第 3 章 信息安全风险管理

信息化建设过程中，以计算机网络为基础的信息系统的广泛应用，使信息面临着越来越严峻的安全威胁，停留在技术层面的安全措施已难以抵御因系统脆弱性引起的安全风险。因此，系统研究信息安全风险管理问题，有效控制风险，防止信息安全事件的发生，已成为当前信息安全保障中的一项基础性工作。

3.1 概　　述

进行有效的风险管理，必须首先了解信息安全风险的含义，明确信息安全风险的相关要素及其相互关系，为风险识别、风险分析、风险计划、风险跟踪和风险应对等后续工作奠定基础。

3.1.1 信息安全风险

只有从风险管理角度出发，系统地分析信息安全所面临的威胁及其存在的脆弱性，评估安全事件一旦发生可能造成的危害程度，才能对风险要素进行准确识别与分析，进一步提出有针对性的防护对策和整改措施。

1. 风险和信息安全风险

“风险”一词被广泛应用于许多领域，如投资风险、医疗风险、决策风险、安全风险等，其含义也会因其应用领域不同而有所差异。从一般意义讲，风险指“可能发生的危险”。系统工程学中，风险指“用于度量在技术性能、成本进度方面达到某种目的的不确定性”。而在指挥决策学中，将风险理解为在决策条件不确定的决策过程中，所面临的无法保证决策方案实施后一定能达到所期望效果的危险。对上述概念进行比较分析，可以发现无论是一般意义上的风险还是特殊应用领域的风险，其概念至少要包含风险的两个基本属性：不确定性和危害性，即风险何时何地发生难以把握，风险一旦发生会带来不利影响和危害。风险的不确定性指风险造成的危害能否发生，以及将会造成危害程度的无规则性和偶然性。风险是客观存在的，而且不以人的意志为转移。但是风险是否发生、在何时何地发生，以及所造成的损失和危害的程度和范围等则是不确定的，不可能被事先准确地加以预测和推断。风险的危害性指风险可能会导致各种损失和破坏，这些可能发生的不同程度的损失和破坏，会对开展正常的实践活动造成干扰、影响和危害。正因为风险具有这种危害性，才使得人们对风险和风险管理问题格外重视。

由此，可以将信息安全风险归结为破坏信息安全或对信息安全带来危害的不确定性。

国内外较为统一和公认的“信息安全风险”的定义是人为或自然的威胁主体利用信息系统及其管理体系中存在的薄弱点，致使信息安全事件发生的可能性及其对活动和所属资产造成影响的组合。简单地讲，信息安全风险就是信息安全事件发生的可能性及其发生后所带来的影响的组合，即可能性越大，风险越高；资产受到的影响和损失越大，风险也越大。

2. 信息安全风险的内涵

解析信息安全风险的内涵，无法脱离对信息安全的诠释。学术界对“信息安全”没有一个统一的概念，若以信息系统为对象，信息安全指对处理信息的信息系统及其涉密信息的安全防护和保持。该定义强调两点：一是信息系统的安全防护，确保系统能安全、可靠和不间断地运行，为依靠信息技术而开展工作的各级机构提供服务和保障；二是涉密信息的安全性保护，确保信息的保密性、完整性、可用性、可控性和抗抵赖性，防止涉密信息被未授权者获悉、使用、更改和破坏。

在充分理解和把握“信息安全风险”和“信息安全”两个概念的基础上，经过分析融合，可以对“信息安全风险”的含义给出一个比较确切的解释。信息安全风险指人为或自然的威胁主体利用信息系统或组织管理体系中存在的薄弱点，对组织的信息资产、任务活动造成损害或影响的潜在可能性，即信息安全事件发生的可能性及其将会带来的后果的组合。

3.1.2　信息安全风险的相关要素

风险评估是对信息资产所面临的威胁、存在的弱点、风险事件造成的影响，以及三者综合作用在当前安全措施控制下所带来的与安全需求不符合的风险可能性评估。风险评估是风险管理的基础，是进一步确定信息安全需求和改进信息安全管理策略的重要途径，属于组织信息安全管理体系策划的过程。信息系统是信息安全风险评估的对象，信息系统中的资产、信息系统面临的可能威胁、系统中存在的脆弱性、安全风险、安全风险对业务的影响，以及系统中已有的安全控制措施和系统的安全需求等构成了信息安全风险评估的基本要素。

1. 资产

资产(asset)指对组织具有价值的信息或资源，是安全策略保护的对象。资产能够以多种形式存在，包括有形的或无形的、硬件或软件、文档或代码，以及服务或形象等诸多表现形式，如表 3-1 所示。

表 3-1　信息系统中的资产分类

分　类	说　明
软件	系统软件：操作系统、语言包、开发系统、各种库/类等。 应用软件：办公软件、数据库软件、工具软件等。 源程序：各种共享源代码、可执行程序、开发的各种代码等
硬件	系统和外围设备：计算机设备、网络设备、存储设备、传输及保障设备等。 安全设备：防火墙、IDS、指纹识别系统等。 其他技术设备：打印机、复印机、扫描仪、供电设备、空调设备等

续表

分　类	说　　明
服务	信息服务：对外依赖该系统开展服务而取得业务收入的服务。 网络通信服务：各种网络设备、设施提供的网络连接服务。 办公服务：各种 MIS 系统提供的为提高工作效率的服务。 其他技术服务：照明、电力、空调、供热等
流程	包括 IT 和业务标准流程、IT 和业务敏感流程，其中敏感流程具有给组织带来攻击或引入风险的潜在可能，如电信公司在新开通线路时可能会引入特殊风险
数据	在传输、处理和存储状态的各种信息资料，包括源代码、数据库数据、系统文档、运行管理规程、计划、报告、用户手册、各类纸质上的信息等
文档	各种文件、传真、财务报告、发展计划、合同等
人员	除了掌握重要信息和核心业务的人员，如主机维护主管、网络维护主管、网络研发人员之外，还包括其他可以访问信息资产的组织外用户
其他	形象与声誉、关系等

在信息安全体系范围内为资产编制清单是一项重要工作，每项资产都应该清晰地定义、合理地估价，并明确资产所有权关系，进行安全分类，记录在案。根据资产的表现形式，可将资产分为软件、硬件、服务、流程、数据、文档、人员等。

