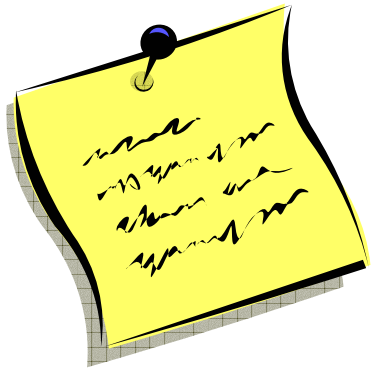
第四部分
风险管理与信息安全工程

风险概念的由来

- 风险　是外来词汇
- 风险　《现代汉语词典》　“可能发生的危险”
- 如何研究风险?
- 要解决实际的问题，必须试图将风险进行量化



风险的定义

- **风险　risk**
  - **事件**（event）发生的**概率**（**probability**）与结果（**consequence**）的结合 [ISO Guide 73：2002]。
  - 是一个指定的威胁利用一项资产或多项资产的脆弱性，并由此造成损害或破坏的**可能性** [ISO/IEC 13335:2004]
  - 是对目标有所影响的某个安全**事件**发生的**可能性**，它根据**影响**（**impact**）和**可能性**（**likehood**）来度量。[AS/NZS 4360：1999]

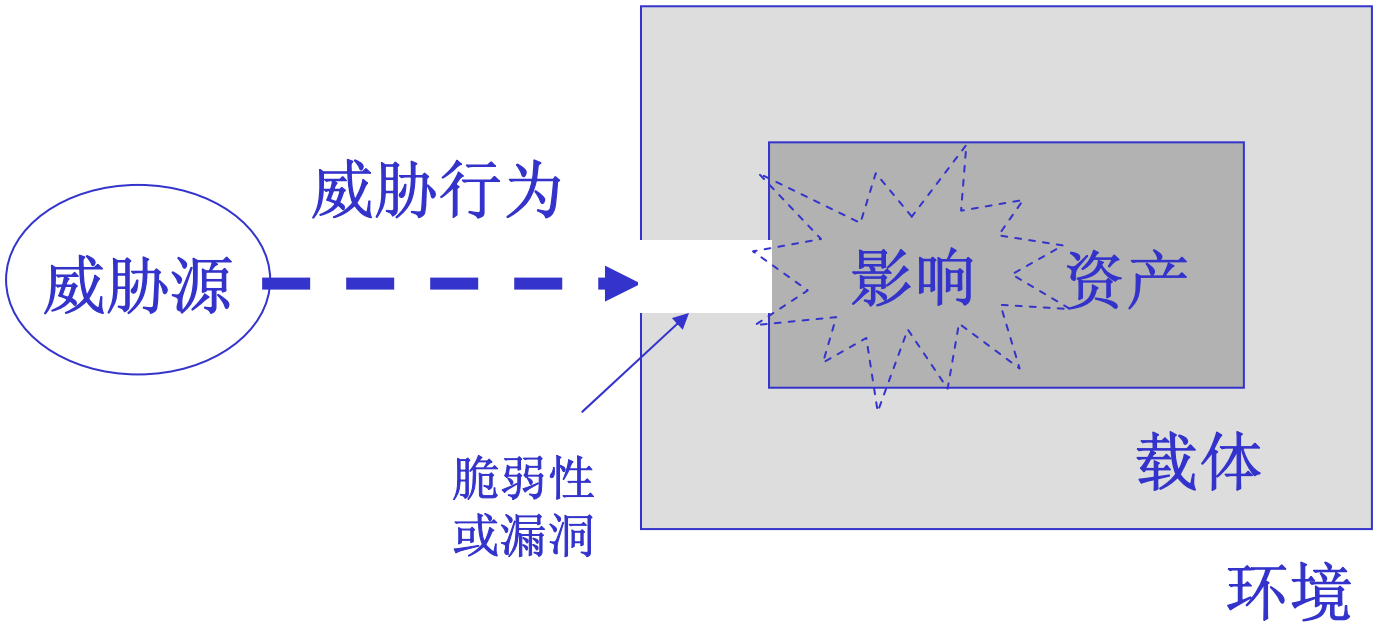
风险与事件的关系

- 安全风险（以下简称风险）是一种潜在的、负面的东西，处于未发生的状态。与之相对应，安全事件（以下简称事件）是一种显在的、负面的东西，处于已发生的状态。风险是事件产生的前提，事件是在一定条件下由风险演变而来的。

