第 5 章

信息安全风险管理与评估

学习目标

- 了解风险评估的概念、特点和内涵；
- 知道风险评估的过程及应注意的问题；
- 了解如何选择恰当的风险评估方法；
- 知道典型的风险评估方法；
- 了解风险评估实施准备。

5.1 信息安全风险管理

信息安全风险管理是指对信息安全项目从识别到分析乃至采取应对措施等一系列过程，它包括将积极因素所产生信息安全风险管理流程的影响最大化和使消极因素产生的影响最小化两方面内容。

5.1.1 定义与基本性质

信息安全风险管理是指通过风险识别、风险分析和风险评价去认识信息安全项目的风险，以此为基础合理地使用各种风险应对措施、管理方法技术和手段，对信息安全项目的风险实行有效的控制，妥善地处理风险事件造成的不利后果，以最少的成本保证信息安全总体目标实现的管理工作。

通过界定信息安全范围，可以明确信息安全项目的范围，将信息安全项目的任务细分为更具体、更便于管理的部分，避免遗漏而产生风险。在信息安全项目进行过程中，各种变更是不可避免的，变更会带来某些新的不确定性，风险管理可以通过对风险的识别、分析来评价这些不确定性，从而向信息安全项目的管理提出任务。

信息安全风险管理基本性质表现为风险的客观性和风险的不确定性。风险的客观性，首先表现在它的存在是不以个人的意志为转移的。从根本上说，这是因为决定风险的各种因素对风险主体是独立存在的，不管风险主体是否意识到风险的存在，在一定条件下仍有可能变为现实。其次，还表现在它是无时不有、无所不在的，它存在于人类社会的发展过程中，潜藏于人类从事的各种活动之中。风险的不确定性是指风险的发生是不确定的，即风险的程度有多大、风险何时何地有可能转变为现实均是不确定的。这是由于人们对客观世界的认识受到各种条件的限制，不可能准确预测风险的发生。

风险一旦产生，就会使风险主体产生挫折、失败、甚至损失，这对风险主体是极为不利

的。风险的不利性要求我们在承认风险、认识风险的基础上做好决策，尽可能地避免风险，将风险的不利性降至最低。风险的可变性是指在一定条件下风险可以转化。

5.1.2 分类

按风险后果分类可分为纯粹风险和投机风险。纯粹风险是指风险导致的结果只有两种，即没有损失或有损失（不会带来利益）。投机风险是指风险导致的结果有三种，即没有损失、有损失或获得利益。纯粹风险一般可重复出现，因而可以预测其发生的概率，从而相对容易采取防范措施。投机风险重复出现的概率小，因而预测的准确性相对较差。纯粹风险和投机风险常常同时存在。

按风险来源划分自然风险和人为风险。自然风险是指由于自然力的不规则变化导致财产毁损或人员伤亡，如风暴、地震等。人为风险是指由于人类活动导致的风险。人为风险又可细分为行为风险、政治风险、经济风险、技术风险和组织风险等。

按风险的形态分静态风险和动态风险。静态风险是由于自然力的不规则变化或由于人的行为失误导致的风险。从发生的后果来看，静态风险多属于纯粹风险。动态风险是由于人类需求的改变、制度的改进和政治、经济、社会、科技等环境的变迁导致的风险。从发生的后果来看，动态风险既可属于纯粹风险，又可属于投机风险。

按风险可否管理分可管理风险和不可管理风险。可管理风险是指用人的智慧、知识等可以预测、可以控制的风险。不可管理风险是指用人的智慧、知识等无法预测和无法控制的风险。

按风险的影响范围分类可分为局部风险和总体风险。局部风险是指由于某个特定因素导致的风险，其损失的影响范围较小。总体风险影响范围大，其风险因素往往无法加以控制，如经济、政治等因素。

按风险后果的承担者分类可分为政府风险、投资方风险、业主风险、承包商风险、供应商风险、担保方风险等。

按照信息安全目标系统的结构进行划分可分为工期风险、费用风险、质量风险、市场风险、信誉风险、人身伤亡安全健康以及工程或设备的损坏、法律责任。

5.1.3 信息安全风险控制与管理方案

风险识别包含两方面内容：识别哪些风险可能影响信息安全进展，及记录具体风险的各方面特征，风险识别不是一次性行为，而应有规律地贯穿整个信息安全中；风险识别包括识别内在风险及外在风险。内在风险指信息安全工作组能加以控制和影响的风险，如人事任免和成本估计等。外在风险指超出信息安全工作组等控力和影响力之外的风险，如市场转向或政府行为等。

