# 第 1 章

# 通过原则和策略的安全治理

**本章中覆盖的 CISSP 考试大纲包含：**

安全和风险管理(例如安全、风险、合规性、法律、法规、业务连续性)

- A. 理解和应用机密性、完整性和可用性的概念
- B. 应用安全治理原则，通过：
  - B.1 安全功能与战略、目标、使命和愿景的一致(例如商业案例、预算和资源)
  - B.2 组织的流程(例如并购、剥离和治理委员会)
  - B.3 安全角色和职责
  - B.4 控制架构
  - B.5 应尽关注
  - B.6 应尽职责
- F. 开发和实现文档化的安全策略、标准、程序和指南
- J. 理解和应用威胁建模
  - J.1 识别威胁(例如竞争对手、供应商、雇员和值得信赖的伙伴)
  - J.2 确定和用图表示潜在攻击(例如社会工程学、欺骗)
  - J.3 执行降低分析
  - J.4 修复威胁的技术和流程(例如软件架构和操作)
- K. 把安全风险考虑到收购策略和实践中
  - K.1 硬件、软件和服务
  - K.2 第三方评估和监控(例如现场评估、文件传递和审查、流程/策略审查)
  - K.3 最小化安全需求
  - K.4 服务级别需求

对于 CISSP 认证考试，在通用知识体(Common body of Knowledge，CBK)的安全和风险管理知识域中有许多安全解决方案的基本要素要处理。这些基本要素包括安全机制的设计、执行和管理。这个知识域的另外一些要素在第 2 章“人员安全和风险管理概念”、第 3 章“业务连续性计划”和第 4 章“法律、法规和合规性”中讨论。请务必检查所有这些章节中针对这一知识域主题的全部观点。

# 1.1 理解和应用机密性、完整性和可用性的概念

安全管理概念与原则是安全策略和解决方案部署中的固有元素。它们既定义了安全环境所需的基本参数，也定义了策略设计人员和系统实现人员为创建安全解决方案所必须达到的目的和目标。透彻地理解这些内容，对现实生活中的安全专业人士以及 CISSP 考生来说是非常重要的。

安全的主要目的和目标被包含在 CIA 三元组(见图 1.1)中。CIA 三元组是三条主要安全原则的名字，这三条安全原则是：

- 机密性(Confidentiality)
- 完整性(Integrity)
- 可用性(Availability)

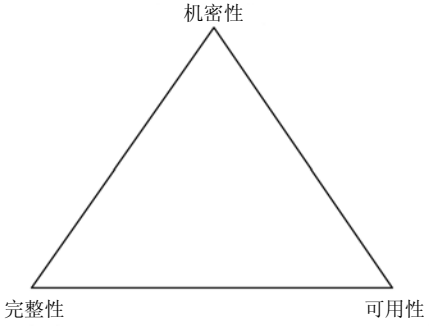


图 1.1 CIA 三元组

对安全控制进行评估时，通常关注是否涉及这些核心的信息安全原则。总的来说，完整的安全解决方案应当充分地涉及所有这些原则。对脆弱性和风险的评估也是基于它们对一个或更多个 CIA 三元组原则的威胁程度。因此，熟悉这些原则，并使用它们作为评判安全相关问题的指导原则，是一个不错的主意。

这三条原则被认为是安全领域内最重要的原则。然而，每条原则对一个特定的组织究竟有多重要，主要取决于组织的安全目标和需求以及安全性所受到的威胁程度。

## 1.1.1 机密性

CIA 三元组的第一条原则是机密性。如果安全机制提供机密性，那么它就为限制未授权主体不能访问数据、客体或资源提供了高级别保证。如果存在对机密性的威胁，那么就有可能发生未授权的泄漏。

通常，在网络上维护机密性时，数据在存储、处理和传输过程中必须受到保护，从而不会出现未授权的访问、使用或暴露。数据、资源和客体的每一种状态都需要唯一的和特殊的安全控制，以便维持机密性。

针对破坏机密性的攻击有很多，这些攻击包括捕获网络通信、窃取密码文件、社会工程学、端口扫描、肩窥、偷听和嗅探攻击等。

对机密性的破坏不限于直接针对机密性的攻击。许多未授权的敏感或机密信息泄露都是由于人为错误、疏忽或失职造成的。造成机密性遭到破坏的事件包括：没能对传输数据进行适当的加密；在传输数据之前，没能对远程系统进行充分的身份认证；一直打开不安全的接入点；访问恶意代码

导致打开后门；传真的误传，在打印机上遗失文件，甚至在显示器上显示数据时，从访问终端离开。如果终端用户或系统管理员的行为不当，或者安全策略存在疏漏以及安全控制配置不正确，那么机密性也会受到破坏。

许多对策有助于保障机密性，抵御潜在威胁。这些措施包括加密、网络流量填充、严格的访问控制、严格的认证程序、数据分类和广泛的人员培训。

机密性和完整性相互依赖。客体如果缺乏完整性，机密性就无法被维护。机密性的其他概念、条件和特征包括：

**敏感性**　敏感性是指信息的品质，如果这种信息被披露，就可能会造成伤害或损坏。维护敏感信息的机密性有助于预防伤害或损坏。

**自主性**　自主性是一种决策行为，操作员可以凭这种权利影响或控制信息的披露，以便将伤害或损坏降到最低。

**关键性**　信息的关键级别是对其关键性的评测。关键级别越高，越需要保持信息的机密性。高级别的关键性对一个组织的运营和功能是必不可少的。

**隐蔽性**　隐蔽是一种隐蔽或防止披露的行为。隐蔽通常被视为覆盖、混淆或干扰的一种手段。

**保密性**　保密是一种保守秘密或防止信息泄露的行为。

**隐私性**　隐私是指要保持信息处于机密状态，这些可能是个人识别信息，或是如果泄露就可能对某人造成伤害、尴尬或丢人的信息。

**隐藏性**　隐藏就是把信息存储到一个偏僻的位置。这个位置还可以附加严格的访问控制。隐藏有助于实施机密性保护。

**隔离性**　隔离是指把特定信息与其他信息分隔开来的行为。隔离可以用来防止信息混杂或信息泄露。

每个组织都需要对他们希望实现的机密性进行细微差别的评估。用于实现一种形式机密性的工具和技术可能不支持或不允许用于其他的形式。

### 1.1.2　完整性

CIA 三元组的第二条安全原则是完整性。为了维护完整性，客体必须保持自身的正确性，并且只能由被授权的主体进行有意修改。如果安全机制提供了完整性，那么它就对数据、客体和资源提供了保持原有受保护状态和不被修改的高级别保证，这也包括当客体在存储、传输或处理过程中发生的变更。因此，维护完整性意味着客体本身不会被改变，并且管理和操纵客体的操作系统与程序实体不会受到安全威胁。

我们可以从下列三个方面查看完整性：

- 应该禁止未授权的主体执行修改操作。
- 应该禁止经过授权的主体执行未授权的修改操作，例如失误。
- 客体应当内外保持一致，这样它们的数据才能正确并真实地反映现实情况，并且与任何子客体、同等客体或父客体的关系都是有效的、一致的和可检验的。

为了在系统上维护完整性，必须对数据、客体和资源的访问进行适当控制。此外，应当使用活动日志记录，从而保证只有经过授权的用户才能够访问他们各自的资源。在存储、传输和处理过程中维护和确认客体完整性时，需要各种各样的控制和监督措施。

针对破坏完整性的攻击有很多。这些攻击包括：病毒、逻辑炸弹、未授权访问、编码和应用程序中的错误、恶意修改、有企图的替换以及系统后门。

与机密性一样，对完整性的破坏不限于有意攻击。许多对敏感信息的未授权修改实际是由于人为错误、疏忽或失职造成的。导致完整性被破坏的事件包括：意外地删除文件；输入无效数据；更改配置，例如命令、代码和脚本中包含的错误；引入病毒以及执行恶意代码(例如，特洛伊木马)。任何用户(包括管理员)的不当行为都可能破坏完整性，安全策略的疏漏或安全控制的配置不正确也可能导致类似事情的发生。

有许多措施可以确保完整性不会受到可能的威胁。这些措施包括：严格的访问控制、严密的身份认证过程、入侵检测系统、对客体/数据进行加密、散列总和认证(详见第 6 章“密码学与对称加密算法”)、接口限制、输入/功能检验以及广泛的人员培训。

完整性依赖于机密性。缺乏机密性，也就无法维护完整性。完整性的其他概念、条件和特征包括：准确性、真实性、可靠性、合法性、不可否认性、可问责性、可信任性、完整性以及可理解性。

### 1.1.3 可用性

CIA 三元组的第三条安全原则是可用性，可用性指的是经过授权的主体被及时准许和不间断地访问客体。如果安全机制提供了可用性，那么它就提供了经过授权的主体能够访问数据、客体和资源的高级别保证。可用性包括有效地不间断地访问客体和阻止拒绝服务(Denial-of-Service，DoS)攻击。可用性还意味着支持基础结构(包括网络服务、通信和访问控制机制)的正常运作，并允许经过授权的用户获得被授权的访问。

为了在系统中维护可用性，必须进行适当的控制，从而确保被授权的访问和可接受的性能等级、快速处理中断、提供冗余度、维持可靠的备份以及避免数据丢失或破坏。

针对可用性的威胁有很多。这些威胁包括：设备故障、软件错误，以及环境问题(如高温、静电、洪水、断电等)。针对可用性的其他攻击形式还包括 DoS 攻击、客体损坏和通信中断。

与机密性和完整性一样，对可用性的破坏不限于有意攻击。许多对敏感信息的未授权修改实际是由于人为错误、疏忽或失职造成的。导致可用性被破坏的事件包括：意外地删除文件；硬件或软件组件的过度使用；私下分配资源；贴错标签或不正确的客体分类。任何用户(包括管理员)的不当行为都可能破坏可用性，安全策略的疏漏或安全控制的配置不正确也可能导致类似事情的发生。

有许多措施可以确保可用性不会受到可能的威胁。这些措施包括：正确设计中间传输系统、有效地使用访问控制、对性能和网络通信进行监控、使用防火墙和路由器阻止 DoS 攻击、为关键系统实现冗余以及维护和测试备份系统。大多数安全策略，以及业务连续性计划(Business Continuity Planning，BCP)，都集中使用各种级别的访问/存储/安全(即磁盘、服务器或站点)来容错，达到消除单点故障的目标，从而维护关键系统的可用性。

可用性依赖于完整性和机密性。缺乏完整性和机密性，就无法维护可用性。与可用性有关的其他概念、条件和特征包括：使用性、可访问性和时效性。

真实场景

**CIA 优先级**

每个组织机构都有自己独特的安全需求。就 CISSP 考试而言，大多数安全概念只是被笼统地讨论，但是在现实生活中，普通概念和最优方法不适用于具体的安全工作。管理团队和安全团队必须一起工作，从而确定组织的各种安全要求的优先顺序。这项工作包括制定预算费用计划、分派技术与时间，以及集中 IT 人员和安全职员的工作成果。这些活动的一个主要方面是确定组织各种安全要求的优先顺序。了解各种原则或资产的重要程度，能够指导安全观点的形成以及安全解决方案的最终部署。通常，开始建立优先顺序是一项艰巨的任务。面对这样的挑战，可行的解决方案是首先确定机密性、完整性和可用性这三条主要安全原则的优先顺序。对于为组织机构设计内容全面的安全解决方案来说，确定最重要的元素是绝对必要的。由此建立的模式能够复制来自设计、体系结构、部署以及维护方面的概念。