2. 威胁

威胁(threat)指可能对组织或资产导致损害的潜在原因。

威胁有潜力导致不期望发生的安全事件发生，从而对系统、组织、资产造成损害。这种损害可能是偶然性事件，但更多的可能是对信息系统和服务所处理信息的直接或间接的蓄意攻击行为，如非授权的泄露、修改、停机等。根据威胁来源，表 3-2 给出了威胁的分类。

表 3-2　安全威胁分类

分类编号	威 胁 名 称	威 胁 描 述
T1	操作失误	应该执行而没有执行响应的操作，或无意执行了错误的操作
T2	滥用权限	通过采用一些措施，超越自己的权限访问了本来无权访问的资源，或滥用自己的权限做出破坏信息系统的行为
T3	行为抵赖	对自己的操作行为或记录进行否认
T4	信息泄露	信息泄露给不应了解的他人
T5	社会工程	利用受害者心里弱点、好奇心、信任、贪婪等心理陷阱进行欺骗、伤害或获取重要信息
T6	漏洞利用	利用网络、主机或应用系统漏洞非法侵入系统，造成信息泄露或使系统受损
T7	行为探测	对网络、主机、应用等进行扫描探测
T8	身份假冒	非法用户冒充合法用户进行操作

续表

分类编号	威 胁 名 称	威 胁 描 述
T9	获取权限	用户获取自己规定权限之外的权限
T10	密码攻击	对系统进行的密码分析与破坏
T11	拒绝服务	利用拒绝服务手段造成系统服务、资源访问性能下降或不可用
T12	恶意代码	故意在信息系统上执行恶意任务的程序代码
T13	窃取数据	通过窃听、入侵等手段盗取重要信息或数据
T14	篡改数据	非法修改信息，破坏信息的完整性使系统的安全性降低或信息不可用
T15	物理破坏	通过物理的接触造成对软件、硬件、数据的破坏
T16	网络欺骗	利用电磁欺骗、IP 欺骗、Web 欺骗等攻击系统的行为
T17	其他杂项威胁	未知的畸形流量、杂项攻击、非标准协议、网络流量超标等发生的可能性
T18	数据意外受损	系统/网络的关键数据服务器发生意外故障
T19	系统故障	对业务实施或系统运行产生影响的设备硬件故障、通信链路中断、系统本身或软件缺陷等问题
T20	电源中断	电源发生中断
T21	灾难	火灾、水灾、雷击、鼠害、地震等自然灾害
T22	电磁泄漏截取	设备电磁辐射不符合要求，造成电磁携带信息泄露
T23	管理不到位	安全管理无法落实，不到位，造成安全管理不规范，或管理混乱，从而破坏信息系统正常运行
T24	其他	其他

威胁主要来源于环境因素和人为因素，其中人为因素包括恶意的和非恶意人员，具体如下。

(1) 环境因素：指地震、火灾、水灾、电磁干扰、静电、灰尖、潮湿、超常温度等环境危害，以及软件、硬件、数据、通信线路等方面的故障。

(2) 恶意人员：对组织不满的或别有用心的人员对信息系统进行恶意破坏，会对信息的机密性、完整性和可用性等造成损害。

(3) 非恶意人员：缺乏责任心、安全意识或专业技能不足导致信息系统故障、被破坏或被攻击，但本身无恶意企图。

3. 脆弱性

脆弱性(vulnerability)指可能被威胁所利用的资产或若干资产的薄弱环节。例如，操作系统存在漏洞、数据库的访问没有访问控制机制、系统机房没有门禁系统等。

脆弱性是资产本身存在的，如果没有相应的威胁，单纯的脆弱性本身不会对资产造成损害，而且如果系统足够强健，则再严重的威胁也不会导致安全事件造成损失。这说明，威胁总是要利用资产的脆弱性来产生危害。

资产的脆弱性具有隐蔽性，有些脆弱性只在一定条件和环境下才能显现，这也是脆弱性识别中最为困难的部分。要注意的是，不正确的、起不到应有作用的或没有正确实施的

安全控制措施本身就可能是一种脆弱性。

脆弱性主要表现在技术和管理两个方面，其中技术脆弱性指信息系统在设计、实现和运行时，涉及的物理层、网络层、系统层、应用层等在技术上存在的缺陷或弱点，管理脆弱性则是指组织管理制度、流程等方面存在的缺陷或不足。

常见的一些脆弱性种类如表 3-3 所示。

表 3-3 信息系统常见的脆弱性

分　类	示　例	说　明
技术脆弱性	未安装杀病毒软件	可能发生系统信息被病毒侵害
	使用口令不当	可能导致系统信息的非授权访问
	无保护的外网连接	可能破坏联网系统中存储与处理信息的安全性
管理脆弱性	安全培训不足	可能造成用户缺乏足够的安全意识，或产生用户错误
	机房钥匙管理不严	可能形成资产的直接丢失或物理损害等
	离职人员权限未撤销	可能引起泄密或业务活动受到损害

4. 安全风险

安全风险(security risk)指使得威胁可以利用脆弱性，从而直接或间接造成资产损害的一种潜在的影响，并以威胁利用脆弱性导致一系列不期望发生的安全事件来体现。

资产、威胁和脆弱性是信息安全风险的基本要素，是信息安全风险存在的基本条件，缺一不可。没有资产，威胁就没有攻击或损害的对象；没有威胁，如果资产很有价值，脆弱性很严重，安全事件也不会发生；系统没有脆弱性，威胁就没有可利用的切入点，安全事件也不会发生。

通过确定资产价值，以及相关的威胁和脆弱性水平，就可以得出最初的信息安全风险的量度值。

根据以上分析，安全风险是关于资产、威胁和脆弱性的函数，即信息安全风险可以形式化表示为 $R=f(a, t, v)$，其中 R 表示安全风险，a 表示资产，t 表示威胁，v 表示脆弱性。

5. 影响

影响(influence)主要指安全风险对业务的影响，即威胁利用资产的脆弱性导致资产价值损失等不期望发生事件的后果。

这些后果可能表现为直接形式，如物理介质或设备损坏、人员损伤、资金损失等，也可能表现为间接形式，如公司信用和名誉受损、市场份额减少、承担法律责任等。在信息安全领域，直接损失常常容易计算且程度较小，而间接损失往往难以估计且程度严重。

6. 安全控制措施

安全控制措施(security control measure)指为保护组织资产、防止威胁、减少脆弱性、限制安全事件的影响、加速安全事件的检测及响应而采取的各种实践、过程和机制。