严格来说，风险仅仅指遭受创伤和损失的可能性，但对信息安全而言，风险识别还牵涉机会选择（积极成本）和不利因素威胁（消极结果）。信息安全风险识别应凭借对“因”和“果”（将会发生什么导致什么）的认定来实现，或通过对“果”和“因”（什么样的结果需要予以避免或促使其发生，以及怎样发生）的认定来完成。

1. 对风险识别的输入

在所识别的风险中，信息安全产品的特性起主要的决定作用。所有的产品都是这样，生产技术已经成熟完善的产品要比尚待革新和发明的产品风险低得多。与信息安全相关的风险常常以“产品成本”和“预期影响”来描述。工作分析结构——非传统形式的结构细分往往能提供给我们高一层次分支图所不能看出来的选择机会。成本估计和活动时间估计——不合理的估计及仅凭有限信息做出的估计会产生更多风险。人事方案——确定团队成员有独特的工作技能使之难以替代，或有其他职责使成员分工细化。必需品采购管理方案——类似发展缓慢的地方经济这样的市场条件往往可能提供降低合同成本的选择。

2. 风险输出

风险因素是指一系列可能影响信息安全向好或坏的方向发展的风险事件的总和，这些因素是复杂的，也就是说，它们应包括所有已识别的条目，而不论频率、发生之可能性，盈利或损失的数量等。潜在的风险事件是指如自然灾害或团队特殊人员出走等能影响信息安全的不连续事件。在发生这种事件或重大损失的可能相对巨大时(“相对巨大”应根据具体信息安全而定)，除风险因素外还应将潜在风险事件考虑在内。风险征兆有时也被称为触发引擎，是一种实际风险事件的间接显示。例如：丧失士气可能是计划被搁置的警告信号；而运作早期即产生成本超支可能又是评估粗糙的表现。风险认定过程应在另一个相关领域中确定一个要求，以便进行进一步运作。

3. 风险量化

风险量化涉及对风险和风险之间相互作用的评估，用这个评估分析信息安全可能的输出。这首先需要决定哪些风险值得反应。如对风险量化的输入，投资者对风险的容忍度。不同的组织和个人往往对风险有着不同的容忍限度。不同工具和方法对风险量化存在一定的偏差。统计数字加总是将每个具体工作课题的估计成本加总以计算出整个信息安全的成本的变化范围。模拟法运用假定值或系统模型来分析系统行为或系统表现。较普通的模拟法模式是运用信息安全模型作为信息安全框架来制作信息安全日程表。决策树是一种便于决策者理解的、来说明不同决策之间和相关偶发事件之间的相互作用的图表。

4. 对策研究

风险对策研究包括对机会的跟踪进度和对危机的对策的定义。对威胁的对策大体分以下三点：避免——排除特定威胁往往靠排除威胁起源，信息安全管理队伍绝不可能排除所有风险，但特定的风险事件往往是可以排除的；减缓——减少风险事件的预期资金投入来减低风险发生的概率(如为避免信息安全产出的产品报废而使用专利技术)，以及减少风险事件的风险系数，或两者双管齐下；吸纳——接受一切后果。这种接受可以是积极的(如制定预防性计划来防备风险事件的发生)，也可以是消极的(如某些工程运营超支则接受低于预期的利润)。如对风险对策研究的输入须跟踪的机会，须反应的威胁和被忽略的机会，被吸纳的威胁。

5. 实施控制

风险对策实施控制包括实施风险管理方案以便在信息安全过程中对风险事件做出回

应。当变故发生时，需要重复进行风险识别、风险量化以及风险对策研究，制定一整套基本措施、风险管理方案和实际风险事件；有些已识别了的风险事件会发生，有些则不会。发生了的风险事件是实际风险事件或者说是风险的起源，而信息安全管理人员应总结已发生的风险事件以便进行进一步的对策研究。附加风险识别；当信息安全进程受到评价和总结时，事先未被识别的潜在风险事件或风险的起源将会浮出水面。

