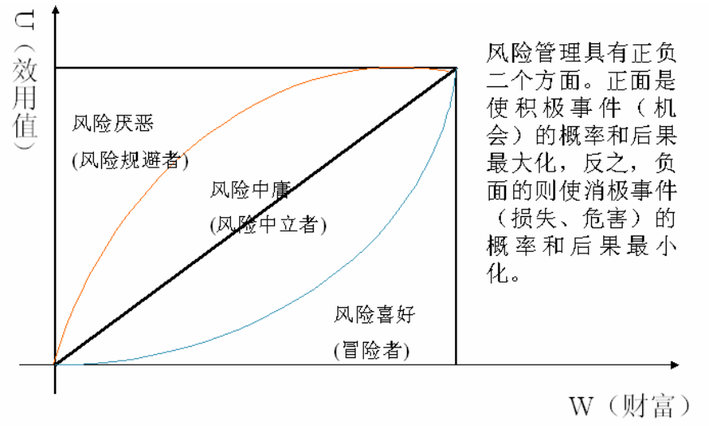
第 12 章　项目的风险管理

风险管理计划编制	风险识别	定性风险分析	定量风险分析	风险应对计划编制	风险监控
1、名称及定义 风险管理计划编制是决定如何采取和计划一个项目的风险管理活动的过程。风险管理的水平、类型和可见度不仅要与风险相称，也要与项目对组织的重要性相称.为了保证这一点，对随后进行的各种风险管理过程做好计划是非常重要. **2、输入** ①项目章程 ②项目范围说明书 ③组织范围说明书 ④项目管理计划 ⑤环境和组织因素 **3、工具和技术** 计划会：项目团队召开计划编制会议来制订风险管理计划。与会人员包括项目经理、项目团队的负责人、组织中任何对风险计划编制和应对措施负有管理责任的人员、关键的项目干系人，以及其他使用风险管理模板和其它适用的输入的必要人员。 **4、输出** 风险管理计划包括： ①方法论 ②角色和职责 ③预算 ④制订时间表 ⑤风险类别 ⑥风险概率和影响力的定义 ⑦概率及影响矩阵 ⑧已修订的项目干系人对风险的容忍度 ⑨报告的格式 ⑩跟踪	**1、名称及定义** 风险识别是确定何种风险可能会对项目产生影响，并将这些风险的特征形成文件。一般而言，风险识别的参与者尽可能地包括以下人员:项目团队、风险管理小组、来自公司其它部分的某一问题的专家、客户、最终用户、其他项目经理、项目干系人和外界的专家等。 风险识别是一个反复重复的作业过程。第一次反复可能是由项目团队的某一部分或由风险管理小组进行的。项目团队整体和主要项目干系人可能做第二次复查。为了取得一个不带偏见的客观分析，可能由没有参与项目的人员进行最终的复查。 风险识别的主要内容包括： ①识别并确定项目有哪些潜在风险；（风险识别的第一目标） ②识别引起这些风险的主要因素；（风险识别的第二目标） ③识别项目风险可能的后果。（风险识别的第三目标，采用定性分析） **2、输入** ①项目章程　；　②项目范围说明书；　③项目管理计划； ④组织过程资产；⑤环境及组织因素 **3、工具和技术** **①文件审核：**项目团队通常采取的第一个步骤是从项目整体和详细的范围层次两个方面对项目计划和假设、以前的项目文件及其它资料进行一次结构性的审核。 **②信息收集技术：**在风险识别中使用的信息收集技术，举例来说包括:头脑风暴法、德尔菲法、访谈和优/劣势/机会/威胁(SWOT)分析。 **③检查表：**从以往类似项目和某些其它信息来源中积累的历史信息和知识，可以用于编制风险识别检查表。使用检查表的一个优点是它使风险识别工作快而简单。它的不足之处在于我们不可能编制一个详尽的风险检查表，检查表的使用者可能会被表中的条目所局限。要注意发现那些在标准检查表中未列出的，而又似乎与某一特定项目相关联的风险。检查表应详细列出项目所有可能的风险类别。将审核检查表作为每一项目收尾程序中的一个正式步骤，来完善可能风险的清单和风险说明是非常重要的。 **④假设分析：**每一个项目都是从一系列假设、设想、推测中孕育和发展而来。假设分析是分析假设有效性的一种技术手段。它从不准确、不连贯、不完整的假设中识别项目的风险。 **5.图解技术：** ⊙因果分析图（鱼骨图）：用于确定风险的起因； ⊙系统或作业流程图：反映某一系统内部各要素之间是如何互相联系的，并反映发生因果关系的机制。 ⊙影响图：一种用图解表示问题的方法，反映变量和结果之间因果关系的相互作用、事件的时间顺序及其他关系。 **4、输出** ①风险记录 风险记录的最初条目是由风险识别的输出构成的，最终则包括风险分析的结果、优先级。 其信息包括：⊙已识别的风险列表； ⊙风险的征兆或警告信号； ⊙潜在风险应对方法列表； ⊙风险根本原因； ⊙更新的风险分类 ②项目管理计划（更新）	**1、名称及定义** 风险定性分析包括对识别风险进行优先级排序。风险定性分析通过风险的发生概率及影响程度的综合评估来确定其优先级的。 