问题。项目政策确立机构对安全的战略导向，并为其实施分派资源。

[49] 对于各种类型的政策没有标准的术语。这些术语的目的是协助读者理解这些内容；并不意味着这些用法被广泛接受。

5.1.1 项目政策的基本部件

项目政策的部件应该涉及到：

目的 项目政策通常包括描述项目建立目的方面的内容。这可能会包括定义项目的目标。安全相关的需要如完整性、可用性和机密性等构成了机构中所建立的政策目标的基础。例如，在负责维护大型的任务关键数据库的机构中，减少错误、减少数据丢失和毁坏，以及执行恢复可能是特别重要的事情。但是，在负责维护个人机密数据的机构中，目标可能就更强调加强对防止非受权泄漏的保护。

范围 项目政策应该清晰地表明计算机安全项目涵盖的资源，包括设施、硬件和软件、信息以及人员。在许多情况下，项目包括所有的系统以及机构人员，但是也不总是这样。在有些情况下，可适当限制机构计算机安全项目的范围。

责任 一旦建立了计算机安全项目，其管理责任将会被设定给新的或现有的人员[50]。

需要涉及到整个机构中所有员工和管理人员的责任问题，包括生产线管理人、应用程序拥有者、用户以及数据处理或IRM部门。政策内容的这个部分应该与计算机服务提供商以及使用所提供服务的应用管理人的责任区别开来。政策还应该确立主要系统的运行安全人员，特别是风险较高和对机构运作非常关键的系统。这也可以作为确立员工职责的基础。

在项目级别上，应该特别为实施计算机安全政策和确保其连续性的机构部门和官员设定责任[51]。

执行 项目政策主要涉及到两个执行方面的问题：

1、通常的执行确保满足建立项目和为机构各种人员设定责任的需求。通常设定一名监督官员（如监察长）负责监督执行情况，包括机构执行项目管理优先顺序的情况。

2、使用具体的惩罚和训诫措施。由于安全政策是级别较高的文件，对于各种违反政策行为的具体惩罚措施一般不会详细记录在这里，政策可能会授权建立执行架构，这一架构包括违反政策的行为及相应的具体惩戒措施[52]。

---

[50] 应该组建最佳的项目管理架构以适应项目的目标以及机构的运行和风险环境。计算机安全项目架构的主要内容涉及到安全相关资源的管理和协调、同各方面的交流、传递重要信息、与各方平衡的能力以及要求上层管理人员采取行动的能力。

[51] 在设定责任的过程中，需要具体化；诸如“计算机安全是所有人员的责任”之类的设定在实际环境中等于没有任何人担负具体责任。

[52] 在涉及到对个人的惩罚和训诫措施的问题时需要征求法律顾问的意见。政策无需重申法律中已包含的惩罚措施，当然，如果政策还做为培养意识或进行培训的文件，也可以将其列入政策之中。

制定执行政策的时侯应该考虑到部分违反政策的人是无意的。例如，他们没有遵守政策是因为缺乏了解或培训。

5.2 专题政策

项目政策涉及到整个机构范围的计算机安全项目，而专题政策是针对目前机构关心（有时候还是有争议的）的某个领域制定的。例如，机构可能发现需要发布关于制定应急计划（集中式或非集中式）或使用特定技术对系统进行风险管理的政策。例如，还可以发布关于在机构中如何正确使用新兴技术的政策。当产生新问题的时侯，也可以发布相关政策，比方说有新的保护特定信息的法律开始施行的时侯。项目政策一般比较广泛，不需要时常修改，而专题政策在技术或相关因素发生变化时可能需要修改，所以其修改频率比较高。

通常，专题和针对系统的政策的发布者是高级管理人员，政策的范围越广泛、内容越具争议性或其实施越消耗资源，那么其发布者的级别就越高。

出现新的技术和新的威胁的时侯通常都需要制定相关的专题政策。

5.2.1 有关专题政策的例子[53]

有关专题政策的领域有很多。下面介绍两个例子：

互联网接入 许多机构将互联网视为延伸其研究机会和进行通信的方法。毫无疑问，连接互联网有很多好处但是也有一些缺点。所发布的互联网接入政策涉及到谁将使用接入、何种类型的系统连接在网络上、何种类型的信息在网络中传输、连接互联网系统的用户认证需求以及防火墙和安全网关的使用。

电子邮件政策 电子邮件系统的用户依靠此服务与同事或其他人进行信息通信。但是，由于系统通常由雇佣机构所有，有时管理者可能会出于各种原因（如确定其仅用于工作目的或其是否被用于传播病毒、发送攻击性邮件或泄漏机构的秘密）希望监控员工的电子邮件。另一方面，用户可能会有需要尊重其隐私的要求，就像对美国邮政的要求那样。这个领域的政策所涉及到的隐私级别根据电子邮件及其环境的不同有所不同，有些可以查阅有些则不行。

其它可能的专题政策包括：风险管理和应急计划的方法、保护机密 / 专有信息、非受权软件、软件的获取、在家中使用计算机工作、将磁盘带出工作场所、访问其他员工的文件、文件和电子邮件的加密、隐私权利、数据正确性的责任、受到怀疑的有害代码、物理紧急情况。

5.2.2 专题政策的基本部件

与项目政策类似，专题政策也可以分为几个基本部件：

[53] 本节中所举的例子并不完全也不意味着所有的机构都需要这些政策。

专题描述 制定某一专题的政策，管理人必须定义专题所包含的相关含义、特性和条件。通常还需要设定政策的目标或理由，这也有利于政策的执行。例如，一个机构要制定一个关于“非官方”软件使用的专题政策，这种软件是指未经机构批准、审查或者不是机构购买、管理和拥有的软件。另外，相关的特性和环境也需要包含其中，例如员工个人拥有但是得到批准可用于工作的软件，以及其它业务单位拥有和使用并得到机构合同确认的软件。

机构立场的描述 一旦叙述完专题及其相关的含义和条件，就要在本节清晰地描述机构对此问题的立场（如管理层的决策）。继续前面的例子，这就意味着要描述在所有的或某些情况下禁止使用所定义的非官方软件，要描述是否有批准和使用方面的详细指导、或者是否可以批准例外情况以及谁来批准、基于什么规则。

适用性 专题政策还需要包括适用性的描述。就是说要清晰的表述特定政策应该在何处、何时、由谁、对谁、怎样施行。比如，前面提到的关于非官方软件的假想政策可以适用于机构本身站点中的资源和员工，但不包括其它办公场所的人员。另外，还需要澄清对于来往于不同站点和／或家中需要在多个站点传送和使用磁盘的员工的适用性。

角色和责任 专题政策通常也包括对角色和责任的设定。例如，如果允许员工私人拥有的非官方软件经过适当的批准在工作中使用，那么就应该描述这样的批准权限的授权情况（政策应该通过使用职位规定谁拥有此授权）。同样的，应该明确规定谁负责确保只有得到批准的软件才能够在机构的计算机资源中使用，或许还要监控用户使用非官方软件的情况。

有关政策的一些有用的提示

为了更加有效，政策需要可见性。可见性通过帮助确定政策在整个机构范围内的沟通来协助政策的实施。管理者的介绍、视频、小组讨论、嘉宾演讲、论坛解答以及通讯报道增加了可见性。机构的计算机安全培训和意识培养项目可以有效地告知用户新的政策。这也可以作为新员工熟悉机构政策的一种方式。

计算机安全政策的推广应该得到管理层的无条件支持，在员工感觉到各种政策、指令、指导和规程材料过于繁杂的时侯这些材料的推广尤其应该得到管理层的支持。机构的政策是强调管理层对计算机安全的许诺和清晰表达对员工的表现、行为和职责的期待的载体。

为了更加有效，政策应该与其它现存的指令、法律、机构文化、指导方针、规程以及机构的整体使命相一致。它还应该与机构的其它政策（如人事政策）相融合相协调。确保如此的一种办法就是在政策的制定过程中与机构的其他人员进行协调。

执行 对于某些类型的政策，可能需要详细的描述那些违反行为是不能允许的，以及这种行为的后果是什么。可能要明确描述惩罚措施并且应该与机构的人事政策和措施相一致。实施的时侯，应该与相关官员和工作人员进行协调，这可能还包括工会。最好能够设定一个特定人员来监督整个机构的实施情况。

联系点和补充信息 对于任何专题政策，应该指明机构适当的人员做为联络点以便获取进一步的信息、指导和执行。由于职位本身的变动比担任职位的人员的变

动要少，所以设定职位做为联系点更加合适。例如，对于某些专题来说，联系点可能是生产线管理人；对于另一些专题可能就是设施管理人、技术支持人员、系统管理员或安全项目代表。再一次引用上面的例子，员工需要知道提出问题和了解规程信息的联系点是否是其直接上级，还是系统管理员或计算机安全人员。

政策通常还有指导方针和规程的协助。例如，关于非官方软件的专题政策可能包括对员工带入的在其它地点使用过的磁盘进行检查的规程和指导方针。

5.3 针对系统的政策

项目政策和专题政策都涉及到比较宽泛的内容，通常涵盖整个机构。但是，它们所提供的信息或指导不够充分，如确定建立访问控制列表或培训用户应采取何种行动等方面。针对系统的政策填补了这个空白。由于只涉及到一种系统，所以其内容更加集中。

针对系统的政策包括两个部件：安全目标和安全的运行规则。政策通常由相应的规程和指导方针配合其执行。

安全目标举例

只有会计和人事部门的人员有权提供或修改工资处理中使用的信息。

许多安全政策的决策只涉及到系统级别，并且在同样的机构中不同的系统有不同的安全政策。虽然这些决策对于政策来说太过详细，但是它们却非常重要，对系统的使用和安全有着重大的影响。这些类型的决策可能由**行政管理人员**作出，而不能由系统的技术管理员作出（但是这些决策的影响经常由系统的[54]技术管理员进行分析）。

为了制定具有凝聚力和内容广泛的安全政策，可能需要使用管理手段将安全目标转化为安全规则。参考系统安全的两级模型可能对此有所帮助：安全目标和安全运行规则，它们组成了针对系统的政策。它们紧密相连通常难以区分，是政策的技术实施。

5.3.1 安全目标

管理手段的第一步是定义特定系统的安全目标。这一步骤开始于对完整性、可用性和机密性的分析，但是并不到此为止。安全**目标**需要更加具体；它应该被具体和正确地定义。还应该对其进行明确描述以便目标能够实现。这一手段也可应用于其它所需的机构政策。

安全目标包括一系列描述对具体资源所采取切实措施的陈述。这些目标应该基于系统的功能或使命的需要，还应该描述支持这些需要的安全行动。

制定针对系统的政策需要管理层进行取舍平衡，因为并不是所有所需的安全目标

[54] 重要的是要记住政策不是在真空中制定的。例如，理解系统的使命以及系统是如何被使用的是非常关键的。在制定政策时用户也可以扮演重要角色。

都能够被满足。管理层面临着费用、操作、技术和其它约束。

5.3.2 安全运行规则

在管理层完成对安全目标的设定之后，应该开始确定运行系统的规则，如定义受权和未受权的更改。谁（通过工作类别、在机构中的位置或名字确定）可以在怎样的条件下针对哪些数据类别或记录做什么（如修改、删除）。

具体所需的安全运行规则有多种多样。规则越详细，**在一定程度上**，当有人违反时就越容易被发现。**在一定程度上**，也就越容易自动执行政策。但是，过分详细的规则可能会使命令计算机实施规则的工作变得困难或计算起来很复杂。

安全运行规则举例

人事部职员可以每周对考勤字段进行更新、并负责年度缺勤、员工地址和电话号码的内容。人事部专门人员可以更新工资信息。员工都不能更新他们自己的记录。

另外，确定详细程度的时侯，管理者还应该考虑制定针对系统政策文档的正式程度。仍然是文档越正式，执行和遵循政策就越容易。另一方面，过分详细和正式的系统级政策也会增加管理负担。通常，在系统访问特权方面，建议最好使用比较正式和详细的说明。这样的访问控制政策（参见第10和17章，《人事 / 用户问题》和《逻辑访问控制》）使以后的遵循和执行更加容易。通常需要详细和正式说明的另一个领域是安全责任的设定。还有一个应该涉及到的领域是系统使用的规则和违反政策的后果方面。

其它计算机安全领域的政策决策，如本章所描述的那些内容通常记录在风险分析、审批意见或规程手册中。但是，任何有争议的、非典型的或不一般的政策还需要正式的说明。非典型的政策包括任何与机构政策或机构通常做法不一致的系统政策，无论其更严厉或更宽松。通常政策的文档会说明本政策与机构标准政策不同的原因。

5.3.3 针对系统的政策实施

技术在执行针对系统的政策中扮演了重要的角色，但它并不是唯一的角色。当使用技术来执行政策时，重要的是不要忽略非技术的手段。例如，基于技术系统的控制可以被用于限制对特定打印机打印机密报告。但是，相应的物理控制手段也应该被用于限制对打印机输出的访问，否则预定的安全目标将无法达成。

技术手段经常被用于执行如**逻辑访问控制**之类的系统安全政策。但是，还有其它一些自动化手段来执行或支持补充逻辑访问控制的安全政策。例如，可以使用技术手段防止电话用户呼叫特定的号码。入侵探测软件可以警告系统管理员发生了可疑活动或采取措施制止这一活动。个人计算机可以被设置为禁止从软盘启动。

系统安全政策基于技术的执行既有优点也有缺点。虽然没有计算机可以强迫用户遵循所有的规程，但是正确设计、编程、安装、设置和管理的[55]计算机系统可以在计算机系统中始终如一地执行政策。管理控制也扮演重要的角色不应被忽略。另外，有时候违反政策的行为是需要也是可行的，这种违反对于一些技术性控制来说可能难以实施。如果安全政策过于严格这种情况就会经常发生（当系统分析员无法预期紧急情况并做好相关的应急准备时就会发生）。

5.4 相互关系

政策与本手册涵盖的多个主题有关：

项目管理 政策是用来建立机构计算机安全项目的，所以它与项目管理和监督紧密相连。项目和针对系统的政策都可以在本手册涵盖的任何领域中被确立。例如，机构可能想要在所有系统的事件处理中采取一致的方法，那么机构就可以发布相关的项目政策来完成这一任务。另一方面，机构可能需要应用之间具有充分的独立性，这样应用管理人就可以独立地进行事件处理了。

访问控制 针对系统的政策通常通过使用访问控制来实施。例如，机构中只能有两个人有权运行支票打印程序可能是一项政策决策。系统使用访问控制来实施（执行）这样政策。

与更宽泛的机构政策相联系 本章重点描述了计算机安全政策的类型和部件。但是重要的是需要明白，**计算机**安全政策通常是机构处理其它种类（如书面文件）信息的**信息**安全政策的**延伸**。例如，机构的电子邮件政策可能与其更宽泛的隐私权政策相连系。计算机安全政策还可能是其它政策的延伸，如关于正确使用设备和设施方面的。

5.5 费用考虑

潜在费用的数额与制定和实施计算机安全政策相关。总体上，政策的主要费用是实施政策的费用以及其对机构的影响。例如，建立计算机安全项目、使用政策完成项目，这是一笔可观的费用。

其它费用可以是政策制定过程中发生的。起草、审查、协调、完成、分发和公布政策需要大量的监督和管理工作。在许多机构中，政策的成功实施可能需要额外的人员和培训以及耗费大量的时间。通常，机构制定和实施计算机安全政策的费用依赖于达到管理层可以接受的风险级别所需要进行改变的程度。

[55] 遗憾的是，正确的完成这些工作通常是极其困难的。系统执行系统政策能力的可信度与保证密切相关（参见第9章《保证》）。

参考书目

1992年十月15日于马里兰州巴尔的摩发表的《第15届国家计算机安全会议论文集》中第244至251页Howe, D.的文章“信息系统安全工程：通向未来的基石”。

1993年Van Nostrand Reinhold出版社于纽约州纽约出版的《信息系统安全：实用参考手册》中第411至427页Fites, P.,和M. Kratz的文章“政策的制定”。

1986年McGraw-Hill出版社于纽约州纽约出版的《阻止系统入侵者》中第57至95页Lobel, J.的文章“建立系统安全政策”。

1992年出版的《计算机和安全》杂志11（3）中第211至215页Menkus, B.的文章“关注计算机安全”。

1987年美国国会技术评估办公室于华盛顿特区发表的《保护秘密的共享数据：电子信息的新锁》中第151至160页技术评估办公室的文章“联邦政策和选择”。

1987年美国国会技术评估办公室于华盛顿特区发表的《保护秘密的共享数据：电子信息的新锁》中第131至148页技术评估办公室的文章“政策制定的主要趋势”。

1992年出版的《ISSA访问》杂志5（4）中第14至17页O'Neill, M.和F. Henninge, Jr.的文章《理解ADP系统和网络的安全》。

1993年出版的《信息安全新闻》杂志4（2）中第30至31页Peltier, Thomas的文章“设计有效的信息安全政策”。

1988年一月改善管理总统委员会于华盛顿特区发表的改善管理总统委员会以及正直和效率总统委员会合著的《自动化信息系统管理控制的模型框架》。

1993年出版的《ACM通信》杂志36（12）中第104页至120页Smith, J.的文章“隐私政策和措施：深入机构的迷宫”。

1991年五月于加利福尼亚州奥克兰发表的《1991年IEEE安全和隐私年会论文集》中第219至230页Sterne, D. F.的文章“时髦用语：‘计算机安全政策’”。