有效的安全控制措施通常是为了提供给资产多级的安全，而应用不同安全控制措施的综合，以实现检测、威慑、防止、限制、修正、恢复、监测和提高安全意识的功能。例如，一

个信息系统的安全访问控制，往往是人员管理、角色权限管理、审计管理、数据库安全、物理安全，以及安全培训等的组合。有些安全控制措施已作为环境或资产固有的一部分而存在，或已存在于系统或组织之中。

安全控制措施的实施领域包括组织政策与资产管理、物理环境、技术控制和人员管理等方面。

7. 安全需求

安全需求（security requirement）指为保证组织业务战略的正常运作而在安全控制措施方面提出的要求。

信息安全体系的安全需求来源于以下 3 个方面。

1）风险评估的要求

评估组织面临的风险，以及该风险的出现将会带来怎样的业务损失，为了降低风险，需要采取的相应安全措施。例如，关键数据或系统的机密性、可用性、完整性需求，信息系统运行时的实时监控需求，安全事件带来的应急响应需求等。

2）法律、法规和合同的要求

在信息安全体系文件中应详细规定组织、贸易伙伴、服务提供商和签约客户需要遵守的有关法律、法规与合同的要求，如数据版权保护、文件保密管理、组织记录的保护等，要保证任何安全控制措施不得违反或损害任何法律法规、商业合同的要求。

3）业务规则、业务目标和业务信息处理的要求

在信息安全体系文件中应详细规定与组织的业务规则、业务目标和业务信息处理相关的安全需求，信息安全体系应支持组织获得竞争优势、现金流和赢利能力的要求，并保证实施安全控制措施不得妨碍业务的正常运营。

3.1.3　风险要素的相互关系

依据《信息安全风险评估指南》，图 3-1 描述了风险要素之间的关系。

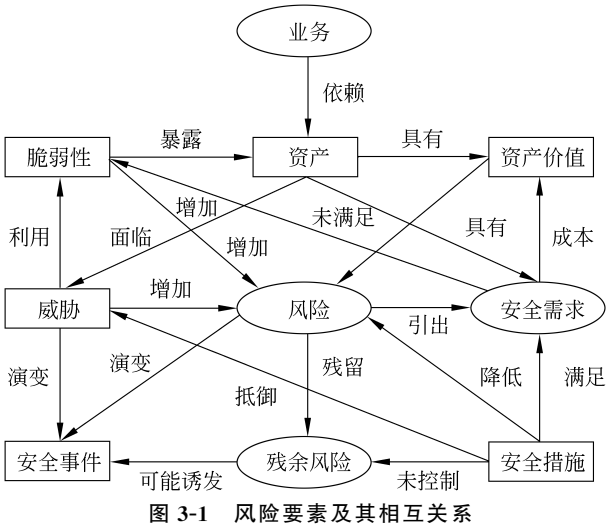

图 3-1　风险要素及其相互关系

风险评估围绕着资产、威胁、脆弱性和安全控制措施等基本要素展开。风险要素之间存在着以下关系。

(1) 相关业务依赖资产去实现,依赖程度越高,要求其风险越小;

(2) 资产具有价值,相关业务对资产的依赖程度越高,资产价值越大;

(3) 风险由威胁主体引发,威胁越多则风险越大,并可能演变成安全事件;

(4) 资产存在安全脆弱性,资产的脆弱性可能暴露资产的价值,脆弱性越强则风险越大;

(5) 风险的存在及对风险的认识引出安全需求;

(6) 当安全需求未被满足时,产生脆弱性,安全需求通过安全措施得以满足,需结合资产价值考虑实施成本;

(7) 安全措施可以抵御威胁,减少脆弱性,降低安全事件造成的影响;

(8) 在实施控制措施后还会有残余风险,残余风险不可能也没有必要降为零;

(9) 残余风险应受到密切监视,防止诱发新的安全事件。

3.2 信息安全风险评估过程

详细的风险评估方法在流程上可能有一些差异,但基本上都是围绕资产、威胁、脆弱性的识别与评价展开,进一步分析不期望事件发生的可能性及对组织的影响,并考虑如何选择合适的安全控制措施,将安全风险降低到可接受的程度。

从总体上看,风险评估过程可分为 4 个阶段。第一阶段为风险评估准备;第二阶段是风险识别,包括资产的识别与估价、威胁的识别与评估和脆弱性的识别与评估等工作;第三阶段是风险分析,包括计算风险、风险的影响分析等,并在此过程建立相关评估文档;第四阶段为根据风险计算结果进行相应的风险管理过程,并提交风险评估报告。

信息安全风险评估的流程如图 3-2 所示。

3.2.1 信息安全风险评估准备

风险评估准备是整个风险评估过程有效性的保证。组织实施风险评估是一种战略性考虑,其结果将受到组织的业务战略、业务流程、安全需求、系统规模与结构等方面的影响,因此,在风险评估实施前,应做好以下准备工作。

(1) 确定风险评估的目标。根据组织在业务持续性发展的安全性需要、法律法规的规定等内容,识别出现有信息系统及管理上的不足,以及可能造成的风险大小。

(2) 明确风险评估的范围。风险评估的范围可能是组织全部的信息及信息处理相关的各类资产、管理机构,也可能是某个独立的信息系统、关键业务流程等。

(3) 组建评估小组。组建风险评估与实施小组,以支持整个过程的推进,如成立由机关、相关业务骨干、技术人员等组成的风险评估小组,评估小组应能够保证评估工作的有效开展。