风险定性分析是建立风险响应计划优先级的快速有效的方法，为定量分析奠定基础。 **2、输入** ①项目管理计划 （包括风险管理计划、风险记录） ②组织过程资产 ③工作绩效信息 ④项目范围说明 **3、工具和技术** ①风险概率及影响评估 ②概率-影响矩阵 利用概率-影响矩阵对风险的重要性及优先级进行评估。 镜像双矩阵将会决定威胁与机会的优先权。 ③风险数据质量评估 风险数据质量包括检验风险理解度、风险数据的精确度、质量、可信度和完整性 ④风险种类 ⑤风险紧急度评估 **4、输出** ①风险记录 更新的风险记录包含在项目计划中，包括： ⊙按优先级（或相对等级）排列的项目风险； ⊙按种类的风险分组； （发现风险的集中性可以提高风险响应的有效性） ⊙需要近期作出响应的风险列表； ⊙需要进一步分析和应对的风险列表； ⊙低优先级风险监视表； （在风险定性分析过程中不重要的风险将被放在监视列表中以备继续监视） ⊙风险定性分析趋势。	**1、名称及定义** 测量风险出现的概率和结果，并评估它们对项目目标的影响。 这一过程通过蒙特卡罗模拟和决策树等技术进行分析： ①量化项目的输出及可能性； ②评估达到特定的项目目的的可能性； ③通过量化每个风险相对项目总体风险的贡献来识别最需要关注的风险； ④按照项目风险情况，制定切实可行的防算、进度安排或范围目标； ⑤在一些情况或结果尚不确定的情况下，作出最有利的项目管理决策。 **2、输入** ①项目管理计划 ②组织过程资产 ③风险记录 **3、工具和技术** 1. 数据收集和表示技术 ①访谈 ②概率分布 ③专家判断 2. 定量风险分析和建模技术 ①灵敏度分析 ②期望货币价值分析（EMV） ③决策树分析 ④建模和仿真 **4、输出** ①更新的风险记录 ②项目可能性分析 ③实现成本和进度目标的可能性 ④已量化风险优选级列表 ⑤定量风险分析结果中的趋势	**1、名称及定义** 开发制定一些程序和技术手段，用来提高实现项目目标的机会和减少风险对实现项目目标的威胁。 **2、输入** ①风险管理计划； ②风险记录 **3、工具和技术** 1、负面风险（威胁）的应对策略 ①规避：风险规避就是通过变更项目计划，从而消除风险或产生风险的条件，或者保护项目目标免受风险的影响。 ②转移：风险转移是设法将某风险的结果连同对风险进行应对的权利转移给第三方。转移风险只是将管理风险的责任转移给另一方。它不能消除风险。 ③减轻：减轻是设法将某一负面风险事件的概率和/或其影响降低到一种可以承受的限度。 2、正面风险（威胁）的应对策略 ①开拓　②分享　③强大 接受：意味着项目队伍决定以不变的项目计划去应对某一风险，或项目队伍不能找到其它合适的风险应对策略。该策略可分为主动或被动方式。最常见的主动接受风险的方式就是建立应急储备，应对已知或潜在的未知威胁或机会。被动地接受风险则不要求采取任何行动，将其留给项目团队，待风险发生时相机处理。 3、同时适用威胁和机会的应对策略 **4、输出** ①风险记录（更新） ⊙已识别的风险及其描述，受影响的项目领域、风险成因以及如何影响项目目标； ⊙风险责任人及其职责； ⊙定性、定量的分析过程的结果； ⊙一致认同的应对策略 ⊙应对策略所需的具体行动 ⊙应对策略执行后的残留风险水平 ⊙风险发生时的预警和信号 ⊙执行风险应对策略的预算和时间 ⊙启动应急计划的触发条件； ⊙风险发生的回退计划 ⊙二级风险，即执行应对措施而引发的新风险； ⊙需要的应急储备量 ②风险相关的合同协议	**1、名称及定义** 在项目的整个生命期内，监视残余风险，识别新的风险，执行降低风险计划，以及评价这些工作的有效性。 **2、输入** ①项目管理计划 ②工作绩效信息 ③批准的变更请求 **3、工具和技术** ①风险评估 ②风险审计和定期的风险评审 ③差异和趋势分析 ④技术绩效评估 ⑤预留管理 **4、输出** ①建议的纠正措施 ②变更申请 ③风险记录（更新） ④组织过程资产（更新）

