风险管理

中国软件评测中心
北京賽迪国软认证有限公司

风险的定义

风险：一种不确定的事件或条件，如果它发生，将会对项目目标造成正面或负面的影响

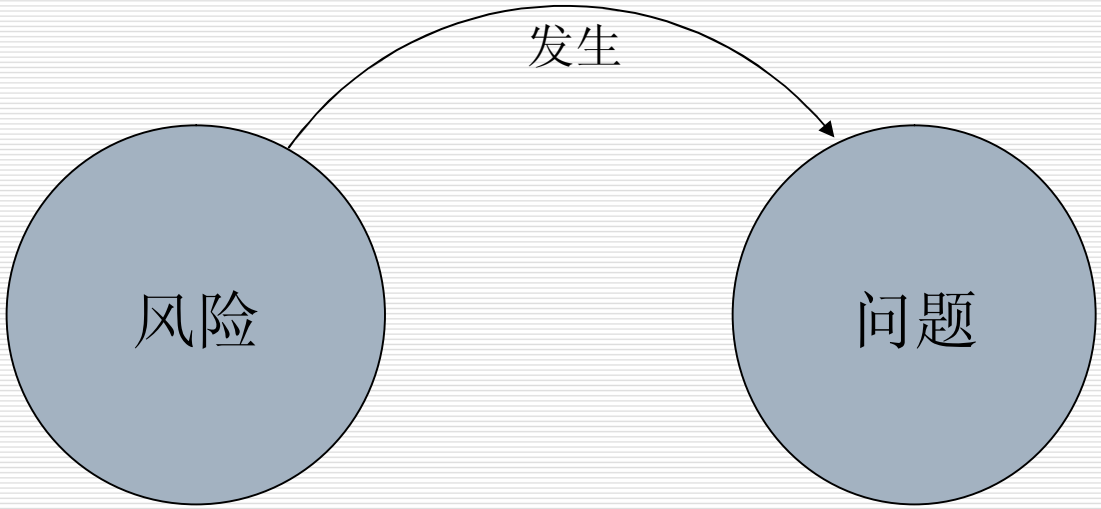
风险有以下属性：

一个事件

发生概率

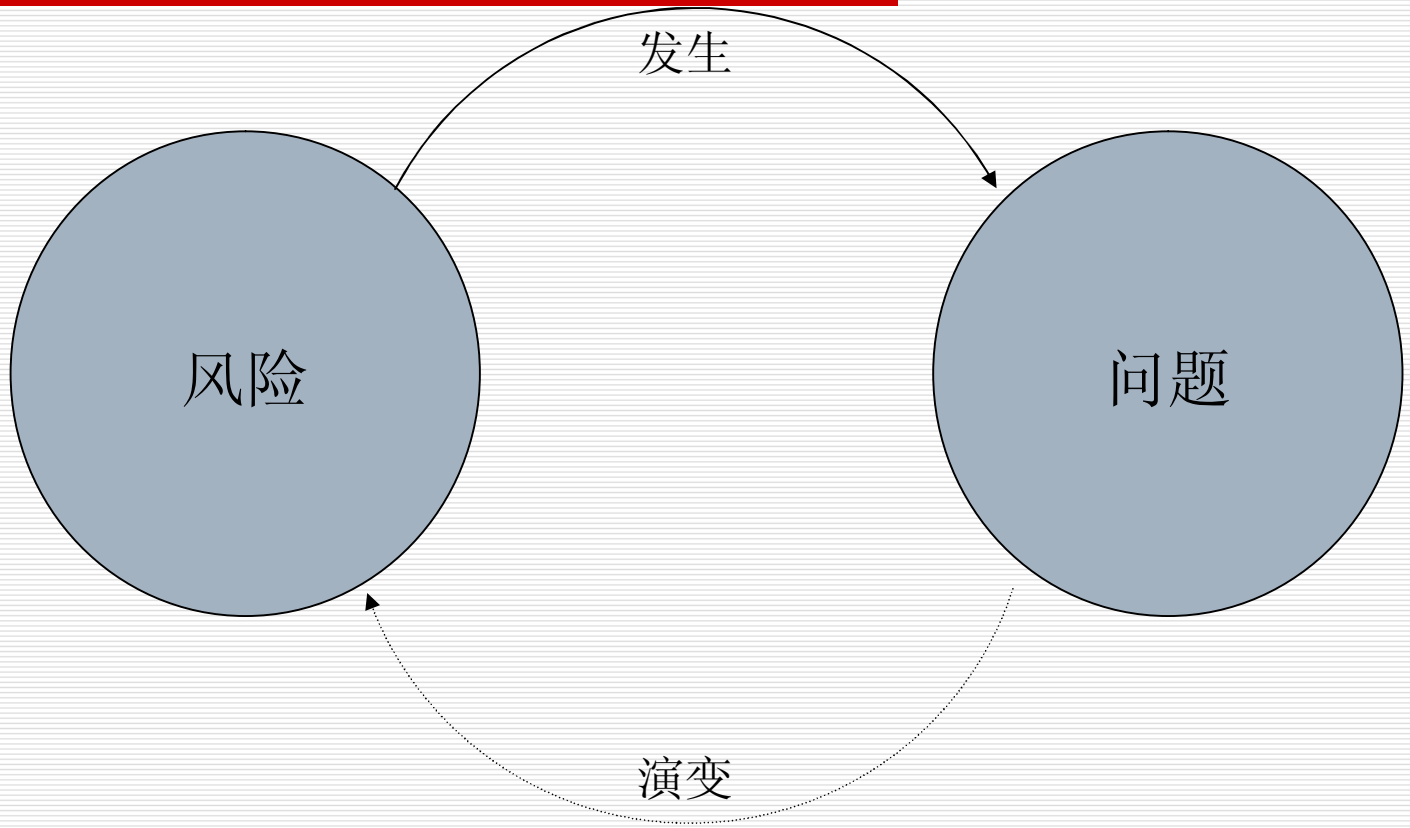
造成影响

风险与问题的关系



风险与问题

风险与问题的演变



风险与问题的演变

风险来源

- 外部
  - 法律
  - 法规
  - 环境
  - 政府
- 内部
  - 进度
  - 成本
  - 范围变更
  - 糟糕的计划
  - 没有经验的项目经理
  - ……

风险分类

分类角度	分类	说明
风险后果	纯粹风险	不能带来机会、无获得利益可能。只有2种可能后果：造成损失和不造成损失，这种损失是全社会的损失，没有人从中获得好处。
	投机风险	既可能带来机会、获得利益，又隐含威胁、造成损失。有3种可能后果：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，项目经理必须避免投机风险转化为纯粹风险。	
风险来源	自然风险	由于自然力的作用，造成财产损毁或人员伤亡的风险。
	人为风险	由于人的活动而带来的风险，可细分为行为、经济、技术、政治和组织风险。
可管理	可管理风险	可以预测，并可采取相应措施加以控制的风险。
	不可管理风险	不可预测的风险。
影响范围	局部风险	影响的范围小
	总体风险	影响的范围大。
	局部风险和总体风险是相对而言的，项目经理要特别注意总体风险。	
可预测性	已知风险	能够明确的，后果也可预见的风险。发生的概率高，但后果轻微。
	可预测风险	根据经验可以预见其发生，但其后果不可预见。后果有可能相当严重。
	不可预测风险	不能预见的风险，也称为未知风险、未识别的风险。一般是外部因素作用的结果。

风险的征兆

- 早期告警迹象 – 应该得到确认和监测
- 触发事件（**Trigger**） – 可以造成风险成真的事件 (将触发按照风险管理计划采取应对行动)