潜在
未发生的状态

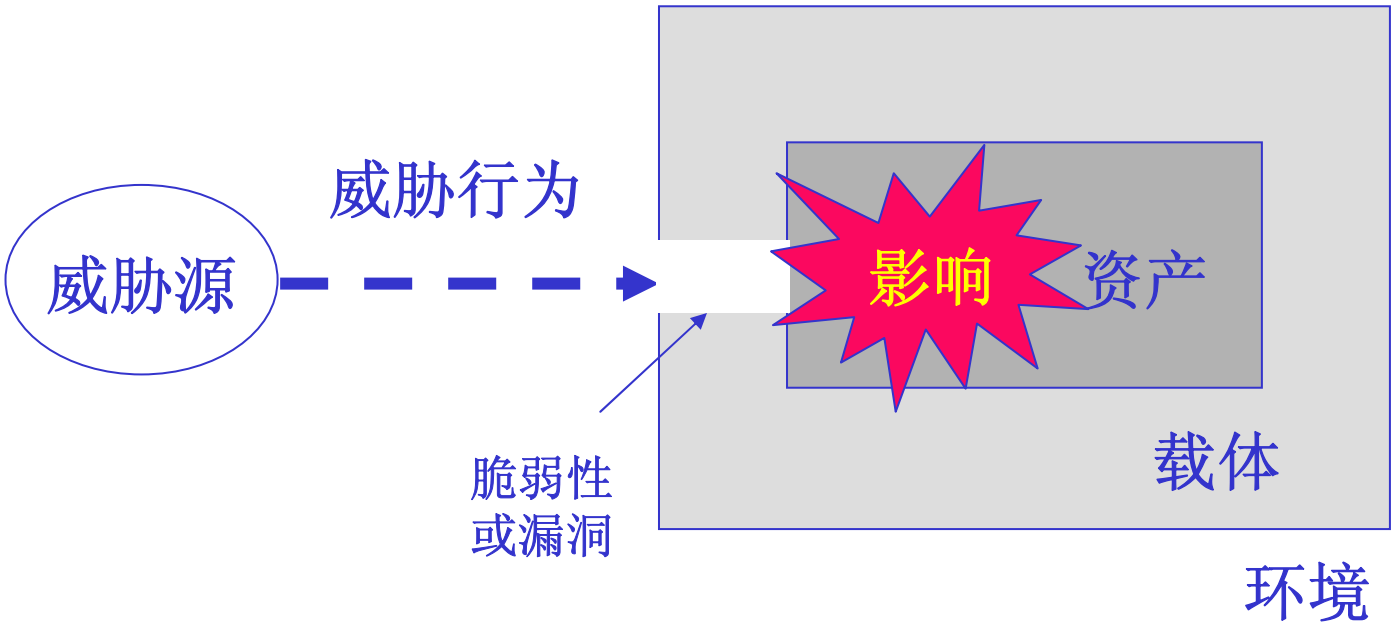
显在
已发生的状态

风险的概念模型



威胁源利用脆弱性，对资产实施威胁行为，造成影响

事件的概念模型

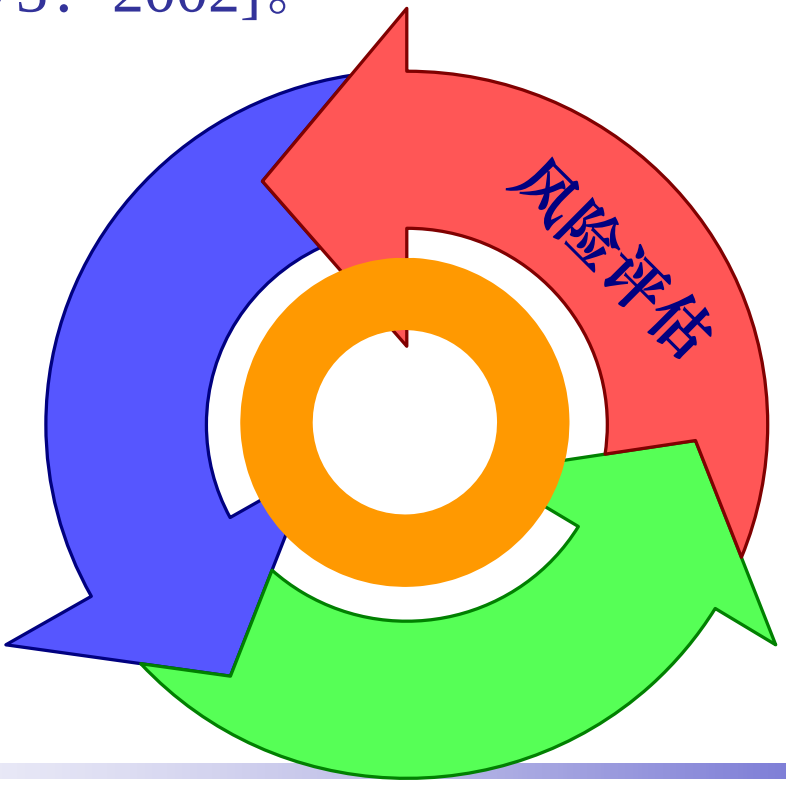


关于风险

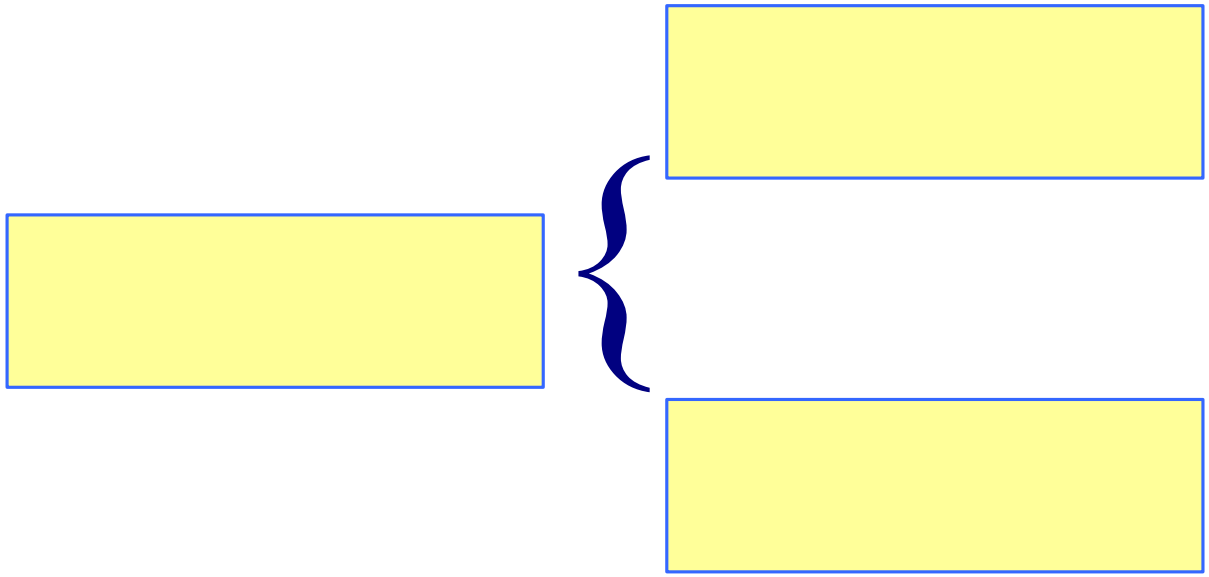
- 风险是客观存在的
- 风险强调的是损害的潜在可能性，而不是事实上的损害
- 风险不能消除至尽，包括人为因素带来的风险，一样不能消除至尽
- 衡量风险的两个基本要素就是事件的概率和其（产生的）后果