6. 管理方案

在全面分析评估风险因素的基础上，制定有效的管理方案是风险管理工作的成败之关键，它直接决定管理的效率和效果。因此，翔实、全面、有效成为方案的基本要求，其内容应包括：风险管理方案的制定原则和框架、风险管理的措施、风险管理的工作程序等。

7. 制定原则

(1) 可行、适用、有效性原则。管理方案首先应针对已识别的风险源，制定具有可操作的管理措施，适用有效的管理措施能大大提高管理的效率和效果。

(2) 经济、合理、先进性原则。管理方案涉及的多项工作和措施应力求管理成本节约，管理信息流畅、方式简捷、手段先进才能显示出高超的风险管理水平。

(3) 主动、及时、全过程原则。信息安全的全过程建设期分为前期准备阶段(可行性研究阶段、勘察设计阶段、招标投标阶段)、施工及保修阶段、生产运营期。对于风险管理，仍应遵循主动控制、事先控制的管理思想，根据不断发展变化的环境条件和不断出现的新情况、新问题，及时采取应对措施，调整管理方案，并将这一原则贯彻信息安全全过程，才能充分体现风险管理的特点和优势。

(4) 综合、系统、全方位原则。风险管理是一项系统性、综合性极强的工作，不仅其产生的原因复杂，而且后果影响面广，所需处理措施综合性强，例如信息安全的多目标特征(投资、进度、质量、安全、合同变更和索赔、生产成本、利税等目标)。因此，要全面彻底地降低乃至消除风险因素的影响，必须采取综合治理原则，动员各方力量，科学分配风险责任，建立风险利益的共同体和信息安全全方位风险管理体系，才能将风险管理的工作落到实处。

(5) 风险管理方案计划书内容框架。计划书一般应包括：①信息安全概况；②风险识别(分类、风险源、预计发生时间点、发生地、涉及面等)；③风险分析与评估(定性和定量的结论、后果预测、重要性排序等)；④风险管理的工作组织(设立决策机构、管理流程设计、职责分工、工作标准拟订、建立协调机制等)；⑤风险管理工作的检查评估。

8. 控制措施

(1) 经济性措施：主要措施有合同方案设计(风险分配方案、合同结构设计、合同条款设计)，保险方案设计(引入保险机制、保险清单分析、保险合同谈判)，管理成本核算。

(2) 技术性措施：技术性措施应体现可行、适用、有效性原则，主要有预测技术措施(模型选择、误差分析、可靠性评估)，决策技术措施(模型比选、决策程序和决策准则制定、决策可靠性预评估和效果后评估)，技术可靠性分析(建设技术、生产工艺方案、维护保障技术)。

(3) 组织管理性措施：主要是贯彻综合、系统、全方位原则和经济、合理、先进性原则，包括管理流程设计、确定组织结构、管理制度和标准制定、人员选配、岗位职责分工，落

实风险管理的责任等。还应提倡推广使用风险管理信息系统等现代管理手段和方法。

5.2　信息安全风险评估基础

5.2.1　与风险评估相关的概念

资产(Asset)：任何对组织有价值的事物。威胁(Threat)：是指可能对资产或组织造成损害的事故的潜在原因。例如，组织的网络系统可能受到来自计算机病毒和黑客攻击的威胁。脆弱点(Vulnerability)：是指资产或资产组中能被威胁利用的弱点。如员工缺乏信息安全意识、使用简短易被猜测的口令、操作系统本身有安全漏洞等。威胁是利用脆弱点而对资产或组织造成损害的，资产、威胁和脆弱点对应关系如图5-1所示。

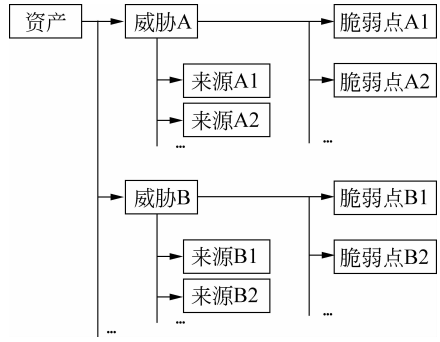

图5-1　资产、威胁和脆弱点对应关系

风险(Risk)：特定的威胁利用资产的一种或一组薄弱点，导致资产的丢失或损害的潜在可能性，即特定威胁事件发生的可能性与后果的结合。风险评估(Risk Assessment)：对信息和信息处理设施的威胁、影响(Impact)和脆弱点及三者发生的可能性的评估。风险评估也称为风险分析，就是确认安全风险及其大小的过程，即利用适当的风险评估工具，包括定性和定量的方法，确定资产风险等级和优先控制顺序。