1992年四月发表的《信息安全的DATAPRO报告》中Wood, Charles Cresson的文章“设计公司的信息安全政策”。

第六章

计算机安全的项目管理

计算机及其处理的信息对于许多公司完成其使命和业务功能是至关重要的[56]。因此高级管理人员通常将计算机安全视为管理问题，他们像保护其它任何有价资产那样寻求对机构计算机资源的保护。为了有效地进行保护就需要制定广泛全面的管理措施。

本章介绍整个机构范围的计算机安全措施并讨论其重要的管理功能。由于[57]机构的规模、复杂程度、管理风格和文化各不相同，不可能描述出一种理想的计算机安全项目。但是本章还是描述了一些对于许多联邦机构都通用的特性和问题。

OMB的A-130规章《联邦信息资源的管理》要求联邦机构建立计算机安全项目。

6.1 计算机安全项目的架构

许多计算机安全项目被分配给整个机构中执行不同职能的不同部门来完成。这种方法有其优点，但是许多机构中计算机安全职能的分配是随意的，通常是基于历史原因（如机构在有工作需要时正好可以使用的人）。理想的情况是，计算机安全职能的分配应该有计划地按照整体的管理思路进行。

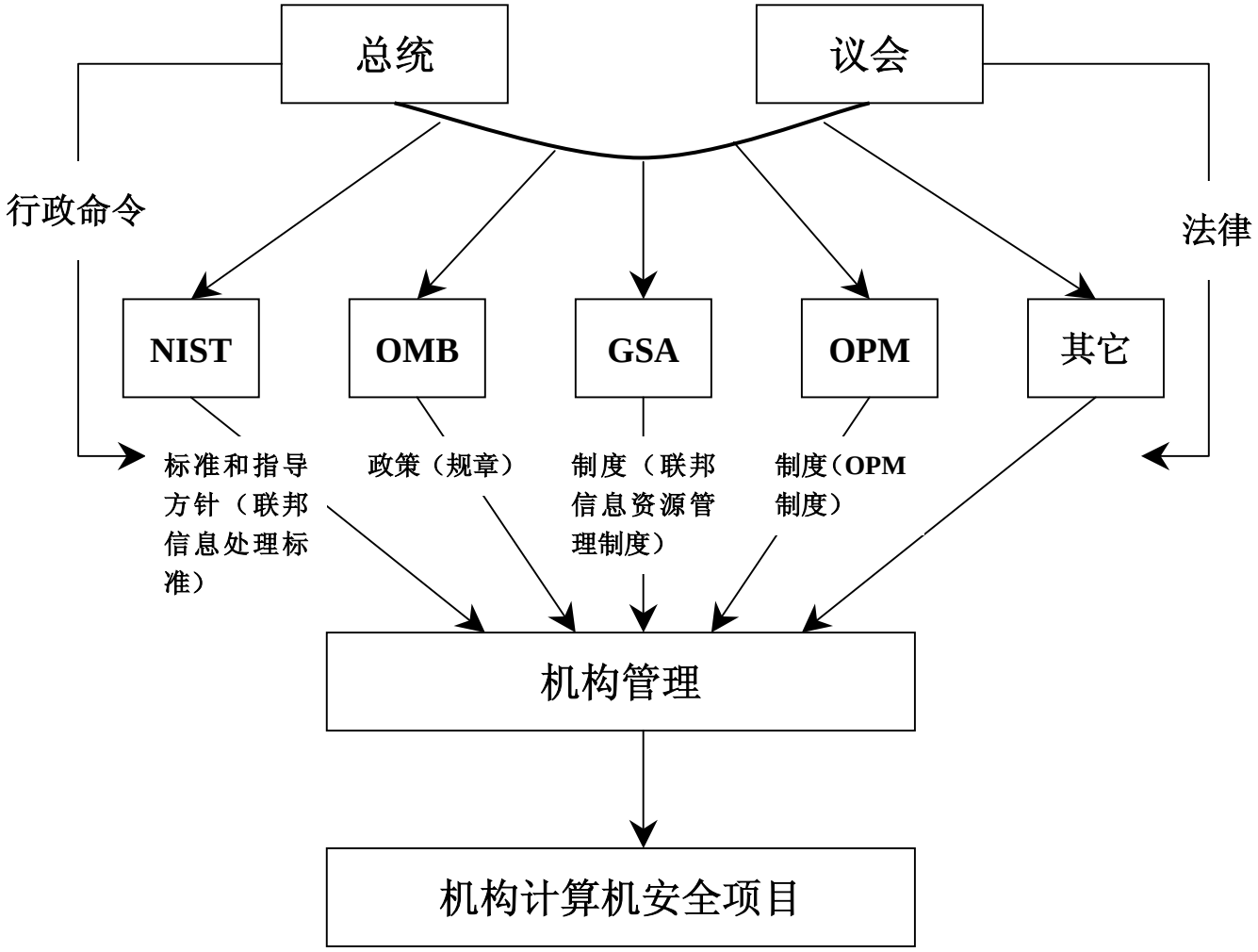
在多个层次进行计算机安全管理能够带来很多好处。每一个层次都能够为整体计算机安全项目提供不同的专门技术、权力和资源。通常，级别越高的官员（如上面所述的部门机构或机构总部的官员）对机构整体的了解越全面其权力也越大。另一方面，官员的级别越低（在计算机设施和应用级的官员）对具体需求就越熟悉，其中包括技术的和规程的需求，也包括系统和用户的问题。计算机安全项目管理的各级别应该互为补充，互相帮助会提高效率。

因为许多机构至少有两个计算机安全管理级别，所以本章将计算机安全管理分为两级：核心级和系统级（当然，每个机构可以有自己独特的架构）。核心级计算机安全项目可以被用于处理机构整体的或机构主要部分的计算机安全管理。系统级计算机安全项目处理特定系统的计算机安全管理。

[56] 本章主要针对联邦机构，这些通常是非常庞大和复杂的机构。本章讨论适合于在这样的环境中进行安全管理的项目。它们可能根本不适合小型机构或私营企业。

[57] 本章涉及到安全项目管理，但是不涉及诸如风险分析员制定应急计划这样构成有效安全项目的各种活动。

联邦非保密计算机安全项目的（部分）需求来源



在联邦机构计算机安全项目的产生和运行环境中有着于比其它机构更丰富的指导方针和指南。图 **6.1** 描绘了一些关于机构处理计算机安全问题的管理需求和指导方针的外部来源。对这些内容逐一进行全面的论述超出了本章的范围，但是重要的是必须理解项目不是在真空中运行的；联邦机构在许多方面受到条列和规章的约束。

图 6.1

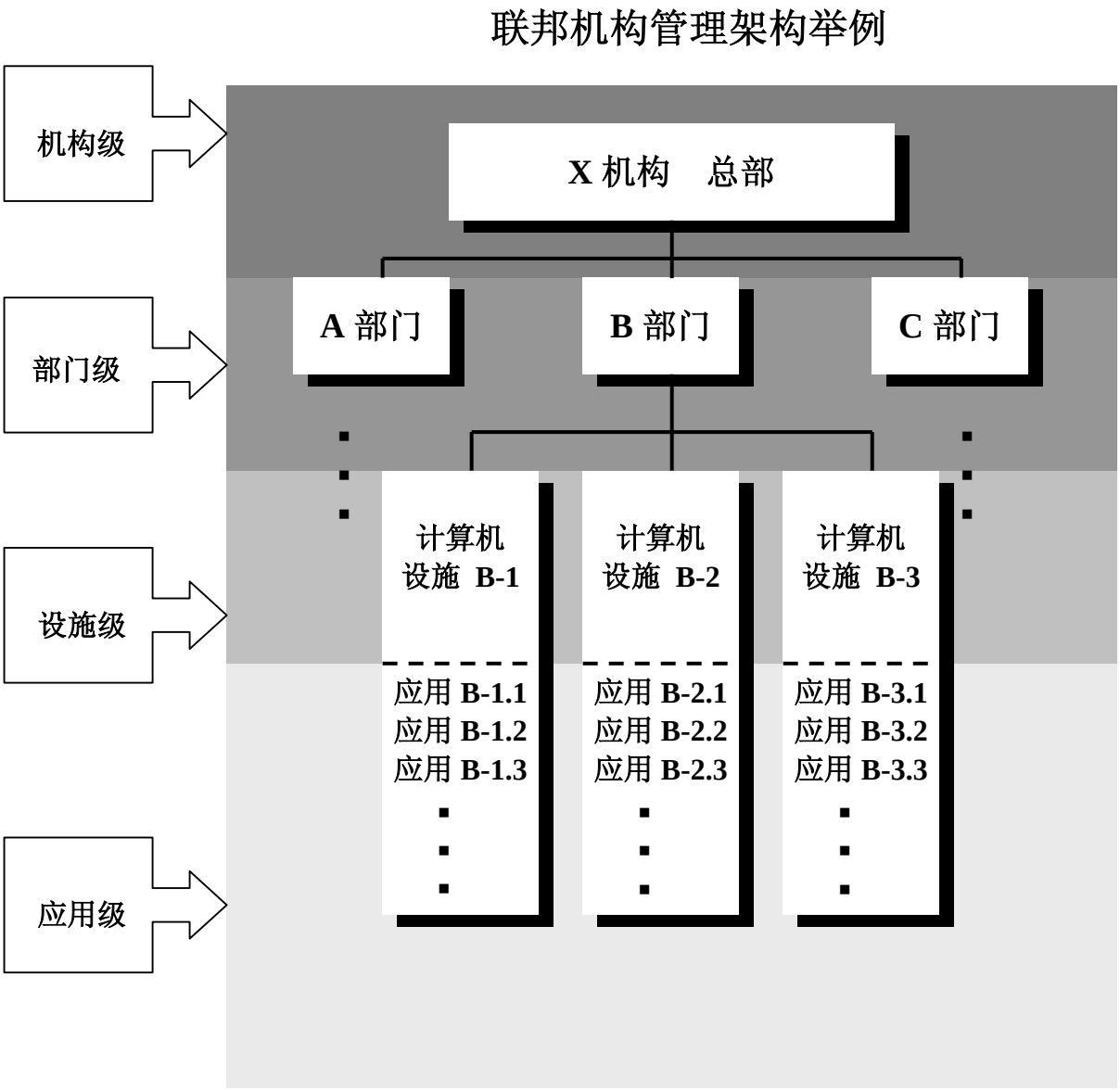


图 6.2 显示了一个基于真实联邦机构的管理架构。机构包含三个主要的部门，每一个部门有若干个运行多个应用的大型计算机设施。这种类型的机构需要在机构级、部门级、计算机设施级和应用级管理计算机安全。

图 6.2

6.2 核心级计算机安全项目

核心级计算机安全项目的目的是处理机构内整体的计算机安全管理。在联邦政府中，机构通常包括部、局或其它重要运行单位。

与所有的资源管理一样，可以使用多种手段和具有成本效益的方式来进行核心级计算机安全管理。良好管理的重要性是怎么强调也不过分的。对计算机安全项目的核心级管理也具有向下的趋势。特别应该引起注意的是，这造成了决策失误在整个机构中广泛传递的巨大风险。管理者在努力达成其目标时，需要考虑建立计

算机安全项目的所有可能选择的全面影响。

6.2.1 核心计算机安全项目的益处

核心安全项目应该提供两种不同类型的益处：

- 提高整个机构中的安全效率和经济性，以及
- 提供集中式的执行和监督能力。

这两种益处都是为了执行OMB的A-130规章并保持与《文书简化法案》的目的相一致。

《文书简化法案》为机构以更有效率、更有效和更经济的方式进行其信息管理活动确立了广泛而基本的要求。无论是维护内部还是商业的系统[58]，机构都应该确保所有机构自动化信息系统的充分安全性。

6.2.2 信息有效性和经济性的协调

核心计算机安全项目帮助对整个机构中安全相关资源的有效使用进行协调和管理。这些资源中最重要的通常是**信息**和**金融资源**。

管理者需要良好和及时的信息以便有效完成其任务。但是，多数机构难以做到在金字塔式的资源架构中收集和有效处理信息并在机构中对信息进行分发。本节讨论计算机安全信息的一些来源和有效使用的问题。

在联邦政府中，诸如管理和预算办公室、总务管理局、国家标准和技术学会以及国家电信和信息管理局等很多机构提供计算机、电信或信息资源的信息。这些信息包括安全相关的政策、法规、标准和指导方针。每个机构的高级特派官员（参见联邦信息资源管理规章［FIRMR］201－2节）做为一部分信息的导入途径。机构应该具有将高级特派官员接收的信息进行分配的机制。

计算机安全相关的信息也可以从私营和联邦专业社团和组织得到。这些组织经常做为公共服务机构提供信息，当然也有一些私人组织提供付费信息。但是，既使是免费或便宜的信息，其信息收集人员的相关费用也可能很高。

内部的安全相关信息，如哪些规程是有效的、病毒的感染、安全问题和解决方案需要在机构中分享。通常，这些信息是针对机构的运行环境和企业文化的。

在机构级别进行管理的计算机安全项目为在整个机构范围内收集内部安全相关信息和根据需要对其进行分配提供了一种途径。有时机构也可以与外部组织分享这些信息。参加图6.3。

[58] OMB的A-130规章第5节；附录III，第3节。

部分主要安全项目的交互关系

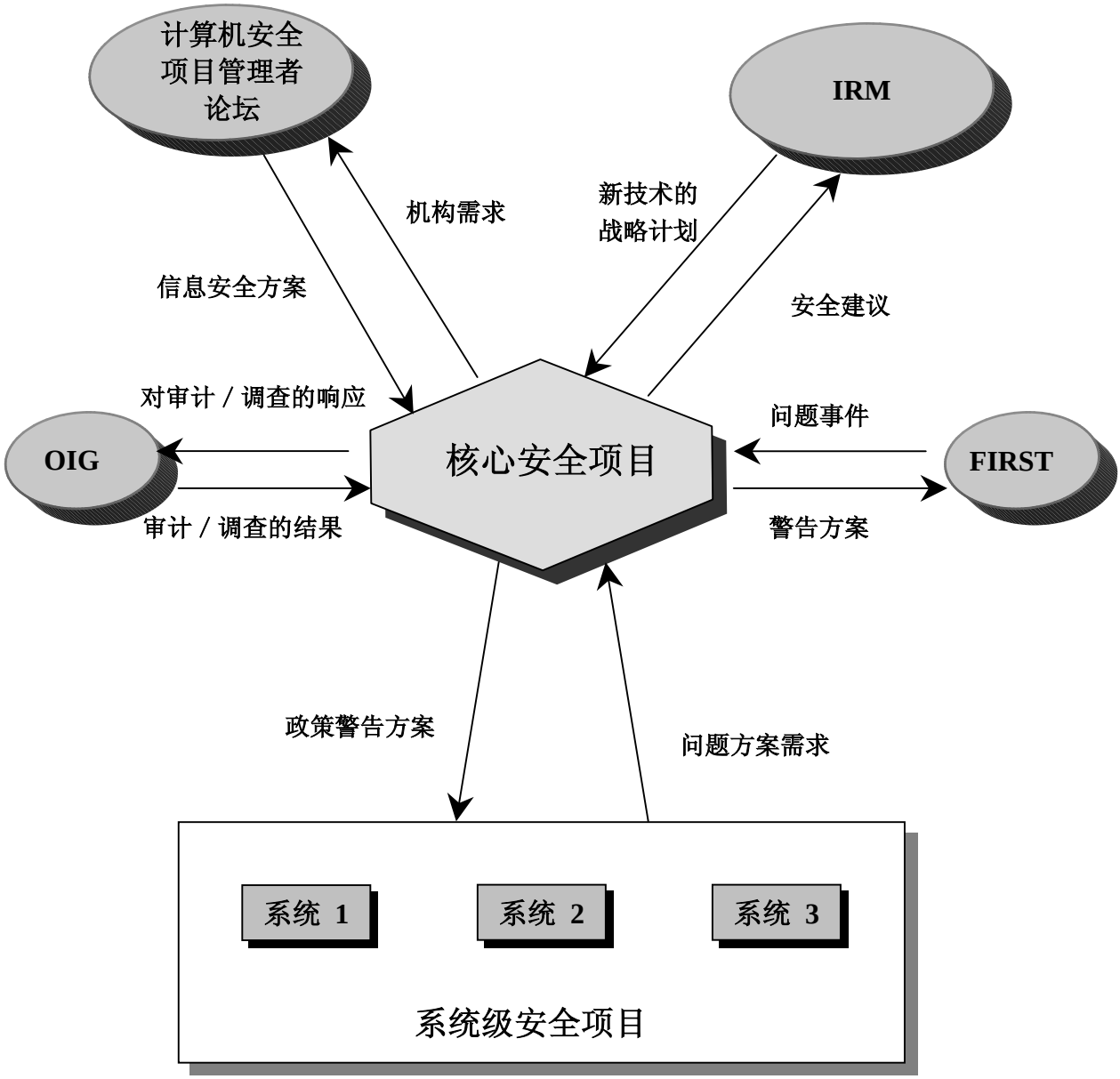


图 6.3 显示了机构中各部分之间以及跨机构的计算机安全相关信息流程图的简化版

图 6.3

有效导入信息的另一种方法是增强核心计算机安全项目影响外部和内部决策的能力。如果核心计算机安全项目人员能够体现整个机构的利益，那么其建议就更能够引起上层管理人员和外部机构的关注。但是，要有效地做到这一点，系统级计算机安全项目和机构级计算机安全项目之间就应该有很好的沟通。例如，如果一个机构考虑将其大型机整合到一个站点（或考虑将现在一个站点中的处理分布出去），核心项目的人员就可以对其所牵涉到的安全问题提出初步意见。但是，要想使其意见更具权威性，核心项目人员就要实际了解将要进行的系统级计算机安全项目预计进行的信息更改将会带来的安全影响。