- 对信息安全而言，导致风险的事件是威胁利用了资产（或系统）的脆弱点

风险管理的定义

- 风险管理（risk management）
  - 指导和控制一个组织（organization）相关风险的活动[ISO Guide 73：2002]。



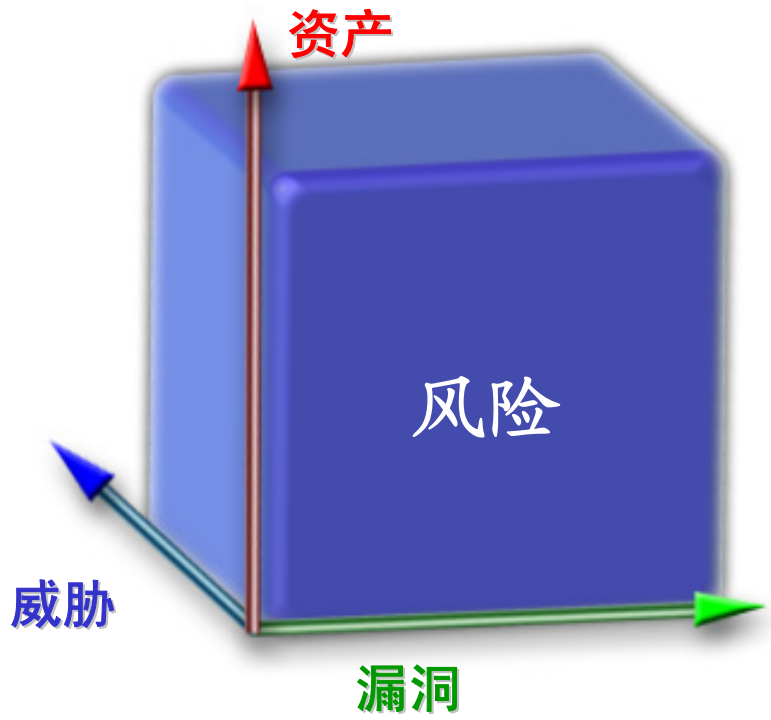
风险评估的定义



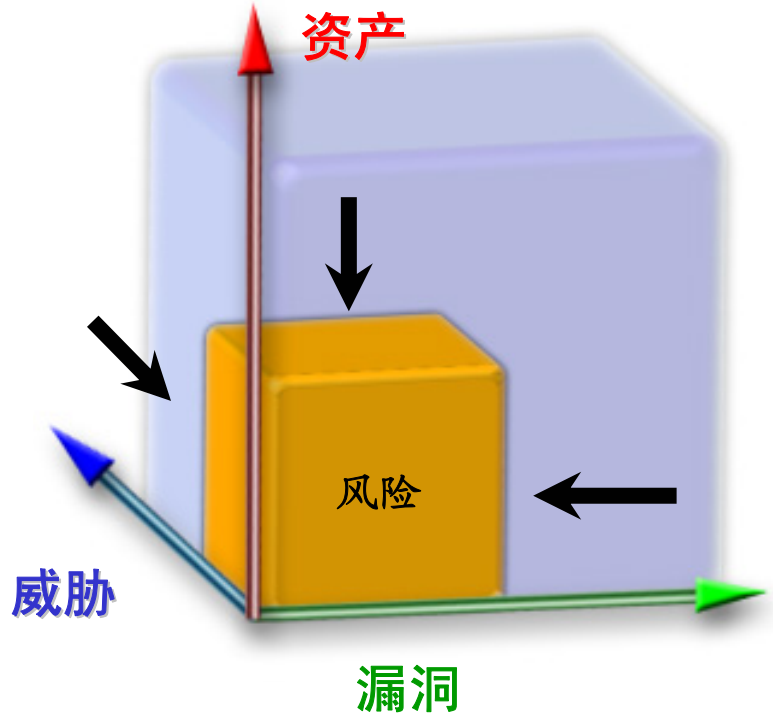
风险处理

- **风险处理（risk treatment）**
  - 选择并执行措施来更改风险的过程。也可称为风险减缓（risk mitigation）或风险控制（risk control）