你是否知道自己组织中 CIA 三元组组件的优先顺序？如果不知道，那么请尝试找出优先顺序。

让我们看一个对 CIA 优先顺序概念的有趣归纳：在许多情况下，军队和政府机构倾向于机密性的优先顺序高于完整性和可用性，而私人公司则倾向于可用性的优先顺序高于机密性和完整性。尽管这种优先顺序更关注于某条安全原则，但并不说明可以忽视或不恰当地应对优先顺序排在第 2 位和第 3 位的安全原则。

### 1.1.4　其他安全概念

除了 CIA 三元组以外，在设计安全策略和部署安全解决方案时，还需要考虑其他很多与安全有关的概念和原则。这一节主要讨论身份标识、身份认证、授权、审计、可问责性(见图 1.2)，以及不可否认性。

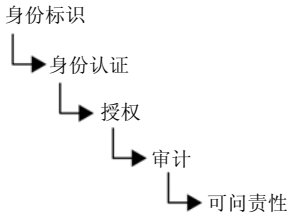


图 1.2　AAA 服务的 5 个要素

#### 1. 身份标识

身份标识是一个过程，在这个过程中，主体会表明身份，并且开启可问责性。主体必须向系统提供身份，从而启动身份认证、授权和可问责性的过程。提供身份的方式可以是：键入用户名、刷智能卡、挥动接近设备、说出一条短语，或将脸、手或手指置于照相机或扫描设备前。提供 ID 号的过程也是身份标识过程。如果没有提供身份，那么系统就没有办法将身份认证因素与主体关联在一起。

一旦主体通过身份标识(也就是识别和验证了主体的身份)，此身份就对主体今后的行为负责。IT 系统根据身份而非主体本身进行跟踪活动。计算机无法区分不同的人，但是却知道不同用户的账户

是有区别的。主体的身份通常被标记为或被视为公共信息。然而，简单地声明身份并不意味着访问或授权。在获得授权访问受控资源之前，身份必须被证明或验证。这个过程称为身份认证。

### 2. 身份认证

认证或测试所声明身份合法性的过程就是身份认证。身份认证要求来自主体的附加信息必须完全对应于被表明的身份。身份认证的最常见形式是使用密码(包括密码的变化形式 PIN 和密码短语)。通过与合法身份(也就是用户账户)数据库中的一种或多种因素进行比较，身份认证能够认证主体的身份。用于认证身份的身份认证因素通常被标记为或被视为私有信息。主体和系统维护身份认证因素隐蔽性的能力直接反映了该系统的安全级别。如果非法获得和使用目标用户身份认证因素的过程相对容易，那么身份认证系统就不安全。如果这个过程相对困难，那么身份认证系统就相当安全。

身份标识和身份认证总是作为一个过程中的两个步骤被一起使用。提供身份是第一个步骤，提供身份认证因素则是第二个步骤。如果不执行上述两个步骤，那么主体就不能获得对系统的访问权限。就安全性而言，缺少其中任何一个步骤都是没用的。

主体能够提供多种身份认证类型(例如，“你知道什么”、“你拥有什么”等)。每种身份认证技术或因素都具有自己独特的优点和弱点。因此，根据每种身份认证技术或因素以及部署的环境来确定是否适用，从而评价每种机制是十分重要的(第13章“管理身份与认证”中详细讨论了身份认证的内容)。

### 3. 授权

一旦主体通过了身份认证，其访问还必须经过授权。授权的过程确保被请求的活动或客体访问，可以获得通过身份认证和指派的权利和特权。在大多数情况下，系统会评估一个访问控制表，这个表会对主体、客体和预计的活动进行比较。如果允许进行指定的操作，那么主体就获得了授权；反之，主体就没有获得授权。

需要记住的是，虽然主体通过了身份标识和身份认证，但是并不意味着在受控环境内被授权执行任何操作或访问所有资源。主体登录某个网络(也就是说，提供了身份标识和通过了身份认证)，但是仍然可能被阻止访问文件或进行打印(也就是说，未授权执行这些活动)。大多数网络用户只是被授权在指定的一组资源上执行数量有限的一些操作。身份标识和身份认证是访问控制的“全有”或“全无”。对于环境中的每个客体，在“全有”与“全无”之间，授权具有非常大的变化。例如，用户也许能够读取某个文件，但是不能删除这个文件；用户也许能够打印文档，但是不能更改打印队列；用户也许能够登录到系统中，但是无法访问任何资源。通常，对授权的定义使用了访问控制模型中的一个概念，例如 DAC、MAC 或 RBAC(参看第 14 章“控制和监控访问”)。

**AAA 服务**

你可能听过 AAA 服务的概念。这三个 A 是 Authentication(认证)、Authorization(授权)和 Accounting(可问责性，有时是 Auditing，意思是审计)的英文缩写。然而，有点让人不明白的是，虽然这是三个英文单词的缩写，但实际上它指的是 5 个元素：身份识别、身份认证、授权、审计和可问责性。因此，第一个和第三个 A 实际上代表了两个概念而非一个概念。这 5 个元素代表了下面的安全性流程:

**识别** 当试图访问受保护区域或系统时声明身份

**认证** 证明身份

**授权**　允许和拒绝对特定身份进行资源和客体的访问

**审计**　记录与系统和主体相关的事件和活动日志

**可问责(又名可问责性)**　审核日志文件，检查符合与违反行为以便主体可为自己的行为负责

虽然 AAA 常用于身份认证系统，但其实 AAA 是所有安全形式的一个基础概念。如果一个安全机制缺少这 5 个元素中的任何一个，这个机制就是不完整的。

### 4. 审计

审计或监控是程序化方式，通过这种方式，主体在系统中经过身份认证的行为是可问责的。审计也是对系统中未授权的或异常的活动进行检测的过程。审计不仅会记录主体及其客体的活动，而且还会记录维护操作环境和安全机制的核心系统功能的活动。通过将系统事件记录写入日志而创建的审计跟踪，可以用于评估系统的健康状况和性能。系统崩溃可能表明存在程序错误、驱动器错误或入侵企图。记录系统崩溃起因的事件日志常常被用于发现系统出现故障的原因。日志文件为重建事件、入侵和系统故障的历史提供了审计跟踪。我们需要通过审计来检测主体的恶意行为、入侵企图和系统故障以及重构事件，为起诉提供证据、生成问题报告和分析结果。审计通常是操作系统、大多数应用程序和服务的内在特性。因此，配置系统功能来记录特定类型事件的相关信息非常简单。

### 5. 可问责性

只有在支持可问责性时，才能够正确实施组织的安全策略。换句话说，只有在主体的活动可问责时，才能够保持安全性。有效的可问责性依赖于检验主体身份以及跟踪其活动的能力。通过审计、授权、身份认证与身份标识这些安全服务和机制，将联机身份的活动与某个人联系在一起，就可以建立可问责性。因此，人员的可问责性最终依赖于身份认证过程的强度。如果没有强大的身份认证过程，那么在发生不可接受的活动时，我们就无法确定与特定用户账户相关联的人员就是实际控制该用户账户的实体。

为了获得切实可行的可问责性，在法律上你必须能够支持自己的安全性。如果不能在法律上支持自己的安全努力，那么就不太可能问责与某个用户账户相关联人员的活动。只使用密码进行身份认证，这显然值得怀疑。密码是最不安全的身份认证形式，针对这种形式的不同攻击方式有数十种之多。不过，如果使用多因素身份认证(例如，组合使用密码、智能卡和指纹扫描)，那么其他人几乎不可能通过攻击身份认证过程来假冒特定用户账户的关联人员。

**法律上的可防御安全性**

安全的要点是：防止坏的事情发生，同时支持好的事情出现。发生坏的事情时，组织常常希望通过法律的实施和法律系统的援助来得到补偿。为了获得法律赔偿，就必须证明存在罪行或者嫌疑人实施了犯罪，以及自己已尽力阻止罪行的实施，只有这样才能从法律上防御保护组织的安全性。如果无法使法庭相信日志文件是准确的，以及只有主体才会实施特定的罪行，那么就无法获得法律赔偿。最终，这就需要一个完整的安全解决方案，这个方案应当使用难以破解的身份认证技术、稳固的授权机制以及完美的审计系统。此外，还必须提供下列证明：组织机构遵守了所有适用的法律和规则；公告了适当的警告和通知；逻辑和物理安全性没有受到其他危害；以及电子证据没有其他可能的合理解释。你要面对这个相当具有挑战性的标准。如果不打算在法律上的可防御安全性的设计和实施方面做出努力，那么尝试低于标准的安全性的要点是什么呢?

#### 6. 不可否认性

不可否认性确保活动或事件的主体无法否认所发生的事件。不可否认性能够防止主体宣称自己没有发送消息、没有执行过某项活动或者不是某个事件的起因。身份标识、身份认证、授权、可问责性和审计使不可否认性成为可能。通过使用数字证书、会话标识符、事务日志以及其他很多传输和访问控制机制，我们能够建立不可否认性。如果没有在系统中构建或正确实施不可否认性，那么就无法认证特定实体是否执行了某种动作。不可否认性是可问责性不可缺少的部分。如果嫌疑人能够否认指控，那么他的行为就无法被问责。

### 1.1.5 保护机制

理解和启用机密性、完整性和可用性概念的另一方面是保护机制的概念，保护机制是安全控制的常见特性。并非所有的安全控制都必须具有这些机制，但是许多控制通过使用这些机制提供对机密性、完整性和可用性的保护。这些机制包括：使用多层次或多级别的访问、利用抽象、数据隐藏以及使用加密。

#### 1. 分层

分层只是简单地使用连续的多重控制，也被称为深层防御。没有一种特定的控制方法能保护并对抗所有可能存在的威胁。使用多层次的解决方案允许引入多种不同的控制方法来应对随时出现的各种威胁。当分层设计安全解决方案时，大多数的威胁都会被消除、缓解或阻挡。

使用连续分层法而不是并行分层法，这一概念非常重要。通过连续方式执行安全限制意味着使用线性的方式依次执行。只有通过一系列配置，才能由每个安全控制对攻击进行扫描、评估或缓解。单个安全控制方法的失败不会使整个解决方案失效。如果安全控制是以并行方式执行的，某个威胁就可能穿过单个检查点，从而无法消除该威胁特殊的恶意活动。

连续配置方法虽然范围很窄，但是层次很深；并行配置方法虽然范围很宽，但是层次很浅。并行系统在分布式计算应用程序中非常有用，但是在安全领域内，并行机制往往不是一种有用的概念。

考虑一下通往建筑物的物理入口。并行安排出入口的方法被用于购物商场，商场周边的许多地方都设置了出入口。连续设置出入口的方式很可能用于银行或机场。这种场合只提供单一的入口，并且此入口实际上是为了获得进入建筑物活动区域而必须按顺序通过的几个关口或检查点。

分层还包括网络由多个独立实体组成的概念，每个实体都有自己独特的安全控制方法与脆弱性。在有效的安全解决方案中，所有构成单个安全防线的网络系统之间存在协同作用，从而共同筑起一道安全防线。使用独立的安全系统会导致生成分层的安全解决方案。