除了能够帮助机构更经济有效地使用信息，计算机安全项目还能够帮助机构更好地使用本来就不多的安全经费。机构可以开发专门技术然后进行分享以减少重复为同一服务签订合同的需要。核心计算机安全项目可以协助进行信息分享。

位于核心计算机安全项目层次上的人员也可以开发他们自己领域的专门技术。例如，他们可以加强自己在应急计划和风险分析方面的技巧以协助整个机构完成其重要的安全任务。

除了允许机构分享专门技术以节约金钱以外，核心计算机安全项目可以利用其所处的地位整合需求以便机构可以基于对安全硬件和软件的批量采购来协商优惠折扣率。它还可以协助诸如战略计划、整个机构范围的事件处理和安全趋势分析等活动。

6.2.3 集中的执行和监督

除了协助机构提高计算机安全项目的经济效益和其效率，核心项目还可以包含独立的评估或执行职能以确保机构的分支单位更经济有效地保护资源和遵循既定政策。虽然总检查长办公室和诸如总审计局等外部机构也执行有效的评估职能，但是他们处于常规的管理通道之外。第8和9章进一步讨论独立审计的内容。有多种理由需要在常规的管理管道中设立监督职能。首先，计算机安全是机构资源管理的重要部分。这是一项无法转嫁或放弃的责任。其次，进行有效的监督可以使机构在避免遭到IG或GAO审计或调查这样可能会导致尴尬处境的前提下发现和解决问题。第三，机构可能发现外部机构无法发现的问题。机构比外部机构更了解其资产、威胁、系统和规程；人们与内部人员合作时更坦白。

6.3 有效的核心级计算机安全项目的要素

为了使核心计算机安全项目发挥效用，应该将其做为机构管理的一部分。如果系统管理者和应用拥有者不需要与安全项目始终如一地相结合，那么它就会变成上层管理者“许诺安全”的华而不实的装饰。

稳定的项目管理职能 制定良好的项目都有一个做为核心级计算机安全项目经理的整个机构公认的项目管理人。项目应该拥有称职的人员，并且应该在项目管理职能与机构其它部门的计算机安全人员之间建立联系。计算机安全项目是一项复杂的职能，需要一个稳定的基础以便指挥对信息和经费等安全资源的管理。如果计算机安全项目在机构中没有给与适当的专家和授权支持，监督职能的优势就不

能有效地发挥。

稳定的资源基础 制定良好的项目都有稳定的人员、经费和其它支持的资源基础。没有稳定的资源基础，就没有可能有效的制定和执行计划和项目。

政策的存在 政策为核心级计算机安全项目提供了基础，是记录和发布重要的计算机安全决策的手段。核心级计算机安全项目还应该公布协助政策执行和扩展政策的标准、规章和指导方针（参加第5章）。

所发布的使命和职能描述 所公布的使命描述为核心计算机安全项目融入机构具体的运行环境提供了基础。这些描述明确地确定了计算机安全项目的职能并且定义了计算机安全项目以及其它相关项目和实体的责任。没有这些描述，就无法制定评估项目有效性的标准。

举例

机构的IRM部门根据《文书简化法案》和OMB的A-130规章的要求参与信息和信息技术的战略和战术规划。安全应该成为这些计划的重要部分。机构的安全需要应该反映在信息技术的选择上，机构的信息需要应该反映在安全项目上。

长期的计算机安全战略 建立适当的项目以便对长期战略进行探索和研究有助于将计算机安全综合到下一代信息技术中去。由于计算机和电信领域发展迅猛，所以对未来的运行环境作出规划是非常重要的。

遵守法规的计划 核心级计算机安全项目需要涉及到对国家政策和需求以及机构特定的需求的遵循。国家需求包括那些1987年计算机安全法案、OMB的A-130规章、FIRMR和联邦信息处理标准所规定的内容。

机构内部的联系 机构中的许多人员能够影响到计算机安全。信息资源管理机构和物理安全人员是两个明显的例子。但是，计算机安全的职能经常与这些人员重叠，如人员安全、可靠性和质量保证、内部控制或总检查长办公室。有效的项目应该与这些团体建立关系以便将计算机安全整合到机构的管理中。这些关系不仅包括分享信息，而且包括人员之间的相互影响。

与外部团体的联系 有很多计算机安全信息的来源，如NIST的计算机安全项目管理人论坛、计算机安全信息交换站以及事件响应和安全团队论坛（FIRST）。所建立的项目应该对外部信息源有所了解并且善加利用。它还可以是信息的提供者。

6.4 系统级计算机安全项目

核心级项目涉及到整个机构范围内的计算机安全，而系统级项目是确保每个系统具有适当和具有成本效益的安全性[59]。这包括对实施何种控制、采购和安装技术性控制、日常计算机安全管理、评估系统缺陷和对安全问题的响应等具有影响力的决策。它包括了手册中所讨论的所有领域。

系统级计算机安全项目人员是计算机安全的本地拥护者。系统安全经理／官员与管辖相关系统的管理人一起提出安全问题并协助制定安全问题的解决方案。例如，应用拥有者是否明确定义了系统的安全需求？新的功能的使用是否会影响安全，如果会，那么是怎样影响的？系统是否容易受到黑客和病毒的攻击？应急计划是否通过了测试？提出这些问题将迫使系统管理人和应用拥有者确定和解决其安全需求。

6.5 有效的系统级项目的要素

正如核心级计算机安全项目一样，许多因素也影响着系统级计算机安全项目的成功与否。这些因素大多与核心项目的类似。本节涉及到一些额外的考虑。

安全计划 计算机安全法案要求机构制定敏感系统的计算机安全和隐私计划。这些计划确保每一个联邦和对联邦重要的系统都具有适当的和有成本效益的安全性。系统级安全人员应该能够制定和实施安全计划。第8章更详细地讨论了计划。

系统特定的安全政策 许多计算机安全政策需要涉及到特定系统的问题。不同的系统有不同的问题，但是访问控制和指定负责安全的人员大概对于每一个系统都是需要的。可以使用由安全目标导出安全规则的过程来制定始终如一和广泛全面的安全政策，这一内容在第5章有所论述。

生存周期管理 如第8章讨论的那样，在整个生命周期中都必须进行安全管理。这特别包括在对系统的更改时确保其对安全的影响得到了关注并且完成了适当的审批手续。

集成到系统运行中 系统级计算机安全项目应该包括了解系统、系统的使命、技术和运行环境的人。有效的安全管理通常需要集成到系统管理中去。有效的集成将确保系统管理人和应用拥有者在计划和运行系统时将安全问题考虑进去。系统安全管理人／官员应该能够参与到选择和实施适当的技术性控制和安全规程的过程中并且了解系统的弱点。系统级计算机安全项目还应该具有对安全问题进行及时响应的能力。

对于大型系统，如大型机数据中心，安全项目经常包括如访问控制、用户管理和

[59] 正如其名称所示，机构一般都会有多个系统级计算机安全项目。在建立这些项目的过程中，机构应该仔细检查每个系统级项目的范围。系统级计算机安全项目可能涉及到如运行部门中的计算机资源、重要的应用或一组类似的系统（技术性的或职能性的）。

应急与灾难计划的管理人和职员。对于小系统，如办公室范围的局域网（LAN），这个LAN的管理员可能会兼有安全责任。

与运行相分离 计算机安全和运行部门之间经常存在固有的紧张关系。在许多场合中，运行部门要变得越来越大也就越来越有影响力，就通过将计算机安全项目并入计算机运行部门来寻求解决这种紧张关系。这种机构战略的典型结果就是计算机安全项目缺乏独立性、缺乏权威、很少引起管理层的注意并且缺少资源。早在1978年，GAO就确认这种机构模式是联邦计算机安全项目的首要的基本弱点[60]。系统级项目常常遇到这个问题。

这种做为系统管理一部分的需求与独立性的需求之间的冲突可以有多种解决方案。许多解决方案的基础是在计算机安全项目和上层管理之间的联系，这种联系经常是通过核心级计算机安全项目建立起来的。建立这种联系的关键是要确立一个不包含系统管理的汇报体系。另一种可能是计算机安全项目完全独立于系统管理并直接向高层管理汇报。还有很多混合以及不同的方式，如计算机安全和系统管理人员在一起工作但是将其汇报（和监管）体系分开。图6.4显示了一个典型的联邦机构中计算机安全项目位置的**例子**[61]。

6.6 核心级和系统级项目的相互作用

系统级项目要是不集成到机构级项目中就难以对机构重要领域的安全性产生影响。系统级计算机安全项目执行核心级计算机安全项目的政策、指导方针和规定。系统级的人员也通过核心项目发布的信息进行学习并利用整个机构的经验和专用资源。如果需要，系统级计算机安全项目进一步向系统管理提供信息。

但是，交流不能是单向的。系统级计算机安全项目将其需求、问题、事件和方案通知核心人员。对这些信息的分析可以使核心级计算机安全项目体现机构管理和外部机构的各种系统并且使项目和政策更有利于所有系统的安全。

6.7 相互关系

计算机安全项目的主要目标是提高安全性，这个目标造成了它与其它机构运作以及手册中讨论的其它安全控制相互交叉重叠在一起。核心级或系统级安全项目将涉及到政策、规程或操作层面上的多数控制。

政策 政策被发布用来建立计算机安全项目。核心级计算机安全项目通常所提出的政策是关于一般性和机构性的安全问题的，并且它还经常提出专题政策。但是，系统级计算机安全项目通常提出系统的政策。第5章提供了额外的指导。

[60] 1978 年审计总署于华盛顿特区发表的GAO报告LCD 78-123《自动化系统的安全－联邦机构应该加强对个人和其它敏感数据的保护》。

[61] 这并不意味着本体系机构是理想的。

计算机安全职能在机构中的位置举例

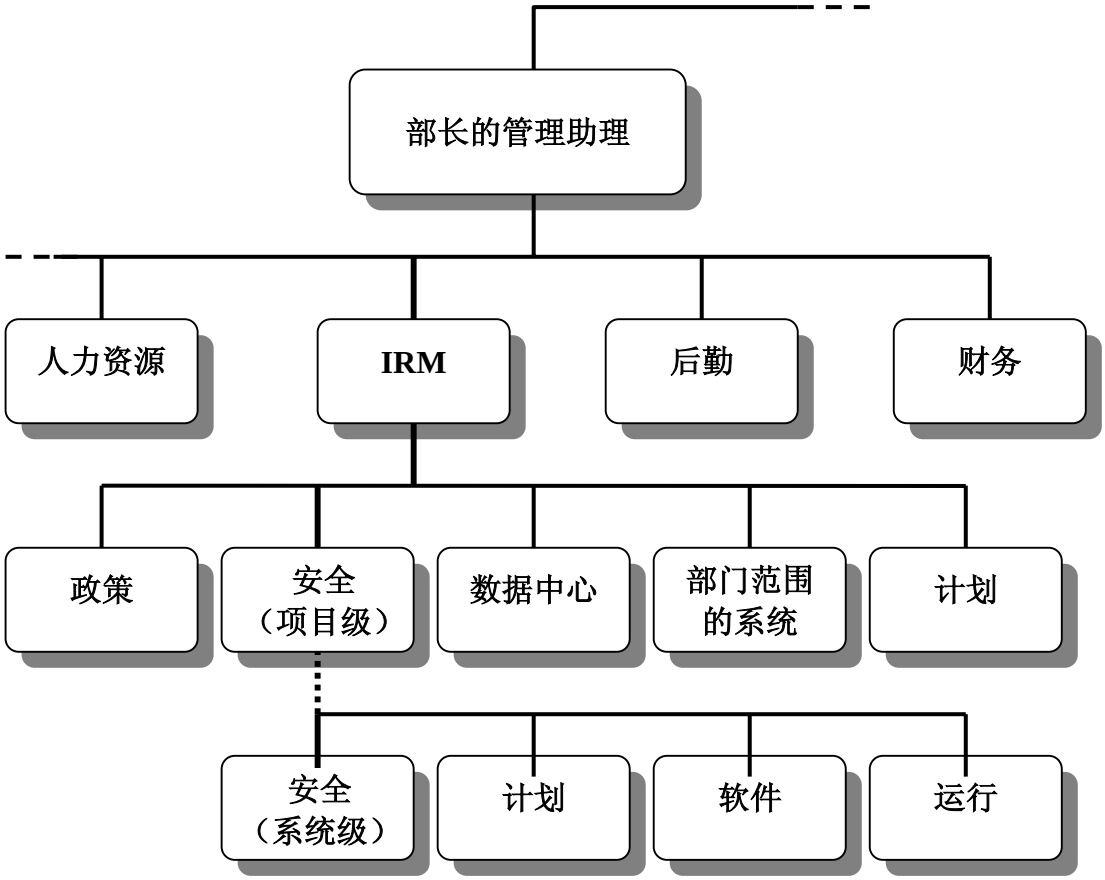


图 6.4 举例描绘了计算机安全的项目级和系统级职能的位置。项目级职能位于 IRM 机构中为整个机构制定政策。系统级职能位于数据中心中，为该站点提供日常安全服务。注意，虽然没有画出，还是存在其它设施（如在另一个部长助理之下）的系统级项目。

图 6.4

生命周期管理 在整个生命周期中对系统进行保护是系统级计算机安全项目的任务。第8章涉及到这些问题。

独立审计 第8和9章所描述的独立审计职能是对核心级计算机安全项目的执行职能的补充。

6.8 费用考虑

本章讨论了机构范围内的计算机安全项目可以如何更有效地管理安全资源，包括金融资源的问题。系统级计算机安全项目的费用考虑与安全对整体费用节省的贡献是一致的。

计算机安全项目的最直接的费用就是人员的费用。另外，许多项目频繁地使用顾问和承包人。项目还需要培训、差旅、监督、信息收集和分发方面以及与不同级别的计算机安全管理人员进行会面的费用。

参考书目

总务管理局于华盛顿特区发表的《联邦信息资源管理规定》，特别是201-2。

1978年总审计署于华盛顿特区发表的GAO报告LCD78-123《自动化系统的安全：联邦机构应该加强对个人和其它敏感数据的保护》。

总务管理局于华盛顿特区发表的《信息资源的安全：联邦管理人究竟需要知道哪些？》。

1989年国家标准和技术学会于马里兰州盖瑟斯堡发表的Helsing, C.、M. Swanson和M. Todd合著的特别报告书500-169《保护信息资源的执行指南》。

1989年国家标准和技术学会于马里兰州盖瑟斯堡发表的Helsing, C.、M. Swanson和M. Todd合著的特别报告书500-170《保护信息资源的管理指南》。

计算机安全学院于加利福尼亚州旧金山开办的课程《管理机构广泛的安全项目》。

1990年管理和预算办公室于华盛顿特区发表的OMB公告90-08《为含有敏感信息的联邦计算机系统进行安全计划准备的指导》。

管理和预算办公室的OMB A-130规章《 联邦信息资源的管理》。

1992年于马里兰州巴尔的摩发表的《第15届国家计算机安全会议论文集》中第584至592页Owen, R., Jr的文章“安全管理：使用质量方法”。

1993年出版的《信息世界》杂志15（52）第49页Spiegel, L.的文章“良好的LAN安全需要对全体数据的分析”。

1988年美国国会发布的公法100-235《1987年计算机安全法案》。

第七章

计算机安全风险管理

风险就是不利事件发生的可能性。风险管理是评估风险、采取步骤将风险消减到可接受的水平并且维持这一风险级别的过程。也许大家没有意识到，其实大家每天都在进行风险管理。像系安全带、预报有雨时带伞或将事情记录下来以免遗忘，这些日常活动都可以归入风险管理的范畴。人们会意识到针对其利益的各种威胁，并采取预防措施进行防范或将其影响减到最小。