风险管理的目标



基本的风险



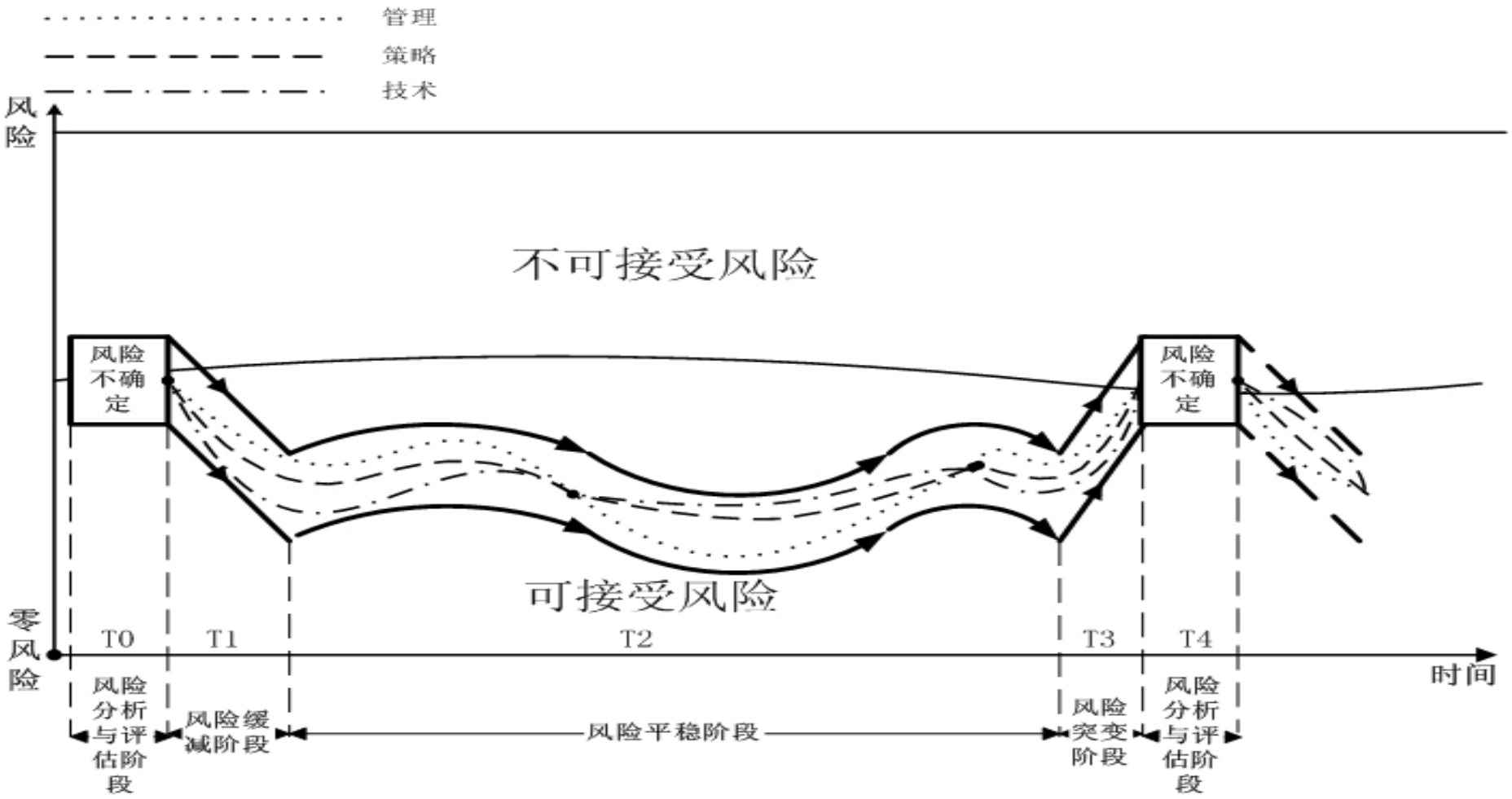
采取措施后剩余的风险

残余风险处于可接受的状态

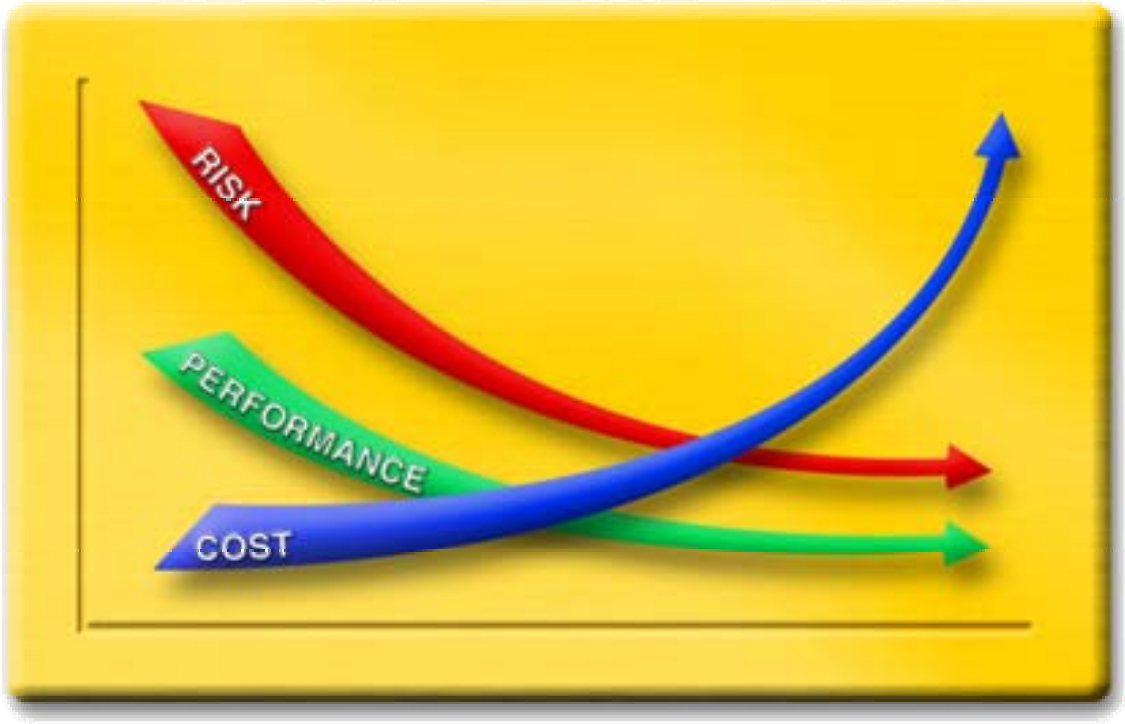
风险管理的必要性和可行性

- 必要性
  - 组织战略的要求
  - 法律法规的需求
- 可行性
  - 技术手段的进步
  - 经验数据的积累
  - 标准的完善

风险周期模型—RC（Risk Cycle）模型