1、风险的属性

随机性、相对性、可变性

2、面对风险的主观承受能力



风险管理具有正负二个方面。正面是使积极事件（机会）的概率和后果最大化，反之，负面的则使消极事件（损失、危害）的概率和后果最小化。

3、风险的分类

⑴按风险后果划分

- 纯粹风险：不能带来机会，无获得利益可能的风险。（造成的损失是绝对损失，总是和威胁、损失、不幸相联系）
  - 造成损失
  - 不造成损失
- 投机风险：既可能带来机会，获得利益，又隐含威胁，造成损失的风险。
  - 造成损失
  - 不造成损失
  - 获得利益

纯粹风险和投机风险在一定条件下可以相互转化。项目管理人员应避免投机风险转化为纯粹风险。

⑵按风险来源划分
- 自然风险
- 人为风险

⑶按风险是否可管理划分
- 可管理风险（风险可否管理，取决于风险不确定性是否可以消除）
- 不可管理风险

⑷按风险影响范围划分
- 局部风险
- 总体风险

⑸按风险后果的承担者划分：业主风险、政府风险、承包商风险等

⑹按风险的可预测性划分
- 已知风险：能明确其经常发生的，一般已知风险发生概率高，但后果转向轻微，不严重。
- 可预测风险：可以预测其发生，但不能预见后果。
- 不可测风险：不可预测其发生

3、风险的成本

- 风险损失的有形成本：直接成本、间接成本
- 风险损失的无形成本：风险损失减少机会、风险阻碍生产率的提高、风险造成资源分配不当
- 风险预防与控制费用
- 风险成本的负担

4、风险管理与项目管理其他过程的关系

①从项目的成本、时间和质量目标来看，风险管理把各种风险造成不良后果减到最低程度，符合各方对时间与质量方面的要求；
②风险管理通过风险分析，对项目范围的不确定性进行识别、估计和评价，向项目范围管理提出任务；
③从项目管理计划职能来看，风险管理为项目计划的制订提出依据，为项目计划的准确性和可行性提供帮助；
④从项目成本职能来看，风险管理难过风险分析指出相关意外费用，为应急费用提供依据，增强成本预算的准确性和现实性，避免项目超支；
⑤风险管理在风险分析基础上，拟定风险应对措施，并对风险实行有效控制；
⑥项目风险管理通过风险分析，指出哪些风险同人有关，项目团队成员身心状态会影响项目的实施。