对待风险的态度

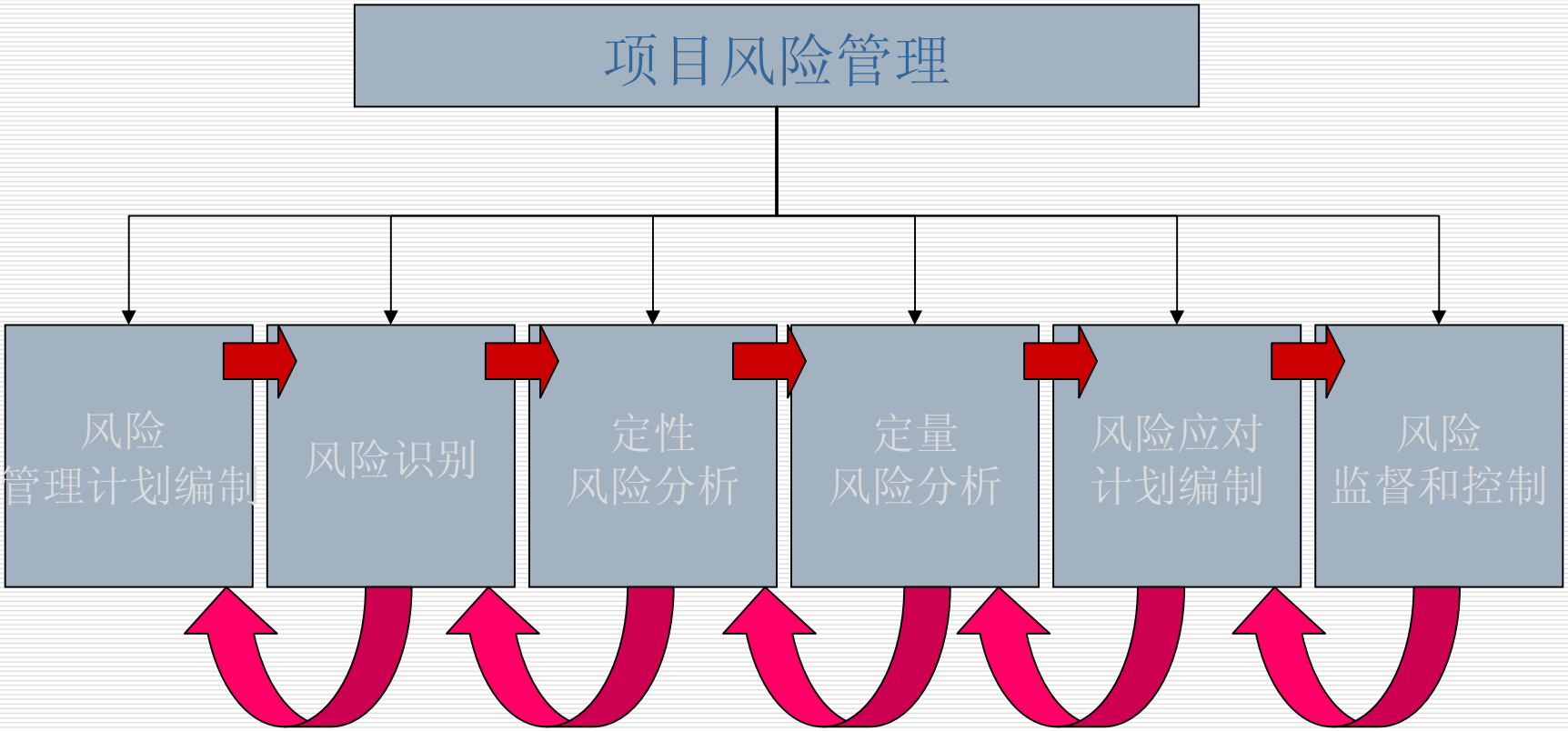
- 一种是被动态度，可比作救火模式
- 另一种是主动态度，可比作防火模式
- 风险管理属于防火模式，目的是在风险产生危害之前识别它们，从而有计划地消除或削弱风险。