#### 2. 抽象

抽象是为提高效率而使用的。相似的元素被放入组、类别或角色(被整体性授予安全控制、限制或权限)中。因此，当为客体分类或为主体分配角色时，就需要使用抽象的概念。抽象的概念还包括客体和主体类型的定义或客体本身的定义(也就是用于为实体类别定义模板的数据结构)。抽象用于定义客体可以包含的数据类型、可以在这个客体上执行的或由该客体执行的功能类型以及这个客体具有的功能。抽象使你能够为按类型或功能分类的客体组分配安全控制方法，并抽象简化了安全措施。

#### 3. 数据隐藏

顾名思义，数据隐藏通过将数据置于主体不可访问或无法看到的存储空间，从而防止主体发现或访问数据。不让未授权的访问者访问数据库是数据隐藏的一种形式，同样，限制分类级别较低的主体访问级别较高的数据也属于这种情况，阻止应用程序直接访问硬件也是数据隐藏的一种形式。在安全控制和程序设计中，数据隐藏通常是一个关键要素。

#### 4. 加密

加密是对计划外的接收者隐藏通信数据的含义或意图的一门艺术和学科。加密可以具有很多形式，并且能够被应用于所有的电子通信类型，包括文本、音频和视频文件以及应用程序本身。加密技术是安全控制中一个非常重要的要素，尤其系统之间的数据传输更是如此。加密的强度各种各样，每种强度的设计都针对一种特定的用途或目的。第 6 章“密码学与对称加密算法”和第 7 章“PKI 和密码学应用”中详细讨论了加密技术。

## 1.2　应用安全治理原则

安全治理是实践行为的集合，这些实践都与支持、定义和指导组织的安全工作相关。安全治理与组织和 IT 治理密切相关，而且经常交织在一起。这三种治理的目标一般是相同或相关的。例如，治理的共同目标就是确保组织能持续且能随时间的推移不断扩大。因此，治理的共同目标就是维持业务流程，同时努力实现增长和弹性。

由于立法和法规遵从性的需要，一些治理要求会被强加于机构，还有其他一些强加的治理要求可能是由于行业指导方针或许可证所要求的。所有的治理形式，包括安全治理，都必须不时地经受评估和认证。可能由于政府的规定或行业最佳实践，都会对组织有各种审计和认证要求。治理合规问题常常因行业和国家的不同而不同。由于机构扩张和不断去适应全球市场，治理问题变得越来越复杂。再加上各国法律不同以及实际的冲突，这个问题也就更加棘手。组织整体上应该有方向、有指导、有工具、有足够的监督能力和管理能力，如此才能应对威胁和风险，并注重消除故障以及将潜在的损失或损坏降到最低。

如你所知，安全治理的各项定义往往是严标准、高要求。最终，安全治理是要实施安全的解决方案和管理方法，而这两个方面紧密相连。安全治理直接监督和参与各级安全。安全不是并且也不应该只被视为属于 IT 事务。相反，安全影响着组织的方方面面。它不是仅靠 IT 人员自己就可以解决的事情。安全是商业运行问题，是组织流程，而不只是 IT 怪才在幕后所谋之事。使用安全治理这个术语就是为了强调这一点，这意味着安全是需要整个组织同时进行管理和控制的，而不只是在 IT 部门。

### 1.2.1　安全功能战略、目标、任务和愿景的一致

安全管理计划能确保安全策略的适当创建、实现和实施。安全管理计划将安全功能与组织的战略、目标、任务和愿景相结合，这包括根据商业论证、预算限制或稀缺资源设计和实现安全性。为了对做出决定或采取某种形式行动的必要性进行定义，商业论证通常会记录参数或说明立场。制定商业论证就是要说明具体的商业需求，以改变现有业务或选择实现商业目标的方法。商业论证的制

定通常能证明启动了一个新的项目，尤其是与安全相关的项目。同样重要的是，要考虑能够分配的预算有多少，这些预算用于以商业需求为基础的安全防范项目。做好安全防护往往成本很高，但这却是长期可靠经营的重要因素。对大多数机构而言，资金和资源，比如人、技术和空间，都是有限的。由于有这样的资源限制，因此需要努力实现利益最大化。

解决安全管理计划编制的最有效方法是采用自上而下的方式。上层、高层或管理部门负责启动和定义组织的安全策略。安全策略为组织中较低级别的人员指出了方向。中层管理部门的职责是在安全策略的指导下制定标准、基准、指导方针和程序。接着，操作管理者或安全专家负责实现在安全管理文档中规定的配置要求。最后，最终用户必须遵守组织制定的所有安全策略。

**注意：**

*与自上而下方式相反的是自下而上。在采用自下而上方式的环境中，IT 人员在没有来自高层管理部门指示时直接进行安全判断。组织极少使用自下而上的方式，在 IT 行业中，这种方式被认为存在问题。*

安全管理部门(而不是 IT 人员)负责更高层的管理，并且考虑的是业务运营问题，而不是 IT 管理问题。安全管理团队或部门负责组织内的安全性，应当独立于其他所有部门。信息安全团队应当由指定的首席安全官(Chief Security Officer，CSO)领导，CSO 必须直接向高级管理者报告。为 CSO 及其团队赋予组织特有分级结构之外的自主权，这不仅能够改善整个组织之间的安全管理，而且有助于避免部门交叉和内部权力斗争问题。

安全管理计划编制的元素包括：定义安全角色；规定如何管理安全性、谁负责安全性以及如何测试安全性的效力；开发安全策略；执行风险分析；以及要求对员工进行安全教育。这些职责要经过管理计划开发的指导。

如果缺少一个关键因素(得到高级管理者的批准)，那么再好的安全计划也是无用的。缺少高级管理者的批准和委托，安全策略就无法取得成功。策略开发团队负责对高级管理部门进行充分的教育，从而使其理解即使采取安全策略所规定的安全措施之后也仍然存在的风险、义务和暴露。开发和实现安全策略能够证明高级管理者对安全性问题进行了适度关注并尽责。如果某个公司没有对安全性进行适度关注并尽责，那么管理者就对疏忽负有责任，并且应当为资产损失和财务损失担责。

安全管理计划编制团队应该开发下列三种计划(如图1.3所示)：

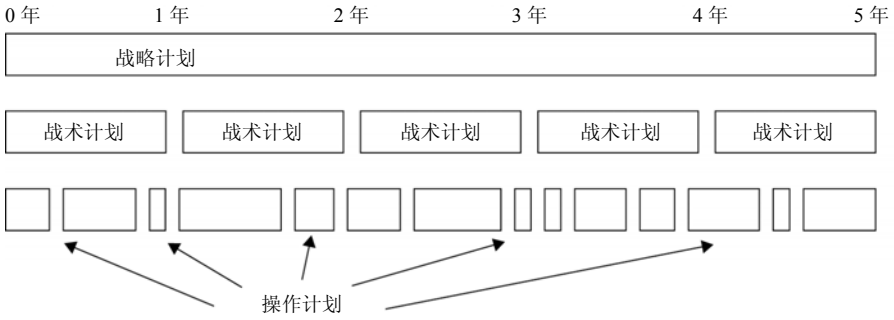


图 1.3　战略计划、战术计划和操作计划的时间线比较

**战略计划**　战略计划是一个相当稳定的长期计划，它定义了组织的目标，也有助于理解安全功能与组织的安全目标、愿景和使命方面的一致性。如果战略计划每年都被维护和更新，那么大约可

以使用 5 年时间。战略计划还可以作为计划编制的基准。未来的长期目标和愿景在战略计划中将被讨论。战略计划还应当包含风险评估。

**战术计划**　战术计划是一个中期计划，它被开发用于提供实现战略计划所提出目标的详细细节。战术计划通常一年有效，并且往往规定和调度实现组织目标所必需的任务。战术计划的一些示例包括：项目计划、采购计划、雇佣计划、预算计划、维护计划、支持计划以及系统开发计划。

**操作计划**　操作计划是一个短期计划，它是基于战略计划和战术计划制定的非常周详的计划。操作计划只在很短的时间内有效或有用。为了服从战术计划，操作计划必须经常被更新(如每个月或每个季度都进行更新)。操作计划是十分周详的计划，它清楚地说明了如何完成组织机构的各种目标。操作计划包括：资源分配、预算要求、人员分配、进度安排以及循序渐进或实现措施。操作计划包括实现如何服从组织安全策略的详细措施细节。操作计划的示例包括：培训计划、系统部署计划和产品设计计划。

维护安全性是一个持续的过程。虽然安全管理计划编制的活动可能具有一个明确的起始点，但是其任务和工作永远不可能完全实现或完成。有效的安全计划重点关注特定的和可完成的目标、预计变化和潜在问题，并且作为整个组织决策的基础。安全文档记录应当是具体的、定义完善的和清晰表述的。为了使安全计划有效，就必须开发、维护和实际应用安全计划。

### 1.2.2　组织流程

安全治理需要照顾到组织的方方面面，包括收购、剥离和治理委员会等组织流程。收购兼并会增加机构的风险等级，这些风险包括不适当的信息披露、数据丢失、故障或未达到足够的投资回报率(Return On Investment，ROI)。除了收购兼并中的典型商业和财务方面，有效的安全监督和强化审查往往也是降低损失可能性的必要措施，比如在转型期。

同样，剥离、任何形式的资产减少或员工减少都会使阶段内的风险等级变高，从而也需要提高集中安全治理的必要性。需要对资产进行无害处理以防止数据泄漏。应该删除和销毁存储介质，因为介质净化处理技术不能完全保证可以防止数据残留被恢复。需要对不再负责相关事宜的员工进行事后审查，这个过程通常被称为离职面谈。这个过程也通常涉及审查所有的保密协议和其他具有约束力的合同或协议，这些文件需在他们离职后依然有效。

通常，安全治理由治理委员会或至少是董事会进行管理。这群人应是有影响力的专家，他们的主要任务是监督和指导确保组织安全与操作的行为。由于安全是一项复杂的任务，很多组织由于太大无法从个人视角理解这个问题。最可靠的策略是集齐一组专家共同为实现可靠安全治理这一目标而努力。

加强安全治理的两个必要额外组织流程的实例是变更控制/变更管理和数据分类。

#### 1. 变更控制/变更管理

安全管理中的另外一个重要方面是对变更进行控制或管理。安全环境的改变可能引入会导致新脆弱性出现的漏洞、重叠、客体丢失和疏漏。面对变更，维持安全性的唯一方法是系统地管理变更，这往往涉及对安全控制和机制相关的活动，进行广泛的计划编制、测试、日志记录、审计和监控。然后对环境变化进行记录，确定变更的作用者，无论这些作用者是主体、客体、程序、通信路径还是网络本身。

变更管理的目标是确保任何变更都不能降低或危及安全性。变更管理还负责能够将任何变更都

回滚到先前的安全状态。变更管理可以在任何系统上实现(不考虑安全级别)。变更管理要求系统遵守信息技术安全评估标准(Information Technology Security Evaluation and Criteria，ITSEC)的 B2、B3 和 A1 分类。最终，通过避免对已实现的安全性带来无意识的、间接的或连带性的降低现象，变更管理能够改善环境的安全性。尽管变更管理的一个重要目标是防止安全性被不期望地降低，但其主要用途是：详细记录和审计所有变更，从而能够通过管理进行详细的检查。