5、完善的风险分析对项目的最大裨益

①通过风险分析，加深对项目风险认识与理解，澄清各方面利弊，了解风险对项目的影响，从而减少风险；
②通过各种信息、数据和资料，明确项目相关的前提和假设；
③提高各种计划的可信度，改善项目组的内部和外部沟通；
④编制应急计划更有针对性；
⑤将风险后果的各种处理方式更灵活地组合起来，在项目管理中减少被动局面；
⑥充分利用机会，把握机会
⑦为日后工作提供反馈，防止和避免风险损失
⑧为制定应急计划提供依据；
⑨为决策提供依据，减少风险，保证项目目标的实现；
⑩可积累有关风险资料和数据，以便改进将来的项目管理。

6、项目风险产生的来源

产品定位——与要建造或要修改的软件的总体规划相关的风险。
商业影响——与管理或市场所加诸的约束相关的风险。
客户特性——与客户的素质以及开发者和客户定期通信的能力相关的风险。
开发体系——与软件过程被定义的程度以及它们被开发组织所遵守的程度相关的风险。
开发环境——与用以建造产品的工具的可用性及质量相关的风险。
开发技术——与待开发软件的复杂性以及系统所包含技术的“新奇性”相关的风险。
团队状况——与参与工作的开发人员的总体素质及项目经验相关的风险。
（希赛认为的主要风险来源：需求风险、技术风险、团队风险、关键人员风险、预算风险、范围风险）

7、硬件集成项目风险产生的原因

1、产品的日趋复杂性；
2、依赖多个厂家的支持和技术来源
3、采用产品组合和功能交叉的方法；
4、项目管理与企业战略的紧密结合
5、产品更新周期的缩短；
6、满足顾客需求
7、市场的激烈竞争；
8、参与者的利益不同
9、多方面专业技术的集成；
10、依赖更复杂的工具

8、主要软件项目的风险

1、 项目规模风险 ； 2. 需求风险 ；3. 外部因素风险；4. 内部管理风险 ；5. 技术风险

9、软件项目风险产生的原因

1、产品定位错误（包括市场定位）；
2. 人员流动；
3. 项目管理失败
4. 开发目标不明确或摇摆不定
5. 开发计划执行受到严重影响；
6. 技术方案有缺陷
7. 项目经费超支或不足
8. 开发环境及过程管理混乱
9. 产品质量低劣
10. 需求发生变化