5.2.2　风险评估的基本特点

信息安全风险评估具有以下基本特点：

(1) 决策支持性：所有的安全风险评估都旨在为安全管理提供支持和服务，无论它发生在系统生命周期的哪个阶段，所不同的只在于其支持的管理决策阶段和内容。

(2) 比较分析性：对信息安全管理和运营的各种安全方案进行比较，对各种情况下的技术、经济投入和结果进行分析、权衡。

(3) 前提假设性：在风险评估中所使用的各种评估数据有两种，一是系统既定事实的描述数据；二是根据系统各种假设前提条件确定的预测数据。不管发生在系统生命周期的哪个阶段，在评估时，人们都必须对尚未确定的各种情况做出必要的假设，然后确定相应的预测数据，并据此做出系统风险评估。没有哪个风险评估不需要给定假设前提条件，因此信息安全风险评估具有前提假设性这一基本特性。

(4) 时效性：必须及时使用信息安全风险评估的结果，过期则可能出现失效而无法使用的情况，失去风险评估的作用和意义。

(5) 主观与客观集成性：信息安全风险评估是主观假设和判断与客观情况和数据的结合。

（6）目的性：信息安全风险评估的最终目的是为信息安全管理决策和控制措施的实施提供支持。

5.2.3 风险评估的内涵

风险评估是信息安全建设和管理的科学方法。风险评估是信息安全等级保护管理的基础工作，是系统安全风险管理的重要环节。风险评估是信息安全保障工作的重要方法，是风险管理理论和方法在信息化中的运用，是正确确定信息资产、合理分析信息安全风险、科学管理风险和控制风险的过程。信息安全旨在保护信息资产免受威胁。考虑到各类威胁，绝对安全可靠的网络系统并不存在，只能通过一定的措施把风险降低到可以接受的程度。信息安全评估是有效保证信息安全的前提条件。只有准确了解系统安全需求、安全漏洞及其可能的危害，才能制定正确的安全策略，制定并实施信息安全对策。另外，风险评估也是制定安全管理措施的依据之一。还有，客户单位业务主管并不是不重视信息安全工作，而是不知道具体的信息安全风险是什么，不知道信息安全风险来自何方、有多大，不知道做好信息安全工作要投入多少人力、财力、物力，不知道应采取什么样的措施来加强信息安全保障工作，对已采取的信息安全措施也不知道是否有效。所以我们说信息安全风险评估应该成为各个单位信息化建设的一种内在要求，各主管和应用单位应该负责好自己系统的信息安全风险评估工作。

风险评估是分析确定风险的过程。风险评估是依据国家标准规范，对信息系统的完整性、保密性、可用性等安全保障性能进行科学、公正地综合评估地活动。它是确认安全风险及其大小的过程，即利用适当的风险评估工具，包括定性和定量的方法，确认信息资产自身的风险等级和风险控制的优先顺序。风险评估是识别系统安全风险并确定风险出现的概率、结果的影响以及提出补充的安全措施以缓和风险影响的过程。风险评估是信息安全建设的起点和基础。风险评估是信息安全建设的起点和基础，科学地分析理解信息和信息系统在保密性、完整性、可用性等方面所面临的风险，并在风险的预防、风险的减少、风险的转移、风险的补偿、风险的分散等之间做出决策。风险评估是在倡导一种适度安全。随着信息技术在国家各个领域的广泛应用，传统的安全管理方法已不适应信息技术带来的变化，不能科学全面地分析、判断网络和信息系统的安全状态，在网络和信息系统建设、运行过程中，出现了不能采取适当的安全措施、投入适当的安全经费，以达到适当的安全目标的偏差。

信息安全风险评估就是从风险管理的角度，运用科学的方法和手段，系统地分析网络与信息系统所面临的威胁及存在的脆弱性，评估安全事件一旦发生可能造成的危害程度，提出针对性抵御的防护对策和整改措施，并为防范和化解信息安全风险或者将风险控制在可接受的水平，最大限度地保障网络和信息安全提供科学依据。