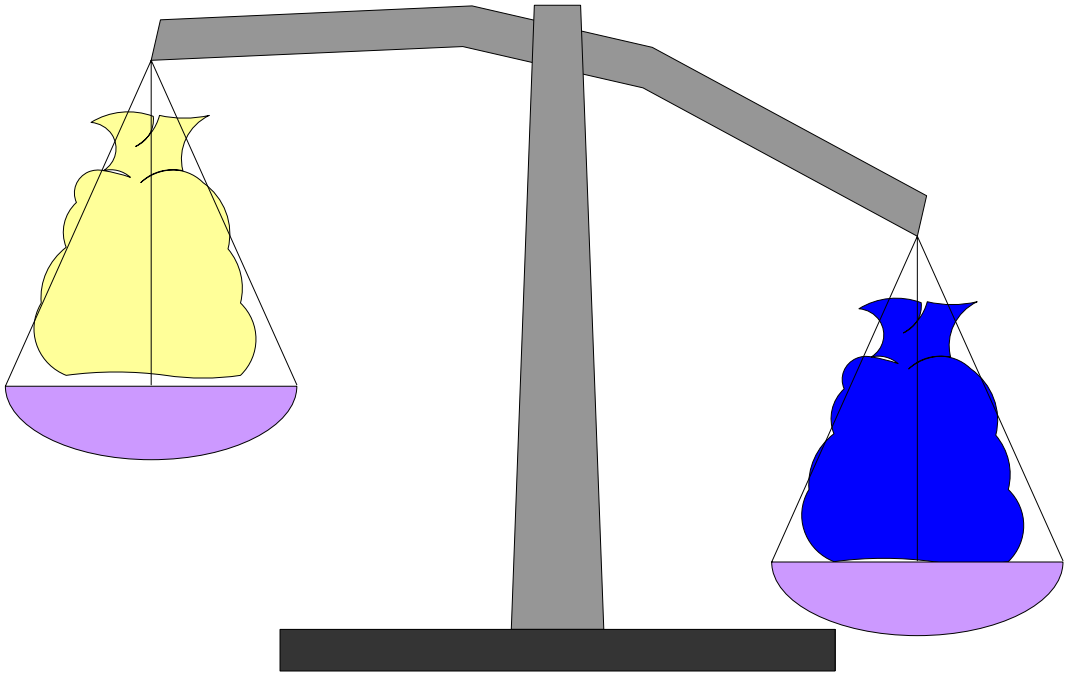


风险管理的基本原则



适度安全

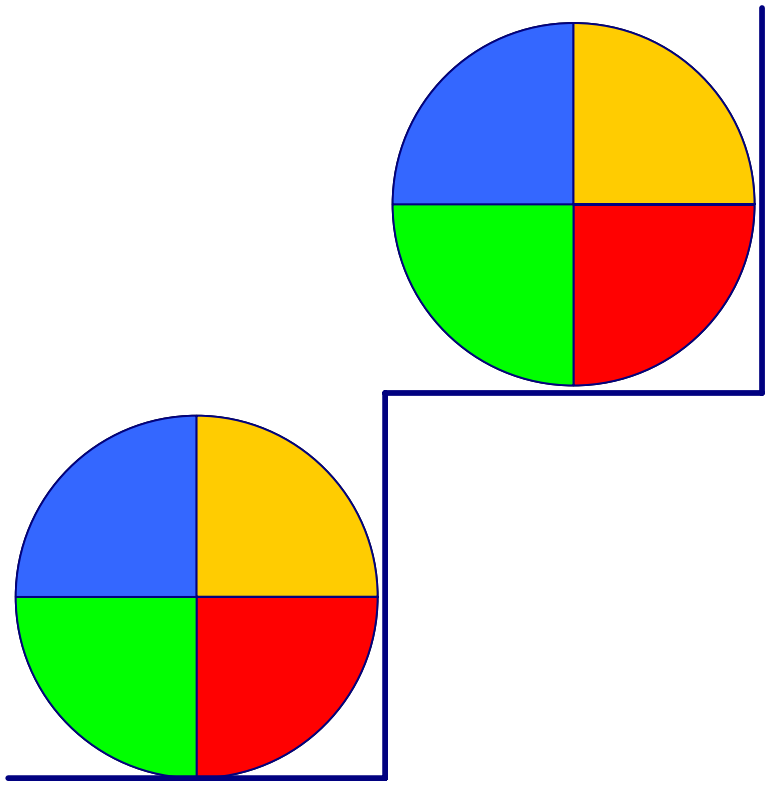
风险管理的基本原则



平衡成本与效益

风险管理目标——持续改进

- 持续循环，不断上升



风险管理的方法

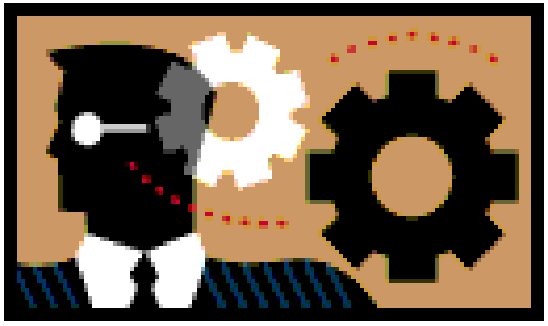
- 反应性方法