10、软件项目经常遇到的 15 种可预料的（包括已知的）风险及其预防措施

（1）合同风险

预防这种风险的办法是项目建设之初项目经理就需要全面准确地了解合同各条款的内容、尽早和合同各方就模糊或不明确的条款签订补充协议。

（2）需求变更风险

预防这种风险的办法是项目建设之初就和用户书面约定好需求变更控制流程、记录并归档用户的需求变更申请。

（3）沟通不良风险

预防这种风险的办法是项目建设之初就和项目各干系方约定好沟通的渠道和方式、项目建设过程中多和项目各干系方交流和沟通、注意培养和锻炼自身的沟通技巧。

（4）缺乏领导支持风险

预防这种风险的办法是主动争取领导对项目的重视、确保和领导的沟通渠道畅通、经常向领导汇报工作进展。

（5）进度风险

预防这种风险的办法是分阶段交付产品、增加项目监控的频度和力度、多运用可行的办法保证工作质量避免返工。

（6）质量风险

预防这种风险的办法一般是经常和用户交流工作成果、采用符合要求的开发流程、认真组织对产出物的检查和评审、计划和组织严格的独立测试等。

（7）系统性能风险

预防这种风险的办法一般是在进行项目开发之前先设计和搭建出系统的基础架构并进行性能测试，确保架构符合性能指标后再进行后续工作。

（8）工具风险

预防这种风险的办法一般是在项目的启动阶段就落实好各项工具的来源或可能的替代工具，在这些工具需要使用之前（一般需要提前一个月左右）跟踪并落实工具的到位事宜。

（9）技术风险

预防这种风险的办法是选用项目所必须的技术、在技术应用之前，针对相关人员开展好技术培训工作。

（10）团队成员能力和素质风险

预防这种风险的办法是在用人之前先选对人、开展有针对性的培训、将合适的人安排到合适的岗位上。

（11）团队成员协作风险

预防这种风险的办法是项目在建设之初项目经理就需要将项目目标、工作任务等和项目成员沟通清楚，采用公平、公正、公开的绩效考评制度，倡导团结互助的工作风尚等。

（12）人员流动风险

预防这种风险的办法是尽可能将项目的核心工作分派给多人（而不要集中在个别人身上）、加强同类型人才的培养和储备。

（13）工作环境风险

预防这种风险的办法是在项目建设之前就选择和建设好适合项目特点和满足项目成员期望的办公环境、在项目的建设过程中不断培育和调整出和谐的人文环境。

（14）系统运行环境风险

预防这种风险的办法是和用户签定相关的协议、跟进系统集成部分的实施进度、及时提醒用户等。

（15）分包商风险

预防这种风险的办法一般是指定分包经理全程监控分包商活动、让分包商采用经认可的开发流程、督促分包商及时提交和汇报工作成果、及时审计分包商工作成果等。

11、项目管理中蒙特卡罗模拟方法的一般步骤是：

蒙特卡罗模拟是一种有效的统计实验计算，蒙特卡罗方法需要大量的实验。实验次数越多，所得到的结果才越精确。蒙特卡罗方法实现了两大优点：一是简单，省却了繁复的数学报导和演算过程，使得一般人也能够理解和掌握；二是快速。简单和快速，是蒙特卡罗方法在现代项目管理中获得应用的技术基础。

⑴对每一项活动，输入最小、最大和最可能估计数据，并为其选择一种合适的先验分布模型。

⑵计算机根据上述输入，利用给定的某种规则，快速实施充分大量的随机抽样。

⑶对随机抽样的数据进行必要的数学计算，求出结果。

⑷对求出的结果进行统计学处理，求出最小值，最大值及数学期望值和单位标准偏差

⑸根据求出的统计学处理数据，让计算机自动生成概率分布曲线和累积概率曲线（通常是基于正态分布的概率累积 S 曲线

⑹依据累积概率曲线进行项目风险分析

12、怎样做好软件项目风险计划

风险计划的要素有：

⑴风险描述 对于风险情况的介绍。

⑵可能性 风险发生的可能性。风险不是必然要发生的，如果一个对项目存在危害的事件是必然要发生的，那这个事件就不能作为风险。对于风险可能性的标识有助于对那些高可能性的风险投入更大的关注。

⑶严重性 风险如果发生对于项目的危害程度。

⑷危害值 一个综合考虑可能性和严重型后对风险的一个评估，这个评估反应了风险应该被关注的程度。

⑸对策 对策分为两个部分：一是对于采取预防措施以阻止风险的发生，另一方面也要考虑如果风险发生后需要采取什么措施。这两方面的计划构成了完整的风险对策。

⑹触发标志 风险是一种可能性，并且制定风险主要的出发点是预防它，但也要考虑到风险发生后情况。对于风险发生后的应对策略，需要争取一定的提前时间以启动必要的各项工作，设立触发标志是为设立一个判别标识，在该触发标志所标明的条件具备时，说明风险已经越来越可能成为现实了。

⑺风险责任人 风险预防和跟踪需要有人的参与，在风险计划中责任明确是一个重要的原则，对每一个列入了视线的风险都要指定对风险预防和跟踪负责的人员。

13、风险管理可以分为四个步骤：识别风险、衡量风险、管理风险、监控项目进程与状态。

（1）风险识别：风险识别包括确定风险的来源，风险产生的条件，描述其风险特征和确定哪些风险事件有可能影响本项目。风险识别不是一次就可以完成的事，应当在项目的自始至终定期进行。

（2）风险量化：涉及对风险及风险的相互作用的评估，是衡量风险概率和风险对项目目标影响程度的过程。风险量化的基本内容是确定那些事件需要制定应对措施。。

（3）风险应对计划制定：针对风险量化的结果，为降低项目风险的负面效应制定风险应对策略和技术手段的过程。风险应对计划依据风险管理计划、风险排序、风险认知等依据，得出风险应对计划、剩余风险、次要风险以及为其它过程提供得依据。