(4) 确定风险评估的依据和方法。利用问卷调查、现场面谈等形式进行系统调研,确定风险评估的依据,并考虑评估的目的、范围、时间、效果、人员素质等因素来选择具体的

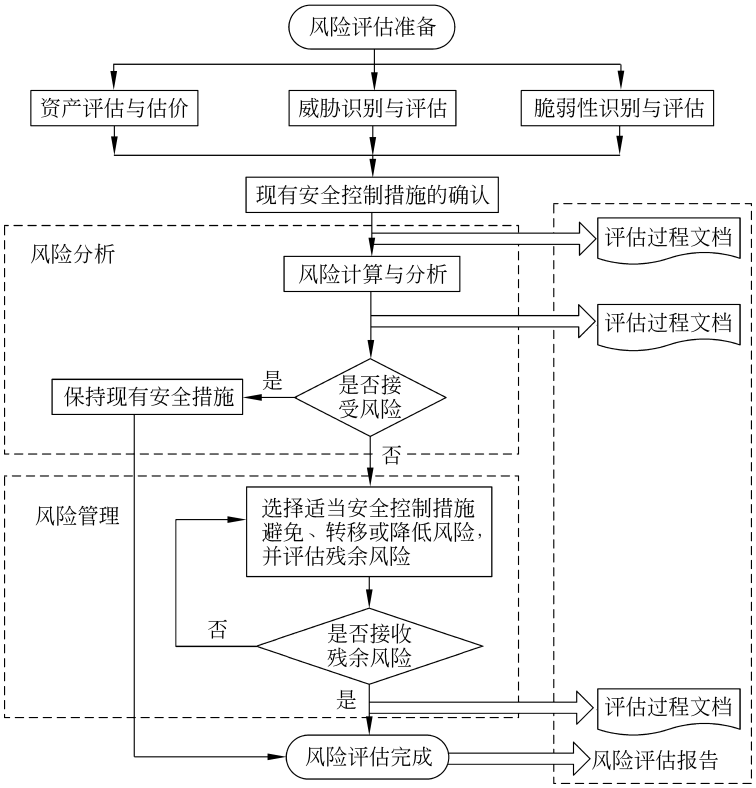

图 3-2　信息安全风险评估流程

风险计算方法和风险评估工具，并使之能与组织环境和安全要求相适应。

（5）制定方案。应制定指导评估实施活动的评估方案，包括团队组织、人员培训、工作计划、时间进度安排等内容。

（6）方案审批。上述所有内容确定之后，应形成较为完整的风险评估实施方案，评估方案应上报相关主管部门审核批准。

3.2.2　资产调查

风险识别始于信息资产的识别，根据资产的类型（见表 3-4），管理者确认组织的信息资产，将它们归于不同的类，并根据它们在总体上的重要性划分优先等级，评估其价值。资产调查包括资产识别、资产定级、资产价值计算和安全措施识别。

1. 资产识别

资产识别是风险识别的必要环节，其任务是对确定的评估对象所涉及的资产进行详细的标识，并建立资产清单。

识别资产的方法主要有访谈、现场调查、文档查阅等方式。在识别的过程中要注意不能遗漏无形资产，同时要注意不同资产之间的相互依赖关系。

1）识别软件和硬件

按计划识别软件和硬件，通过数据处理过程建立相关的信息资产清单，并明确每一种

信息资产的哪些属性需要在使用过程中受到追踪，而这需要根据组织及其风险管理工作的需要，以及信息安全技术团体的需要和偏好来做出决定。当确定每一种信息资产需要追踪的属性时，应考虑以下潜在的属性。

（1）名称：程序或设备的名单。

（2）IP 地址：对网络硬件设备很有用。

（3）MAC 地址：电子序列号或硬件地址，具有唯一性。

（4）资产类型：描述每一种资产的功能或作用。

（5）产品序列号：识别特定设备的唯一序列号。

（6）制造商：有助于与生产厂家建立联系并寻求帮助。

（7）型号或编号：能准确识别资产。

（8）版本号：在资产升级或变更时，需要这些版本值。

（9）物理位置：指明何处可使用该资产。

（10）逻辑位置：指定资产在组织内部网络中的位置。

（11）控制实体：控制资产的组织部门。

表 3-4　资产的类型

分类	描　　述
数据	保存在信息媒介上的各种数据资料，包括源代码、数据库数据、系统文档、运行管理规划、计划、报告、用户手册、各类纸质的文档等
软件	系统软件：操作系统、数据库管理系统、语句包、开发系统等。 应用软件：办公软件、数据库软件、各类工具软件等。 源程序：各类共享源代码、自行或合作开发的各种代码等
硬件	网络设备：路由器、网关、交换机、网管设备等。 计算机设备：大型机、小型机、服务器、工作站、台式计算机、便携式计算机等。 存储设备：磁带机、磁盘阵列、磁带、光盘、移动硬盘等。 通信设备：卫星、电台、移动电话、固定电话、程控交换机、汇聚交换机、微波接力机、软交换设备、边界会话控制器等。 传输设备：不间断电源(UPS)、变电设备、空调、保险柜、文件柜、门禁、消防设备等。 安全保密设备：防病毒系统、防火墙、入侵检测系统、网络隔离控制设备、网络介入控制设备、网络安全管理设备、主机安全监控设备、身份鉴别系统、信源保密机、信道保密机等。 其他：打印机、复印机、扫描仪、传真机等
服务	信息服务：对外依赖该系统开展的各类服务。 网络服务：各种网络设备、设备提供的网络连接服务。 办公服务：为提高效率而开发的管理信息系统，包括各种内部配置管理、文件流转管理等服务
人员	掌握着重要信息和核心业务的人员，如指挥、研发、管理、保障人员等
制度	管理制度、执勤维护制度、系统运维制度等
其他	形象、士气等

2）识别服务、流程、数据、文档、人员和其他

与软件和硬件不同，服务、流程、数据、文档和人力资源等信息资产不易被识别和引

证，因此，应该将这些信息资产的识别、描述和评估任务分配给拥有必要知识、经验和判断能力的人员。一旦这些资产得到识别，就要运用一个可靠的数据处理过程来记录和标识它们，如同在软件和硬件中使用一样。

对这些信息资产的维护记录应当较为灵活，在识别资产的过程中，要将资产与被追踪的信息资产的属性特征联系起来，仔细考虑特定资产中哪些属性需要跟踪。以下列出这些资产的一些基本属性。

（1）服务。包括服务的描述、类型、功能、提供者、服务面向的对象、满足服务的附加条件等。

（2）流程。包括流程的描述、功能、相关的软件/硬件/网络要素、参考资料的存储位置、更新数据的存储位置等。

（3）数据。包括数据的类别、数据结构及范围、所有者/创建者/管理者、存储位置、备份流程等。

（4）文档。包括文档的描述、名称、密级、制定时间、制定者/管理者，以及纸质的各种文件、传真、财务报告、发展计划、合同等。

（5）人员。包括姓名/ID/职位、入职时间、技能等。

完成上述工作后，要填写资产及资产属性列表。该列表是所有资产的汇总表，包括了每个资产属性的详细信息，资产及资产属性列表形式见表 3-5，根据该表形成重要资产列表。

表 3-5　资产及资产属性列表

序号	资产名称	所属部门	…	应用描述	保密性等级	完整性等级	可用性等级	资产价值
1								
2								
3								
4								
⋮								
n								

2. 资产定级

一旦识别所有的信息资产，建立的资产清单必须反映每一项信息资产的敏感度和安全等级，并根据这些属性对资产制定一项分类方案，同时确定分类对组织的风险评估计划是否有意义。