风险管理

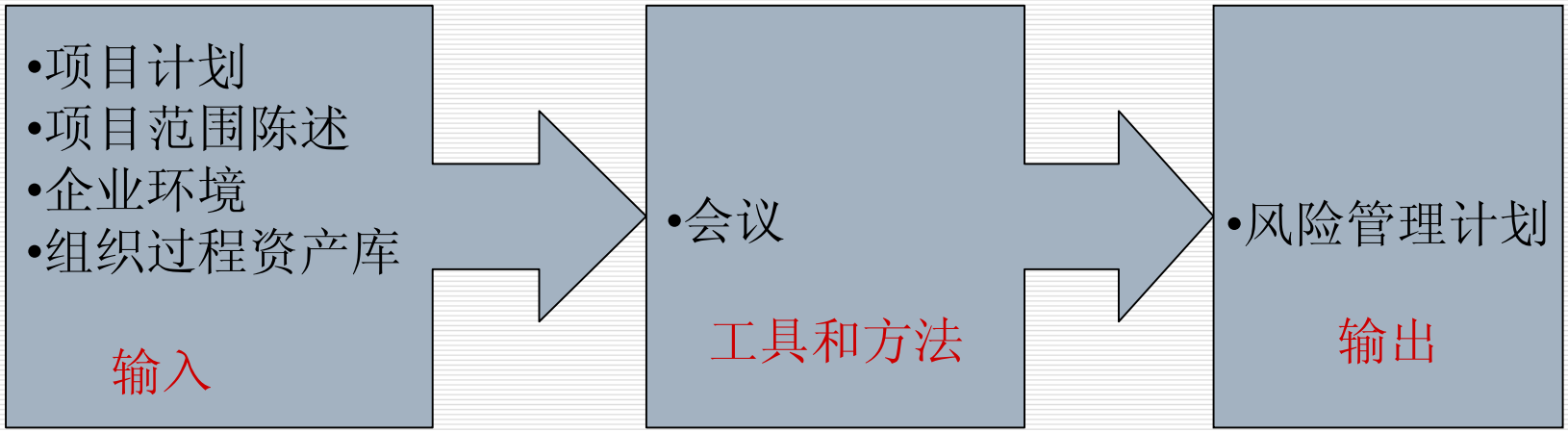
风险管理：

一种对项目风险进行识别、分析、应对的系统过程。它包括鼓励对项目目标有正面影响的风险发生并加强其影响、减小对项目目标有负面影响的风险发生并减弱其影响。

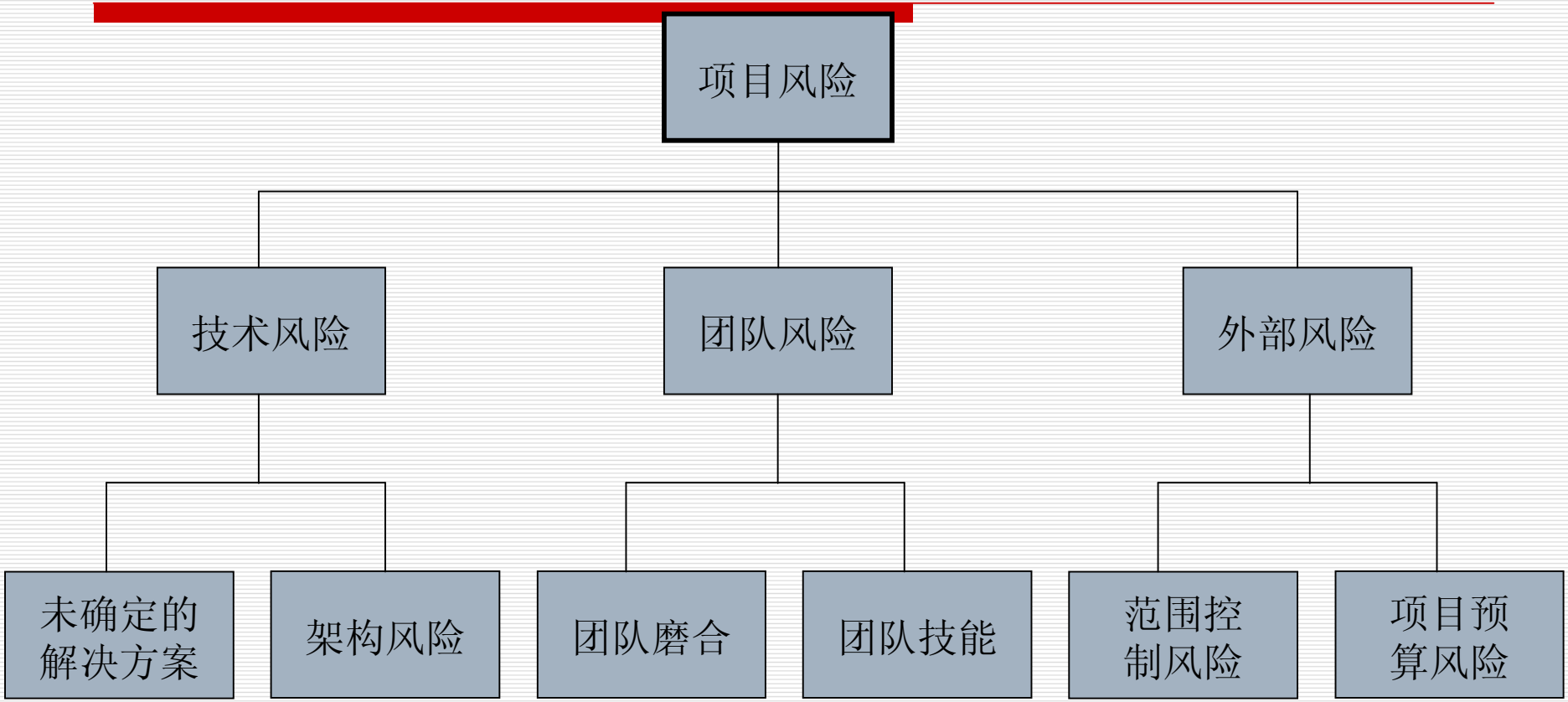
风险管理过程



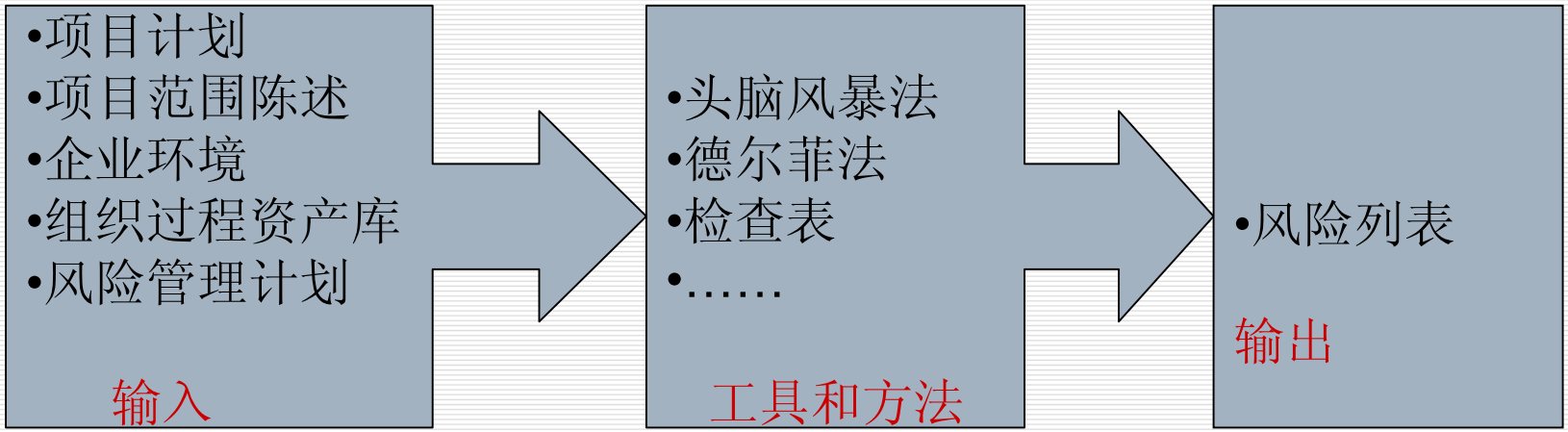
制定风险管理计划的过程



RBS的风险分解结构



风险识别


•项目计划
•项目范围陈述
•企业环境
•组织过程资产库
•风险管理计划
输入
•头脑风暴法
•德尔菲法
•检查表
•……
工具和方法
•风险列表
输出

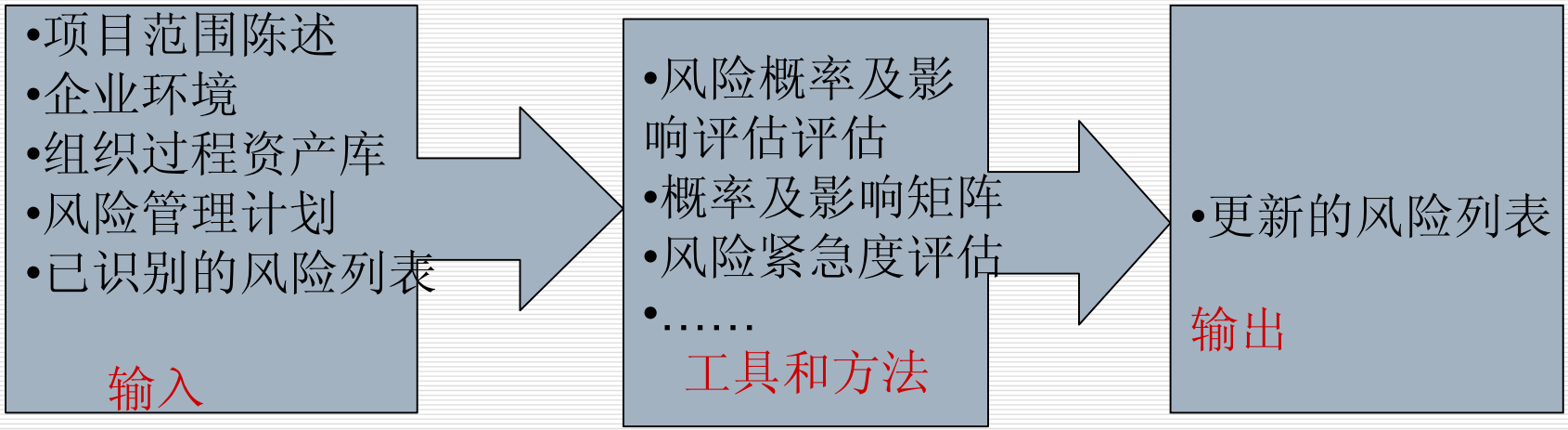
风险识别

- 参与风险识别的人员
  - 项目团队成员
  - 风险管理团队成员
  - 客户
  - 最终用户
  - 项目干系人
  - 其他项目经理
  - 专家

何时识别风险？

- 在项目开始时就进行风险识别，并且在每一个阶段，特别是在每个阶段的开始进行风险识别
- 反复执行的（Iterative）

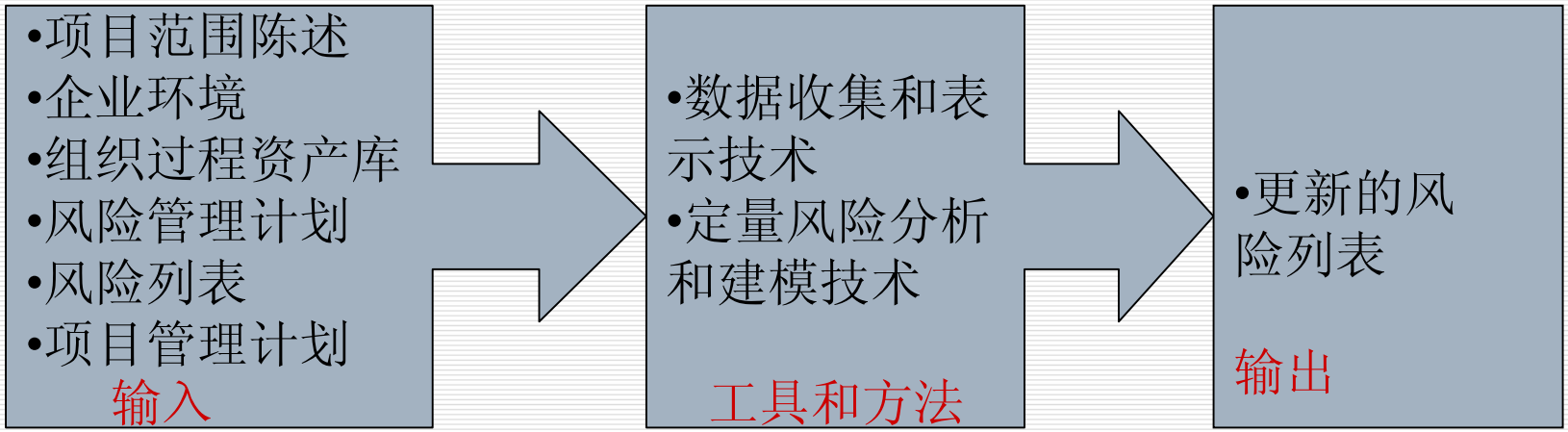
风险定性分析


•项目范围陈述
•企业环境
•组织过程资产库
•风险管理计划
•已识别的风险列表
输入
•风险概率及影响评估评估
•概率及影响矩阵
•风险紧急度评估
•……
工具和方法
•更新的风险列表
输出

风险优先级矩阵

影响 / 可能性	很大	较大	中	较低	很低
很高					
较高					
中					
较低					
很抵					

风险定量分析


•项目范围陈述
•企业环境
•组织过程资产库
•风险管理计划
•风险列表
•项目管理计划
输入
•数据收集和表示技术
•定量风险分析和建模技术
工具和方法
•更新的风险列表
输出

定量风险分析

- 这个过程不总是必要的