  - 事件发生之后，最大程度降低影响，并采取措施降低再发生的可能性
- 前瞻性方法
  - 事件发生之前，最大程度地降低坏事情发生的可能性

风险管理与SDLC

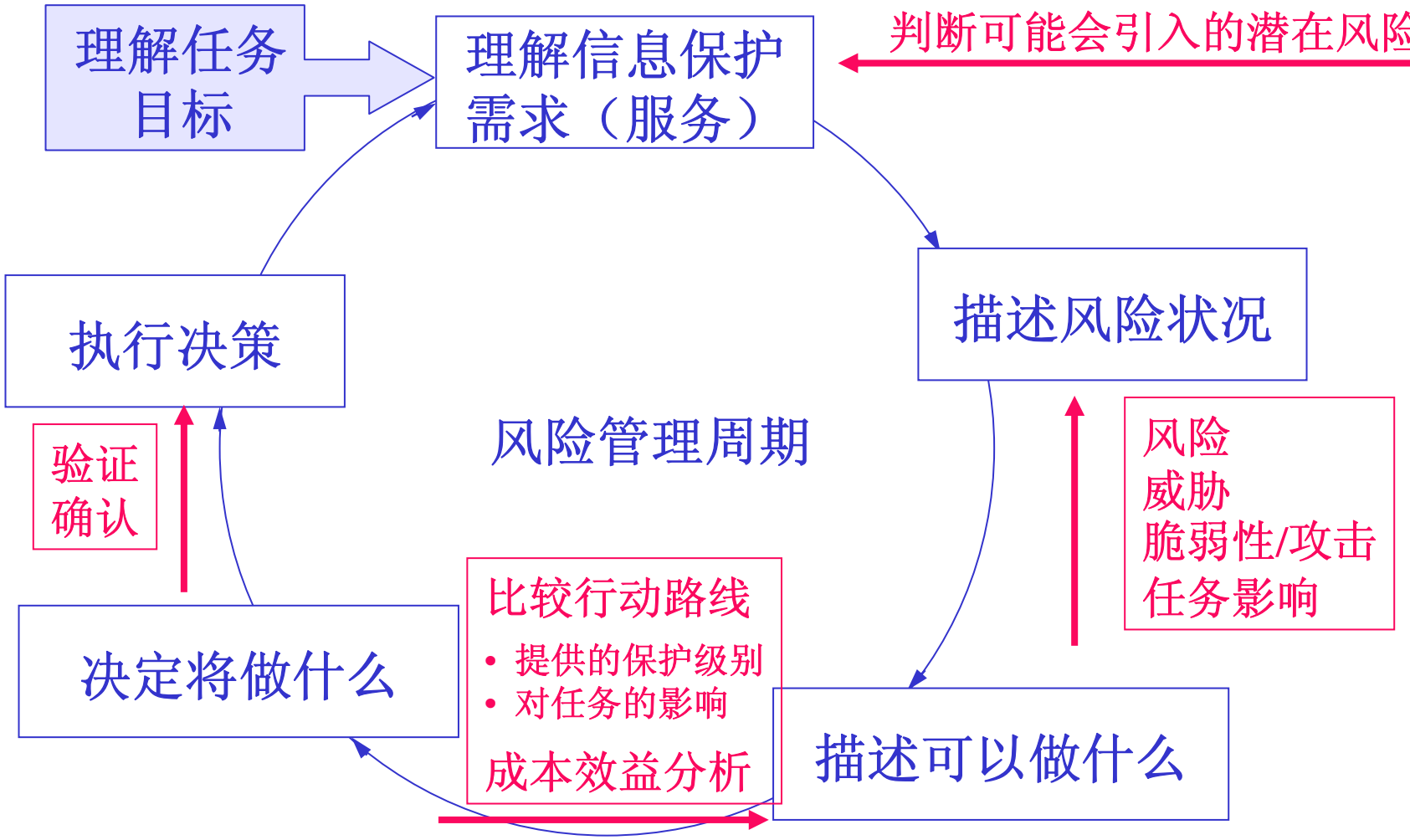
- **有效的风险管理必须完全地集成到SDLC（**System Development Life Cycle）**中**
  - 启动
  - 开发或采办
  - 实现
  - 运行或维护
  - 废弃