可考虑以下资产分类方案：按机密性分类、按完整性分类和按可用性分类。每一种分类方案中可按从低到高的要求进行级别标识，即对每一项分类都指明特定信息资产的保护等级，具体赋值方法如下。

1）保密性赋值

参照 GB/T 22239—2019 的防护要求，将资产保密性分为 5 级，即公开、内部、秘密、机密、绝密，依次赋值为 1、2、3、4、5。

2）完整性赋值

资产完整性分为5级，赋值方法见表3-6。

表3-6 资产完整性赋值

赋 值	等 级	描 述
5	很高	完整性价值非常关键，未经授权的修改或破坏会对造成重大的或无法接受的影响，对业务冲击重大，并可能造成严重的业务中断，难以弥补
4	高	完整性价值较高，未经授权的修改或破坏会造成重大影响，对业务冲击严重，较难弥补
3	中等	完整性价值中等，未经授权的修改或破坏会造成影响，对业务冲击明显，但可以弥补
2	低	完整性价值较低，未经授权的修改或破坏会造成轻微影响，可以忍受，对业务冲击轻微，容易弥补
1	很低	完整性价值非常低，未经授权的修改或破坏造成的影响可以忽略，对业务冲击可以忽略

3）可用性赋值

资产可用性分为5级，赋值方法见表3-7。

表3-7 资产可用性赋值

赋 值	等 级	描 述
5	很高	可用性价值非常高，合法使用者对信息系统及资源的可用度达到年度99.9%以上，或系统不允许中断
4	高	可用性价值较高，合法使用者对信息系统及资源的可用度达到每天90%以上，或系统允许中断时间小于10分钟
3	中等	可用性价值中等，合法使用者对信息系统及资源的可用度在正常工作时间内达到70%，或系统允许中断时间小于30分钟
2	低	可用性价值较低，合法使用者对信息系统及资源的可用度在正常工作时间内达到25%，或系统允许中断时间小于60分钟
1	很低	可用性价值可以忽略，合法使用者对信息系统及资源的可用度在正常工作时间内低于25%

3. 资产价值计算

完成资产的识别和定级之后，就必须赋予资产一个相对价值。在信息安全管理中，一般的做法是以定性分析的方式建立资产的相对价值，以相对价值作为确定重要资产的依据和为该资产投入多少保护资源的依据。

相对价值是一种比较性的价值判定，能确保在信息安全管理中，最有价值的信息资产被赋予最高优先级。或者说，资产受到威胁时所带来的损失是不可预知的，但评估值却有助于确保价值较高的资产首先得到保护。

资产的价值应当由资产的所有者和相关用户来确定，因为只有他们最清楚资产对组织业务的重要性，从而能较准确地评估出资产的实际价值。

在评估资产的价值时，要考虑资产的购买成本和维护成本，同时也要考虑资产的机密

性、完整性和可用性等受到损害时对组织的影响程度。组织要通过广泛和仔细的调查研究，按要求制定出符合自己需要的信息资产评估价值级别。在资产的价值确定之后，应该按重要性列出资产，并按照 NIST SP 800-30 的建议，使用 0.1～1.0 的数值对其进行打分，即赋予一个权重因子，用来表示资产在组织中的相对重要性。资产价值分为 5 级，赋值方法见表 3-8。

表 3-8　资产价值赋值

赋　值	等　级	描　　述
5	很高	资产的重要程度很高，其安全属性破坏后可能导致系统受到非常严重的影响
4	高	资产的重要程度较高，其安全属性破坏后可能导致系统受到比较严重的影响
3	中	资产的重要程度较高，其安全属性破坏后可能导致系统受到中等程度的影响
2	低	资产的重要程度较低，其安全属性破坏后可能导致系统受到较低程度的影响
1	很低	资产的重要程度都很低，其安全属性破坏后可能导致系统受到很低程度的影响，甚至忽略不计

4. 安全措施识别

评估人员归并汇总信息系统各资产所采取的安全措施，形成已有安全措施列表。根据已采取的安全措施及其发挥的效果，根据风险评估的结果，选择控制点及应采用的控制措施。

3.2.3　威胁分析

1. 威胁识别

任何信息资产都会面临各种各样的威胁。与威胁有关的信息可能从信息安全管理体系的参与人员和相关业务流程处收集获得。一项资产可能面临多个威胁，同样一个威胁可能对不同的资产造成影响。

威胁识别的任务是对信息资产面临的威胁进行全面的标识。

识别威胁的方法主要有基于威胁源分类的识别方法、基于某些标准或组织提供的威胁参考目录的识别方法等。

威胁源主要是一些环境因素和人为因素，根据表 3-2 的安全威胁分类，不同的威胁能造成不同形式的危害，在威胁的识别过程中应针对相关资产考虑这些威胁源可能构成的威胁。

很多标准对信息系统可能面临的威胁进行了列举。例如，《IT 安全管理技术》(ISO/IEC 13335)在附录中提供了可能的威胁目录明细，如地震、洪水、飓风、火灾、闪电、工业活动、炸弹攻击、使用武力、恶意破坏、断电、水供应故障、空调故障、硬件失效、电力波动、极端温度和湿度、灰尘、电磁辐射、静电干扰、偷窃、存储介质的未授权使用、存储介质的老化、操作人员失误、维修错误、软件失效、软件被未授权用户使用、软件的非法使用、恶意软件、软件的非法来源、用户身份冒充、未授权用户访问网络、用未授权方式使用网络设备、网络组件的技术性失效、传输错误、线路损坏、流量过载、窃听、通信渗透、流量分析、信息

的错误路径、信息重选路由、抵赖、通信服务失效、资源的滥用等。这些参考目录可以作为进行威胁识别的重要依据。

威胁识别的具体方法包括访谈、问卷调查、动态检测等手段和工具。

2. 威胁评估

威胁评估是对威胁出现的频率和强度进行评估，这是风险评估的重要环节。

每种威胁都对信息资产的安全提出了挑战，在威胁识别之后，威胁评估的首要任务就是检查每种威胁对目标信息资产的潜在影响，提出下面的问题可以帮助理解威胁和威胁对信息资产的潜在影响。

（1）当前哪些威胁对组织的信息资产产生了威胁？

因为并不是所有的威胁都会危及信息资产，所以此时可以检查表 3-2 中的每种分类，并排除那些不适用于本组织的威胁，这样做可以减少风险评估的时间。一旦确定好组织面临的威胁种类，还要识别每一类威胁中的特例，并排除那些不相干的威胁。