  - 太小的项目
  - 不可能做分析 – 项目缺乏明确的定义
  - 不可能做分析 – 项目太不寻常
  - 不可能做分析 – 项目太紧急
- 如果可能，我们可以使用
  - 决策分析
  - 模拟

风险影响的评估

评估风险对项目的主要目标的影响大小

对以下项目目标的影响	发生的概率				
	非常低	低	中等	高	非常高
	0.05	**0.1**	**0.2**	**0.4**	**0.8**
成本	成本略有提高，但不重要	<5%的增长	5-10%的增长	10-20% 的增长	>20% 的增长
进度	进度略有滞后，但不重要	<5%的滞后	5-10% 的滞后	10-20% 的滞后	>20% 的滞后
范围	范围略有缩小，但很难察觉	范围中次要部分收到影响	范围中主要部分收到影响	客户不可接受的范围缩减	项目结束时，项目成果毫无用处
质量	质量略有下降，但很难察觉	只有要求过分的应用收到影响	质量下降影响到客户是否接受	客户不可接受的质量下降	项目结束时，项目成果毫无用处

影响/概率 矩阵风险值

一个具体风险的风险值					
概率	风险值 = 概率（P） X影响（ I）				
0.9	0.05	0.09	0.18	0.36	0.72
0.7	0.04	0.07	0.14	0.28	0.56
0.5	0.03	0.05	0.10	0.20	0.40
0.3	0.02	0.03	0.06	0.12	0.24
0.1	0.01	0.01	0.02	0.04	0.08
	0.05	**0.1**	**0.2**	**0.4**	**0.8**
	非常低	低	中	高	很高
	对某一项目目标（如成本、时间、范围）的影响				

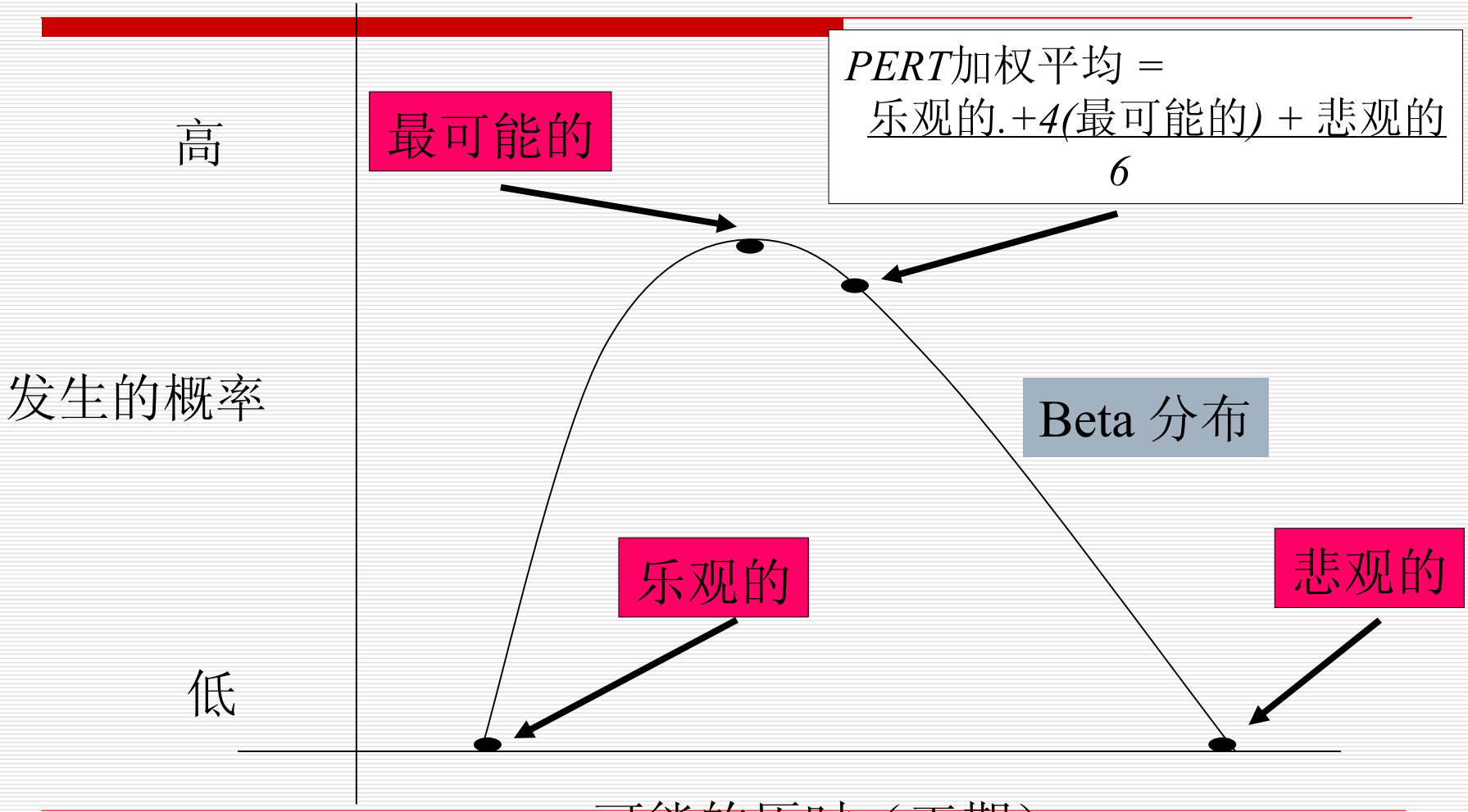
PERT

- 一种很好的风险管理技术，对每一个认为都考虑它在时间和成本上的数值范围 – 乐观的,悲观的 和最可能的
- 接下来使用PERT公式 (假设以正态分布，或者叫Beta分布)计算结果的期望值