政府和企业日常的风险管理是金字塔型的。例如，为了将投资回报最大化，决定是采用高速增长型（但是高风险）还是采用低速增长型（但是更安全）的投资计划是常见的商业决策。这些决策需要对风险、相应的潜在收益、对其它选择的考虑进行分析，最终实施管理层决定采取的最佳行动。

> 管理层关注多种类型的风险。计算机安全风险管理与机构使用信息技术而产生的风险有关。

虽然有很多风险管理的模型和方法，但是有几种基本的活动和方法是应该普遍应用的。在讨论风险管理的过程中，重要的是要认可一个最基本的假设：计算机不可能绝对安全。总是有风险存在，无论这种风险是由受到信任的员工欺诈系统造成的，还是火灾摧毁关键资源造成的。风险管理由两个主要的和一个基础的活动构成；风险评估和风险消减是主要活动，而不确定性分析是基础活动。

7.1 风险评估

风险评估是分析和解释风险的过程，包括三项基本活动：（1）确定评估的范围和方法；（2）收集和分析数据；以及（3）解释风险分析的结果[62]。

> 风险分析经常会有重要的附带好处——在风险分析试图指出系统和职能是如何相互影响时，对系统和机构有了更深一步了解。

7.1.1 确定评估的范围和方法

评估风险的第一步是确定所要考虑的系统，要对该系统的哪一部分进行分析，以及分析的详细和正式程度以及相应的分析方法。

评估应该集中于风险程度未知或已知但风险较高的特定领域。系统不同部分其分析的详细程度也不同。范围和界限的定义可以帮助确保进行有成本效益的评估。对范围产生影响的因素包括系统处于生命周期的何种阶段：对于新开发系统的分析可能要比对已存在将升级系统的分析更详细。另一个因素是所检查系统的相对

[62] 有许多不同的术语被用来描述风险管理及其要素。本文所使用的定义基于NIST的风险管理框架。

重要性：越是重要的系统越要进行全面的风险分析。第三个因素可能是自从最近一次风险分析以来所发生的变化的数量和类型。增加新的接口和安装新的操作系统涉及到不同的分析范围。

方法可以是正式的或非正式的、详尽的或简洁的、高级的或低级的、定量的（基于计算值）或定性的（基于描述或分级）、或多种方法的综合。不存在适用于所有用户和环境的最佳方法。

> 风险评估可以集中于许多不同的领域如：针对设计用于新应用的技术和运行控制、针对电信的使用、数据中心或整个机构。

边界、范围和方法的定义会对（1）风险管理所需的总体工作量和（2）评估结果的类型和用处等多个方面产生重要影响。确定边界和范围的方式应该能够在详细分析的前提下，对相关系统和环境作出明确、具体和有用结果的判断。

7.1.2 收集和分析数据

风险有许多不同的部件：资产、威胁、缺陷、安全措施、后果、可能性。风险分析通常包括对受威胁领域有关数据进行收集，**并**对这些信息进行综合分析使其更有用处。

由于存在收集到的信息比分析所需还要多的可能性，所以应该采取措施对信息的收集和分析进行限制。这个过程被称为**过滤**。风险管理工作应该集中于对机构影响最大的领域（如造成严重伤害的）。这可以通过对威胁和资产进行分级来实现。

> 对风险分析的良好记录将节省以后在风险分析上所花费的时间，如果发生了什么问题，它将帮助解释特定安全决策的原因。

风险管理方法不要求对每个部件进行单独分析。例如资产 / 影响或威胁 / 可能性可以一起分析。

资产估值 这包括信息、软件、人员、硬件和物理资产（如计算机设施）。资产的价值包含其固有价值以及对其破坏造成的近期冲击和长期影响。

影响评估 影响评估评价可能造成的损害或损失的程度。**影响**是指所发生的整体、总体的损害，而不仅仅是近期或立即的冲击。这些影响通常造成的是关闭、更改、毁坏或拒绝服务，影响是更严重和长期的如失去业务、无法完成系统使命、失去信誉、侵害隐私、造成生命的伤害或损失。威胁的影响越严重，对系统（结果就是对机构）的风险就越大。

威胁识别 威胁是对系统有潜在伤害的实体或事件。典型的威胁是错误、欺诈、心怀不满的员工、火灾、水害、黑客和病毒。应该对威胁进行识别和分析以确定其发生的可能性和对资产的潜在损害。

另外对于“大宗”威胁，风险分析应该对了解不够、新的或未记录的领域进行调

查。如果一个设施的物理风险控制系统通过了严格测试，对其进行威胁识别所花费的精力就可以少于对那些不明确和未经测试的软件备份规程进行的识别。

风险分析应该集中于最可能发生的和影响重要资产的威胁。在某些情况下，在威胁分析开始前无法确定哪些威胁是真实的。第4章提供了当今最普遍威胁的更多讨论。

安全措施分析 安全措施是用于减少受威胁系统缺陷的任何行动、设备、规程、技术或其它方法。安全措施分析应该包括对现有安全方法的有效性检查。也可以是确定可部署在系统中的新安全措施，但这通常是在风险管理的后期进行。

缺陷分析 缺陷是存在于安全规程、技术性控制、物理控制或其它控制中的，可以被威胁所利用的条件或弱点。存在缺陷往往是因为缺少安全措施。缺陷引起风险是因为它们可能“允许”威胁损害系统。

风险分析的结果

风险分析的结果通常被表现为定量的和/或定性的。定量的方法会使用预期金钱损失的降低来表现，如年度损失预期或所发生的单次损失。定性的方法是描述性的，使用高、中、低或者1到10级的分级方式来表现。

缺陷、威胁和资产的相互关系对于风险分析来说是至关重要的。图7.1描绘了一些这样的相互关系。但是还有其它类型的关系存在，如呈现一个缺陷来引诱威胁。（例如，可能会让一个平时表现不错的员工看到一个未退出的无人终端来诱使其修改数据。）

可能性分析 可能性是对于威胁发生的频率或机会的评价。可能性评估关注威胁的存在、持续性和强度，以及安全措施的有效性（或缺陷的存在）。威胁的历史信息通常是很缺乏的，特别是人类造成的威胁；所以这方面的经验很重要。一些威胁数据——特别是如火灾或洪水等物理威胁——是很充足的。在使用威胁统计数据时要小心；数据的来源或对其的分析有可能不正确或不完整。通常，威胁发生的可能性越大，风险也就越大。

7.1.3 解释风险分析的结果[63]

风险评估被用来支持两个相关的功能：对风险的接受和对有成本效益控制的选择。为了完成这些功能，风险评估必须要得出有意义的结果，这些结果要能够反映出什么是对机构真正重要的。将风险的解释活动限制在重大的风险上是风险管理过程集中于减少整体风险而又获得有用结果的另一种方式。

如果风险在整个机构中能够得到一致的解释，这个结果就可以被用于对受保护的系统排定优先顺序。

[63] NIST风险管理框架将分析解释视为风险措施。选择“解释”这一术语强调了风险评估可能有各种各样的结果。

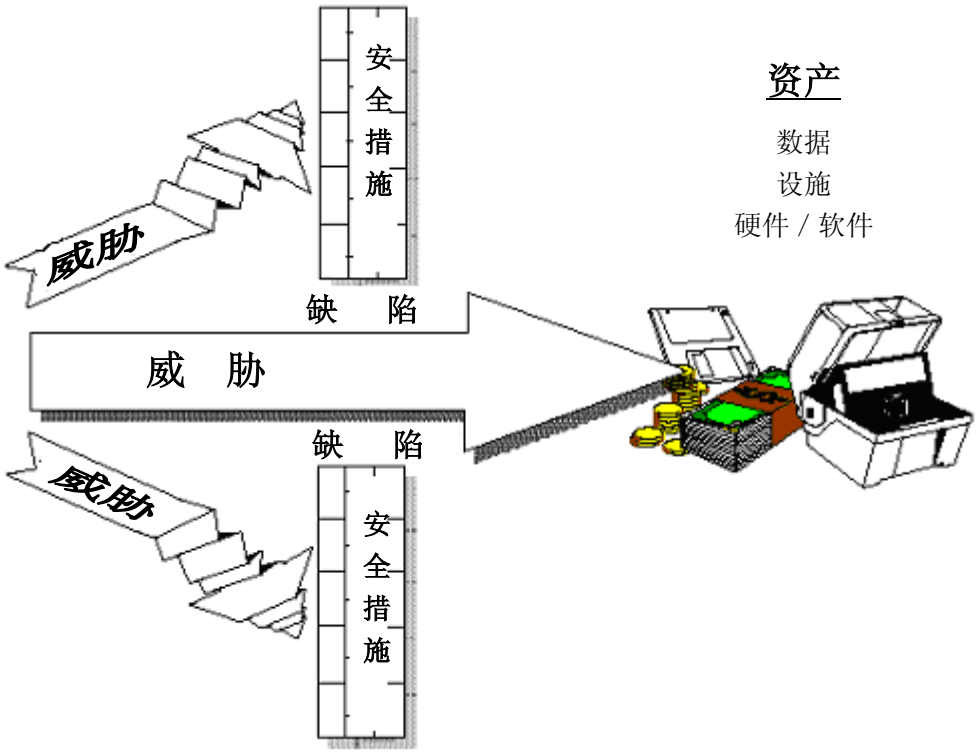


图 7.1 防止威胁损害资产的安全措施。如果没有适当的安全措施，威胁就可以利用存在的缺陷，因此就对资产构成了风险。

图 7.1

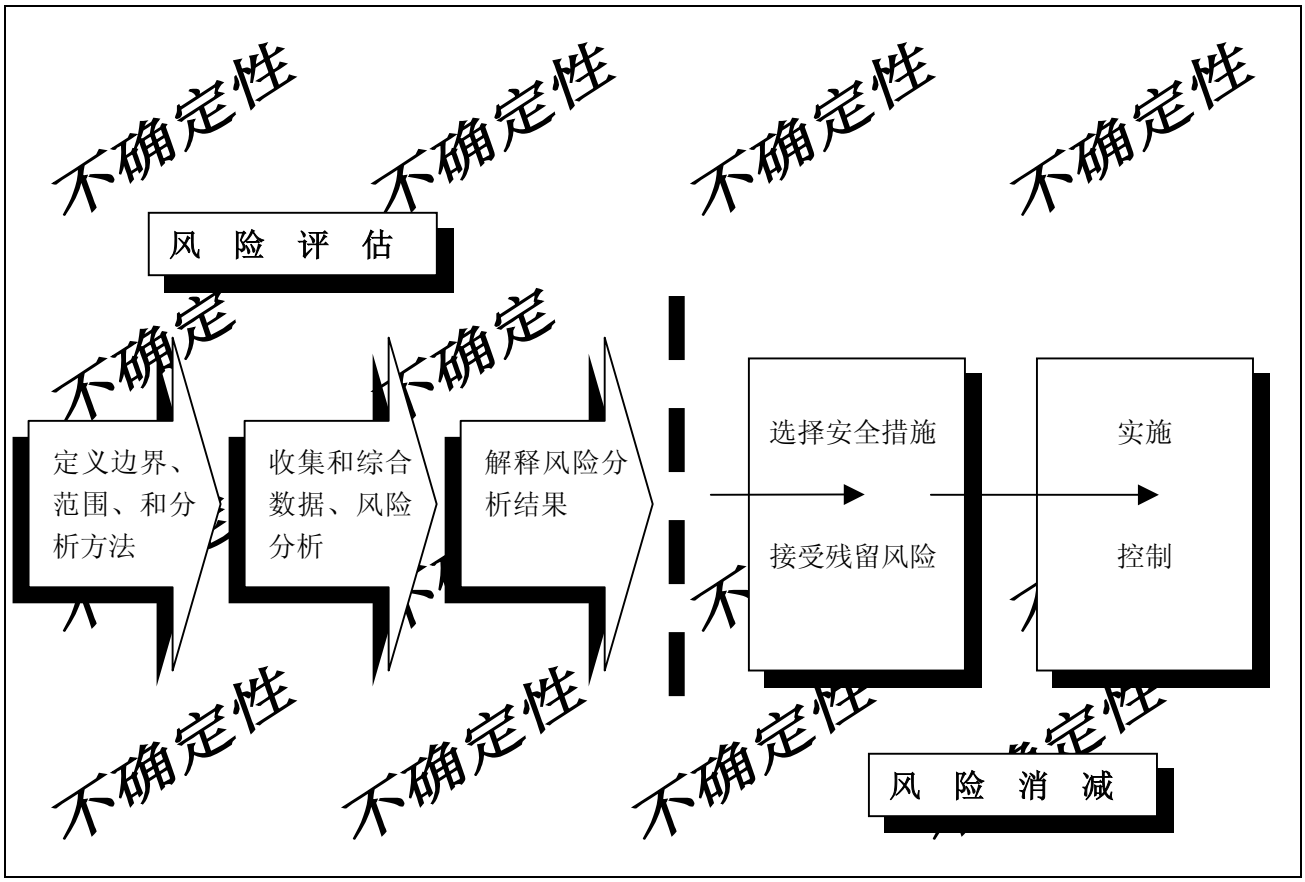
7.2 风险消减

风险消减涉及到在现有的约束条件下，为了将风险降低到管理者可以接受的水平而进行的安全控制的选择和部署。虽然执行风险评估的方式是灵活的，但是确定边界、分析信息和得出结论是非常基本的顺序。风险消减的过程具有更大的灵活性，顺序也各不相同，这取决于机构的文化和风险管理活动的目的。虽然按照特定的顺序讨论这些活动，但是不需要按照这样的顺序执行。尤其是安全措施的选择和风险接受测试可能可以同时

风险管理可以帮助管理者选择最适当的控制，但它不是瞬间解决一切难题的魔棒。结果的质量取决于分析所使用信息和所使用方法的质量。在某些情况下，获得用于分析的高质量信息所要完成的工作会造成极高的成本。在有些情况下就无法获得用于分析的高质量信息，特别是具体威胁的流行情况或所推荐的安全措施的有效性这样的参数。在任何情况下，完全的信息是都是无法得到的，总是有不确定的因素。虽然有这些障碍，风险管理还是为分析计算机系统相关的风险提供了强大的工具

进行[64]。

风险管理是如何工作的



- **安全措施的选择有很多可能的方法。有一些涉及到循环和重复检查风险分析数据。**

图 7.2 显示了风险管理活动和过程的流程。风险评估和风险消减之间是风险管理的重要分界线（如虚线所示）。两边都是风险管理过程的重要部分。总是存在不确定性

图 7.2

[64] 这通常被视为循环的、反复的过程。

7.2.1 选择安全措施

计算机安全风险管理的主要职能是确定适当的控制。在设计（或检查）系统安全的过程中，添加某些控制的理由（如有法律要求或因为具有明显的成本效益）是很明显的。有时理由虽然明显但是费用却很昂贵（既有金钱方面的因素也有非金钱方面的因素）。例如，对于管理者来说，将某个包含局域网设备的房间门关上并落锁是明显需要的控制，但是在门口安排一个警卫可能就太昂贵和不友好了。

在每一次风险评估中，都会存在许多领域不知道使用什么控制为好。即使只考虑金钱问题，如控制的成本是否比要防范的损失更大，控制的选择不是一项简单的事情。但是，在选择适当的控制过程中，管理者应该考虑以下因素：

- 机构的政策、法规和制度；
- 人员安全、可靠性和质量需求；
- 系统性能需求；
- 技术性、正确性和完全性需求；
- 安全措施的生命周期成本；
- 技术性需求；以及
- 文化约束。

什么是假设性问题分析法？

假设性问题分析法观察各种控制组合的成本和收益来确定对于具体环境的最佳组合。下面是个简单的例子（仅涉及到一个控制），假如黑客的入侵引起机构计算机安全人员对使用口令安全风险的警惕。他们就可能考虑用更强大的识别和认证机制来更换掉口令系统，或者只是加强其口令规程。首先是检查**现状**。现有的系统对用户和系统管理员的要求最少，而机构在过去的六个月有三次黑客入侵。

如果加强口令会怎样？需要人们更频繁地更换口令或使用长口令或在口令中使用非字母字符。没有直接的金钱花费，不过会增加人员的管理工作（如培训和更换遗忘的口令）。估计这种方法可以将黑客的成功入侵数量减少到每年三到四次。