风险评估在信息安全保障体系建设中具有不可替代的地位和重要作用，它是实施等级保护的前提，又是检查、衡量系统安全状况的基础工作。风险评估是分析确定风险的过程。分析确定系统风险及其大小，进而决定采取什么措施去减少、转移、避免和对抗风险，确定把风险控制在可以容忍的范围内，这就是风险评估的主要流程。

5.2.4　风险评估的两种方式

信息安全风险评估是提高我国信息安全保障水平的一项重要举措，应当贯穿于网络与信息系统建设运行的全过程。根据评估发起者的不同，风险评估可分为自评估、检查评估两种方式。自评估是信息安全风险评估的主要形式，是指信息系统拥有、运营或使用单位发起的对本单位信息系统进行的风险评估，以发现信息系统现有弱点。实施安全管理为目的的检查评估是指信息系统上级管理部门或信息安全职能部门组织的信息安全风险评估。检查评估是通过行政手段加强信息安全的重要措施。

风险评估应以自评估为主，检查评估在自评估过程记录与评估结果的基础上，验证和确认系统存在的技术、管理和运行风险，以及用户实施自评估后采取风险控制措施取得的效果。自评估和检查评估应相互结合、互为补充。自评估和检查评估都可依托自身技术力量进行，也可委托具有相应资质的第三方机构提供技术支持。

美国等发达国家，自评估工作已经运行多年，逐步形成了标准和规范，大体进入了制度化阶段。在此基础上，他们开始强调联邦一级的认证认可，即检查评估。我国开展信息安全风险评估工作滞后于发达国家。因此，现阶段应该把自评估工作尽快开展、规范起来，打好风险评估工作的基础。

1. 自评估

自评估是风险评估的基础。要落实“谁主管谁负责，谁运营谁负责”的原则，信息系统资产的拥有者、主管者、运行者首先应通过自评估的方式对自己负责，这样才能随时掌握安全状况，不断调整安全措施，有效进行安全控制。

自评估是信息系统拥有者依靠自身力量，依据国家风险评估的管理规范和技术标准，对自有的信息系统进行风险评估的活动。信息系统的风险不仅仅来自信息系统技术平台的共性，还来自于特定的应用服务。由于具体单位的信息系统各具特性，这些个性化的过程和要求往往是敏感的，没有长期接触该单位所属行业和部门的人难以在短期内熟悉和掌握。而且只有拥有者对威胁及其后果的体会最深切。目前的信息技术企业，通过技术平台的脆弱性分析，难以真正掌握和了解具体行业或部门的资产、威胁和风险。这些企业不但需要深入研究信息技术平台的共性化风险，还需要推动不同行业部门的个性化风险的专门研究，否则风险评估将会出现关注面的缺失。

自评估方式的优缺点非常明显，主要包括以下两点。

优点：有利于保密；有利于发挥行业和部门内的人员的业务特长；有利于降低风险评估的费用；有利于提升本单位的风险评估能力与信息安全知识。

缺点：如果没有统一的规范和要求，在缺乏信息系统安全风险评估专业人才的情况下，自评估的结果可能不深入、不规范、不到位；自评估中，也可能会存在某些不利的干预，从而影响风险评估结果的客观性，降低评估结果的置信度；某些时候，即使自评估的结果比较客观，也必须与管理层进行沟通。

为了扬长避短，在自评估中可以采用如下改进办法：发挥专家的指导作用或委托专业评估组织参与部分工作；委托具有相应资质的第三方机构提供技术支持；由国家建立的测评认证机构或安全企业实施评估活动。它既有自评估的特点（由单位自身发起，且本单

位对风险评估过程的影响可以很大),也有第三方评估的特点(由独立于本单位的另外一方实施评估)。

委托第三方机构组织或参与自评估活动的好处在于:在委托评估中,接受委托的评估机构一般拥有风险评估的专业人才;风险评估的经验比较丰富;对信息技术风险的共性了解得比较深入;评估过程较为规范,评估结果的客观性比较好,置信度比较高。

但在委托第三方机构组织或参与自评估活动时也要考虑以下三个问题:①评估费用可能会较高;②可能会难以深入了解行业应用服务中的安全风险;③由于风险评估中必然会接触到被评估单位的敏感情况,且评估结果本身也属于敏感信息,因此委托评估中容易发生评估风险。