SDLC阶段	阶段特征	来自风险管理活动的支持
阶段1——启动	记录IT系统的需求以及IT系统的目的和范围	风险的识别活动可以用来支持系统需求的开发包括安全需求和运行安全概念
阶段2——开发或采办	信息系统被设计、购买、规划、开发或建造。	在本阶段标识的风险可以用来为IT系统的安全分析提供支持，这可能会导致系统在开发过程中对体系结构和设计方案进行权衡。
阶段3——实现	信息系统的安全特性应该被配置、激活、测试并得到验证。	风险管理过程可支持对系统实现效果的评估，考察其是否能满足要求，并考察系统所运行的环境是否是预期设计的。有关风险的一系列决策必须在系统运行之前做出。
阶段4——运行或维护	信息系统开始执行其功能，一般情况下系统要不断修改，添加硬件和软件，或改变机构的运行、策略或流程等。	当定期对系统进行重授权（或重认可）时，或者IT系统在其运行性生产环境（例如新的系统接口）中做出重大变更时，要对其进行风险评估活动。
阶段5——废弃	涉及到对信息、硬件和软件的废弃。这些活动可能包括信息的移动、备份、丢弃、破坏以及对硬件和软件进行的销密。	当要废弃或替换系统组件时，要对其进行风险评估活动，以确保硬件和软件得到了适当的废弃处置，且残留信息也恰当地进行了处理。并且要确保系统的更新换代是以一个安全和系统化的方式完成的。

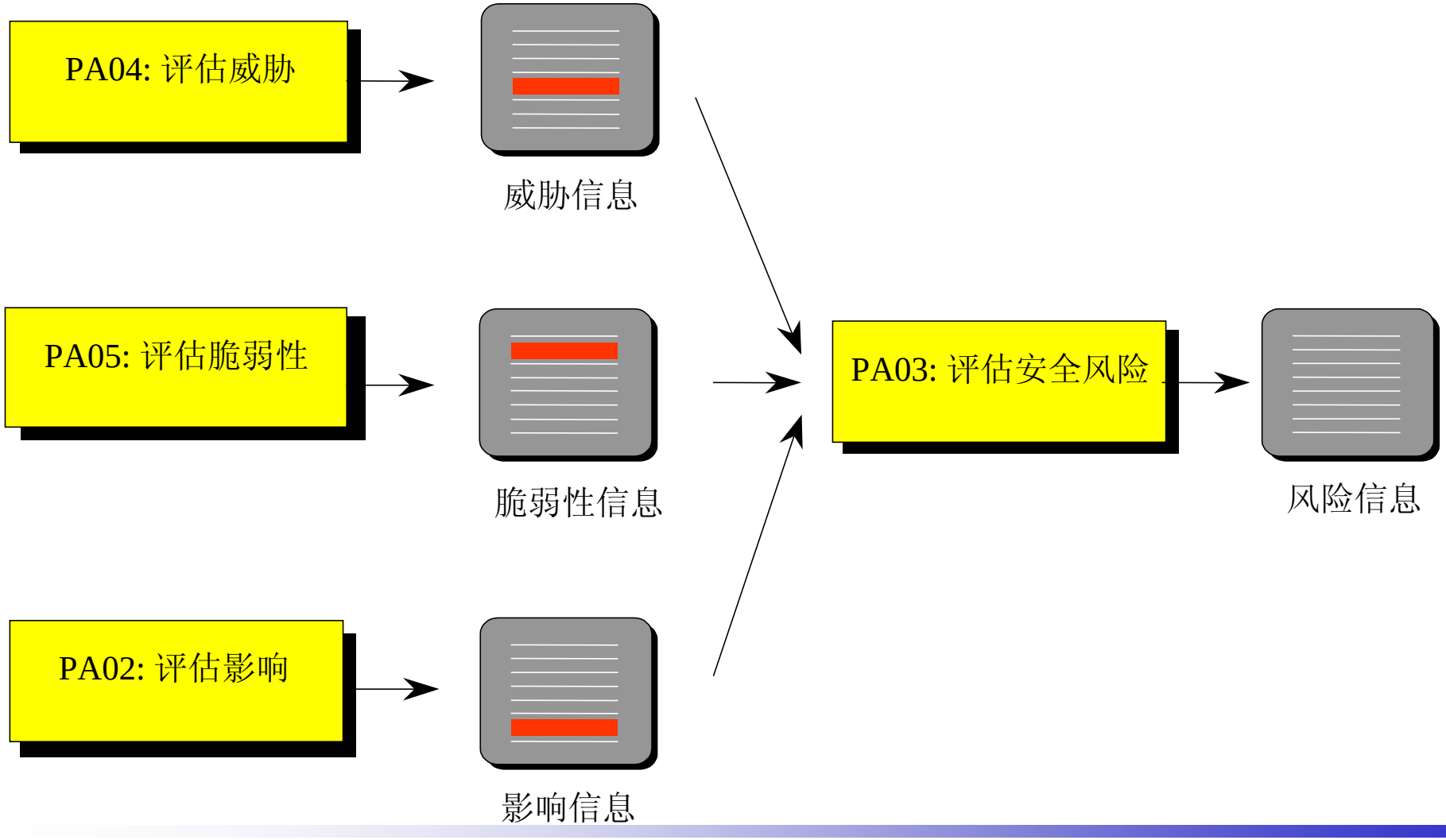
风险管理与信息安全工程的关系?