$$\frac{\text{乐观的} + 4*\text{最可能的} + \text{悲观的}}{6}$$

- 在95%的情况下不会超出这个期望值。

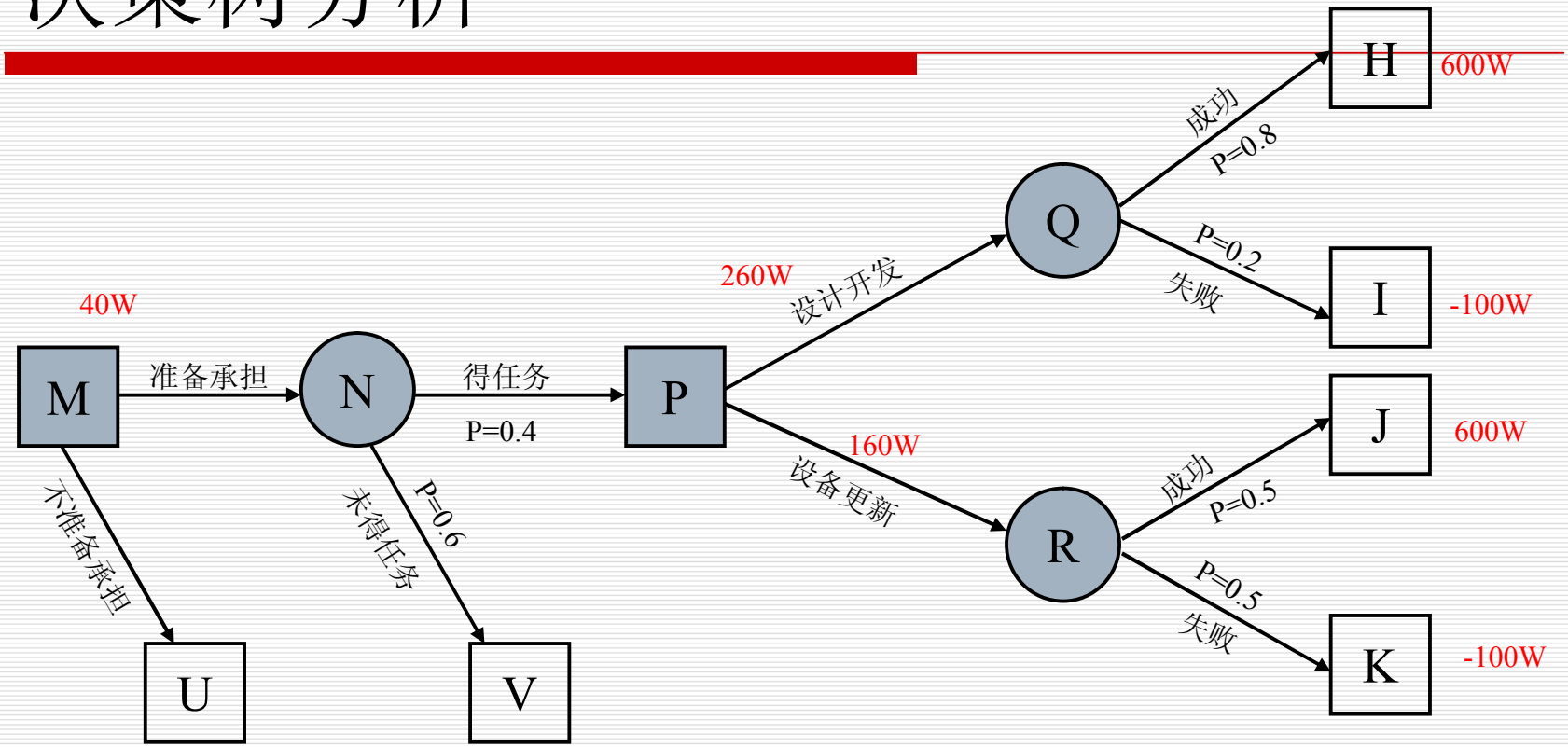
PERT –活动历时


PERT加权平均 =
乐观的.+4(最可能的) + 悲观的
6
最可能的
高
发生的概率
Beta 分布
乐观的
悲观的
低
可能的历时（工期）

PERT举例

估计 / 工作包	乐观	中性	悲观
需求	3周	4周	6周
设计	4周	6周	7周
开发	10周	15周	17周
合计	17周	25周	30周

决策树分析



Q点=(600-260-40)*0.8+(-100-260-40)*0.2=160

R点=(600-160-40)*0.5+(-100-160-40)*0.5=50

N点=160*0.4+(-40)*0.6=40

灵敏度分析

- 敏感性分析是指从众多不确定性因素中找出对投资项目经济效益指标有重要影响的敏感性因素，并分析、测算其对项目经济效益指标的影响程度和敏感性程度，进而判断项目承受风险能力的一种不确定性分析方法。

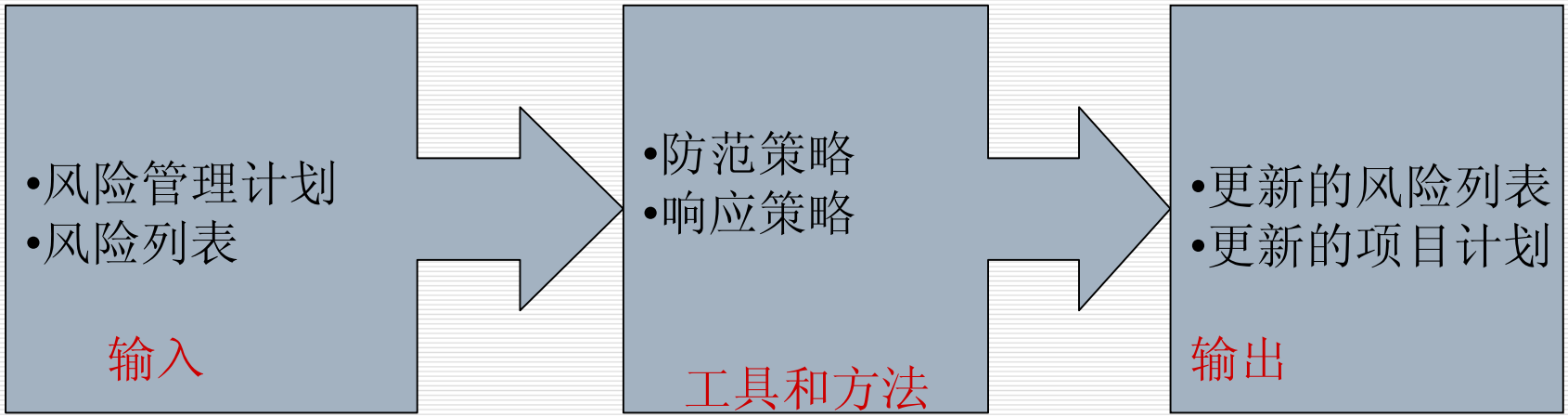
蒙特卡罗（ Monte Carlo）仿真法

- 基本思想
  - 是人为地造出一种概率模型，使它的某些参数恰好重合于所需计算的量
  - 然后再通过实验，用统计方法求出这些参数的估值
  - 把这些估值作为要求的量的近似值