变更管理应该用于监督系统每个方面发生的变更，包括硬件配置、操作系统和应用软件的变更。变更管理应该被包含在设计、开发、测试、评估、实现、分发、演变、发展、持续操作以及修改中。变更管理不仅需要每个组件和配置的详细目录，而且还需要为每个系统组件(从硬件到软件，以及从配置设置到安全特性)收集和维护完整的文档。

配置或变更管理的变更控制过程具有以下几个目标或要求：

- 以受监控的和有序的方式实现变更。变更总是处在控制之下。
- 包含正式的测试过程，这种过程用于确认变更产生的预期结果。
- 所有的变更都可以撤消(也被称为回退或回滚计划/流程)。在变更发生前向用户发出通知，以避免降低生产率。
- 对变更的影响应进行系统分析。
- 变更对能力、功能和性能产生的负面效应最小化。
- 变更由变更审批委员会(Change Approval Board，CAB)审阅和批准。

并行运行是变更管理过程的一个示例，在这种新系统部署测试中，新系统和旧系统并行运行。每个主要的或重要的用户进程在所有系统上同时执行，从而确保新系统支持老系统所支持或提供的所有必需的业务功能性。

### 2. 数据分类

数据分类是根据数据的秘密性、敏感性或机密性需求来保护数据的主要方式。在设计和实现安全系统时，因为某些数据项需要更高的安全性，所以对所有数据采取同样的处理方法是低效率的。用较低安全级别来保护所有数据，意味着敏感数据很容易被访问。用较高安全级别保护所有数据，成本太高且对未分类的非关键数据访问限制太多。数据分类用于确定需要分配多少工作量、资金和资源去保护数据以及控制对数据的访问。数据分类或归类，是根据相似，性组织项、对象和主题到组、类别和集合中的过程。这些相似性可能包括价值、成本、灵敏度、风险、脆弱性、权力、特权、损失或损害的可能水平以及“需知”原则。

数据分类方案的主要目的是：根据重要性和敏感性给数据分配标签，对数据安全保护过程进行规范化和层次化。数据分类用于为数据存储、处理和传输提供安全机制，此外还可以确定如何从系统中删除数据和销毁数据。

使用数据分类方案具有下列优点：

- 能够证明组织致力于保护宝贵的资源和资产。
- 能够有助于确定对组织最关键的或最有价值的资产。
- 为安全机制的选择提供安全保证。
- 常常是遵守规范或法律约束所必需的。
- 帮助定义访问级别、授权使用类型，以及对不再有价值的资源进行解除分类和/或对于销毁操作所需的参数。
- 在数据生命周期管理中，对于确定数据的存储(保留)时长、使用和销毁是有帮助的。

数据分类标准取决于执行分类的组织。不过，从通用或标准化分类系统中可以找到很多一般性原则：

- 数据的有用性。
- 数据的时效性。
- 数据的价值或成本。
- 数据的成熟度或年龄。
- 数据的生存期(或何时过期)。
- 与人员的关联。
- 数据泄露的损失评估(也就是数据泄露会对组织有何影响)。
- 数据修改的损失评估(也就是修改数据会对组织有何影响)。
- 数据的国家安全性含义。
- 对数据的已授权访问(也就是谁可以访问数据)。
- 对数据的访问限制(也就是谁对数据的访问受到限制)。
- 数据的维护和监控(也就是谁应该维护并监控数据)。
- 数据的存储。

使用适用于组织的标准、评估数据以及适当地分配数据分类标签。在某些情况下，数据分类标签被添加到数据对象中。在其他情况下，通过把数据放入存储机制或放在安全保护机制之后就可以分配数据分类标签。

为了实现分类方案，必须完成下列 7 个主要的步骤或阶段：

(1) 确定管理人员并定义他们的职责。

(2) 指定如何对信息进行分类和标记的评估标准。

(3) 为每个资源进行分类和添加标签(所有者主导这个步骤，但是必须有监督人员进行检查)。

(4) 记录发现的分类策略的所有例外，并且将这些例外集成到评估标准中。

(5) 选择应用于每个分类级别的安全控制，从而提供必要的保护级别。

(6) 指定解除资源分类的过程以及将资源的保管权转移给外部实体的过程。

(7) 创建一份整个组织范围内都知晓的计划，从而指导所有人员对分类系统的使用。

在设计分类系统和记录使用过程时，往往会忽视解除分类。一旦某个资产不再需要当前分配的分类或敏感性级别保护，就需要解除分类。换句话说，如果资产是新的，它会被分配一个比当前级别更低的敏感性标签。在资产不能根据需要被解除分类时，安全资源就会被浪费，并且更高敏感性级别的价值和保护会被降低。

两种通用的分类方案是政府/军方分类(见图 1.4)和商业/私营部门分类。政府/军方分类具有 5 个级别(以下按从高到低列出)：

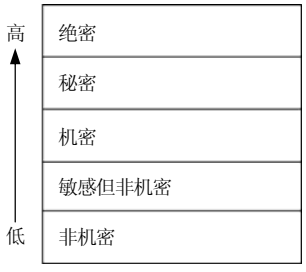


图 1.4　政府/军队分类的级别

**绝密(top secret)** 最高的分类级别。未授权而泄露绝密数据将会有灾难性的后果，并导致对国家安全的毁灭性破坏。

**秘密(secret)** 用于具有受限特性的数据。未授权而泄露秘密数据将会有严重后果，并导致对国家安全的重大破坏。

**机密(confidential)** 用于具有机密特性的数据。未授权而泄露机密数据将会有重大后果，并导致对国家安全的严重破坏。这个分类级别被用于处在“秘密”级别和“敏感但非机密”级别之间的所有数据。

**非机密(unclassified)** 最低的分类级别。用于既不敏感，也不必分类的数据。非机密数据的泄露既不会危及机密性，也不会造成任何明显的损坏。

**提示：**

采用首字母记忆法可以按照从低到高的安全顺序轻易地记住政府或军方分类方案的 5 个级别：U.S.Can Stop Terrorism(美国能够制止恐怖主义)。你会看到：从左至右的 5 个大写字母分别表示从低到高的 5 个指定分类级别(或者说图 1.4 中自下而上地列出 5 个级别项)。

机密级别、秘密级别和绝密级别统称为分类的级别。通常，对未授权的个人泄露真实的数据分类是一种数据侵权行为。因此，术语“分类的”通常用于指示敏感但非机密级别以上的被分级的数据。所有分类的数据都免受信息自由法案以及其他很多法律与规章的限制。美国军队的分类方案与数据的敏感度关系最密切，而且关注于对机密性的保护(也就是防止泄漏)。根据危害机密性事件的破坏程度，可以粗略地定义每个分类级别或标签。绝密级别的数据泄漏会对国家安全造成毁灭性破坏，而非机密级别的数据泄漏则不会对国家安全或地方安全造成任何严重破坏。

商业/私营部门的分类系统通常相差很大，因为他们的特点就是不会坚守一个标准或法规。CISSP 考试侧重于 4 种常见或可能的商业分类级别(图 1.5 显示了从最高到最低的级别)：

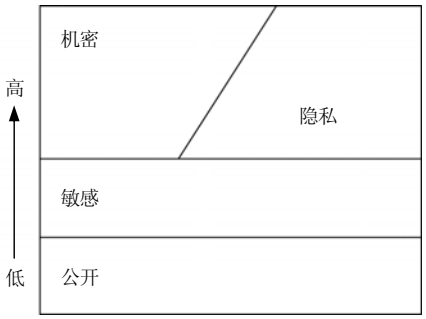


图 1.5 商业/私营部门分类的级别

**机密** 最高的分类级别，用于极端敏感的和只能内部使用的数据。如果机密数据被泄露，那么会对公司产生重大的负面影响。有时也用标签“专有数据”来替代标签“机密信息”。如果专有数据被泄露，将会对组织的竞争力产生灾难性后果。

**隐私** 用于具有隐私性或个人特性以及只供内部使用的数据。如果隐私性数据被泄漏，那么会对公司或个人产生重大的负面影响。

**注意：**

商业/私营部门分类方案中的机密和隐私性数据要求大致相同的安全保护级别。这两个标签的实际差异是：机密数据被用于公司数据，而隐私性数据则被用于与个人有关的数据(例如医疗数据)。

**敏感**　用于分类级别高于公开数据的数据。如果敏感数据被泄漏，那么会对公司产生负面影响。

**公开**　最低的分类级别，用于不属于任何一种较高分类级别的所有数据。这种数据的泄漏不会对组织造成严重的负面影响。

数据分类还要考虑的一个相关因素就是所有权。所有权是对个人或群体职责的正式指定。所有权可以明确区分操作系统中的哪些文件或其他类型客体被分配给一个所有者。通常，一个所有者对其拥有的客体具有完整的功能和权限。所有权通常归属于操作系统内功能最强大的账户，比如 Windows 系统中的管理员或 Unix 和 Linux 系统中的 root 用户。在大多数情况下，主体在创建新客体时，该客体的所有者是默认的。但有些环境的安全策略要求在创建新对象时，必须对从最终用户到管理员或管理用户的所有权进行正式变更。在这种情况下，管理员账户可以直接获取新客体的所有权。

除了正规的 IT 结构，其他结构的客体的所有权通常都不明显。公司文档可以为设施、商业任务、流程、资产等定义所有者。然而，这样的文档编制在现实世界中并不总能够“执行”。文件客体的所有权是由操作系统和文件系统执行的，其中物理客体、无形资产或机构概念(如研发部门或项目)的所有权只能进行书面定义，所以容易遭到破坏。必须对物理世界中的所有权实施额外的安全治理，如此才能达到加强效果。

### 1.2.3　安全角色和责任

安全角色是指个人在组织内部的整个安全实现和管理方案中所扮演的角色。因为并不总是明确的或静态的，所以安全角色在工作描述中不是必须被规定的。熟悉安全角色将对在组织内部建立通信和支持结构很有帮助，这种结构能够支持安全策略的部署和执行。接下来，我们将按照在安全环境中出现的逻辑顺序介绍 6 种安全角色：

**高级管理者**　组织所有者(高层管理者)的角色被分配给最终负责组织机构安全维护和最关心保护资产的人。高层管理者必须对所有策略问题签字。事实上，所有活动在被执行之前，都必须得到高层管理者的认可和签字。如果没有高层管理者的授权和支持，那么就不存在有效的安全策略。高层管理者对安全策略的认同表明承认在组织机构内部实现的安全性的所有权。高层管理者对安全解决方案的总体成败负有责任，并且负责对组织机构建立安全性予以适度关注并尽职尽责。

虽然高层管理者对安全负有最终责任，但他们实际上很少去实现安全解决方案。在大多数情况下，相应的责任会被委派给组织内部的安全专家。

**安全专家**　安全专家、信息安全官或计算机应急响应团队(Computer Incident Response Team，CIRT)的角色被分配给受过培训和经验丰富的网络工程师、系统工程师和安全工程师，他们对落实高层管理部门下达的指示负责。安全专家的职责是保证安全性，包括制定和实现安全策略。安全专家的角色可以被标记为 IS/IT 职能角色。安全专家的角色通常由负责设计和实现安全解决方案的团队担任，安全解决方案则是根据已批准的安全策略制定的。安全专家不是决策制定者，他们只是实现者。所有的决策都必须由高层管理者制定。