如果使用更强大的识别和认证技术会怎样？机构可能想要部署基于加密的一次性口令这种更强大的安全措施，这样即使口令被截获也没有什么利用价值。直接成本估计是$45,000，每年重复发生的费用是$8,000。需要的初始培训费用$17,500。机构估计这样可以防范所有的入侵。计算机安全人员使用这个分析结果来得出给管理人员的建议，管理人员衡量成本和效益以及其它约束条件（如预算）后选择解决方案。

安全措施的一种选择方法是假设性问题分析法。使用这种方法对增加各种安全措施的效果进行测试，以观察每种措施对成本、效力和其它相关因素，如上面提到的那些因素的不同影响。还应该在这些因素之间进行平衡调整。平衡调整工作还包括下面讨论的对残留风险的接受。这种方法通常涉及到进行多次风险分析，以观察所推荐的变化是如何影响风险分析结果的。

另外一种方法是对安全措施进行分类，并推荐其部署的风险级别。例如，可以将强大的控制部署在高风险的系统上而不是低风险的系统上。这种方法通常不需要反复进行风险分析。

从其它风险管理的观点来说，可以使用过滤来将精力集中于高风险的领域。例如，可以集中于会产生严重后果的风险，如高额的金钱损失或生命损失或经常发生的

威胁。

7.2.2 接受残留风险

从某些角度来看，管理层需要决定计算机系统在给定类型和程度的剩余风险中运行是否是可接受的。许多管理者不完全了解基于计算机的风险有几个原因：（1）这些风险与以前遇到的机构或功能相关风险在类型上不同；（2）这些风险可能是技术性的，对于个人来说难以理解，或者（3）计算能力的增长和非集中化使得很难确定处于风险中的关键资产。

风险的接受正如安全措施的选择一样应该考虑到风险评估所涉及到的各种因素。另外，风险的接受还应该考虑到风险评估的局限性（参见以下关于不确定性的章节）。风险的接受与安全措施相关，因为在某些情况下，由于安全措施过于昂贵（由于金钱或非金钱因素）所以不得不接受风险。

在联邦政府中，风险的接受与被授权使用计算机系统是密切相关的，通常被称为**审批**，将在第8和9章讨论。审批是管理层通过对系统投入或保持运行的正式批准而接受风险。正如在本章早些时候讨论的那样，风险管理的两个主要功能之一是出于接受风险目的的风险解释。

7.2.3 实施控制和监视有效性

仅选择正确的安全措施还没有降低风险；需要有效地实施这些安全措施。此外，为了使其持续有效，风险管理应该是一个不间断进行的过程。这需要定期评估和改进安全措施和重新进行风险分析。第8章讨论了如何将定期的风险评估融入整体的系统管理之中。（此内容参见59页的图表。）

风险管理过程通常生成用于设计、采购、构建或以别的方式获取安全措施或实施系统更改时的安全需求。在第8章讨论将风险管理融入生命周期过程的问题。

7.3 不确定性分析

风险管理经常必须依赖于推测、猜想、不完全的数据和许多未经证实的假设。不确定性分析试图记录这些内容以便更加明智地使用风险管理的结果。在风险管理过程中有两个主要的不确定性来源：（1）风险管理模型或方法缺乏可信度和或精确性，以及（2）缺乏足够的信息来确定风险模型要素的确切值，如威胁的频率、安全措施的效率或结果。

本章提出的风险管理框架是风险管理要素及其基本关系的一般性描述。要使方法具有实用性，还应该进一步细化这些关系并提供一些甄别信息的含义。在这个过程中，可能会作出未准确反映用户环境的假设。这种情况在安全措施的选择时尤其明显，这时资产、威胁和缺陷之间的多重关系会变得难以处理。

数据是另一个不确定性的来源。用于风险分析的数据一般有两个来源：统计数据和专家分析。统计数据和专家分析听起来会比实际上要权威。统计数据中有许多潜在的问题。例如，样本可能太小，影响数据的其它参数计算可能不正确，或者

使用误导的方式陈述结果。在许多情况下，可能没有足够的数据。当使用专家分析推测未来事件时，应该认识到推测是主观的，是基于专家所作出的（不总是明确的）假设。

7.4 相互关系

风险管理涉及到本手册的所有控制和所有章节。但是它与生命周期管理和安全计划过程的关系最紧密。进行风险管理的需求通常在机构政策中讨论并且是整个机构范围的话题。这些问题在第5和第6章讨论。

7.5 费用考虑

本章描述的风险管理构件可以被用于创建一种方法，该方法将昂贵的分析工作专注于最需要的领域。如果经常扩充范围并且内容繁琐，风险管理可能很快就变得昂贵起来。使用本章讨论的筛选技术是很重要的，这样可以减少整体工作量。在选择和制定方法时应该始终想着风险管理的目标。方法应该关注于风险的识别和所需的具有成本效益的防范措施的选择上。

不同方法的成本可能相差很大。“信封背面”分析或高－中－低分级通常可以提供所需的所有信息。但是，尤其在选择昂贵的防范措施或系统分析包含未知结果时，可能需要进行更深入的分析。

参考书目

Caelli, William, Dennis Longley, and Michael Shain. *Information Security Handbook*. New York, NY: Stockton Press, 1991.

Carroll, J.M. *Managing Risk: A Computer-Aided Strategy*. Boston, MA: Butterworths 1984.

Gilbert, Irene. *Guide for Selecting Automated Risk Analysis Tools*. Special Publication 500-174. Gaithersburg, MD: National Institute of Standards and Technology, October 1989.

Jaworski, Lisa. "Tandem Threat Scenarios: A Risk Assessment Approach." *Proceedings of the 16th National Computer Security Conference*, Baltimore, MD: Vol. 1, 1993. pp. 155-164.

Katzke, Stuart. "A Framework for Computer Security Risk Management." *8th Asia Pacific Information Systems Control Conference Proceedings*. EDP Auditors Association, Inc., Singapore, October 12-14, 1992.

Levine, M. "Audit Serve Security Evaluation Criteria." *Audit Vision*. 2(2), 1992. pp. 29-40.

National Bureau of Standards. *Guideline for Automatic Data Processing Risk Analysis*. Federal Information Processing Standard Publication 65. August 1979.

National Institute of Standards and Technology. *Guideline for the Analysis of Local Area Network Security*. Federal Information Processing Standard Publication 191. November 1994.

O'Neill, M., and F. Henninge, Jr., "Understanding ADP System and Network Security Considerations and Risk Analysis." *ISSA Access*. 5(4), 1992. pp. 14-17.

Proceedings, 4th International Computer Security Risk Management Model Builders Workshop. University of Maryland, National Institute of Standards and Technology, College Park, MD, August 6-8, 1991.

Proceedings, 3rd International Computer Security Risk Management Model Builders Workshop, Los Alamos National Laboratory, National Institute of Standards and Technology, National Computer Security Center, Santa Fe, New Mexico, August 21-23, 1990.

Proceedings, 1989 Computer Security Risk Management Model Builders Workshop, AIT Corporation, Communications Security Establishment, National Computer Security Center, National Institute of Standards and Technology, Ottawa, Canada, June 20-22, 1989.

Proceedings, 1988 Computer Security Risk Management Model Builders Workshop, Martin Marietta, National Bureau of Standards, National Computer Security Center, Denver, Colorado, May 24-26, 1988.

Spiegel, L. "Good LAN Security Requires Analysis of Corporate Data." *Infoworld*. 15(52), 1993. p. 49.

Wood, C. "Building Security Into Your System Reduces the Risk of a Breach." *LAN Times*. 10(3), 1993. p. 47.

Wood C., et al., *Computer Security: A Comprehensive Controls Checklist*. New York, NY: John Wiley & Sons, 1987.

第八章

计算机系统生命周期中的安全和计划

如信息处理系统的其它方面一样，如果安全的计划和管理工作贯穿于整个计算机系统生命周期中从最初的计划到设计、实施和运行以至废弃[65]的全过程，那么它将是最有效和最有效率的。生命周期中会发生很多安全相关事件和分析工作。本章介绍它们之间的关系，以及如何将其整合在一起[66]。还要讨论安全计划在帮助确保安全问题得到完全处理中的重要作用。

本章考察：

- 系统安全计划，
- 计算机系统生命周期的组件，
- 将安全整合到计算机系统生命周期中的好处，以及
- 处理生命周期中安全问题的技术。

8.1 联邦系统有关计算机安全法案的相关问题

计划用于协助确保安全问题在整个生命周期中得到完全的处理。对于联邦系统，1987年计算机安全法案对所有敏感系统[67]的计算机安全计划的准备提出了法定需求。法案的本意和精神是改善联邦政府的计算机安全状况，而不仅仅是增加文案工作。为了达成这种意图，行政管理与预算局（OMB）和NIST负责指导机构的计划过程，并强调计算机安全计划和管理在机构和每一个计算机系统中的重要性。正如本章强调的那样，计算机**安全**管理应该做为计算机**系统**管理的一部分。拥有专门的计算机安全计划的好处是确保不会忽视计算机安全。

法案要求将计划提交给NIST和国家安全局（NSA）以便对所完成的工作进行检查和评价。实施法案的当前指导方针要求机构将其计算机安全计划交付独立检查。根据机构的情况，这种检查可以是内部的或外部的。

> “计算机安全计划的目的是提供安全的基本概况和目标系统的特定需求，以及机构满足这些需求的计划。系统安全计划也可以被视为制定系统充分和具有成本效益的安全保护过程的结构化文档。”
>
> - OMB 公告 90-08

[65] 计算机系统是指执行功能的过程、硬件和软件的集合。这包括应用程序、网络和支持系统。

[66] 虽然本章涉及的生命周期过程始于系统创始阶段，但是该过程可以起始于生命周期的任何时刻。

[67] 通常机构会有很多计算机安全计划。但是无需每个物理系统（如PC）都有专门的计划。计划可能涉及诸如运行单元中的计算资源、主要应用，或一组类似（技术的或功能方面）的系统等。

“典型的”计划简要描述系统重要的安全考虑事项，并提供更详尽文档如系统安全计划、应急计划、培训计划、审批意见、事件处理计划或审计结果的索引。这样就可以使计划在无需重复已有文件的条件下做为管理工具使用。对于较小的系统，计划可能包含所有的安全文档。与其它的安全文档一样，如果计划涉及到可能破坏系统的具体缺陷或其它信息，它就应该是保密的。它还应该保持更新状态。

8.2 将安全集成到计算机系统生命周期中的益处

在系统生命周期中很多人可以提供安全输入数据，包括审批官员、数据用户、系统用户和系统技术人员。

虽然可以在系统生命周期的任何时刻制定计算机安全计划，但是建议在计算机系统生命周期的开始阶段制定计划。安全与计算机系统的其它方面一样，对整个计算机系统生命周期各阶段都进行计划是最好的管理方式。计算机界长期以来认同的原则就是，系统设计完成后在其中增加特性比在系统初始的设计阶段包含该特性要多花费十倍的时间。在系统开发期间进行安全部署主要是因为在其后部署更困难（通常这样做的成本更高）。它还很可能打断系统的持续运行。安全也需要融入到计算机系统生命周期的后期，以协助确保安全能够跟得上系统环境、技术、规程和人员的变化。它还确保在系统升级时考虑到安全问题，包括采购新的部件或设计新的模块时。在安全入侵、灾难或审计后对系统增加新的安全控制会造成无计划的安全实施，这种实施比一开始就将安全集成到系统中要更昂贵和缺乏效率。它还会严重地降低系统的性能。当然，事先考虑到系统生命期中所有的问题实际上也是不可能的。所以，通常至少应该在生命周期每个阶段结束时，或每次重新审批后更新计算机安全计划。对于许多系统，可能需要更频繁地更新。

生命周期管理除了帮助确保管理活动在所有阶段都充分考虑到安全问题以外，还可以帮助记录安全相关决策。这种记录文档对于系统管理人员以及督察和独立审计人员是有用的。系统管理人员将文档用于自我检查和决策理由的提示，这样就可以更容易地对环境更改的影响进行评估。督察和独立审计人员在检查中使用文档来验证系统管理工作的充分性，并用来突出安全可能被忽视的领域。这包括检查文档是否正确地反映了系统的实际运行情况。

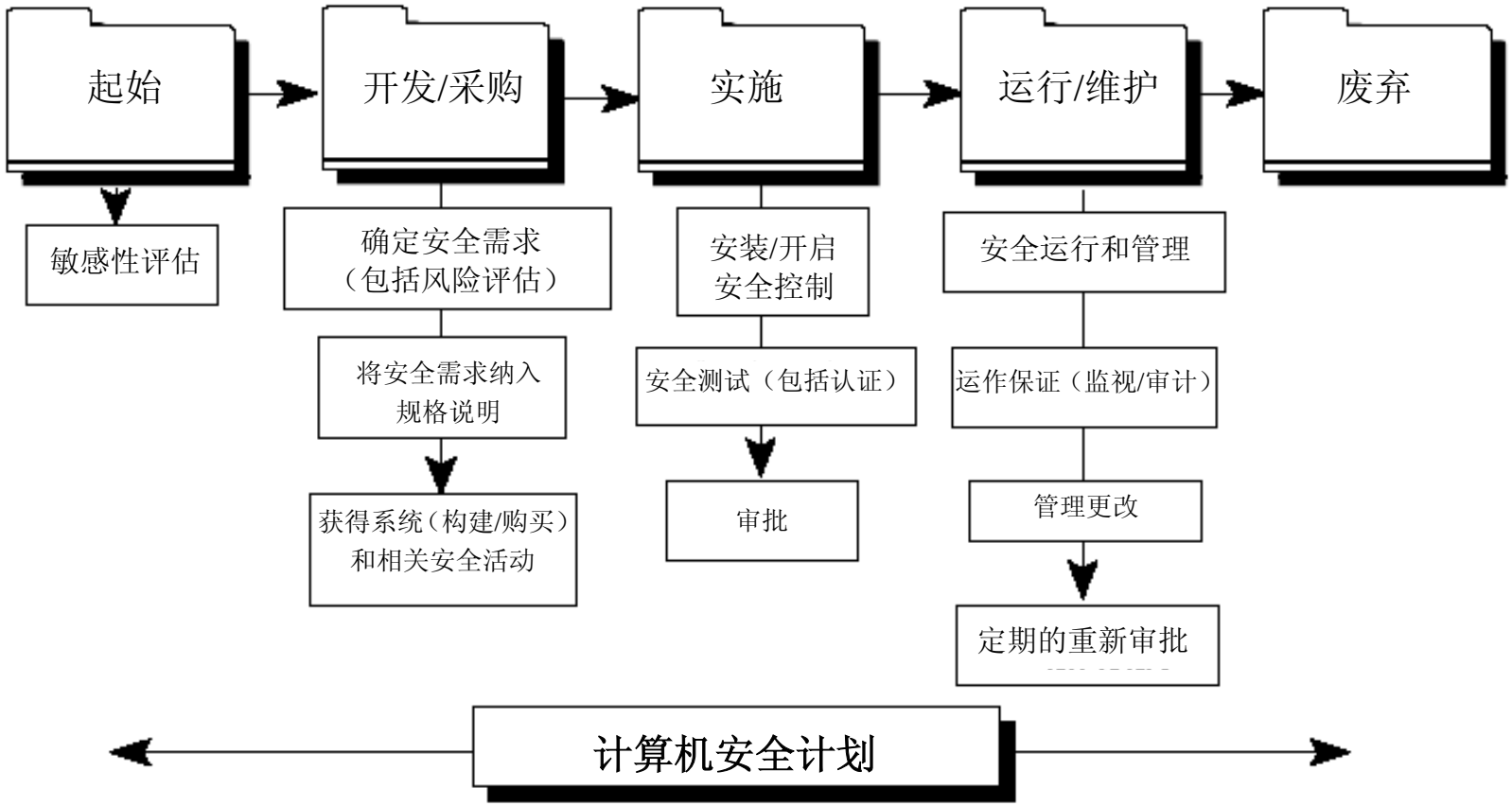
在联邦政府中，1987年计算机安全法案及其实施的指令提供了计算机安全计划的需求。这些计划是一种文档形式，它帮助确保不仅在系统设计和开发阶段，而且在生命周期的其它阶段考虑安全问题。计划也可被用于满足OMB A－130规章中附录III的需求，以及其它所涉及到的相关需求。