（2）哪种威胁会对组织的信息资产带来最严重的危害？

在威胁评估的初期阶段，可以大概地由威胁攻击的频率，以及检查现有的准备等级和应改进的信息安全策略管理来确定威胁可能产生的危害程度。这样进行初步的信息收集，有助于按危险次序来划分威胁等级。

威胁评估的结果一般都是定性的。GB/T 22239—2019 将威胁频度等级划分为 5 个等级，用来代表威胁出现的频率高低。等级数值越大，威胁出现的频率越高，如表 3-9 所示。

表 3-9　威胁赋值表

赋　值	等　级	描　　述
5	很高	出现的频率很高（或≥1 次/周）；在大多数情况下几乎不可避免；或可以证实经常发生过
4	高	出现的频率较高（或≥1 次/月）；在大多数情况下很有可能会发生；或可以证实多次发生过
3	中	出现的频率中等（或≥1 次/半年）；在某种情况下可能会发生；或被证实曾经发生过
2	低	出现的频率较小；一般不太可能发生；或没有被证实发生过
1	很低	威胁几乎不可能发生；仅可能在非常罕见和例外的情况下发生

在实际的评估中，威胁频率的判断依据应在评估准备阶段根据历史统计或行业判断予以确定，并得到被评估方的认可。

3. 安全威胁列表

根据资产面临的威胁，确定被评估各类资产面临的具体威胁，评估其威胁发生的频率，得到资产安全威胁列表。确定威胁发生的频率是风险评估的重要环节，应根据经验和有关的统计数据来判断威胁发生的频率或威胁发生的概率。威胁发生的频率可能受下列因素影响。

（1）资产的吸引力；

（2）资产转化成报酬的容易程度；

（3）威胁的技术含量；

（4）脆弱点被利用的难易程度。

资产安全威胁列表示例见表 3-10。

表 3-10　资产安全威胁列表示例

资 产 名 称	威 胁 名 称	威胁发生频率
资产 A1	威胁 T1	2
	威胁 T2	1
	威胁 T3	2
资产 A2	威胁 T5	4
…	…	…
资产 An	威胁 Ti	a
	威胁 Tj	b
	…	…
	威胁 Tk	c

注：a、b、c 为取值 1～5 的整数。

3.2.4　脆弱性分析

1. 脆弱性识别

脆弱性是信息资产固有的属性，表现为存在一系列的脆弱点或漏洞。脆弱性的识别主要按脆弱性的类型，即从技术和管理两方面进行。其中技术方面主要指软件、硬件和通信设施等方面存在的脆弱性，管理方面主要指在人员管理、业务管理和行政管理中的过程与控制等方面存在的脆弱性。

识别脆弱性的方法主要有问卷调查、工具检测、工人核查、渗透性测试和文档查阅等。在识别的过程中要注意其数据应来自于资产的所有者、使用者，以及相关业务领域的专家和软硬件方面的专业人员等。

对不同的识别对象，其脆弱性识别的具体要求应参照相应的技术或管理标准实施。例如，对物理环境的脆弱性识别应按《计算机场地通用规范》（GB/T 2887—2011）中的技术指标实施；对操作系统、数据库应按《计算机信息系统 安全保护等级划分准则》（GB 17859—1999）中的技术指标实施；对网络、系统、应用等信息技术安全性的脆弱性识别应按《信息技术 安全技术 信息技术安全评估准则》（GB/T 18336—2001）中的技术指标实施；对管理脆弱性识别方面应按《信息技术 安全技术 信息安全控制实践指南》（GB/T 22081—2016）的要求对安全管理制度及其执行情况进行检查，发现并管理脆弱性和不足。

2. 脆弱性赋值

与每一种威胁相关的脆弱性都应当评估出来，因为在一定条件下威胁会利用这些脆

弱性导致安全事件的发生。

可以根据脆弱性对信息资产的暴露程度、技术实现的难易程度、流行程度等，采用等级方式对已识别的脆弱性的严重程度进行评估。由于很多脆弱性反映的是某一方面的问题，或可能造成相似的后果，评估时应综合考虑这些脆弱性，以确定这方面脆弱性的严重程度。

对于某个资产，其技术脆弱性的严重程度同时受到组织管理脆弱性的影响。因此，衡量资产的脆弱性还应参考技术管理和组织管理脆弱性的严重程度。

脆弱性严重程度可以进行等级化处理，不同的等级分别代表资产脆弱性严重程度的高低。等级数值越大，脆弱性严重程度越高。

脆弱性评估的结果一般也是定性的。GB/T 22239—2019 将脆弱性严重程度划分为 5 个等级，如表 3-11 所示。

表 3-11　脆弱性赋值表

赋　值	等　级	描　　述
5	很高	如果被威胁利用，将对资产造成完全损害
4	高	如果被威胁利用，将对资产造成重大损害
3	中	如果被威胁利用，将对资产造成一般损害
2	低	如果被威胁利用，将对资产造成较小损害
1	很低	如果被威胁利用，将对资产造成的损害可以忽略

在风险评估过程中，将会发现许多系统的脆弱点或漏洞，威胁也会以多种方式显露出来。为每一项信息资产建立脆弱性评估列表，并确定哪个脆弱性会对受保护的资产产生最大的威胁，这是风险识别人员每天都要面临的挑战。

在风险识别的最后，完成资产、威胁及脆弱性的列表清单。该清单将作为风险分析过程的支持文档。

3. 脆弱性列表

根据技术工具检测结果和问卷调查结果，确定被评估信息资产存在的安全脆弱性及其严重程度，得到资产安全脆弱性列表。资产脆弱性列表示例如表 3-12 所示。

表 3-12　资产脆弱性列表示例

资产名称	脆弱性名称	脆弱性严重程度
资产 A1	脆弱性 V1	3
	脆弱性 V2	2
	脆弱性 V3	4
	脆弱性 V4	3

续表

资产名称	脆弱性名称	脆弱性严重程度
资产 A2	脆弱性 V5	5
	脆弱性 V2	1
	脆弱性 V3	3
	脆弱性 V4	4
	脆弱性 V10	3
…	…	…
资产 An	脆弱性 Vi	a
	…	…
	脆弱性 Vj	b
	脆弱性 Vk	c