2. 检查评估

检查评估是由信息安全主管部门或业务主管部门发起的一种评估活动,旨在依据已经颁布的法规或标准,检查被评估单位是否满足了这些法规或标准。信息安全检查是通过行政手段加强信息安全的重要措施,形式有安全保密检查、生产安全检查、专项检查等。被查单位应配合评估工作的开展。

检查评估的实施可以多样化,既可以依据国家法规或标准的要求,实施完整的风险评估过程,也可以在对自评估的实施过程、风险计算方法、评估结果等重要环节的科学合理性进行分析的基础上,对关键环节或重点内容实施抽样评估。

检查评估应覆盖但不限于以下内容:自评估方法的检查;自评估过程记录检查;自评估结果跟踪检查;现有安全措施的检查;系统输入/输出控制的检查;软硬件维护制度及实施状况的检查;突发事件应对措施的检查;数据完整性保护措施的检查;审计追踪的检查。

检查评估一般由主管机关发起,通常都是定期的、抽样进行的评估模式,旨在检查关键领域或关键点的信息安全风险是否在可接受的范围内。鉴于检查评估的性质,在检查评估实施之前,一般应确定适用于整个评估工作的评估要求或规范,以适用于所有被评估单位。

由于检查评估是由被评估方的主管机关实施的,因此,其评估结果最具权威性,因为被检查单位自身不能对评估过程进行干预。

但是,检查评估也有如下限制:间隔时间较长,如一年一次,有时还是抽样进行;不能贯穿一个部门信息系统生命周期的全过程,很难对信息系统的整体风险状况做出完整的评价。

检查评估也可以委托风险评估服务技术支持方实施,但评估结果仅对检查评估的发起单位负责。由于检查评估代表了主管机关,涉及评估对象也往往较多,因此,要对实施检查评估机构的资质进行严格管理。

5.3 风险评估的过程

5.3.1 风险评估基本步骤

风险评估方法具有多样、灵活的特点。此外,对风险评估方法的选择又可依据组织的

特点进行，因此又具有一定的自主性。但无论如何，信息安全风险评估过程应包括以下基本操作步骤：第一步，风险评估准备，包括确定评估范围、组织评估小组；第二步，风险因素识别；第三步，风险确定；第四步，风险评价；第五步，风险控制。信息安全风险评估过程如图 5-2 所示。

为使风险评估更加有效，这一过程应该作为组织业务过程的一部分来看待。风险管理人员希望风险分析和评估过程能够对组织的业务目标起到积极的支持作用。需要强调的是，风险评估过程成功与否关键在其能否被组织所接受。一个有效的风险评估过程将发现组织的需求，并与组织的管理人员积极合作，共同达成组织目标。

为使风险评估能够成功进行，评估人员需要了解客户/企业管理者真正需要什么，并努力满足其需求。对一个信息安全从业人员来说，风险评估过程主要关注的是信息资源的机密性、可用性和完整性。

风险评估过程应根据组织机构的业务运作情况随时进行调整，许多时候企业的管理者都被告知需要增加一些安全控制措施，并且这些安全控制措施是审计的需要或者是安全的需要，而不是商业方面的要求。风险评估工作就是要在风险分析的基础上，帮助用户找到对业务运行有利的安全控制措施和对策。

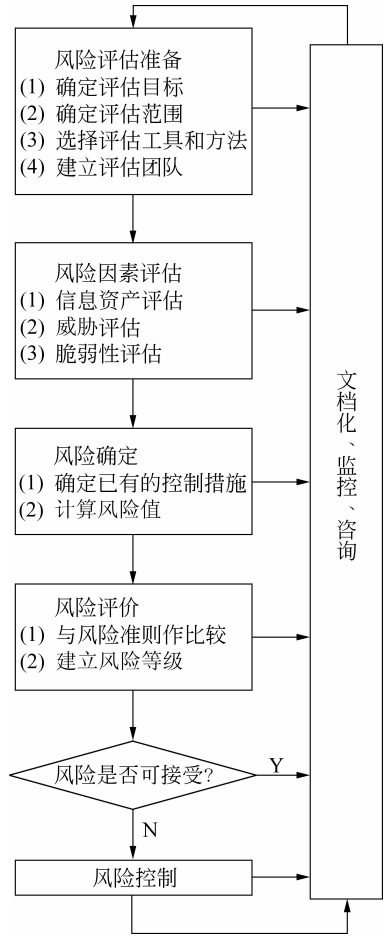

图 5-2　信息安全风险评估过程

5.3.2　风险评估准备

良好的风险评估准备工作是使整个风险评估过程高效完成的保证。计划实施风险评估是组织的一种战略性考虑，其结果将受到组织业务战略、业务流程、安全需求、系统规模和组成结构等方面的影响。因此，在实施风险评估之前，应做到以下几点。