8.3 计算机系统生命周期概述

计算机系统生命周期模型有很多，但是大多包含图8.1中描绘的五个基本阶段。

- **起始** 在起始阶段，表述系统的需要并记录系统的目的。

系统生命周期中的安全



本章描述的生命周期过程包含五个不同的阶段。每个阶段都有安全问题。

图 8.1

- **开发/采购** 在这个阶段对系统进行设计、购买、编程、开发或其它形式的构建。这个阶段经常包含所定义的其它周期，如系统开发周期或采购周期。

- **实施** 在初期的系统测试后，系统被安装到位。

- **运行/维护** 在这个阶段系统执行其工作。几乎总是要对系统进行修改，增加硬件、软件或发生其它大量的事情。

- **废弃** 当完成向新计算机系统转移的工作后，计算机系统被废弃。

每个阶段都可以适用于整个系统、一个新的组件或模块，或一次系统升级。与系统管理的其它方面一样，这里描述的每一个活动的具体情况取决于许多因素，包括规模、复杂度、系统成本和敏感性。

与计算机系统有关的各种“生命周期”包括系统开发、采购和信息生命周期。

许多人发现计算机系统生命周期的概念令人迷惑，因为**整个**计算机系统生命周期的大框架下有很多周期。例如，一个机构可以使用系统**开发**生命周期开发一个系统。在系统生命中，机构可能使用**采购**生命周期购买新的组件。另外，计算机系统生命周期本身只是其它生命周期的一部分。例如，考虑一下**信息生命周期**。通常如人事数据之类信息的使用年限比一个计算机系统要长。如果一个员工为机构工作了三十年，并且还要工作二十年才能退休，该员工的自动化人事记录将可能经历公司拥有的很多不同的计算机管理系统。另外，一部分信息还会被用于其它计算机系统，如美国国内税局和美国社会保障总署的系统。

8.4 计算机系统生命周期中的安全活动[68]

本节考察计算机系统生命周期（参见图8.1）每个阶段发生的安全活动。

8.4.1 起始

确定系统概念和早期设计过程涉及到新系统需求的发现，或对现有系统的增强；系统特征的初期建议和所推荐的功能；关于体系结构、性能或功能系统方面的自由讨论会；以及环境、财政、政治或其它方面的约束。同时，系统**安全**方面的主要问题应该在系统设计早期一并予以考虑。这可以通过**敏感性**评估来进行。

8.4.1.1 进行敏感性评估

敏感性评估既考察所处理信息的敏感性，也考察系统本身的敏感性。评估应考虑法规要求、机构政策（如果是联邦系统则要包括联邦和机构的政策）、以及系统的功能需要。敏感性通常以完整性、可用性和机密性来表示。在评估敏感性时需要考察系统对机构使命的重要性，系统或数据的非受权更改、泄漏或无法使用的

[68] 鉴于篇幅和每个系统的独特性，这些讨论不可能包括各种具体的生命周期阶段的所有可能的安全活动的细节。

影响这类因素。为了处理这些问题，使用或拥有系统或信息的人应该参与评估。

敏感性评估应该回答以下问题：

- 系统处理什么信息？
- 数据或系统的错误、非受权泄漏、更改或无法使用会造成什么样的潜在损害？
- 影响安全的法律或法规（如隐私法案或公平贸易行为法案）有哪些？
- 系统或信息对于什么威胁特别脆弱？
- 是否有需要特别考虑的环境因素(如系统处于危险的位置)？
- 用户群体有什么安全相关的特点（如技术掌握和培训水平或安全许可证）？
- 适用于系统的安全标准、法规或指导方针有哪些？

敏感性的定义经常被人曲解。敏感性是**重要**或**贵重**的同义词。一些数据敏感是因为必须保持其机密性。但是更多的数据敏感是因为必须保证其完整性或可用性。计算机安全法案和OMB A-130规章明确地提出，如果其非受权泄漏、更改（也就是丧失完整性）或无法使用会伤害到机构那么信息就是敏感的。通常，系统对于机构的使命越是重要，它就越是敏感。

敏感性评估是安全分析的开始并贯穿于整个生命周期。评估协助确定项目是否需要特殊的安全督察，在决定开始系统开发前是否需要进一步的分析（以确保在合理成本上的可行性），或者在少数情况下，由于安全要求过于苛刻和昂贵以至于不能继续系统的开发或采购。敏感性评估可以被包括在系统起始的文档中，或者是其它计划文档的一部分。安全特性、规程以及下一章描述的保证的制定是基于敏感性评估的。

敏感性评估也可以在系统升级（可以是通过采购或者自主开发进行的升级）的计划阶段进行。在这种情况下，评估集中于受到影响的领域。如果升级很大程度上影响到原来的评估，可能就要分析它对系统其它领域的影响。例如，是否需要新的控制？有些控制是否变得没有必要？

8.4.2 开发/采购

对于大多数系统来说，开发/采购阶段比起始阶段更复杂。安全活动可以被分为三个部分：

- 确定安全特性、保证和运行措施；
- 将这些安全需求纳入设计规格说明；以及
- 实际获得这些内容。

这些内容适用于自主设计和构建的系统、购买的系统，以及使用混合模式开发的系统。

在这个阶段，技术人员和系统发起人应该经常在一起工作以确保技术设计反映系

统的安全需要。为了与其它系统需求协调一致，这个过程需要在技术人员和系统发起人之间进行开放式的对话。这对于在整个系统的开发过程中同步和有效地解决安全需求是很重要的。

8.4.2.1 确定安全需求

在开发/采购阶段的初期，系统计划者定义系统的需求。**安全需求应该与此同时制定**。可以使用技术特性（如访问控制）、保证（如对系统开发者的背景调查）或运行措施（如意识培养和培训）来体现这些需求。系统安全需求与其它系统需求一样，是从法律、政策、适用的标准和指导方针、系统的功能需要，以及成本效益的平衡取舍等方面导出的。

法律 除了涉及到信息安全需求的特定法律以外，诸如1974年隐私法案、法律案件、司法意见和其它类似的法律资料都可能直接或间接地影响到安全。

政策 如第5章论述的那样，管理官员发表不同类型的政策。系统安全需求经常由专题政策导出。

标准和指导方针 国际、国家和机构的标准和指导方针是确定安全特性、保证和运行措施的另一个来源。标准和指导方针经常以“如果…则”的形式（例如，如果系统对数据进行加密，则应该使用特定的加密算法）书写。许多机构设定了不同系统类型的基线控制，如行政的、任务或业务关键的、或专利的。根据需要，应该特别注意互操作性标准。

系统的功能需要 安全的目的是支持系统的功能，而不是破坏它。所以，系统功能的许多方面与安全需求有关。

成本效益分析 当涉及到安全时，成本效益分析是通过风险评估进行的，评估考察系统的资产、威胁和缺陷以便确定最合适和具有成本效益的防范措施（符合相关法律、政策、标准和系统功能需要）。适当的防范措施通常是收益高于成本的。收益和成本包括金钱或非金钱的，如所避免的损失、维护机构的声誉、降低用户友好性，或增加系统管理工作。

风险评估与成本效益分析一样是支持决策的。它帮助管理者选择具有成本效益的防范措施。风险评估的程度与其它成本效益分析一样，应该与系统的复杂度和费用指标以及**评估**的预期收益相当。分析评估在第7章有更详细论述。

风险评估可以在采购需求分析阶段或系统开发周期的设计阶段进行。通常也在系统升级的开发/采购阶段评估风险。依据项目的方法体系，可以进行一次或多次风险评估。

应该注意区分**安全**风险评估和**项目**风险评估的差别。许多系统开发和采购项目要分析无法成功完成项目的风险，这是与安全风险评估不同的活动。

8.4.2.2 将安全需求纳入规格说明

确定安全特性、保证和运行措施可以获得大量的安全信息以及通常是众多的需求。需要对这些信息进行确认、更新并将其整理为系统设计者或购买者使用的、详细的安全保护需求和规格说明。依据开发系统的方法体系不同，如全部或是部分采购成品系统，规格说明可以具有完全不同的形式。

早期制定测试规格说明对于安全特性的具有成本效益的测试是至关重要的。

在制定规格说明时，可能需要更新初始的风险评估。风险评估建议的防范措施可能与其它需求不兼容，或者控制措施难以实施。例如，安全需求禁止拨号访问可能阻止员工离开办公室后查看其电子邮件[69]。

除了系统的技术运行控制以外，还要涉及到保证。应该在早期确定所需的保证（以便安全特性和措施可以并且正确、有效地工作）程度。一旦确定了所需的保证级别，就有必要指明系统将得到怎样的测试和检查以便确定是否满足规格说明（以获得所需的保证）。这适用于系统开发和采购。例如，如果需要严格的保证，就需要将测试系统或提供其它形式初始和持续保证的能力设计到系统中，或通过其它方式提供。更多信息参见第9章。

8.4.2.3 获得系统和安全相关活动

在这个阶段，系统被实际构建或购买。如果构建系统，安全活动可能包括开发系统安全方面的内容、监视开发过程本身以防范安全问题、响应更改、以及监视威胁。在开发阶段可能遇到的威胁或缺陷包括木马、不正确的代码、功能低劣的开发工具、对代码的操纵和恶意的内部人员。

在制定联邦政府的合同中，较好的做法通常是让具有安全专业知识的人参与其中做为资源选择委员会的成员帮助评测候选对象的安全情况。

如果是采购成品的系统，安全活动可能包括监视以确保在市场调查、合同洽商文件，以及候选系统的评测中考虑到安全问题。许多系统采用开发和采购的混合模式。这种情况下，安全活动包括上述两个方面的内容。

在系统构建或采购时，对系统的选择可以影响到安全。这些选择包括特定成品的选择、最终对体系机构的确定，或选择处理站点或平台。可能需要更多的安全分析。

除了获得系统以外，还需要制定运行措施。这是指围绕系统发生的人的活动，如应急计划、意识培养和培训，以及准备文档。本书运行控制部分的章节论述了这些内容。这需要与系统一起开发，但是通常由不同的人来完成。这些内容与技术规格说明一样应该在开发和采购阶段的初期加以考虑。

[69] 这是一个基于风险决策的例子。

8.4.3 实施

在一些生命周期计划中可能没有特定的实施阶段。（它通常被纳入开发和采购的后期或运行和维护的前期。）但是，从安全的角度出发，一项关键的安全活动－**审批**在开发和系统开始运行之间发生。本节描述的其它活动，开启控制和测试，经常被纳入开发/采购阶段的后期。

8.4.3.1 安装/开启控制

虽然很明显，但是这个活动还是经常被忽略。系统在获得时经常处于安全特性禁止状态。这就需要开启和配置。对于许多系统来说，这是需要很高技巧的复杂工作。定制开发的系统也可能需要类似的工作。

8.4.3.2 安全测试

系统安全测试包括对所开发或采购的系统特定部分的测试和整个系统的测试。安全管理、物理设施、人事、规程、商业或内部服务（如网络服务）的使用，以及应急计划是对整体系统安全产生影响但可能处于开发或采购周期之外的领域的例子。因为只有在开发或采购周期之内的部分才会在系统接收测试中得到测试，所以可能需要对这些额外的安全组件进行独立的测试或审查。

安全认证是对部署在计算机系统中的安全防范措施的正式测试以确定其是否满足相关的需求和规格说明[70]。为了提供更可靠的技术信息，认证通常由独立的审查者而不是由设计系统的人进行。

8.4.3.3 审批

系统安全审批是审批（管理）官员对系统运行的**正式授权**和**对风险的明确接受**。它通常由对系统管理、运行和技术控制等的检查支持。此检查可以包括详细的技术评测（如特别针对复杂、关键或高风险系统的联邦信息处理标准102认证）、安全评测、风险评估、审计或其它此类检查。如果生命周期过程被用于管理一个项目（如系统升级），认识到审批是针对整个系统而不仅是新增部分是很重要的。

看待计算机安全审批的最佳方式是将其作为质量控制的一种形式。它强迫管理者和技术人员一起工作，以发现在给定技术约束、运行约束和使命需求下的最佳安全方法。审批过程迫使管理者作出提供充分安全防范措施的关键决定。基于技术和非技术防范措施的有效性以及残留风险的可靠信息所作出的的决定更可能是个好决定。

审批意见举例

在这里，我依照（机构指令）发布对（系统名称）的审批意见。

此审批意见是我对运行安全达到满意水平并且系统可以在合理的风险下运行的正式声明。此审批意见的有效期是三年。此系统将每年进行评测以确定是否发生了影响其安全的更改。

[70] 一些联邦机构使用认证这一术语更广泛的定义来指发生在审批之前并用于支持审批的正式或非正式的检查或评测。

在决定安全防范措施和残留风险的可接受性后，审批官员应该发表正式的审批意见。当系统安全中的大多数缺点没有严重到足以使运行的系统停止服务或阻止新的系统进入运行状态时，缺点可能要求对运行进行一些限制（如限制拨号访问或与其它机构的电子连接）。在一些情况下，可能会执行临时审批，允许系统运行并在过渡期结束时接受检查，这时应该完成了安全升级。

8.4.4 运行和维护

许多安全活动发生在系统生命的运行阶段。通常，这被分为三部分：（1）安全运行和管理；（2）运行的保证；以及（3）定期对安全的重新分析。图8.2用图表方式描述了运行阶段安全活动的流程。

8.4.4.1 安全运行和管理

系统运行涉及到本手册讨论的许多安全活动。执行备份、举办培训课程、管理密钥、更新用户管理和访问特权、以及更新安全软件就是一些例子。

8.4.4.2 运行保证

运行的系统**没有**完美的安全。另外，系统用户和操作员发现新的方法来有意无意地绕过或颠覆安全。系统或环境的更改可能产生缺陷。一贯严格坚持规程的情况很少见，规程会变得过时。认为风险很小，用户可能会想要绕过安全措施和规程。

> 运行保证检查系统是否按照其当前安全需求运行。这包括操作和使用系统的人的行为和技术控制的运作。

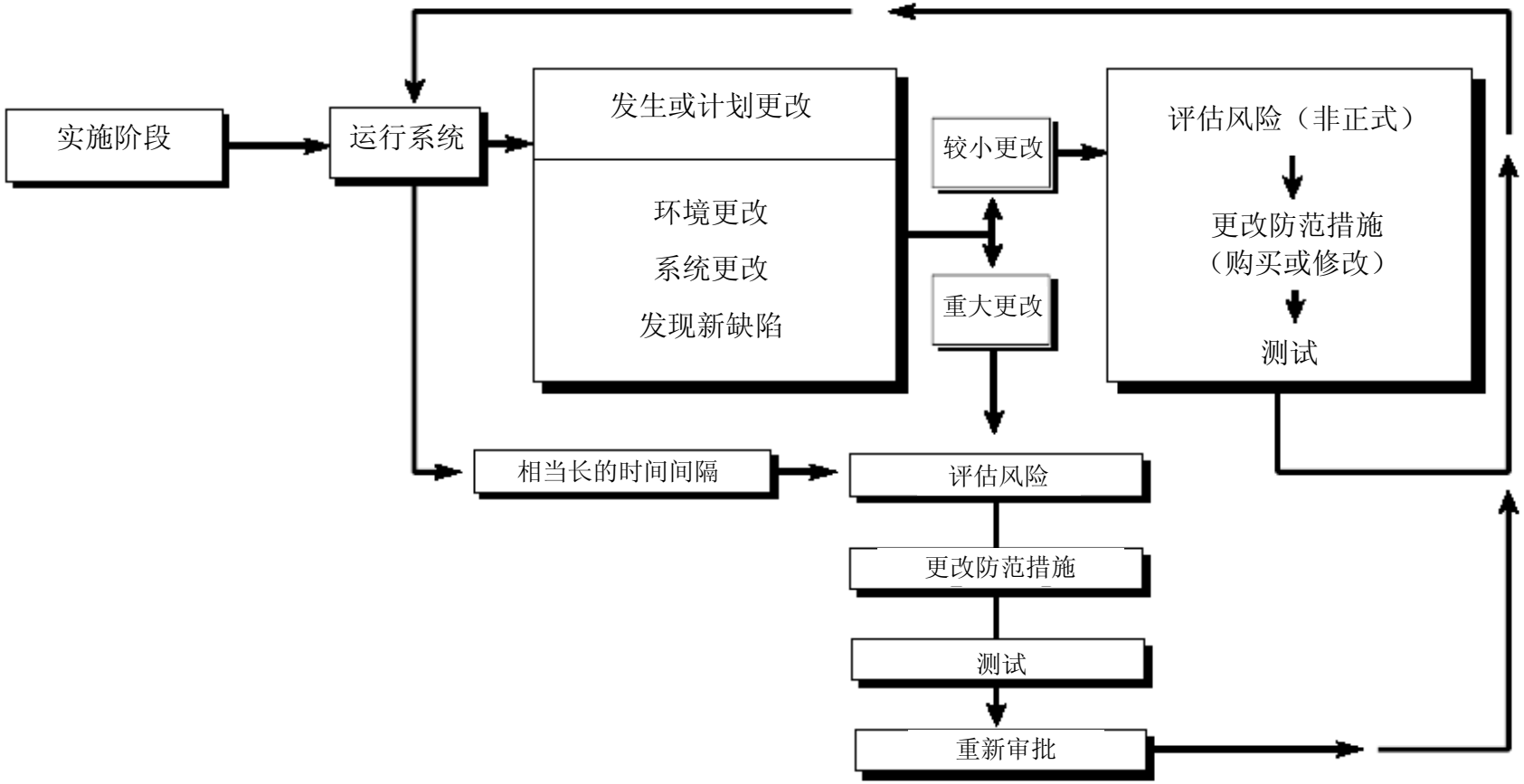
如图8.2所示，有更改发生。运行保证是了解这些更改是否是新的缺陷（或未被更正的老缺陷）、系统更改、或环境更改的一种方式。运行保证是检查运行系统来了解自动的或人工的安全控制是否运行正确和有效的过程。