**数据所有者**　数据所有者的角色被分配给在安全解决方案中为了放置和保护信息而负责对信息进行分类的人。通常，数据所有者是层次较高的、最终负责数据保护的管理者。然而，数据所有者一般会将实际管理数据的任务委派给数据管理员。

**数据管理员**　数据管理员的角色被分配给负责实施安全策略和上层管理者规定的保护任务的用户。数据管理员通过执行所有必要的措施为数据提供适当的 CIA 三元组(机密性、完整性和可用性)

保护，并完成上层管理者委派的要求和责任。这些必要的措施包括：完成和测试数据备份、确认数据的完整性、部署安全解决方案以及根据分类管理数据存储。

**用户** 用户(最终用户或操作者)的角色被分配给具有安全系统访问权限的任何人。用户的访问权限与他们的工作任务联系在一起并且受到限制，所以他们只具有工作职务所要求的能保证完成任务所需的权力(也就是最小特权原则)。用户负责了解组织的安全策略，并遵守规定的操作过程，在已定义的安全参数内进行操作，以便维护安全策略。

**审计人员** 另一个角色是审计人员。审计人员负责测试和认证安全策略是否被正确实现以及衍生的安全解决方案是否合适。审计人员的角色可以被分配给安全专家或受过培训的用户。审计人员要完成遵守情况报告和有效性报告，高层管理者会审查这些报告。通过这些报告发现的问题，会由高层管理者转换成下达给安全专家或数据管理员的新指示。不过，因为审计人员需要将用户或操作者在环境中的工作作为审计和监控的活动来源，所以审计人员被列为最后一个角色。

所有这些角色在安全环境中都起着重要的作用。对于确定义务和责任以及确定分级管理和任务委派方案，这些角色都非常有用。

### 1.2.4 控制架构

为组织起草安全性立场通常会涉及很多事情，不只是写下几条远大的理想。在多数情况下，制定可靠的安全策略会涉及很多规划。许多读者可能认识到这个看似荒谬的概念，即召开会议为未来制定计划。事实证明，为安全制定计划必须从规划计划开始，然后规划标准和合规，最后再进行实际的计划开发和设计。跳过这些“规划计划”中的任何一步都可能使计划在开始之前就发生偏移。

安全计划步骤中最重要的一步，也是第一步，就是考虑组织想要的安全解决方案的整体控制框架或结构。可以从几个与安全性相关的概念基础设施中进行选择；而 CISSP 考试覆盖的一个方面是信息及相关技术控制目标(Control Objectives for Information and Related Technology，COBIT)。COBIT 记录了一整套优秀的 IT 安全实践，这些是由国际信息系统审计协会(Information System Audit and Control Association，ISACA)起草的。COBIT 规定了安全控制的目标和要求，鼓励将 IT 的理想安全目标映射到商业目标中。COBIT 5 的基础是企业 IT 治理和管理的 5 条关键原则：原则 1：满足利益相关者的需求；原则 2：对企业做到端到端的覆盖；原则 3：使用单一的集成框架；原则 4：使用整合处理法；原则 5：把治理从管理中分离出来。COBIT 不仅可用于计划组织的 IT 安全，也可以作为组织审计师的指导方针。

幸运的是，这一考试只是参考了COBIT的大体内容，不需要了解很多详细内容。但是如果对这个概念有兴趣，可访问ISACA网站(www.isaca.org)，或者如果想有个总体概览，可阅读维基百科对COBIT条目的解释。IT安全还有很多其他的标准和指导方针，包括《开源安全测试方法手册》(OSSTMM)、ISO/IEC 27002(取代了ISO 17799)和信息技术基础设施库(ITIL，更多信息可参见www.itlibrary.org)。

### 1.2.5 应尽关注和应尽职责

为什么规划安全计划如此重要？一个原因就是，这是应尽关注和应尽职责的要求。应尽关注是通过合理的关注保护组织利益。应尽职责是不断实践能够维持应尽关注成果的活动。例如，应尽关注会开发规范化的安全结构，这个结构会包含安全策略、标准、基线、指导方针和程序；而应尽职

责是继续将这个安全结构应用到机构的 IT 基础设施中。操作性安全需要组织内各责任方都能够对应尽关注和应尽职责保持持续不断的维护。

当今的商业环境，必须要谨慎。做到应尽关注与应尽职责是唯一能够证明损失发生不是因为疏忽的方法。高管必须做到应尽关注和应尽职责才能在出现损失时减少他们的过失和责任。

## 1.3　开发和文档化安全策略、标准、指导方针和程序

对于大多数的组织来说，维护安全性是业务发展的重要组成部分。如果安全受到严重危害，那么许多组织就无法正常运作。为了减少出现安全故障的可能性，已经在一定程度上规范了实现安全性的过程。这种规范化过程大大减少了为 IT 基础架构设计和实现安全解决方案中的混乱和复杂性(开发和实现文档化的安全策略、标准、指导方针和程序能产生坚实可靠的安全基础设施。安全解决方案的规范化采取了文档的分级组织形式，每个级别都关注信息和问题中的一个特定类型或类别。

### 1.3.1　安全策略

规范化的最高层次被称为安全策略。安全策略是一个文档，这个文档定义了组织所需的安全范围，并且讨论了需要保护的资产以及安全解决方案为提供必要保护而应当涉及的范围。安全策略概述或归纳了组织的安全需求，定义了主要的安全目标，并且概述了组织的安全架构。安全策略还确定了数据处理的主要功能领域，并且澄清和定义了所有相关的术语。安全策略应当清楚地定义为什么安全性很重要以及哪些资产是有价值的。它是实现安全性的战略计划。安全策略应当广泛地概括出用于保护组织切身利益的安全目标和原则。文档讨论了安全性对于日常营业每个方面的重要性以及高层职员对实现安全措施予以支持的重要性。安全策略被用于分配职责、定义角色、指定审计要求、概述实施过程、指明遵循要求以及定义可接受的风险级别。这个文档通常用于证明高层管理部门为保护不遭受入侵、攻击和灾难予以应有的关注。安全策略是强制性的。

许多组织都采用多种类型的安全策略来定义或概括它们整体的安全策略。组织安全策略的重点集中在与组织所有方面的相关问题上。特定问题的安全策略集中在特定的网络服务、部门、功能或有别于组织整体的其他方面。特定系统的安全策略关注个别系统或系统类型，并且规定了被认可的硬件和软件，概述了锁定系统的方法，甚至委托防火墙或其他特定的安全控制。

除了这些针对特定部分的安全策略类型以外，还有三种综合的安全策略类别；规章式的策略、建议式的策略和信息式的策略。只要行业或法律标准适用于你的组织，那么就需要规章式的策略(regulatory policy)。这种策略讨论了必须遵守的规章制度，并概略说明了用于让人们遵守规章制度的安全措施。建议式的策略(advisory policy)讨论可接受的行为和活动，并且定义违背安全性的后果。这种策略解释了高层管理部门对组织内部安全和遵守规定的期望。大多数安全策略都是建议性的。信息式的策略(informative policy)被设计用于提供特定主体的相关信息或知识，例如公司目标、任务声明或者组织如何与合作伙伴和客户进行交流。信息式的策略提供了与整个策略特定元素相关的支持、研究或背景信息。

从安全策略可以引出完整安全解决方案所需的其他很多文档或子元素。策略是广泛的概述，而标准、基准、指导方针和程序包括了更加特定的、详细的与实际安全解决方案有关的信息。标准处于安全策略的下一个层次。

**安全策略与个体**

作为一条经验法则，安全策略(以及标准、指南和程序)应当不针对特定的个体。安全策略并不为某个人分配任务和职责，而是为特定的角色定义任务和职责。这个角色可能具有行政管理控制或人员管理职责。因此，安全策略会定义安全基础架构内不同角色必须执行的操作，而不会定义哪些人负责做哪些事情。随后，这些已定义的角色作为工作描述或指定的工作任务被分配给个人。

**可接受的使用策略**

可接受的使用策略是一个常规生成的文档，它属于整个安全文档记录基础架构的一部分。可接受的使用策略被特别设计用于分配组织内的安全角色以及确保职责与这些角色相联系。此策略定义了可接受的性能级别以及对行为和动作的期望。不遵循该策略会导致工作行动警告、惩罚或解聘。

### 1.3.2 安全标准、基准及指南

一旦设定了主要的安全策略，就可以在这些策略的指导下拟定剩余的安全文档。标准为硬件、软件、技术和安全控制方法的统一使用定义了强制性要求。标准提供了操作过程，在这个过程中，整个组织内部统一实现技术和措施。标准是战术文档，定义了达到安全策略指定的目标和总体方向的步骤或方法。

下一个层次是基准。基准定义了安全性的最低级别，组织中的所有系统都必须达到基准要求。没有达到基准的所有系统都应该被排除在生产系统之外，直至这些系统被提升达到基准要求为止。基准建立了通用的安全状态基础，所有附加的和更严格的安全措施可以被建立在这个基础之上。基准通常是系统特定的，并且往往指的是行业或政府标准，例如可信任计算机系统评估标准(TCSEC)、信息技术安全评估和标准(ITSEC)以及 NIST(美国国家标准技术研究院)标准。

指南是规范化安全策略结构的下一个元素。指南提供了如何实现标准和基准的建议，并且能够作为安全专家和用户的操作指南。指南具有灵活性，因此为了适合每种特定的系统或条件，它们可以被定制，并且能够在新措施的创建过程中使用。指南说明了应当部署哪些安全机制，而不是规定特定的产品或控制以及详细的配置设置。指南概述了一套方法(包括行动建议)，但并非强制性的。

### 1.3.3 安全程序

程序是规范化安全策略结构的最后一个要素。程序是详细的、按部就班的指导文档，它描述了实现特定安全机制、控制或解决方案所需的确切行动。程序可以讨论整个系统的部署操作或者关注单个产品或方面，例如部署防火墙或更新病毒定义。大多数情况下，程序仅限于具体的系统和软件。随着系统硬件和软件的发展，程序必须被不断更新。程序的目的是确保业务流程的完整性。如果通过某个详细的程序能够达到所有目的，那么所有活动都应当遵循策略、标准和指导方针。程序有助于在所有系统之间确保安全性的标准化。

通常，策略、标准、基准、指导方针和程序只是在顾问或审计人员的敦促下，作为事后产生的想法进行发展。如果这些文档没有被使用和更新，那么安全环境的管理就无法将它们作为指南使用。如果没有这些文档提供的计划编制、设计、结构和监督，就无法维持环境的安全，也无法代表已经

尽责并给予适度的关注。

此外，开发一个包含上述所有元素方面的文档是一种惯用做法。事实上，我们应该避免这种做法。这些结构中的每一个都必须作为独立的实体存在，其原因在于每种结构执行不同的特殊功能。在规范化结构的顶层(也就是安全策略)，因为只包含全面的、一般性的观点和目标，所以文档较少。在规范化结构的较低层(也就是指南和程序)有比较多的文档，因为它们包含数量有限的系统、网络、部门和区域的特定详细信息。

将这些文档作为独立的实体保存，具有以下一些好处：

- 不是所有的用户都需要知道所有安全分类层次中的安全标准、基准、指导方针和程序。
- 当发生变化时，可以较为方便地只更新和重新分配受影响的资源，而不用更新整个策略以及在整个组织机构中进行重新分配。