（1）确定风险评估的目标。在风险评估准备阶段应明确风险评估的目标，为风险评估的过程提供导向。信息系统是企业的重要资产，其机密性、完整性和可用性对维持企业的竞争优势、获利能力、法规要求和企业形象等具有十分重要的意义。企业要面对日益增长的、来自内部和外部的安全威胁。风险评估目标须满足企业持续发展在安全方面的要求，满足相关方的要求，满足法律法规的要求等。

（2）风险评估的范围。基于风险评估目标确定风险评估范围是完成风险评估的又一个前提。风险评估范围可能是企业全部的信息以及与信息处理相关的各类资产、管理机构，也可能是某个独立的系统、关键业务流程、与客户知识产权相关的系统或部门等。

（3）选择与组织机构相适应的具体风险判断方法。在选择具体的风险判断方法时，应考虑到评估的目的、范围、时间、效果、人员素质等诸多因素，使之能够与组织环境和安

全要求相适应。

(4) 建立风险评估团队。组建适当的风险评估管理与实施团队,以支持整个过程的顺利推进。如成立由管理层、相关业务骨干、信息技术人员等组成的风险评估小组。风险评估团队应能够保证风险评估工作的高效开展。

(5) 获得最高管理者对风险评估工作的支持。风险评估过程应得到企业最高管理者的支持、批准,并对管理层和技术人员进行传达,应在组织内部对风险评估的相关内容进行培训,以明确相关人员在风险评估中的任务。

5.3.3 风险因素评估

1. 资产评估

信息资产的识别和赋值是指确定组织信息资产的范围,对信息资产进行识别、分类和分组等,并根据其安全特性进行赋值的过程。

信息资产识别和赋值可以确定评估的对象,是整个安全服务工作的基础。另外,本阶段还可以帮助客户实现信息资产识别和价值评定过程的标准化,确定一份完整的、最新的信息资产清单,这将为客户的信息资产管理工作提供极大帮助。

信息资产识别和赋值的首要步骤是识别信息资产,制定《信息资产列表》。信息资产按照性质和业务类型等可以分成若干资产类,如数据、软件、硬件、设备、服务和文档等。根据不同的项目目标与项目特点,重点识别的资产类别会有所不同,在通常的项目中一般以数据、软件和服务为重点。

资产赋值可以为机密性、完整性和可用性这三个安全特性分别赋予不同的价值等级,也可以用相对信息价值的货币来衡量。根据不同客户的行业特点、应用特性和安全目标,资产三个安全特性的价值会有所不同,如电信运营商更关注可用性,军事部门更关注机密性等。

《信息资产列表》将对项目范围内的所有相关信息资产做出明确的鉴别和分类,并将其作为风险评估工作后续阶段的基础与依据。

2. 威胁评估

威胁是指对组织的资产引起不期望事件而造成损害的潜在可能性。威胁可能源自对企业信息直接或间接的攻击,如非授权的泄露、篡改、删除等,从而使信息资产在机密性、完整性或可用性等方面造成损害;威胁也可能源自偶发或蓄意的事件。

一般来说,威胁只有利用企业、系统、应用或服务的弱点才有可能对资产成功实施破坏。威胁被定义为不期望发生的事件,这些事件会影响业务的正常运行,使企业不能顺利达成其最终目标。一些威胁是在已存在控制措施的情况下发生的,这些控制措施可能是没有正确配置或过了有效期的,因此为威胁进入操作环境提供了机会,这个过程就是我们通常所说的利用漏洞的过程。威胁评估是指列出每项抽样选取的信息资产面临的威胁,并对威胁发生的可能性进行赋值。威胁发生的可能性受以下两方面因素影响:①资产的吸引力和曝光程度、组织的知名度,这主要在考虑人为故意威胁时使用;②资产转化成利润的容易程度,包括财务的利益、黑客获得运算能力很强和带宽很大的主机的使用权等利益,这主要在考虑人为故意威胁时使用。