为了维护运行保证，机构使用两种基本的方法：**系统审计**和**监视**。这些术语在计算机安全界的使用比较模糊并且经常重叠。系统审计是一次性或定期的评测安全的事件。监视是指检查系统或用户的持续活动。通常，活动越是“实时”，越是被归为监视类型。（参见第9章）

8.4.4.3 管理更改

计算机系统及其运行的环境会发生持续的更改。为了响应诸如用户的抱怨、出现新的特性和服务、或发现新的威胁和缺陷，系统管理者和用户修改系统并增加新的特性、新的规程和对软件进行升级。

系统运行的环境也会更改。网络和网络互连有增加的趋势。可能会增加新的用户组，这可能是外部用户组或匿名用户组。新的威胁可能会出现，如网络入侵的增加或个人计算机病毒的扩散。如果系统有配置控制委员会或其它管理系统技术更改的机构，可以安排安全专家在委员会中工作以便就更改是否（如果有，如何）影响安全作出决定。



在系统生命周期的运行阶段，会发生重大和较小的更改。本图用图表的方式描述了协助确保系统安全持久保持在审批官员能够接受的水平上的正确响应。

图 8.2

安全更改管理协助制定新的安全需求。

在系统升级（以及计划的更改）和决定计划外更改影响的过程中也应该考虑安全问题。如图8.2所示，当发生或计划更改时，要决定更改是重大的还是较小的。重大的更改，如重新设计系统的结构，会极大影响到系统。重大更改经常涉及到购买新的硬件、软件、服务或对新的软件模块进行开发。

机构无需设定决定重大－较小更改的界线。使用以下方法的组合可以构成具有弹性的辨别两种更改的标准。

重大更改 重大更改需要进行分析以确定安全需求。可以使用上面描述的过程，当然分析可能仅仅集中在发生或将要发生更改的领域。如果在整个生命周期中原来的分析和系统的更改都被记录在文档中，分析一般会很容易。因为这种更改源自重要系统的获得、开发工作，或政策的更改，所以应该重新审批系统以确保残留风险仍然是可接受的。

较小更改 对系统的许多更改无需进行像对重大更改那样的深入分析，但是还是需要一些分析。每一个更改都可以进行有限的分析来衡量优点（收益）和缺点（成本），这甚至可以在会议上当场进行。即使进行非正式的分析，决定还是应该被适当地记录在文档中。在这个过程中，即使是“很小”的决定也最好是基于风险作出的。

8.4.4.4 定期重新审批

从整体上对系统安全进行定期的重新检查是有益的。为重新审批而进行的分析应该涉及到这种问题：安全仍然是充分的吗？需要重大更改吗？

重新审批应该涉及到高级别的安全和管理层的关注以及安全的实施。并不总是需要在重新审批时进行新的风险评估或认证，但是这些活动是互相支持的（并且都需要定期执行）。系统进行更改的范围越广，所要进行分析（如风险评估或重新认证）的范围也就越广泛。风险分析可能发现与系统更改有关的安全问题。系统被更改后，可能需要对其进行测试（包括认证）。然后如果风险是可接受的，管理层就重新批准系统的运行。

8.4.5 废弃

在废弃系统时考虑记录保存期的法律需求是很重要的。对于联邦系统，系统管理官员应该向负责保存联邦记录的官员咨询。

计算机系统生命周期的废弃阶段涉及到信息、硬件和软件的处置。信息可以转移到其它系统、存档、丢弃或销毁。当存档信息时应该考虑未来取回信息的方法。用于创建记录的技术在未来可能无法随时获得。

硬件和软件可以被出售，赠送或丢弃。除了一些包含保密信息的存储介质只有用销毁的方式清除以外，很少有硬件需要被销毁。如果有必要的话，软件的处置应

遵循许可证和其它与开发商的协议。一些许可证是针对站点的或包含防止软件被转移的其它协议。也可能要采取措施对数据进行加密以便将来使用，如采取适当的步骤确保对密钥的长期和安全存储。

介质清除

因为电子介质容易被复制和传送，所以，为了防止泄漏敏感信息经常需要在整个计算机系统生命周期中予以控制以便管理者可以确定其得到了适当的处置。从存储介质（如硬盘或磁带）中除去信息被称为清除。不同的清除方法提供了不同级别的保护。可以对清理（使其无法被键盘攻击恢复）和净化（使信息无法被实验室攻击回复）进行区分。有三种常见的净化介质的方法：覆盖、消磁（只对磁介质）和销毁。

8.5 相互关系

与许多管理控制一样，对生命周期的计划依赖于其它控制。三个联系紧密的控制领域是政策、保证和风险管理。

政策 针对系统的政策制定是确定安全需求的重要一环。

保证 良好的生命周期管理为在系统设计和运行中正确考虑安全问题提供保证。

风险管理 在系统的运行阶段对安全的维护是一种风险管理过程：分析风险、消减风险和监视防范措施。风险评估是设计系统安全和重新审批的关键部分。

8.6 费用考虑

安全是系统整个生命周期的一个要素。有时安全选择是很随意作出的，没有人分析选择的原因；有时安全选择是基于分析谨慎作出的。第一种情况可能造成系统处于恶劣的安全状态而容易遭受各种损失。第二种情况下，生命周期管理的花费要**远远小于**所避免的损失。生命周期管理的主要费用是人员费用和在生命周期中系统为了完成分析、检查和获得管理层批准而造成的延迟。

有可能对系统进行了过度管理：不必要地花费大量时间用于计划、设计和分析风险。计划本身不会推进机构的使命或业务。所以，虽然安全生命周期管理可以获得可观的收益，但是工作量还是要与系统的规模、复杂度、敏感性以及系统相关的风险相称。通常，系统的价值越高，系统的体系、技术和措施越新、系统安全失效后的影响越严重，越要花费更多的精力在生命周期管理上。

参考书目

Communications Security Establishment. *A Framework for Security Risk Management in Information Technology Systems.* Canada.

Dykman, Charlene A. ed., and Charles K. Davis, asc. ed. *Control Objectives Controls in an Information Systems Environment: Objectives, Guidelines, and Audit Procedures*. (fourth edition). Carol Stream, IL: The EDP Auditors Foundation, Inc., April 1992.

Guttman, Barbara. *Computer Security Considerations in Federal Procurements: A Guide for Procurement Initiators, Contracting Officers, and Computer Security Officials*. Special Publication 800-4. Gaithersburg, MD: National Institute of Standards and Technology, March 1992.

Institute of Internal Auditors Research Foundation. *System Auditability and Control Report*. Altamonte Springs, FL: The Institute of Internal Auditors, 1991.

Murphy, Michael, and Xenia Ley Parker. *Handbook of EDP Auditing*, especially Chapter 2 "The Auditing Profession," and Chapter 3, "The EDP Auditing Profession." Boston, MA: Warren, Gorham & Lamont, 1989.

National Bureau of Standards. *Guideline for Computer Security Certification and Accreditation*. Federal Information Processing Standard Publication 102. September 1983.

National Institute of Standards and Technology. "Disposition of Sensitive Automated Information." Computer Systems Laboratory Bulletin. October 1992.

National Institute of Standards and Technology. "Sensitivity of Information." Computer Systems Laboratory Bulletin. November 1992.

Office of Management and Budget. "Guidance for Preparation of Security Plans for Federal Computer Systems That Contain Sensitive Information." OMB Bulletin 90-08. 1990.

Ruthberg, Zella G, Bonnie T. Fisher and John W. Lainhart IV. *System Development Auditor*. Oxford, England: Elsevier Advanced Technology, 1991.

Ruthberg, Z., et al. *Guide to Auditing for Controls and Security: A System Development Life Cycle Approach*. Special Publication 500-153. Gaithersburg, MD: National Bureau of Standards. April 1988.

Vickers Benzel, T. C. *Developing Trusted Systems Using DOD-STD-2167A*. Oakland, CA: IEEE Computer Society Press, 1990.

Wood, C. "Building Security Into Your System Reduces the Risk of a Breach." *LAN Times*, 10(3), 1993. p 47.

第九章

保证

计算机安全保证是对技术和运行安全措施、保护系统的工作及其所处理信息的信任程度。但是，保证不是对措施能起作用的绝对担保。同与其紧密相关的可靠性和质量领域一样，保证分析起来可能比较困难，但是它却是人们所期待和获得的（经常是在没有意识到的情况下）。例如，人们可能经常性地得到同事的产品建议但可能没有考虑到这种建议提供了保证。

保证是一种信任程度，而不是如何实际保护系统的真实措施。这种区分是重要的，因为确切了解系统的实际安全状况是非常困难的，很多情况下是不可能的。

> 安全保证是对安全控制正确运行以及系统得到预期保护的信任程度。

保证并不是一件容易的事情，它难以描述更难量化。因此，很多人将保证称为对控制能够正常工作的“模糊而温暖的感觉”。但是，有两件事可能使其成为更严格的方法：（1）谁需要得到确定？以及（2）可以获得什么类型的保证。需要得到确定的人是对系统安全负有最终责任的管理官员。在联邦政府中，此人是**授权和审批**官员[71]。

有许多获得保证的方法。出于讨论的目的，本章按照常见的系统生命周期对保证进行分类。本章首先讨论保证的计划，然后提供两类保证的方法和工具：（1）设计和实施保证，以及（2）运行保证。运行保证又被分为审计和监视。

设计和实施保证与运行保证的界线可能比较模糊。像配置管理或审计这样的问题在运行保证中讨论，而它们在系统开发中也可能是很重要的。讨论倾向于关注设计和实施保证的技术问题，要注意的是其分类在一定程度上是人为的，实际上存在交叉内容。

9.1 审批和保证

审批是管理官员对系统安全适当性的正式接受。看待计算机安全审批的最好方式是将其视为质量控制的一种形式。它强迫管理者和技术人员一起工作，以发现在给定安全需要、技术约束、运行约束和使命或业务需求条件下可行的、具有成本效益的解决方案。审批过程迫使管理者作出能够提供适当安全防范措施的关键决定，从而体现和执行其在保护系统方面的角色。为了作出良好的决定，他们需要基于技术和非技术防范措施的可靠信息。这些信息包括：

[71] 审批主要是应用于联邦政府中的过程。它是对进行处理的管理授权过程。不同机构可能使用不同的术语表示这个批准功能。这里使用的术语与联邦信息处理标准102，《计算机安全认证和审批》是一致的。（参见本站的参考书目部分）

- 技术特性（它们如预期的那样运行吗？）
- 运行措施（系统是根据发布的规程操作的吗？）
- 整体安全（有技术特性和运行措施没有解决的威胁吗？）
- 剩余风险（它们是可接受的吗？）

计算机系统应该在投入运行前得到批准，并且在系统重大更改或一定时间间隔[72]后定期进行重新审批。即使系统一开始没有得到审批，审批过程还是可以从任意时刻开始。第8章更深入讨论了审批。

9.1.1 审批和保证

保证虽然极其重要，但并不是审批的唯一内容。如图所示，保证涉及到技术措施以及（1）按照一系列安全需求和规格说明或者（2）按照一般的质量原则进行操作的规程。审批也涉及到系统安全需求是否正确和得到很好实施，质量水准是否足够高这样的问题。这些活动在第7和8章论述。

9.1.2 选择保证方法

审批官员对系统需要多少以及何种保证作出最后决定。为了作出明智的决定，它应源于审批官员认为适当的安全检查，如风险评估或其它研究项目（如认证）[73]。

[72] OMB A-130规章要求联邦系统的运行要获得管理层的安全授权。

[73] 过去，审批曾经被定义为需要进行对技术控制深入测试的认证。现在认识到，在联邦政府中，其它分析（如风险评估或审计）也可以为审批提供充分的保证。

审批官员需要设身处地地分析保证花费的利弊、控制的成本和对机构的风险。在审批过程后期，审批官员将是接受剩余风险的人。所以应该与审批官员协调保证方法的选择。

在选择保证方法时，应该权衡保证的需要及其花费。保证可能会非常昂贵，特别是在进行广泛的测试时。每种方法在花费和能够实际提供何种保证方面都存在优势和劣势。方法的组合经常可以提供很好的保证，因为没有一种方法是完美的，而且这样能够比广泛测试花费更少的成本。

审批官员不是唯一的仲裁者。也应该咨询使用系统的其它官员。（例如，依赖于供应系统的生产经理应该提供供应系统方面的意见。）另外，可能会有审批官员控制范围以外并对方法选择产生影响的约束。例如，一些方法可能过度限制联邦信息处理资源采购方面的竞争，或可能违背机构的隐私政策。某些保证方法是机构政策或指令要求的。

9.2 计划和保证

无论对于新系统还是系统升级，保证计划都应该始于系统生命周期的计划阶段。保证计划为系统其它计划的制定提供帮助。如果系统要接受广泛测试，系统就应以协助这种测试进行的方式构建。

保证计划帮助管理者在何种保证具有成本效益方面做出决策。如果管理者等到系统建成或购买回来后再考虑保证，获得保证的方式就可能比管理者早期就进行计划要少很多，而且余下的保证选项可能更昂贵。

9.3 设计和实施保证

设计和实施保证与系统、应用或组件特性是否满足安全需求和规格说明以及其设计和构建是否良好有关。第8章论述了安全需求和规格说明的来源。设计和实施保证考察系统的设计、开发和安装。虽然设计和实施保证通常与系统生命周期的开发/采购和实施阶段相关；但是在整个生命周期中发生系统更改的情况下也都应该对此加以考虑。

> 应该依据两个方面检查设计和实施保证：组件和系统。组件保证考察特定产品或系统组件的安全，如某一操作系统、应用、附件的安全功能、或电信模块。系统保证考察整个系统的安全，包括产品和模块之间的交互。

如前所述，保证可以涉及到产品或系统是否满足一系列安全规格说明，或是否能提供其它质量方面的证据。本节概述获得设计和实施保证的主要方法。

9.3.1 测试和认证

测试可能涉及到所构建、实施或运行系统的质量。因此，可以在开发周期、系统安装后以及整个运行阶段进行。一些常见的测试技术包括功能测试（考察某功能

是否按照其需求运作）或渗透测试（考察是否能够绕过安全限制）。这些技术手段可以从一般的尝试性测试到使用计量装置、自动工具或多种精密测试工具的深入研究。

认证是依据特定安全需求序列测试组件或系统的正式过程。认证一般由独立检查人员执行，而不是与构建系统有关的人。认证对于复杂或高风险系统经常具有更高的成本效益。。不太正式的测试可以用于低风险系统。可以在系统设计和实施过程的多个阶段进行认证，可以在实验室、运行环境或分别在两个环境中进行。

9.3.2NIST符合性测试和验证套件

NIST创建了验证套件和符合性测试来确定产品（软件、硬件、固件）是否满足特定的标准。这些测试套件是为特定标准开发的并使用了很多方法。对标准的符合之所以重要是由很多原因造成的，包括互操作性或所提供安全的强度。NIST每季度都发表一个已验证产品清单。

9.3.3 使用先进的和可信的开发

无论是在商业成品或是更加客户化的系统开发过程中，使用先进的或可信的系统体系、开发方法或软件工程技术都可以提供保证。例子包括安全设计和开发检查、形式化模型、数学验证、ISO9000质量技术或使用安全体系概念，如受信计算基或参考监视器。

9.3.4 使用可靠的体系

一些系统结构具有更加高的内在稳定性，如使用容错、冗余、映像或廉价磁盘冗余阵列（RAID）特性。这些例子主要与系统的可用性相关。

9.3.5 使用可靠的安全

可靠安全的一个因素是**安全使用的简便性**概念，它提出容易保护的系统更可能是安全的。当系统的初始默认设置是“最安全”选项时，安全特性最可能被使用。另外，如果系统不使用未经“真实”使用环境测试的非常新的技术（经常被称为“未成熟”技术），那么它可能被认为是更可靠的。相反的，使用旧的、经过良好测试软件的系统包含的错误可能会更少。

9.3.6 评价

产品评价一般包括测试。评价可以由各种类型的机构进行，包括国内和国外的政府机构；独立机构如贸易和专业机构；其它供应商或商业组织；个人用户或用户公会。商业文献的产品评论是一种评价形式，更正式的检查是依据特定标准进行的。使用评价的重要考虑因素包括评价组织的独立性程度、评价标准是否反映了所需的安全特性、测试的严格性、测试环境、评价的使用期、评价机构的能力以及评价组织为评价设置的限制条件（如关于威胁或运行环境的假设）。