拟定整个安全策略及所有支持性文档是一个令人畏惧的任务。许多组织只是致力于定义基本的安全参数，较少详细说明日常活动的每个方面。不过在理论上，详细和完整的安全策略以针对性的、有效的和特定的方式支持现实生活中的安全性。如果安全策略文档相当完整，就可以用于指导决策、培训新用户、回应问题以及预测未来的发展趋势。安全策略不应当是一种事后的考虑或想法，而应当是建立组织的一个关键部分。

对包含完整安全策略的文档的理解还有一些其他视角。图 1.6 展示了这些组件的依赖关系：策略、标准、指南和程序。安全策略是有组织的安全文档的总体结构的基础。然后，标准基于策略并受规章制度的管辖。指南从中衍生而来。最后，程序基于结构的三个基本层。使用倒金字塔来表示每个文档的体积或大小。完整安全策略中的程序通常都要比任何单个元素中的程序要多得多。相比较而言，指南要比策略少，标准也比策略少，并且通常整体或全组织范围内的安全策略甚至也更少。

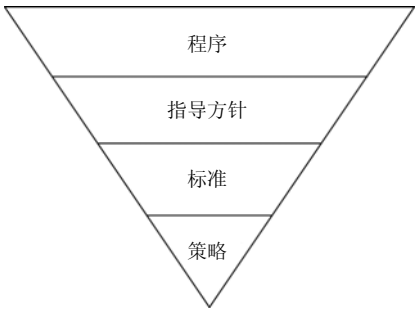


图 1.6　完全策略组件的比较关系

## 1.4　理解和应用威胁建模

威胁建模是潜在威胁被识别、分类和分析的安全流程。威胁建模在设计和开发过程中可以作为一种积极主动的措施执行，而产品一旦被部署，就会被作为一种被动式措施。在这两种情况下，流程会识别潜在危害、发生的概率、问题优先级以及消除或减少威胁的手段。

威胁建模并不意味着是一个单独的事件。相反，组织在系统设计流程早期就开始威胁建模并在整个系统周期内一直持续是很常见的。例如，微软使用安全开发生命周期(Security Development Lifecycle，SDL)流程在产品的每个开发阶段考虑和实现安全。这支撑了这句箴言：“设计安全、默认安全、部署和沟通安全”(也称为 SD3 + C)。这一流程有两个目标：

- 减少安全相关的设计和编码缺陷的数量
- 降低剩余缺陷的严重程度

换句话说，试图减少漏洞，降低任何存在缺陷的影响。总的结果是减少风险。

威胁建模的主动式方法发生于系统开发的早期阶段，特别是在初始设计和规范建立阶段。这种类型的威胁建模也被称为防御方式。这种方式基于编码和制作流程中对威胁的预测和特定防御中的设计，而不是依靠部署后的更新和补丁。大多数情况下，集成安全解决方案更符合成本效益，比后面硬塞的方案更成功。遗憾的是，并不是所有的威胁都可以在设计阶段预测出来，所以仍然需要被动式的威胁建模来解决不可预见的问题。

威胁建模的被动式方法发生在产品被创建和部署之后。此部署可以在测试或实验室环境中，或是指被部署到一般市场上。这种类型的威胁建模也被称为对抗方式。这种威胁建模的技术是道德黑客攻击、渗透测试、代码审查和模糊测试背后的核心概念。尽管这些流程通常有助于发现需要解决缺陷和威胁，但遗憾的是，它们需要额外的编码努力来增加到新对策中。从长远来看，回到设计阶段可能会产生更好的产品，但从头开始是非常昂贵的，并会造成产品发布时间的极大延迟。因此，捷径是在部署后精心制作需要增加到产品中的更新或补丁。这样的结果就是，可能在牺牲了功能性和用户友好性的前提下，也未带来更有效的安全改进(相比主动式威胁建模来说)。

**注意：**

模糊测试是一项专门的动态测试技术，它向软件提供了许多不同类型的输入，来强调其局限性并发现先前未被发现的缺陷。模糊测试软件向软件提供无效输入，可能是随机生成，也可能是专门制作以触发已知的软件漏洞。然后，模糊测试者会监控应用程序的性能，观察软件崩溃、缓冲区溢出或其他不良和/或不可预知的结果。可参考第 15 章“安全评估和测试”以查看更多有关模糊测试的内容。

### 1.4.1 识别威胁

可能的威胁几乎是无限的，所以使用一种结构化的方法来准确地识别相关威胁是很重要的。例如，一些组织使用以下三种方法中的一种或多种：

**关注资产** 这种方法使用资产的估值结果，并试图识别对于宝贵资产的威胁。例如，可以评估一个特定的资产，以确定其是否容易受到攻击。如果资产寄存着数据，则可以评估访问控制来识别能够绕过身份认证或授权机制的威胁。

**关注攻击** 一些组织能够识别潜在的攻击者，并能够基于攻击者的目标识别他们所代表的威胁。例如，政府往往能够识别潜在的攻击者，并识别攻击者想要达到的目标。然后他们可以使用这种知识来识别并保护他们的相关资产。这种方法面临的一个挑战是，可能会出现以往未被视为一种威胁的新攻击者。

**关注软件** 如果一个组织开发了一个软件，则可能会考虑针对软件的潜在威胁。尽管几年前组织一般不自己开发软件，但如今这已非常常见。具体地说，大多数组织都有网络存在，许多都创建了自己的网页。精美的网页带来更多的流量，但他们也需要更复杂的编程，并会受到更多的威胁。

如果威胁被确定为攻击者(而不是自然威胁)，那么威胁建模尝试确定攻击者可能会试图达到什么目的。有些攻击者可能想禁用系统，而其他攻击者可能想要窃取数据。一旦确认了这种威胁，就会基于目标或动机对他们进行分类。此外，将威胁和漏洞进行并列，来识别可能通过利用漏洞给组

织带来重大风险的常见威胁。威胁建模的一个终极目标就是优先处理针对组织宝贵资产的潜在威胁。

当试图对威胁进行盘点并分类时，使用指南或参考通常是有用的。微软开发了一个称为 STRIDE 的威胁分类方案。STRIDE 的使用经常与对应用程序或操作系统威胁的评估相关。然而，它也可以用于其他情境。STRIDE 是以下几个单词的首字母缩写：

- 电子欺骗(Spoofing)——通过使用伪造身份获得对目标系统访问的攻击行为。电子欺骗可以用于 IP 地址、MAC 地址、用户名、系统名称、无线网络名称、电子邮件地址以及许多其他类型的逻辑标识。当攻击者将自己伪装成一个合法或授权的实体时，他们往往能够绕过针对未授权访问的过滤器和封锁。一旦电子欺骗攻击让攻击者成功访问目标系统，后续的滥用、数据盗窃或特权提升攻击就都可以发起。
- 篡改(Tampering)——任何对数据进行未授权的更改或操纵的行为，不管是传输中的数据还是被存储的数据。使用篡改来伪造通信或改变静态信息。这种攻击是对完整性和可用性的侵害。
- 否认(Repudiation)——用户或攻击者否认执行了一个动作或行为的能力。通常攻击者会否认攻击，以便保持合理的推诿，从而不为自己的行为负责。否认攻击也可能会导致无辜的第三方因安全违规而受到指责。
- 信息披露(Information disclosure)——将私人、机密或受控信息揭露、传播给外部或未授权实体的行为。这可能包括客户身份信息、财务信息或自营业务操作细节。信息披露可以利用系统设计和实现错误，如未能删除调试代码、留下示例应用程序和账户、未对客户端可见内容的编程注释(如 HTML 文档中的注释)进行净化或将过于详细的错误消息暴露给用户。
- 拒绝服务(DoS)——指攻击试图阻止对资源的授权使用。这可以通过缺陷开发、连接重载或流量泛滥实现。DoS 攻击并不一定会导致对资源的完全中断；而是会减少吞吐量或造成延迟，以阻碍对资源的有效利用。尽管大多数 DoS 攻击都是暂时的，只在攻击者进行袭击时存在，但还是存在一些永久性的 DoS 攻击。永久 DoS 攻击可能涉及对数据集的破坏、使用恶意软件对软件进行替换，或强迫可以被打断或安装错误固件的固件 flash 操作。这些 DoS 攻击将造成系统的永久受损，使其不能使用简单的重启或通过等待攻击者结束而恢复正常操作。要从永久 DoS 攻击中恢复过来，将需要进行完整的系统修复和备份恢复。
- 权限提升(Elevation of privilege)——此攻击是指有限的用户账号被转换成拥有更大特权、权力和访问权的账户。这可能会通过盗窃或开发高级账户(如管理员或 root 账户)凭证来实现。有的系统或应用程序还可能会为原本有限的账户临时或永久授予额外权力。

STRIDE 虽然通常被专门用于应对应用程序威胁，但也适用于其他情况，比如网络威胁和主机威胁。其他的攻击可能会比网络和主机问题更具体，比如网络嗅探和劫持、恶意软件和主机的任意代码执行，但是 STRIDE 的 6 个威胁概念使用相当广泛。

一般来说，威胁建模中 STRIDE 和其他工具的目的是考虑被危害问题的范围，并关注攻击的目标或结果。试图识别每一个特定的攻击方法和技术是不可能完成的任务，因为新的攻击正在不断开发中。虽然攻击的目标或目的仅能粗略地进行分类和分组，但它们是保持相对稳定的。

**警惕个人威胁**

竞争通常是企业成长的一个关键部分，但过头的对抗性竞争会增加个人的威胁等级。除了黑客和心怀不满的雇员，对手、承包商、员工甚至是信赖的合作伙伴都可能由于关系的恶化而对组织形成威胁。

- 不要相信顾问或承包商对组织的忠诚度会如同长期员工一样。承包商和顾问实际上就是雇佣兵，谁出价高就为谁工作。也不要把员工的忠诚视为理所应当。员工如果对他们的工作环境感到不满或觉得他们受到了不公平待遇，就有可能试图报复。有经济困难的员工可能会有不道德行为和违法活动，他们为了自己的利益可能会对组织构成威胁。
- 可信的合作伙伴仅仅是值得信赖的伙伴，前提是你们各自的利益对彼此合作是友好的。如果最后的合作关系恶化或变得敌对，那么先前的伙伴可能会采取行动，对组织构成威胁。

组织的潜在威胁多种多样。公司面临的威胁可能来自自然环境、技术以及人。大多数组织在预防威胁上会关注自然灾害和 IT 攻击，但需要注意来自个人的潜在威胁同样重要。一定要事先想好企业活动、决策和交互行为带来的最好和最坏的可能结果。识别威胁是设计防御、减少故障、降低危害和避免损失的第一步。

## 1.4.2 确定和用图表示潜在攻击

一旦明白开发的项目或部署的基础设施可能面临的威胁，那么下一步是进行威胁建模，确定可能发生的潜在攻击概念。通常通过创建事务中的元素图表、数据流指向和特权边界来完成(见图 1.7)。