（4）风险监控：涉及整个项目管理过程中的风险进行应对。该过程的输出包括应对风险的纠正措施以及风险管理计划的更新。

每个步骤所使用的工具和方法详见表 1：

风险管理步骤	所使用的工具、方法
风险识别	头脑风暴法、面谈、Delphi法、核对表、SWOT技术
风险量化	风险因子计算、PERT估计、决策树分析、风险模拟
风险应对计划制定	回避、转移、缓和、接受
风险监控	核对表、定期项目评估、挣值分析

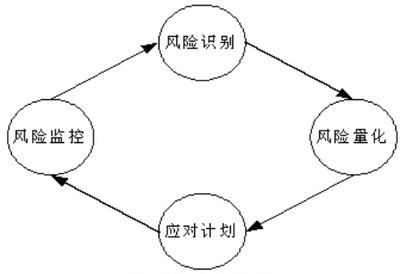


图1 项目风险管理过程

信息系统安全风险评估

一、安全威胁的分类

风险类型	
1、自然事件风险	
2、人为事件风险	⑴意外的人为事件风险　　⑵有意的人为事件威胁
3、软件系统风险	⑴兼容风险；⑵维护风险；⑶使用风险
4、软件过程风险	⑴软件需求分析阶段的风险；　⑵设计阶段的风险； ⑶实施阶段的风险；　　⑷维护阶段的风险
5、项目管理风险	⑴应用软件产品的不可预见性；　⑵软件的生产过程不存在绝对正确； ⑶信息系统应用项目的独特性；
6、应用风险	⑴安全必；⑵未授权访问和改变数据；⑶未授权的远程访问； ⑷不精确的信息；⑸错误或虚假的信息输入；⑹授权的终瑞用户滥用；⑺不完整的处理；⑻重复数据管理；⑼不及时管理；⑽通信系统失败；⑾不充分的测试；⑿不充分的培训；⒀不充分的支持；⒁不充分的文档
7、用户使用风险	⑴不充分的使用资源；⑵不兼容的系统；⑶冗余系统；⑷无效的应用； ⑸职责不分明；⑹用户开发可能会对开发阶段的分析不全面； ⑺非授权访问数据与程序；⑻侵犯版权；⑼病毒破坏信息

二、项目管理的职责划分

参与者	职责
项目经理	把握全局，侧重于项目的商务方面，负责项目组与客户的正式交流；
项目负责人	制定项目开发计划和策略，参与项目核心系统的分析设计；并保证开发计划的按时按质完成；保证开发策略的贯彻实施；
行业专家	在软件分析阶段，帮助分析人员界定系统实现边界和实现功能，对特定检测点进行算法审核，同时对测试策略和软件操作界面提出参考意见。
质量监督组	⊙编制软件质量控制计划，并负责落实； ⊙控制必要文档的生成，通过文档，监督项目实施过程中的软件的质量；并提供软件进行报告，提请项目经理和项目负责人审阅； ⊙对于项目中出现的质量问题，主持召开质量复审会议。
系统分析员	⊙协同项目负责人进行系统分析和设计工作； ⊙编写软件需求分析和系统设计相关文档； ⊙在软件实现阶段，进行测试策略的编制和性能测试和指导；
程序员	⊙协助分析员进行详细设计，负责软件系统的代码实现； ⊙进行适当的白盒测试
测试员	⊙对软件组件，构件或系统进行正确性验证测试，进行系统性能测试等； ⊙书写测试报告和测试统计报告，并提请质量监督组复审查；
技术支持	⊙协同系统分析员听取用户需求，对需求分析进行参考性复审。 ⊙协同测试人员进行测试 ⊙书写操作手册和在线帮助； ⊙在项目交付后进行跟踪服务
文档组	⊙对各部门产生的文档进行格式规范、版本编号和控制、存档文件的检索； ⊙协助质量监督组进行软件质量监督； ⊙通过适当的人员配备和职责划分，有效降低软件开发的失控的可能性。 ⊙设法降低对软件对某些关键人员的依赖性；

三、信息安全与安全风险关系示意图