9.3.7 保证文档

描述安全需求以及其如何被满足的能力可以反映系统和产品设计者对相关安全问题的理解程度。没有对需求的良好理解，设计者就不大可能满足它们。

保证文档可以涉及到针对系统或是针对组件的安全。系统级文档应该描述系统的安全需求以及如何满足这些需求，包括应用、操作系统和网络之间的相互关系。系统级文档不仅涉及到操作系统、安全系统和应用，它还描述系统的**集成**和在**特殊环境中的部署**。组件文档通常是关于成品的，而通常系统设计者或实施者会制定系统文档。

9.3.8 运行于类似环境的产品审批

运行于类似环境的产品或系统的审批可以被用来提供一些保证。但是，重要的是要认识到审批是针对特定环境和系统的。因为审批对风险和利益作出平衡，所以相同的产品在一种环境中可能得到使用批准，而即使是相同的审批官员却可能不会批准其在另一个环境中的运行。

9.3.9 自我认证

供应商、集成商或系统开发商的自我认证在不依赖于公平或独立机构的条件下对系统进行技术评价以考察其满足相关安全需求的情况。虽然它并不能做到不偏不倚，但还是可以提供保证。自我认证者的信誉是可以了解到的，可以阅读认证结果报告来确定安全需求是否被定义以及是否进行了有意义的检查。

混合认证也是可能的，可以由独立机构通过分析结果报告、抽查或其它监督的形式对其工作进行协助或检查。这种方法可以结合自我认证的低成本和快速以及独立检查的公正性的优点。但是，这种检查可能没有独立评价或测试那么全面。

9.3.10 担保、完整性条款和责任

担保是另一种保证的来源。如果制造商、生产商、系统开发者或集成商想要在一定时间范围内或下一个版本中更正错误，这会给系统管理者一种对产品和产品质量有承诺的感觉。完整性条款是产品的正式声明或认证。它可以通过（a）修复部件（担保）或（b）赔偿因无法实现完整性条款而带来的损失（责任）的方式进行支持。

9.3.11 制造商发表的声明

制造商或开发商发表的声明或正式公告提供了基于本身信誉的程度较低的保证。

9.3.12 分配保证

了解到达的软件没有受到更改经常是很重要的，尤其是在通过电子方式分配时。在这种情况下，检查位或数字签名可以提供代码未被更改的高度保证。反病毒软件可以用于检查源于可靠性未知地点（如公告牌）的软件。

9.4 运行保证

设计和实施保证涉及到构建于系统中的安全特性的质量。运行保证涉及到系统的技术特性是否能够被绕过或有缺陷以及所需的规程是否被遵循。它不涉及因系统及其操作或威胁环境的更改引起的系统安全需求的更改。（第8章涉及到这些更改）。

在系统生命周期的运行阶段安全有降低的趋势。系统用户和操作员发现有意无意绕过或破坏安全的新方式（特别是在感觉到绕过安全会改善功能性时）。用户和管理员经常认为其系统和自身不会出问题而跨越安全。严格遵循规程的情况很少见，它们会变得过时，系统管理也经常会犯错误。

机构使用两种基本方法来维持运行保证：

- **系统审计** — **一次性**或**定期**评价安全的事件。审计范围多种多样：它可能出于重新审批的目的检查整个系统，也可能调查一个异常事件。

- **监视** — 检查系统、其用户或环境的**持续**活动。

通常，越是“实时”的活动，越是被归于监视类型。这种区别会产生一些不必要的文字游戏，特别是与系统产生的审计跟踪有关时。每天或每周检查审计跟踪（非受权访问尝试）通常是监视，而对几个月的审计跟踪进行历史检查（追踪特定用户的行动）可能就是审计。

9.4.1 审计的方法和工具

用来支持运行保证的审计检查系统是否满足包括系统和机构政策在内的明确或暗示的安全需求。一些审计还检查安全需求是否适当，但是这超出了运行保证的范畴。（参见第8章）不太正式的审计经常被称作**安全检查**。

> 执行独立审计的人应该没有可能妨碍其独立性的人事和外部约束并应该在组织关系上是独立的。

审计可以是自我管理或独立进行的（内部或外部）[74]。两种方式都可以提供技术、规程、管理或其它安全方面的有效信息。自我审计和独立审计的重要区别是客观性。由系统管理人员进行的检查经常被称为自我审计/评估，它存在内在的利益冲突。系统管理人员可能不太愿意提出计算机系统设计低劣或者操作马虎之类的意见。而另一方面，他们可能很愿意改善系统的安全状况。另外，他们了解系统并可能发现隐藏的问题。

相反的，独立审计机构与系统没有特殊的利益关系。独立审计可以由专业审计人员根据普遍接受的审计标准进行。

有很多方法和工具可以被用于系统审计，下面描述一些方法和工具。其中有些内容有互相重叠的关系。

9.4.1.1 自动化工具

即使对于小的计算机系统，人工检查安全特性也是一项繁重工作。自动化工具甚至能够使检查大型计算机系统的各种安全问题成为可能。

[74] 联邦政府内部审计的例子是总监察长。美国审计总署可以担当联邦政府外部审计机构的角色。在私营机构，公司审计官员做为内部审计员角色，而会计师事务所是外部审计机构。

有两种自动化工具：（1）主动工具，通过攻击找到缺陷，以及（2）被动测试，仅检查系统并通过系统的状态推断存在的问题。

自动化工具可以被用于帮助发现各种威胁和缺陷，如不恰当的访问控制或访问控制配置、脆弱的口令、系统软件缺乏完整性或者没有充分进行相关软件的升级和修补。这些工具经常在发现缺陷方面非常成功而且有时被黑客用来攻击系统。不充分利用这些工具会使系统管理员处于不利的地位。很多工具使用起来很简单，但是有些程序（如对于大型机系统的访问控制审计工具）需要特殊的技巧来使用和解释。

9.4.1.2 内部控制审计

审计员可以检查运行中的控制并确定其是否有效。审计员会经常分析基于计算机和不基于计算机的控制。其使用的技术包括询问、观察和测试（对控制本身和数据）。审计还探测非法活动、错误、异常或违背法律和法规的行为。还可能使用下面讲到的安全检查列表和渗透测试。

> 美国审计总署为联邦机构的内部控制审计提供了标准和指导方针。

9.4.1.3 安全检查列表

在政府中，计算机安全计划提供了对系统进行审计的检查列表。第8章讨论的计划概述了系统的主要安全考虑，包括管理、运行和技术问题。使用计算机安全计划的一个优点是它反映系统的独特安全环境，而不是通用的控制清单。还可以制定包括国家或机构安全政策和措施（经常被称为**基线**）的其它检查列表。也可以使用“普遍接受的安全措施”（GSSP）。要注意的是，与列表不同也并不意味着错误，因为它们可能适合于系统的特殊环境或技术约束。

> 警告：得到通过（如得到B+或更好成绩）的安全检查列表经常被错误地用做安全充分性的证据（而不是指标）。无法完成检查列表的系统管理者经常把精力过度集中于“获得分数”而不是确定安全措施是否被正确部署和在特定环境中发挥作用。

检查列表也被用于验证是否从安全角度检查了对系统的更改。审计一般要检查系统的配置以发现已发生但没有从安全角度分析的重大更改（如接入互联网）。

9.4.1.4 渗透测试

渗透测试可以使用许多方法来进行系统入侵尝试。除了如上所述使用主动的自动化工具以外，渗透测试还可以采用“人工”方式。大多数有价值的渗透测试类型都是使用可能真正用来攻击系统的方法。对于互联网上的主机，这肯定包括自动化工具。对于许多系统，松懈的规程或缺乏对应用的内部控制是渗透测试瞄准的常见缺陷。另一种方法是“社会工程”，这涉及到使用户或管理员泄漏系统信息，

包括其口令。[75]

9.4.2 监视方法和工具

安全监视是查找缺陷和安全问题的持续行为。许多方法与审计所使用的类似，但更频率更高，且自动化工具是在实时状态下使用的。

9.4.2.1 系统日志的检查

如第8章所述，对系统生成日志的定期检查可以探测安全问题，包括超越访问授权或在非正常时间获得系统访问的尝试。

9.4.2.2 自动化工具

多种类型的自动化工具监视系统的安全问题。下面是一些例子：

- **病毒扫描**是检查病毒感染的常见方法。这些程序测试可执行程序文件中出现的病毒。

- **检查校验和**假设程序文件在更新之间不会更改。它们通过基于特定文件的内容生成算术值来实现。在检验文件的完整性时，生成当前文件的校验和并与以前生成的值进行比较。如果两个值相等，文件的完整性就得到了验证。检查校验和程序能够探测病毒、木马、由于硬件故障造成的对文件的意外更改以及对文件的其它更改。但是它们有可能被系统入侵者更换。还可以使用数字签名。

- **口令破解**使用字典（可以是“常规”字典或者易于猜测口令的特殊字典）检查口令并且还检查口令是否是用户识别码的变换。特殊字典条目的例子可以是当地体育运动队和明星的名字;常见变换可以是用户识别码的反向拼写。

- **完整性校验程序**可以被应用程序用来查找对数据的篡改、错误和遗漏。这些技术包括一致性和合理性检查以及数据录入和处理的验证。这些技术可以根据预期值或取值范围检查输入或处理的数据项；分析交易的正确流向、顺序和授权；或检查数据项预期的相互关系。这些程序组成了处理的重要一环，因为它们能够被用来确定人们是否无意或有意做了不应该做的，他们会被发现的。许多这样的程序依赖于对每个用户行为的记录。

- **入侵探测器**分析系统的审计跟踪，特别是登录、连接、操作系统调用和各种命令参数，因为这些活动能够体现非受权行为。入侵探测的内容包含在第12和18章中。

- **系统性能监视**实时分析系统性能日志以发现可用性问题，包括主动攻击（如1988年互联网蠕虫）以及网络缓慢和崩溃。

[75] 渗透测试是一项非常强大的技术，它应该在系统管理人员了解和同意的情况下进行。未知的渗透测试会给运行人员带来很大压力，并且可能造成不必要的干扰。

9.4.2.3 配置管理

从安全角度来看，配置管理为系统运行于正确版本（配置）以及对任何更改进行安全方面的检查提供保证。配置管理可以被用于帮助确保更改是在确定和受控环境下进行并且不会无意中损害到任何系统特性，包括安全。一些机构特别是拥有非常大型系统的机构使用配置控制委员会进行配置管理。当有委员会存在时，计算机安全专家参与其中是很有帮助的。在任何情况下，计算机安全官员参与到系统管理决策中都是有益的。

对系统的更改可能会牵涉到安全问题，因为它们可能引入或消除缺陷，并且重大更改可能需要更新应急计划、风险分析或审批。

9.4.2.4 商业文献/出版物/电子新闻

除了监视系统以外，监视外部资源的信息也是有用的。如书面和电子的商业文献会有关于安全缺陷、补丁和其它影响到安全的信息。事件响应组论坛（FIRST）有接收威胁、缺陷和补丁信息的邮件列表。[76]

9.5 相互关系

保证是关系到本手册讨论的每个控制和防范措施的问题。用户识别码和访问特权是否保持更新状态？应急计划是否得到测试？审计跟踪是否会被篡改？这里要强调的重要一点是保证不仅是针对技术控制的，也同样针对运行控制。虽然本章关注的是信息系统的保证，但是对管理控制正常工作的保证也很重要。安全项目是否有效？政策是否被理解和遵循？如本章介绍中提到的，保证的需要比人们通常意识到的更广泛。

生命周期保证与系统生命周期的安全计划紧密相关。系统可以被设计为易于进行对特定安全需求的各种测试。通过在过程早期对这些测试的计划能够降低成本；在一些情况下，没有适当的计划，就无法获得某些类型的保证。

9.6 费用考虑

有许多获得安全特性正常工作保证的方法。由于保证方法有容易定性但不容易定量的趋势，所以需要对其进行评价。保证也可能很昂贵，尤其在进行广泛测试时。对付出的成本和获得的保证进行评价对于做出最合算的决策是有用的。通常，人员的费用驱动了保证成本的上升。自动化工具通常在处理特殊问题时作用有限，虽然它们可能比较便宜。

参考书目

Borsook, P. "Seeking Security." *Byte*. 18(6), 1993. pp. 119-128.

Dykman, Charlene A. ed., and Charles K. Davis, asc. ed. *Control Objectives Controls*

[76] 关于FIRST方面的信息，请发电子邮件到 FIRST-SEC@FIRST.ORG。

in an Information Systems Environment: Objectives, Guidelines, and Audit Procedures. (fourth edition). Carol Stream, IL: The EDP Auditors Foundation, Inc., April 1992.

Farmer, Dan and Wietse Venema. "Improving the Security of Your Site by Breaking Into It." Available from FTP.WIN.TUE.NL. 1993.

Guttman, Barbara. *Computer Security Considerations in Federal Procurements: A Guide for Procurement Initiators, Contracting Officers, and Computer Security Officials*. Special Publication 800-4. Gaithersburg, MD: National Institute of Standards and Technology, March 1992.

Howe, D. "Information System Security Engineering: Cornerstone to the Future." *Proceedings of the 15th National Computer Security Conference*, Vol 1. (Baltimore, MD) Gaithersburg, MD: National Institute of Standards and Technology, 1992. pp. 244-251.

Levine, M. "Audit Serve Security Evaluation Criteria." *Audit Vision*. 2(2). 1992, pp. 29-40. National Bureau of Standards. *Guideline for Computer Security Certification and Accreditation*. Federal Information Processing Standard Publication 102. September 1983.

National Bureau of Standards. *Guideline for Lifecycle Validation, Verification, and Testing of Computer Software*. Federal Information Processing Standard Publication 101. June 1983.

National Bureau of Standards. *Guideline for Software Verification and Validation Plans*. Federal Information Processing Standard Publication 132. November 1987.

Nuegent, W., J. Gilligan, L. Hoffman, and Z. Ruthberg. *Technology Assessment: Methods for Measuring the Level of Computer Security*. Special Publication 500-133. Gaithersburg, MD: National Bureau of Standards, 1985.

Peng, Wendy W., and Dolores R. Wallace. *Software Error Analysis*. Special Publication 500-209. Gaithersburg, MD: National Institute of Standards and Technology, 1993.

Peterson, P. "Infosecurity and Shrinking Media." *ISSA Access*. 5(2), 1992. pp. 19-22. Pfleeger, C., S. Pfleeger, and M. Theofanos, "A Methodology for Penetration Testing." *Computers and Security*. 8(7), 1989. pp. 613-620.

Polk, W. Timothy, and Lawrence Bassham. *A Guide to the Selection of Anti-Virus Tools and Techniques*. Special Publication 800-5. Gaithersburg, MD: National Institute of Standards and Technology, December 1992.

Polk, W. Timothy. *Automated Tools for Testing Computer System Vulnerability*. Special Publication 800-6. Gaithersburg, MD: National Institute of Standards and Technology, December 1992.

President's Council on Integrity and Efficiency. *Review of General Controls in Federal Computer Systems*. Washington, DC: President's Council on Integrity and Efficiency, October 1988.

President's Council on Management Improvement and the President's Council on Integrity and Efficiency. *Model Framework for Management Control Over Automated Information System*. Washington, DC: President's Council on Management Improvement, January 1988.

Ruthberg, Zella G, Bonnie T. Fisher and John W. Lainhart IV. *System Development Auditor*. Oxford, England: Elsevier Advanced Technology, 1991.

Ruthburg, Zella, et al. *Guide to Auditing for Controls and Security: A System Development Life Cycle Approach*. Special Publication 500-153. Gaithersburg, MD: National Bureau of Standards, April 1988.

Strategic Defense Initiation Organization. *Trusted Software Methodology*. Vols. 1 and II. SDI-SSD- 91-000007. June 17, 1992.

Wallace, Dolores, and J.C. Cherniasvsky. *Guide to Software Acceptance*. Special Publication 500- 180. Gaithersburg, MD: National Institute of Standards and Technology, April 1990.

Wallace, Dolores, and Roger Fugi. *Software Verification and Validation: Its Role in Computer Assurance and Its Relationship with Software Product Management Standards*. Special Publication 500-165. Gaithersburg, MD: National Institute of Standards and Technology, September 1989.

Wallace, Dolores R., Laura M. Ippolito, and D. Richard Kuhn. *High Integrity Software Standards and Guidelines*. Special Publication 500-204. Gaithersburg, MD: National Institute of Standards and Technology, 1992.

Wood, C., et al. *Computer Security: A Comprehensive Controls Checklist*. New York, NY: John Wiley & Sons, 1987.