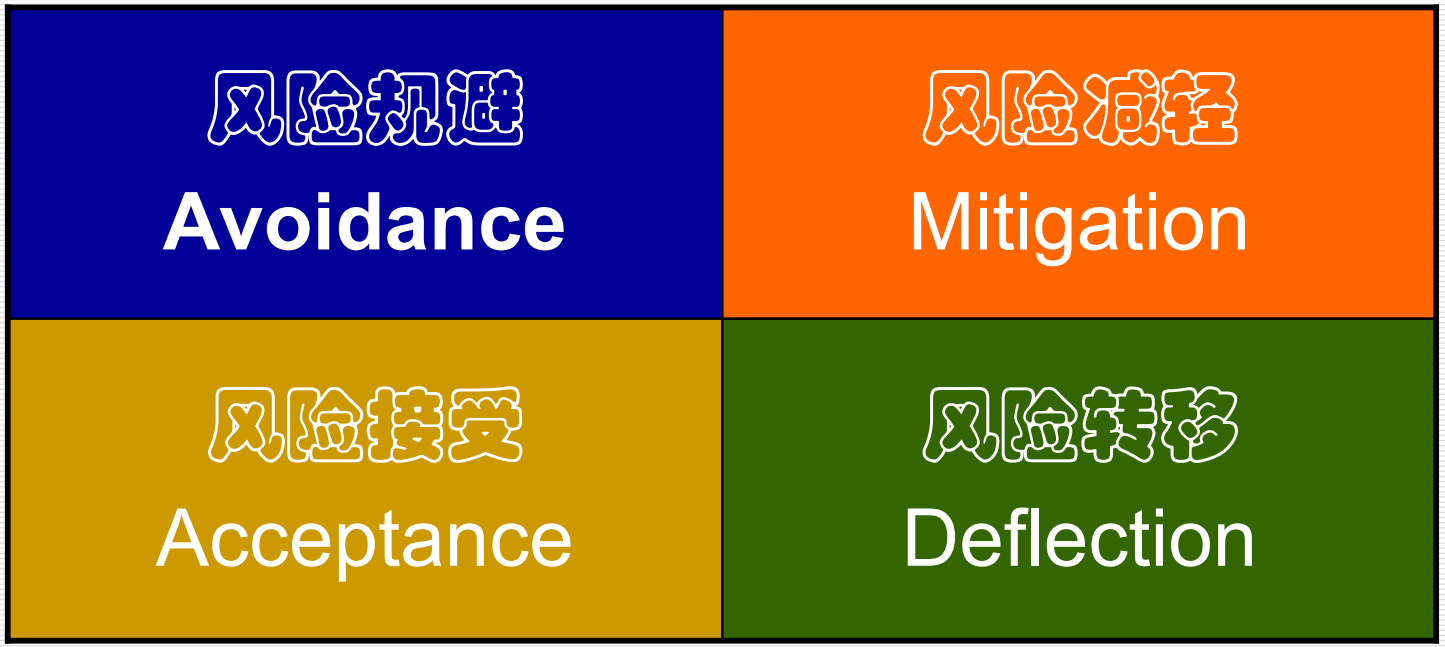
蒙特卡罗（Monte Carlo）仿真法

- 项目管理中蒙特卡罗模拟方法的一般步骤是：
  - 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；
  - 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；
  - 对随机抽样的数据进行必要的数学计算，求出结果；
  - 对求出的结果进行统计学处理，求出最小值、最大值以及数学期望值和单位标准偏差；
  - 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)；
  - 依据累积概率曲线进行项目风险分析。

风险应对



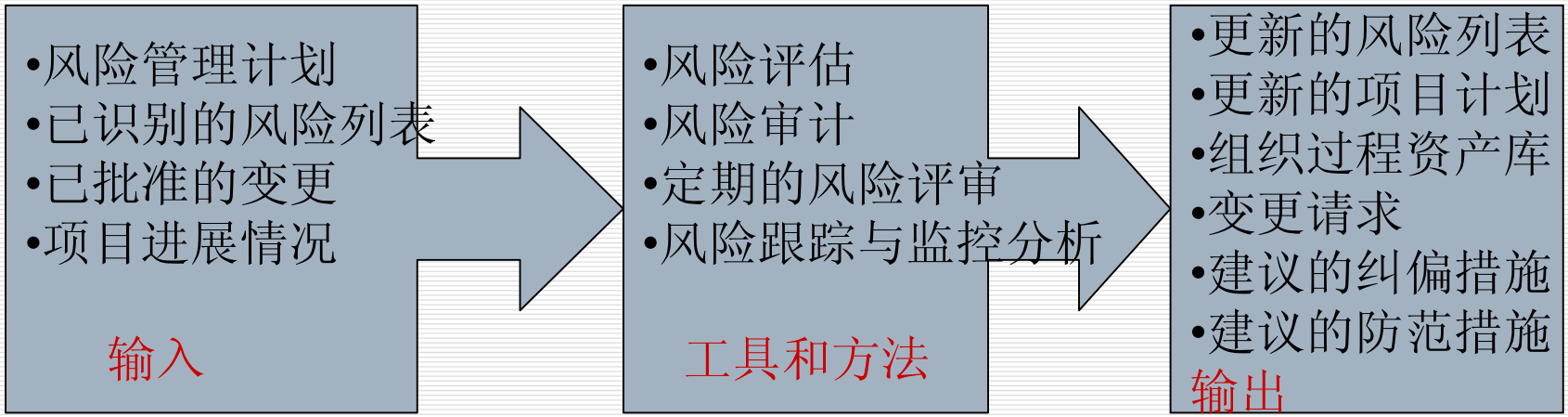
风险管理策略


风险规避
Avoidance
风险减轻
Mitigation
风险接受
Acceptance
风险转移
Deflection

风险应对计划编制，必须:

- 适当的（**Appropriate**） – 与风险的严重程度(和项目的复杂度)相配
- 成本的有效（**Cost effective**） – 用于克服风险
- 及时的（**Timely**） – 成功的
- 符合实际的（**Realistic**） – 在项目的环境中
- 一致同意的（**Agreed**） – 有关各方同意
- 风险有其所有者（**Owned**） – 风险对应有负责人
- 最佳方案（**Best Option**） – 必须被选出来

风险跟踪与监控


•风险管理计划
•已识别的风险列表
•已批准的变更
•项目进展情况
输入
•风险评估
•风险审计
•定期的风险评审
•风险跟踪与监控分析
工具和方法
•更新的风险列表
•更新的项目计划
•组织过程资产库
•变更请求
•建议的纠偏措施
•建议的防范措施
输出

风险监督和控制

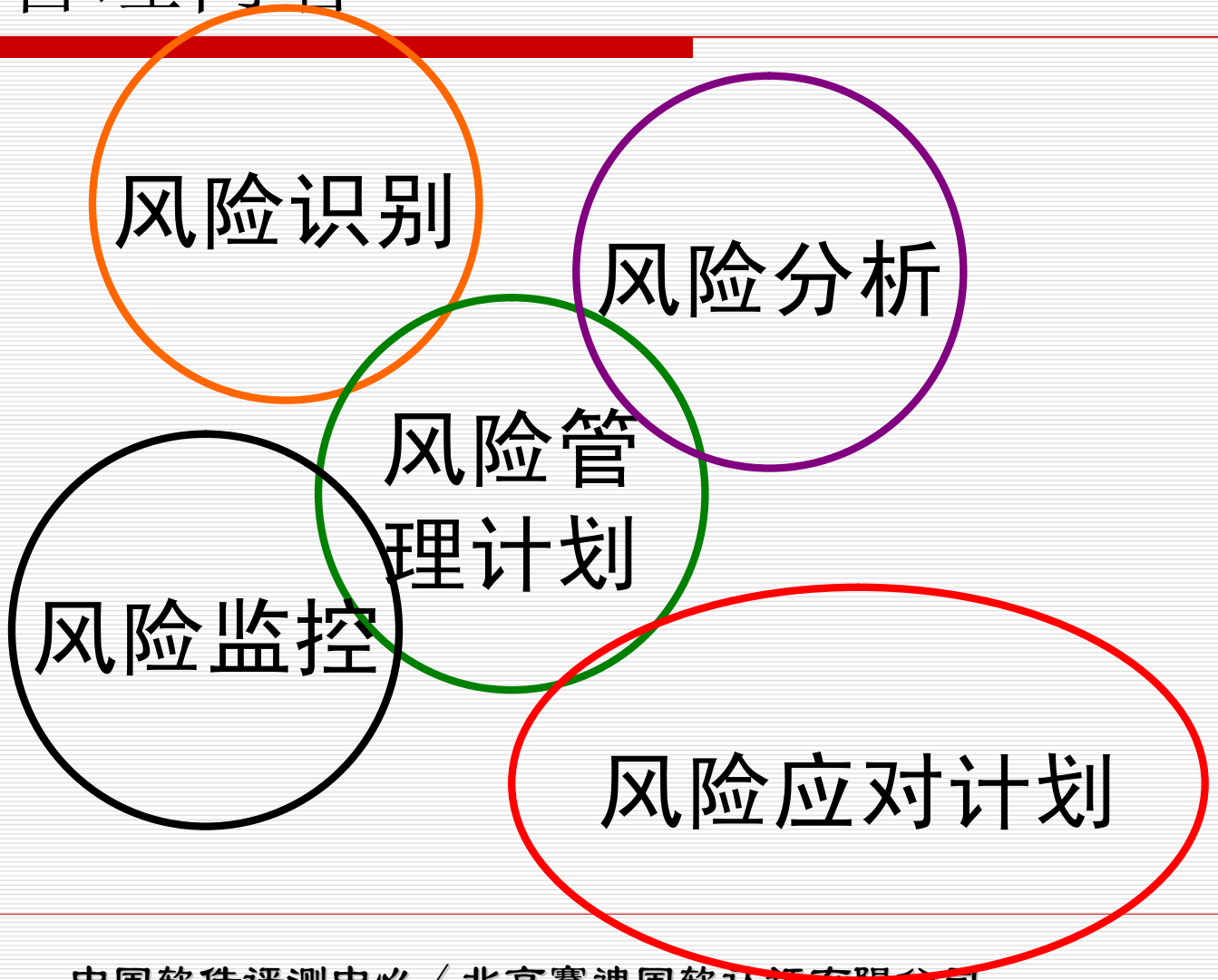
- 提前为做决策提供帮助
- 沟通十分重要
- 风险会发生变化，新的风险会出现，风险也会消失