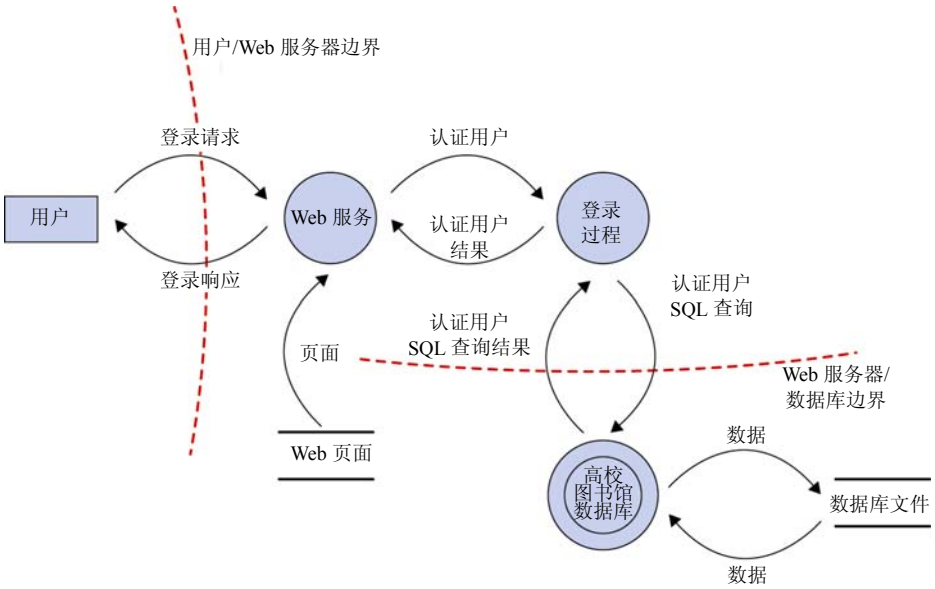


图 1.7 揭示威胁问题的图表实例

这些数据流图通过可视化表示，能更好地帮助理解资源和数据流动的关系。图表流程也被称为制作架构图。创建图表有助于详述商业任务、开发流程或工作活动中每个元素的功能和目的细节。一定要包括执行具体任务或操作的用户、处理器、应用程序、数据存储和所有其他的基本要素，这一点十分重要。该图表是一种高度概括，不是对编码逻辑的详细评估。然而，如果系统更复杂，则需要创建多个图表，关注不同的焦点且把细节进行不同程度的放大。

完成图表的创建后，要识别出图表中涉及的所有技术，包括操作系统、应用程序(基于网络服务和客户端)和协议。需要具体到使用的版本号和更新/补丁级别。

接着，识别可能对图表中每个元素发起的攻击。记住，要考虑到各种形式的攻击，包括逻辑/

技术、物理层面和社会层面的工具。例如，一定要包括电子欺骗、篡改和社交工程学。这个过程能很快帮助你进入威胁建模的下一阶段：执行降低分析。

### 1.4.3　执行降低分析

威胁建模的下一步是执行降低分析。执行降低分析是为了分解应用程序、系统或环境。这个任务的目的是更好地理解产品逻辑及其与外部的交互元素。不管是应用程序、系统还是整个环境，都需要被分成更小的容器或隔间。如果关注的是软件、电脑或操作系统，这些可能是子程序、模块或客体；如果关注的是系统或网络，这些可能是协议；如果关注的是企业的整个基础设施，这些可能是部门、任务和网络。应该对识别出的每个子元素进行评估，以便理解输入、处理、安全性、数据管理、存储和输出。

在这个分解流程中，必须了解 5 个关键概念：

- **信任边界**　信任或安全等级发生改变的位置。
- **数据流路径**　数据在两个位置之间的流动。
- **输入点**　接收外部输入的位置。
- **特权操作**　需要比标准用户账户或流程有更大特权的任何活动，通常需要进行系统修改或改变安全性。
- **安全立场和方法细节**　安全策略、安全基础和安全假设的声明。

把系统分解成各个组成部分能更容易识别每个元素的必要组件，同时也能注意到漏洞和攻击点。越能准确理解程序、系统或环境的运作方式，就越容易识别威胁。

### 1.4.4　优先级和响应

因为威胁要通过威胁建模进行识别，所以需要规定额外活动来完善整个流程。下一步是记录归档全部威胁。在文档编制中，应该对威胁的手段、目标和后果进行定义。要考虑实施某项开发可能需要的技术，以及列明潜在的对策和保障措施。

编制文档后，要对威胁进行排序或定级。可以利用各种技术完成这个过程，如使用概率×潜在损失的排名、高/中/低评级或 DREAD 系统。

概率×潜在损失的排名技术能产生一个代表风险严重性的编号，编号是从 1 到 100，100 代表可能发生的最严重的风险。概率和潜在损失的初始值可以在数字 1 到 10 之间指定，1 是最低，10 是最高。这些排名从某种层面看可以是武断或主观的，但因为同一个人或同一支团队会将编号分配给自己的组织，所以仍然应该在相对准确的偏差基础上准确估值。

高/中/低的评级流程更加简单。每个威胁都会被标注为这三种优先级标签中的一种。那些有高优先级标签的威胁需要立即解决。那些有中优先级标签的威胁最终也要解决，但无须立即采取行动。那些有低优先级标签的威胁可能需要解决，但如果解决这类威胁与整个项目相比需要付出很多的努力或费用，是否解决它们是可选的。

设计 DREAD 评级系统是为了提供灵活的评级解决方案，其基于对每种威胁的 5 个主要问题的回答：

- 潜在破坏——如果威胁成真，可能造成的损失有多严重？
- 再现性——攻击者重现这一漏洞有多复杂？

- 可利用性——实施攻击有多难?
- 受影响用户——有多少用户可能受到攻击的影响(按百分比)?
- 可发现性——攻击者发现弱点会有多难?

通过询问这些以及潜在的额外自定义问题，并对这些回答标注 H/M/L 或 3/2/1 值，就可以建立一张详细的威胁优先级表。

一旦设置了威胁的优先级，就需要确定对这些威胁的响应。应根据解决威胁的技术以及流程的成本和效率，对这些技术和流程进行考察权衡。反应选项应包括调整软件架构、改变操作和流程以及实现防御和检测组件。

## 1.5 把安全风险考虑到收购策略和实践中

将网络安全风险管理与收购策略和实践进行综合，是确保组织安全策略成功强健的一种手段，而不管机构的规模是什么样的。如果在没有考虑安全性的情况下贸然购买，那么所购买的这些产品的固有风险将在整个部署过程中一直存在。将收购元素的固有威胁最小化能减少安全管理成本，并且有可能减少安全违规。

选择带有弹性集成安全性的硬件、软件和服务往往比选择那些没有安全基础的产品和解决方案更贵一些。然而，这些额外的初始费用与满足不良设计产品安全需求的费用相比，通常更具成本效益。因此当考量收购成本时，很重要的一点是要考虑产品在整个部署周期内所有权的总花费，而不是只考虑初期购买和实施费用。

收购涉及的不只是软硬件，还包括外包、供应商承包和顾问咨询等。当与外部实体协同工作时，综合安全评估同确保产品设计考虑了安全因素一样重要。

许多情况下可能需要进行不间断的安全监测、管理和评估。可能会是行业的最佳实践或规章。组织内部可以进行这样的评估和监测，也可以由外部审计师进行。当有第三方参与评估和监控服务时，要记住，外部实体需要在他们的业务操作中体现出安全性意识。如果外部组织无法在安全的基础上管理他们自己的内部操作，那他们又将如何为你提供可靠安全的管理功能呢?

在为了安全整合而对第三方进行评估时，应考虑以下流程：

**现场评估** 访问该组织的网址，与其成员进行交谈并观察他们的操作习惯。

**公文交换和审核** 调查交换数据和文档的方式以及他们执行评估和审核的正式流程。

**流程/策略审核** 要求提供他们的安全策略、流程/程序、审查事件和响应文档的副本。

对所有的收购设立最低限度的安全需求。这些应该以现有的安全策略为模板。对新的硬件、软件或服务的安全要求，应该达到或超过现有基础设施的安全性。在处理外部服务时，一定要审查所有的 SLA(Service-Level Agreement，服务层级协议)，确保承包服务中有关于安全的规定。这可能包括根据特定需求定制服务层面的要求。这里有一些关于收购安全的不错资源：

- 通过收购提高网络安全和弹性。*Final Report of the Department of Defense and General Services Administration*(www.gsa.gov/portal/getMediaData?mediaId=185371)。
- NIST *Special Publication 800-64 Revision 2*：*Security Considerations in the System Development Life Cycle*(http://csrc.nist.gov/publications/nistpubs/800- 64-Rev2/SP800-64-Revision2.pdf)。

## 1.6　本章小结

安全治理、管理概念与原则是安全策略和解决方案部署中的固有元素。它们不仅定义了安全环境所需的基本参数，也定义了策略设计人员和系统实现人员为创建安全解决方案所必须达到的目的和目标。

安全性的主要目标和目的包含在 CIA 三元组中：机密性、完整性和可用性。这三条原则被认为是安全领域内最重要的原则。然而，每条原则对一个特定的组织究竟有多重要，主要取决于组织的安全目标和需求以及安全性所受到的威胁程度。

CIA 三元组的第一条原则是机密性，也就是客体不能暴露给未授权主体的原则。安全机制提供了机密性，也就为限制未授权主体不能访问数据、客体或资源提供了高级别保证。如果存在对机密性的威胁，那么就有可能发生未授权的泄漏。

CIA 三元组的第二条原则是完整性，也就是客体保持自身的正确性和只能由已授权主体进行有意识修改的原则。如果安全机制提供了完整性，也就对数据、客体和资源提供了保持原有受保护状态并不被修改的高级别保证，这包括当客体在存储、传输或处理过程中发生的变更。维护完整性意味着客体本身不会被改变，并且管理和操纵客体的操作系统与程序实体不会受到安全威胁。

CIA 三元组的第三条原则是可用性，也就是经过授权的主体被及时准许和不间断地访问客体的原则。如果安全机制提供了可用性，也就提供了经过授权的主体能够访问数据、客体和资源的高级别保证。可用性包括有效地、不间断地访问客体和阻止拒绝服务攻击。可用性还意味着支持基础设施的正常运作，并允许经过授权的用户获得被授权的访问权。

除了 CIA 三元组以外，在设计安全策略和部署安全解决方案时，还需要考虑其他很多与安全有关的概念和原则，包括隐私性、身份标识、身份认证、授权、可问责性、不可否认性和审计。

安全解决方案的概念和原则的其他方面是保护机制的元素：分层、抽象、数据隐藏以及加密。这些元素是安全控制的常见特性。并非所有的安全控制都必须具有这些元素，但是许多控制通过使用这些机制提供对机密性、完整性和可用性的保护。

安全角色决定谁对组织机构的资产安全负有责任。担任高管角色的人对任何资产损失最终负责和承担义务，并且对安全策略进行定义。安全专家负责实现安全策略，用户负责遵守安全策略。担任数据所有者角色的人负责对信息进行分类，数据管理员负责维护安全环境和备份数据。审计人员负责确认安全环境是否能恰当地保护资产。

规范化的安全策略结构由策略、标准、基准、指导方针和程序组成。这些独立的文档是在任何环境中设计和实现安全的必要元素。

安全管理实践中的一个重要方面是对变更的控制或管理。安全环境的改变很可能引入会导致新脆弱性出现的漏洞、重叠、客体丢失和疏漏。面对变更，能维持安全性的唯一方法是要系统地管理变化，这往往涉及对与安全控制和机制相关的活动进行广泛的日志记录、审计和监控。最终得到的数据随后用于确定变更的作用者，无论这些作用者是客体、主体、程序、通信路径还是网络本身。