注：a、b、c 为取值 1～5 的整数。

3.2.5　已有安全措施分析与评估

安全控制措施可以分为预防性安全控制措施和保护性安全控制措施两种。预防性安全控制措施可以降低威胁利用脆弱性导致安全事件发生的可能性；而保护性安全控制措施可以减少因安全事件发生后对组织或系统造成的影响，如业务持续性计划。在识别脆弱性的同时，评估人员应对这些已采取的安全控制措施的有效性进行确认。该步骤的主要任务是对当前信息系统所采取的安全控制措施进行标识，并对其预期功能、有效性进行分析，再根据检查的结果来决定是否保留、去除或替换现有的控制措施。

安全控制措施的确认应评估其有效性，即是否真正地降低了系统的脆弱性，抵御了威胁。对有效的安全控制措施继续保持，以避免不必要的工作和费用，防止安全措施的重复实施。对认为不适当的安全控制措施应核实其是否应被取消或对其进行修正，或用更合适的安全控制措施替代。

已有安全控制措施的确认与脆弱性的识别存在一定的联系。一般来说，安全控制措施的使用将减少系统技术或管理上的脆弱性，但确认安全控制措施并不需要像脆弱性识别过程那样具体到每个资产、组件的脆弱性，而是一类具体控制措施的集合，为风险处理计划的制定提供依据和参考。

3.2.6　风险计算与分析

在完成了资产识别、威胁识别、脆弱性识别，以及已有安全措施确认后，将采用适当的方法与工具确定威胁利用脆弱性导致安全事件发生的可能性。综合安全事件所作用的资产价值及脆弱性的严重程度，判断安全事件造成的损失对组织的影响，即安全风险。

如前所述，风险可以表示为威胁发生的可能性、脆弱性被威胁利用的可能性、威胁的潜在影响三者的函数，在风险评估过程中，计算风险时还要减去一个常数，即现有安全控

制措施的实施降低的风险，可记为

$$R = R(A,T,V) - R_C = R[P(T,V),I(Ve,Sz)] - Rc$$

其中，R 为安全风险，A 为资产，T 为威胁，V 为脆弱性，Rc 为已有控制所减少的风险，Ve 为安全事件所作用的资产价值，Sz 为脆弱性严重程度，P 为威胁利用资产的脆弱性导致安全事件的可能性，I 为安全事件发生后造成的影响。

由于 Rc 是一个常数，在函数表示式中可以省略，故上式可简化为

$$R = R[P(T,V),I(Ve,Sz)]$$

下面介绍计算该式的 3 个关键环节。

1. 计算安全事件发生的可能性

根据威胁出现频率及脆弱性的状况，计算威胁利用脆弱性导致安全事件发生的可能性，即安全事件的可能性 $= P$（威胁出现频率，脆弱性）$= P(T,V)$。

在具体评估中，应综合攻击者技术能力（专业技术程度、攻击设备等）、脆弱性被利用的难易程度（可访问时间、设计和操作知识公开程度等）、资产吸引力、威胁出现的可能性、脆弱点的属性、安全控制措施的效能等因素来判断安全事件发生的可能性。

可能性分析方法可以是定量的，也可以是定性的。定量方法可将发生安全事件的可能性表示成概率形式，而定性方法将安全事件发生的可能性给予如极高、高、中、低等类似的等级评价。

2. 计算安全事件发生后造成的影响

根据资产价值及脆弱性严重程度，计算安全事件一旦发生后造成的影响，即

$$\text{安全事件造成的影响} = I(\text{资产价值，脆弱性严重程度}) = I(Ve,Sz)$$

安全事件的发生造成的影响可体现在以下方面：直接经济损失、物理资产损坏、业务持续性影响、法律责任、人员安全危害、信誉（形象）受损等。

部分安全事件造成的影响判断还应参照安全事件发生可能性的结果，对发生可能性极小的安全事件（如处于非地震带的地震威胁、在采取完备供电措施状况下的电力故障威胁等）可以不计算其影响或损失。

由于安全事件对组织影响的多样性，相关数据也比较缺乏，目前这种影响造成的损失的定量计算方法还不成熟，更多的是采用定性的分析方法，根据经验对安全事件发生后所造成的影响或损失进行等级划分，给予极高、高、中、低、可忽略等评价。

3. 计算风险值

根据计算出的安全事件的可能性以及安全事件造成的影响，计算风险值，即

$$\text{风险值} = R(\text{安全事件的可能性，安全事件造成的影响}) = R[P(T,V),I(Ve,Sz)]$$

评估者可根据自身情况选择相应的风险计算方法计算风险值，如矩阵法或相乘法。矩阵法通过构造一个二维矩阵，形成安全事件的可能性与安全事件造成的影响之间的二维关系；相乘法通过构造经验函数，将安全事件的可能性与安全事件造成的影响进行运算得到风险值。

3.3　信息安全风险管理

3.3.1　风险管理的概念

根据《信息安全技术信息安全风险管理指南》(GB/Z 24364—2009)的定义，信息安全风险管理是识别、控制、消除或最小化可能影响系统资源的不确定因素的过程。风险管理有两种方法，一种是前瞻性风险管理方法，通过风险评估、风险控制决策、实施风险控制和评定风险管理的有效性，实现事前最大程度地降低可能性；另一种方法是反应性风险管理方法，通过遏制和评估损害、确定损害部位、修复损害部位、审查响应过程并更新安全策略，实现事后降低影响并降低再次发生的可能性。将前瞻性风险管理方法和反应性风险管理方法相结合是风险管理的最佳实践。正确的风险管理流程让组织能够以最具成本效益的方式运行，并且使已知的业务风险维持在可接受的水平。它还使组织可以用一种一致的、条理清晰的方式来组织有限的资源并确定优先级，从而更好地执行风险管理过程。

风险管理包括 4 个阶段。①风险评估：综合定性和定量的风险评估方法，分析风险并确定风险，给出一份相对较短的经过详细检查的风险优先级列表。②风险控制：提议并评估潜在的控制解决方案，选择合适的控制措施并形成最合适的解决方案作为缓解顶级风险的推荐交给组织的安全指导部门。③实施控制：实际实施风险控制方案。④评定计划有效性：用于验证控制措施实际提供的保护程度，并观察环境变化。

3.3.2　风险管理的方法和过程

风险管理的方法包括前瞻性风险管理方法和反应性风险管理方法。前瞻性方法可以在事件发生之前，最大程度地降低坏事情发生的可能性；反应性方法可以在事件发生之后，遏制和评估受到的损害，确定并修复损害部位，并进行审查和策略更新，以最大程度地降低影响，并采取措施降低再次发生的可能性。如果这两种风险管理的主要方法都做好了，那么风险管理的两个阶段就能都管理好，这就是风险管理的方法。