牢记这是一个“积极主动”的过程

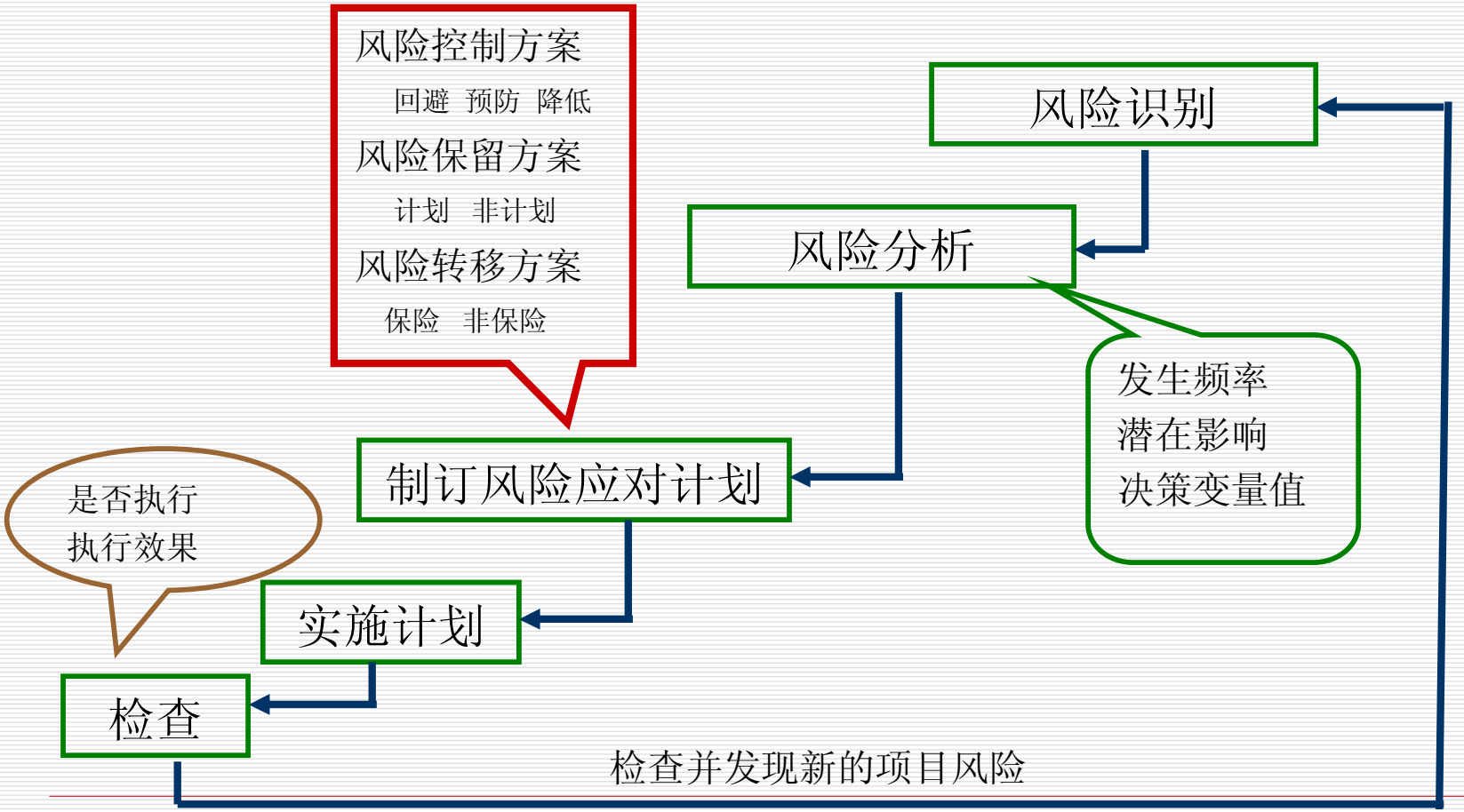
风险监督和控制 – 考察是否：

- 风险应对措施按照计划安排执行
- 风险应对措施的有效性与期望的一样，决定是否采取新的应对措施
- 项目的假设条件是否依然有效
- 风险暴露（risk exposure）发生了改变，需要对其变化趋势进行分析
- 风险的触发事件（Risk Trigger）发生了
- 按照合适的方针和程序
- 风险已经发生，但之前没有被发现

风险管理内容



风险管理过程


风险控制方案
回避 预防 降低
风险保留方案
计划 非计划
风险转移方案
保险 非保险
风险识别
风险分析
发生频率
潜在影响
决策变量值
制订风险应对计划
是否执行
执行效果
实施计划
检查
检查并发现新的项目风险

软件项目中的常见风险

- 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

需求、技术、成本、进度

软件项目风险管理模型

- Barry Boehm模型
- SEI的CRM(Continuous Risk Management)模型
- SERIM(Software Engineering Risk Model)模型

Barry Boehm模型 -- 1

- 用公式RE=P(UO)*L(UO)对风险进行定义
  - P(UO)：风险发生的概率
  - L(UO)：风险发生的影响

- 风险管理由风险评估和风险控制两大部分组成
  - 风险评估又可分为识别、分析、设置优先级
  - 风险控制则包括制定管理计划、解决和监督风险

Barry Boehm模型 -- 2

- Boehm思想的核心是10大风险因素列表(其中包括人员短缺、不合理的进度安排和预算、不断的需求变动等)
  - 针对每个风险因素，Boehm都给出了一系列的风险管理策略
  - 在实际操作时，以10大风险列表为依据，总结当前项目具体的风险因素，评估后进行计划和实施
  - 在下一次定期召开的会议上再对这10大风险因素的解决情况进行总结，产生新的10大风险因素表
  - 依此类推……

Barry Boehm模型 -- 3

- 模型优点：
  - 10大风险列表的思想可以将管理层的注意力有效地集中在高风险、高权重、严重影响项目成功的关键因素上，而不需要考虑众多低优先级的细节问题。

SEI的CRM模型

- SEI的风险管理原则是：
  - 不断地评估可能造成恶劣后果的因素
  - 决定最迫切需要处理的风险
  - 实施控制风险的策略
  - 评测并确保风险策略实施的有效性
- CRM模型要求在项目生命周期的所有阶段都关注风险识别和管理，它将风险管理划分为5个步骤：风险识别、分析、计划、跟踪、控制。