数据分类是根据数据的秘密性、敏感性或机密性需求来保护数据的主要方式。在设计和实现安全系统时，因为某些数据项需要更高的安全性，所以对所有的数据采取同样的处理方法是低效率的。在较低的安全级别保护所有的数据，意味着敏感数据很容易被访问到。在较高的安全级别保护所有的数据，成本太高且对未分类的非关键数据的访问限制太多。数据分类用于确定需要分配多少工作量、资金和资源去保护数据以及控制对数据的访问。

安全管理计划的一个重要方面是实施适当的安全策略。为确保有效，安全管理方法必须是自上而下的。启用和定义安全策略的责任属于组织上层或高管人员。安全策略是为组织下层人员提供方向的。中层管理人员负责把安全政策充实为具体标准、基准、指导方针和步骤。对安全管理文件中预定的参数进行配置是运营经理或安全专家的责任。最后，最终用户的责任是要遵循组织的所有安全策略。

安全管理计划编制的元素包括：定义安全角色；开发安全策略；执行风险分析；以及要求对员工进行安全教育。这些职责要经过管理计划开发的指导。安全管理团队应当开发战略计划、战术计划和操作计划。

威胁建模是一种安全流程，能识别、分类和分析潜在威胁。威胁建模在设计开发阶段可作为一种提前措施来执行，或在产品被部署后作为一种被动性措施来执行。在这两种情况下，这个安全流程能识别潜在危害、发生概率、优先级问题以及消除或减少威胁的手段。

将网络安全风险管理与收购策略和实践进行综合，是确保组织安全策略成功和完善的一种手段，而不管组织的规模是什么样的。如果在没有考虑安全性的情况下贸然购买，所购买的这些产品的固有风险将在其整个部署过程中一直存在。

## 1.7 考试要点

**理解 CIA 三元组的元素：机密性、完整性和可用性**。机密性是客体不能暴露给未授权主体的原则。了解这条原则为什么重要、支持该原则的机制、针对该原则的攻击以及有效的对策。完整性是客体保持自身的正确性以及只能由已授权主体进行有意识修改的原则。了解这条原则为什么重要、支持该原则的机制、针对该原则的攻击以及有效的对策。可用性是经过授权的主体被及时准许和不被打断地访问客体的原则。了解这条原则为什么重要、支持该原则的机制、针对该原则的攻击以及有效的对策。

**能够解释身份标识是如何工作的**。身份标识是一个过程，在这个过程中，主体会表明身份，并且开始提供可问责性。主体必须向系统提供身份，从而启动身份认证、授权和可问责的过程。

**理解身份认证的过程**。认证或测试所声明身份合法性的过程就是身份认证。身份认证要求来自主体的附加信息必须完全对应于被表明的身份。

**了解如何在安全计划中实现授权**。一旦主体通过了身份认证，其访问还必须经过授权。授权的过程确保请求的活动或客体访问，可能获得了为通过身份认证的身份而指派的权利和特权。

**理解安全治理**。安全治理是关于组织支持、定义和指导安全工作的实践集合。

**能够解释审计过程**。审计或监控是程序化方式，通过这种方式，主体在系统中经过身份认证的行为是可问责的。审计也是对系统中未经授权的或异常的活动进行检测的过程。我们需要通过审计来检测主体的恶意行为、入侵企图和系统故障以及重构事件，为起诉提供证据、生成问题报告和分析结果。

**理解可问责性的重要性**。只有在支持可问责性时，组织的安全策略才能够被正确实施。换句话说，只有在主体的活动可问责时，才能够保持安全性。有效的可问责性依赖于检验主体身份以及跟踪其活动的能力。

**能够解释不可否认性**。不可否认性确保活动或事件的主体无法否认所发生的事件。不可否认性能够防止主体宣称自己没有发送消息、没有执行过某项活动或者不是某个事件的起因。

**理解安全管理计划编制**。安全管理基于三种类型的计划：战略计划、战术计划和操作计划。战略计划是长期计划，并且是相当稳定的，用于定义组织机构的目的、任务和目标。战术计划是中期计划，用来提供更加详细的实现战略计划所提出目标的计划。操作计划是短期计划，是基于战略和战术计划的非常周详的计划。

**了解规范化安全策略结构的元素**。为了生成全面的安全计划，需要适当地遵守下列要求：安全策略、标准、基准、指导方针和程序。这些文档清楚地描述了安全需求并反映了责任方的适度关注。

**理解重要的安全角色**。主要的安全角色有高层管理者、组织机构所有者、上层管理者、安全专家、用户、数据所有者、数据管理员以及审计人员。通过构建安全角色的层次，就可以全面限制风险。

**了解如何实现安全意识培训**。在真正的培训开始之前，必须为用户建立树立为公认实体的安全意识。一旦树立了安全意识，培训或教育员工执行工作任务和遵守安全策略就可以开始了。所有的新员工都需要进行培训，这样他们才能够遵守安全策略中规定的所有标准、指导方针和程序。教育是一项更细致的工作，学生/用户需要学习比他们完成工作任务实际所需知识多得多的知识。教育往往与用户参加认证考试或寻求职务晋升相关联。

**了解分层如何简化安全**。分层是串联使用多个控制层次。使用多层次解决方案，使用许多控制去防范威胁。

**能够解释抽象的概念**。抽象用于将相似的元素放入组、类别或角色(被整体性授予安全控制、限制或权限)中，抽象提高了实施安全计划的效率。

**理解数据隐藏**。顾名思义，数据隐藏防止主体发现或访问数据。在安全控制和程序设计中，数据隐藏通常是一个关键要素。

**理解对加密的需求**。加密是对计划外的接收者隐藏通信数据的含义或意图的一种艺术和学科。加密可以具有很多形式，并且能够用于所有的电子通信类型，包括文本、音频和视频文件以及应用程序本身。加密技术是安全控制中一个非常重要的元素，尤其系统之间的数据传输更是如此。

**能够解释更改控制和更改管理的概念**。安全环境的改变很可能引入会导致新脆弱性出现的漏洞、重叠、客体丢失和疏漏。面对更改，维持安全性的唯一方法是系统地管理更改。

**了解为什么和如何进行数据分类**。数据分类旨在简化给客体组(而不是单独客体)分配安全控制的过程。两种通用的分类方案是政府/军方分类和商业/私营部门分类。了解政府/军方分类中的 5 个级别和商业/私营部门分类中的 4 个级别。

**理解解除分类的重要性**。一旦某个资产不再需要当前分配的分类或敏感性级别保护，就需要解除分类。

**了解 COBIT 的基础知识**。信息及相关技术控制目标(COBIT)是一种安全概念基础架构，用于组织公司的复杂安全解决方案。

**了解威胁建模的基础知识**。威胁建模是一种安全流程，能识别、分类和分析潜在威胁。威胁建模在设计开发阶段可作为一种提前措施来执行，或在产品被部署后作为一种被动性措施来执行。关键概念包括资产/攻击者/软件、STRIDE、图形表示、约简/分解和 DREAD。

**了解安全并购的必要性**。将网络安全风险管理与收购策略和实践进行综合是确保组织的安全策略成功强健的一种手段，而不管组织的规模是什么样的。如果在没有考虑安全性的情况下贸然购买，所购买的这些产品的固有风险将在其整个部署过程中一直存在。

## 1.8 书面实验室

1. 讨论和描述 CIA 三元组。
2. 为了能够问责与特定用户账户相关联人员的活动，具体有哪些需求？
3. 描述变更控制管理的优点。
4. 实现分类方案的 7 个主要步骤是什么？
5. 指出$(ISC)^2$为 CISSP 定义的 6 种主要安全角色。
6. 完整的组织安全策略的 4 个组成部分及其基本目的是什么？

## 1.9 复习题

1. 下列哪一项包含安全性的主要目标和目的？
   A. 网络的外围边界
   B. CIA 三元组
   C. 一个独立的系统
   D. 互联网
2. 脆弱性和风险是基于它们对下列哪一项的威胁评估？
   A. 一条或多条 CIA 三元组原则
   B. 数据有效性
   C. 应尽关注
   D. 责任范围
3. 下列哪一项在 CIA 三元组原则中用于说明授权主体被及时授予和不间断地访问对象？
   A. 识别
   B. 可用性
   C. 加密
   D. 分层
4. 下列哪一项不被视为违反保密性？
   A. 窃取密码
   B. 窃听
   C. 硬件破坏
   D. 社会工程学
5. 下列哪一项是不正确的？
   A. 保密性的违反包括人为错误。
   B. 保密性的违反包括管理监督。
   C. 保密性的违反仅限于直接故意攻击。
   D. 当传输未正确加密时保密性违反可能发生。
6. STRIDE 通常与用于评估针对应用程序或操作系统的威胁有关。以下哪一项不是 STRIDE 的元素？
   A. 欺骗

B. 权限提升

C. 否认

D. 披露

7. 如果一个安全机制提供可用性，也就提供了高级别保证，该授权对象可以 _____ 数据、对象和资源。

A. 控制

B. 审计

C. 访问

D. 否认

8. _____指的是保持信息的机密性，防止一旦泄露，个人身份可能造成伤害、尴尬或丢人。

A. 隐居

B. 隐蔽

C. 隐私

D. 临界

9. 对于所有个人的影响，除了下面哪一项以外都需要注意？

A. 制约个人电子邮件

B. 记录电话交谈

C. 收集关于上网习惯的信息

D. 用于保留电子邮件的备份机制

10. 数据分类管理的什么元素可以覆盖所有其他访问控制的形式？

A. 分类

B. 物理访问

C. 监管者职责

D. 取得所有权

11. 什么确保了活动或事件的主体不能否认发生过的事件？

A. CIA 三元组

B. 抽象

C. 不可否认性

D. 哈希总数

12. 以下哪一项相对于分层安全是最重要和独特的概念？

A. 多层

B. 系列

C. 并行

D. 过滤

13. 下列哪一项不被认为是数据隐藏的例子？

A. 防止对象的授权阅读者删除该对象

B. 阻止未经授权的访问者访问数据库

C. 限制较低级别的主体访问较高级别的数据

D. 阻止应用程序直接访问硬件

14. 变更管理的主要目标是什么？
    A. 维护文档
    B. 保持用户得到变更通知
    C. 允许失败变更的回滚
    D. 防止安全危害
15. 数据分类方案的主要目标是什么？
    A. 控制授权主体访问对象
    B. 为了形式化和根据重要性和敏感性分配标签以分层保护数据的过程
    C. 为审计可问责性建立交易跟踪
    D. 为操作访问控制以提供最有效的手段来授予或限制功能
16. 在分类数据时，下列哪一项通常是不考虑的特征？
    A. 价值
    B. 物体的大小
    C. 使用寿命
    D. 国家安全的影响
17. 两种常见的数据分类方案是哪些？
    A. 军事和私营部门
    B. 个人和政府
    C. 私营部门和非限制性行业
    D. 分类和未分类
18. 下列哪一项是机密数据的最低军事数据分类？
    A. 敏感
    B. 机密
    C. 专有
    D. 隐私
19. 下列商业/私营部门的哪一个数据分类用来控制组织内的个人信息？
    A. 机密
    B. 隐私
    C. 敏感
    D. 专有
20. 数据分类都用于关注安全控制，除了以下哪一个？
    A. 存储
    B. 处理
    C. 分层
    D. 转移