在日常工作生活中提倡的是先做好事前的风险管理，前瞻性风险管理的过程包括 4 个阶段：风险评估、风险控制、实施控制和评估计划有效性。

风险评估阶段主要是综合运用定性和定量两种评估方法，给出一份相对较短的经过详细检查的最重要风险列表，风险评估是风险管理的起点。风险控制阶段主要是提议并评估潜在的控制解决方案，然后将最好的解决方案作为缓解顶级风险的推荐交给组织。实施控制阶段是组织实际实施控制解决方案。评定计划有效性阶段是用于验证控制措施实际提供的保护程度，并观察环境的变化，一旦环境发生变化，如发生了安全事件或增加了信息资产时，要考虑是否再次执行风险管理的这个过程。

可以看出风险管理具有永不终止的生命周期，通过这样一种前瞻性的风险管理方法，能让组织以最具成本效益的方式运行，并使风险维持在可接受水平。下面详细介绍风险管理过程的 4 个阶段。

1. 风险评估阶段

风险评估先要做好风险评估准备，例如，确定风险评估的范围，即要评估哪些资产、采

用哪种风险评估方法、依据哪个风险评估标准、组成风险评估团队，并且要确定风险评估的方案。做好准备之后，就要在刚才确定的风险评估范围内进行资产识别、威胁识别和漏洞识别。然后确认一下现有的安全控制措施并进行风险的分析和计算。最后给出安全控制措施建议，并形成风险评估报告。

2. 风险控制

风险控制即考虑如何制定风险控制方案。

（1）对实施控制措施的优先级进行排序。

基于在风险评估报告中提出的风险级别对风险处理的实现行动进行优先级排序。在分配资源时，对标有不可接受的高等级（如被定义为“非常高”或“高”风险级的风险）风险项应该给予较高的优先级。

（2）评估所建议的安全选项。

风险评估结论中建议的控制措施对于具体的单位及其信息系统可能不是最适合和最可行的，因此要对所建议控制措施的可行性（如兼容性、用户接受程度）和有效性（如保护程度和风险控制级别）进行分析，目的是选择出最适当的控制措施。

（3）实施成本效益分析。

为了帮助管理层做出决策并找出成本有效性最好的控制措施，要实施成本效益分析，并为决策管理层提供风险控制措施的成本效益分析报告。

（4）选择风险控制措施。

在成本效益分析的基础上，管理人员应确定成本有效性最好的控制措施来降低单位的风险。

（5）责任分配。

遴选出那些拥有合适专长、技能，并且可实现所选控制措施的人员（内部人员或外部合同商）赋以相应责任。

（6）制定控制措施的实施计划。

制定控制措施的实施计划，计划内容主要包括风险评估报告给出的风险、风险级别及所建议的安全措施、实施控制的优先级队列、预期安全控制列表、实现预期安全控制时所需的资源、负责人员清单、开始日期、完成日期及维护要求等。

（7）分析计算残余风险。

风险控制可以降低风险级别，但是不能根除风险，因此安全措施实施后仍然存在残余风险。

风险评估报告中给出了所建议的控制措施，所以第一步就是要把这些推荐的控制措施进行优先级排序，但是风险评估报告中建议的控制措施对于具体的单位可能不一定适合和可行，所以第二步要对这些控制措施进行评估，以得到合适的清单。那么到底该如何控制风险呢？

风险控制有 4 种策略：规避风险、转移风险、降低风险和接受风险。规避风险通常在风险损失无法接受、又难以通过控制措施减低风险的情况下采用。转移风险一般用于那些发生概率低，但一旦发生会对组织产生重大影响的风险，通常只有当风险不能被降低或避免且被第三方（被转嫁方）接受时才被采用。降低风险通常在安全投入小于负面影响价

值的情况下采用。接受风险是当要保护资产的成本抵不上安全措施的开销，或是在采取了降低风险和避免风险措施后的残余风险仍然较大时采用。

3. 实施控制阶段

首先要对人员进行责任分配，遴选出那些拥有合适专长和技能、可实现所选控制措施的人员，并赋以责任，然后按照上一阶段制定的风险控制实施计划进行实际控制措施的实施。目标就是将组织面临的风险降低到可以接受的水平以下。

4. 评估计划有效性阶段

主要是验证所选择的控制措施实际提供的保护效果如何，并观察环境变化。一旦出现组织新增信息资产时、系统发生重大变更时或发生严重信息安全事故时，当然也包括组织认为有必要时，都要重新开展风险评估。因此，风险管理是动态的、持续的管理过程，需要定期进行风险评估，还要根据环境的变化及时进行临时评估。

这 4 个阶段就组成了风险管理的过程。

3.3.3　风险管理与控制

1. 选择安全控制措施

在经过风险识别和风险计算后，就可以对不可接受的风险情况引入适当的安全控制措施，对风险实施管理与控制，将风险降低到可以接受的程度。

选择安全控制措施时，要考虑以下因素。

1）控制的成本费用

控制的选择要基于安全平衡的原则，要考虑技术的、非技术的控制因素，也要考虑法律法规的要求、业务的需求及风险的要求。

如果实施与维护这些控制的费用要高于资产遭受威胁所造成损失的预期值，那么所选择的控制措施是不适合的；如果控制费用比组织计划的安全预算还要高，也是不适当的。但如果因为控制费用预算的不足使得控制措施的数量与质量下降，又会使系统产生不必要的风险，因此，对此要特别注意。

2）控制的可用性

在使用所选择的安全控制措施时，有时候会发现有些控制因为技术、环境等原因，实施和维护起来非常困难，或根本就不可能实施和维护。另外，如果某些控制对用户来说不可操作或无法接受，那么这些控制也是不可行的。因此，在选择安全控制措施时，一定要注意控制的可用性，例如，可以采取相近的技术控制或非技术的物理、人员、过程等措施来替代或弥补那些可行性差的技术控制，或作为技术控制的备用项。

3）已存在的控制

所选择的安全控制措施应当与组织中已存在的控制有机结合起来，共同服务于安全目标。因此，需要注意它们之间的协调关系。

当已存在的控制不能提供足够的安全保障时，在选择新的安全控制措施之前，组织应先对是否取消原有的控制或是补充现有的控制作出决策。这种决策依赖于控制的成本大小、更新是否必需、安全需求是否迫切等因素。

所选择的控制与已存在的控制是否兼容（不存在冲突）。例如，物理访问控制可以用