SERIM模型 -- 1

- SEIRM从技术和商业两个角度对软件风险管理进行剖析，考虑的问题涉及开销、进度、技术、性能等。它还提供了一些指标和模型来估量和预测风险，由于这些数据来源于大量的实际经验，因此具有很强的说服力。
- 模型的主要目的是识别、分析、交流和消除技术风险。技术风险包括：潜在的设计、界面、实现、验证和维护的问题；二义性，技术上的不确定性，过时的技术和主要的边缘技术。用风险分类学和基于分类的问卷来识别开发中的商业风险，商业风险包括：市场风险，产品风险，管理风险和预算风险。

SERIM模型 -- 2

- 模型优点：
  - 提供的关于风险管理的数据来源于大量的实际经验，表明了实际开发中的经验在此后软件开发中所起的重要作用，对他们有重要的指导意义和实施开发的依据。
- 缺点：
  - 经验的获取需要一定的时间积累，对于新公司或开发不规范的公司来说，没有经验数据的积累减小了其适用范围。

软件项目常见风险的分析和规避

Top 10

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

风险管理

中国软件评测中心

赛迪国软认证有限公司

风险管理

目的:

识别潜在的风险，以便策划应对风险的措施，必要时在整个项目生存周期中实施这些措施，以缓解风险对目标实现的影响。

风险管理 – 特定目标

- **SG 1: 准备风险管理**

  进行风险管理准备

- SG 2: 识别并分析风险

  识别并分析风险，以确定其相对重要性

- SG 3: 缓解风险

  适当时处理或缓解风险，以减少对实现目标的不利影响

SP1.1 确定风险来源和类别

即在公司组织层面，定义公司所有风险的来源和类别

- 风险来源
  - 需求不确定
  - 测试和评估不充分
  - 开发者能力欠缺
  - 缺乏足够的人力资源
  - ……
- 风险类别
  - 商务类
  - 管理类
  - 技术类
  - ……

风险来源存在于项目内部和外部。随着项目的推进，还可能发现新的风险来源

SP1.2 定义风险参数

- 即对每一个风险，定义清晰的风险属性
  - 一般风险属性包括：
    - 风险的发生机率
    - 风险发生的影响和严重性
    - ……
  - 定义风险属性的目的是用来分析风险、分类风险以及用来进行风险管理

SP1.3 制订风险管理策略

- 即制订并维护风险管理计划
  - 所谓的风险管理策略，指得就是风险如何记录、跟踪、采取什么缓解措施等所有关于风险管理的组织级别的要求

风险管理 – 特定目标

- **SG 1: 准备风险管理**

  进行风险管理准备

- **SG 2: 识别并分析风险**

  识别并分析风险，以确定其相对重要性

- **SG 3: 缓解风险**

  适当时处理或缓解风险，以减少对实现目标的不利影响

SP2.1 识别风险

- 即在项目层面，识别风险并记录风险

SP2.2 对风险进行评价、分类和排序

- 即根据已经定义好的风险分类及属性，评估和分类每一个风险，并决定其优先级

风险管理 – 特定目标

- SG 1: 准备风险管理

  进行风险管理准备

- SG 2: 识别并分析风险

  识别并分析风险，以确定其相对重要性

- **SG 3:** 缓解风险

  适当时处理或缓解风险，以减少对实现目标的不利影响

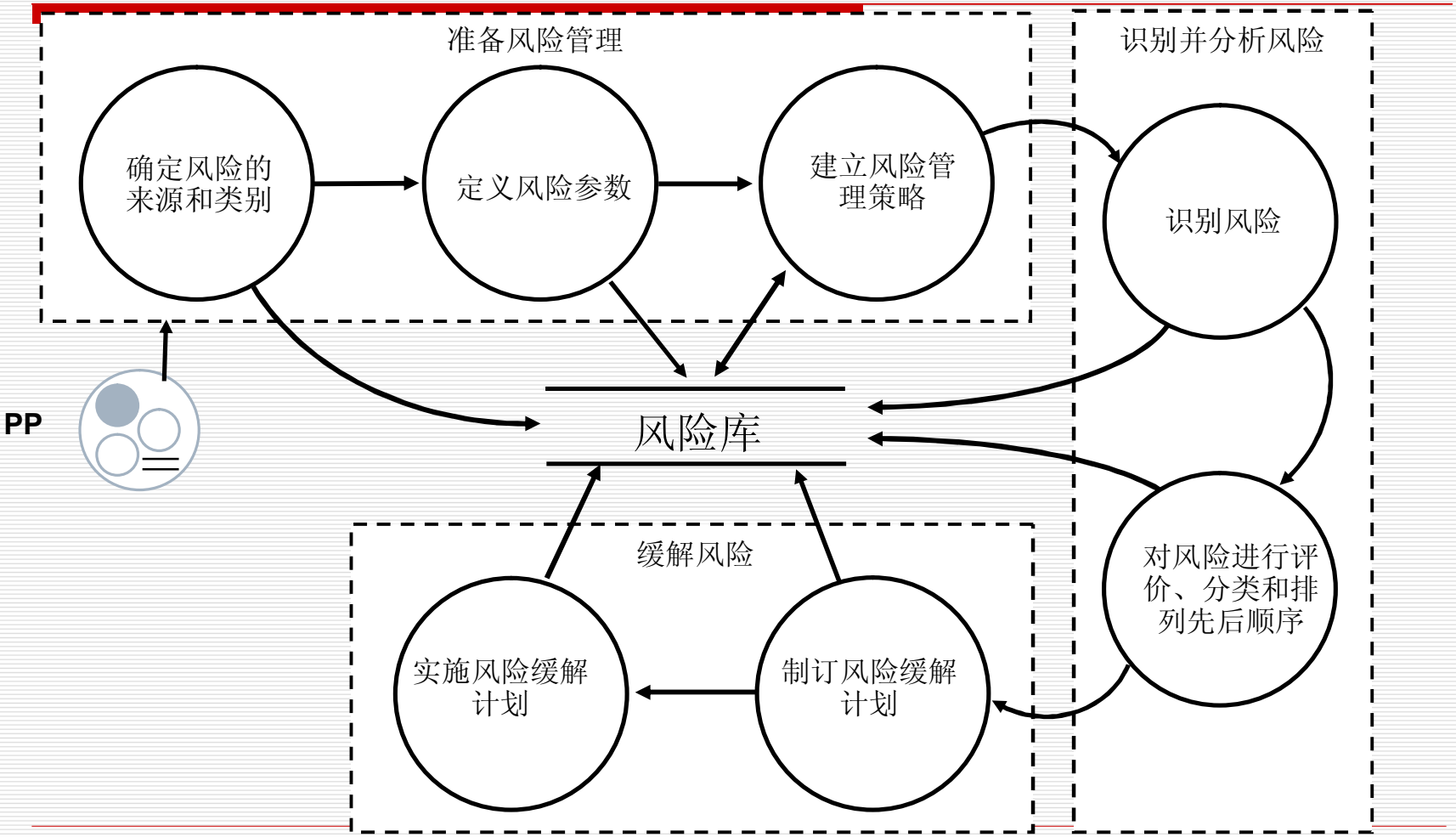
SP3.1 制订风险缓解计划

- 即根据风险管理策略，对项目最重要的风险制定风险缓解计划。
- 风险缓解措施是指，降低风险发生机率及风险发生时采取的减低影响的措施。

SP3.2 实施风险缓解

- 即周期性地跟踪风险状态，在需要的时候实施风险缓解计划

风险管理


准备风险管理
识别并分析风险
确定风险的来源和类别
定义风险参数
建立风险管理策略
识别风险
PP
风险库
缓解风险
实施风险缓解计划
制订风险缓解计划
对风险进行评价、分类和排列先后顺序

RSKM----总结

- 风险管理计划
- 风险识别检查表
- 风险清单
- 已发生风险清单
- ……

结束语

好好学习，天天向上。