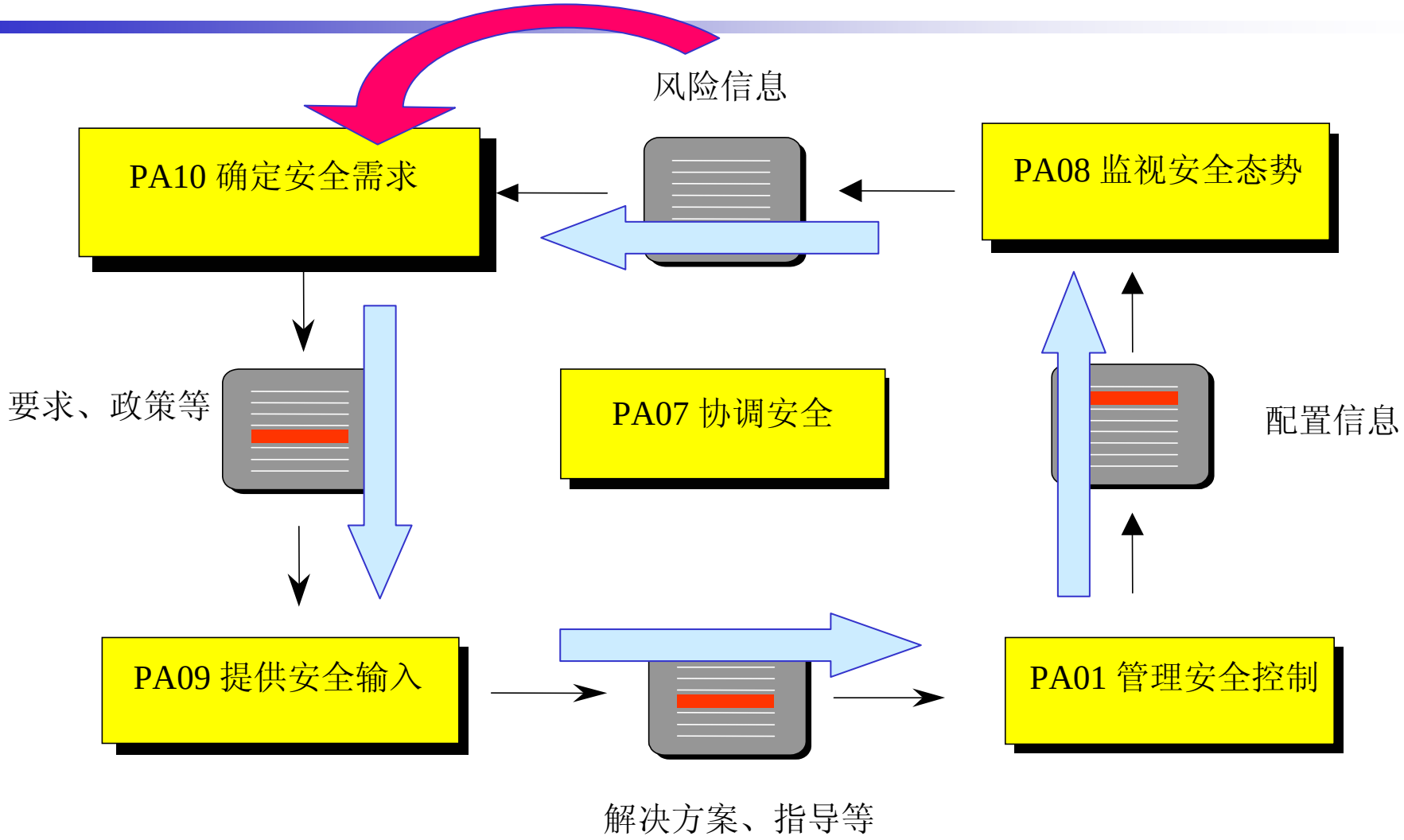
ISSE的风险管理过程



与风险过程相关的过程域



与工程过程相关的过程域



风险过程的特殊性

- 就隶属关系，风险过程应属于工程过程的一部分，不能与工程过程并列。
  - 风险过程为工程过程提供了基本的需求信息，
  - 风险过程为安全工程的结果提供了有效的评估手段
- 强调风险过程是因为：安全的动态性、相对性
- SSE-CMM中没有规定风险评估的定量方法（也不可能），但将风险评估的流程及评估中各因素的关系明确，具有可实施性和指导作用

SSE-CMM与ISSE的区别

SSE-CMM

- 强调了风险评估，没有规定风险评估的定量方法（也不可能），但将风险评估的流程及评估中各因素的关系明确

ISSE

- 在发掘需求阶段，考虑到了威胁评估，和相关的脆弱性评估和影响评估的内容，但尚未形成完成、全面的风险评估方法

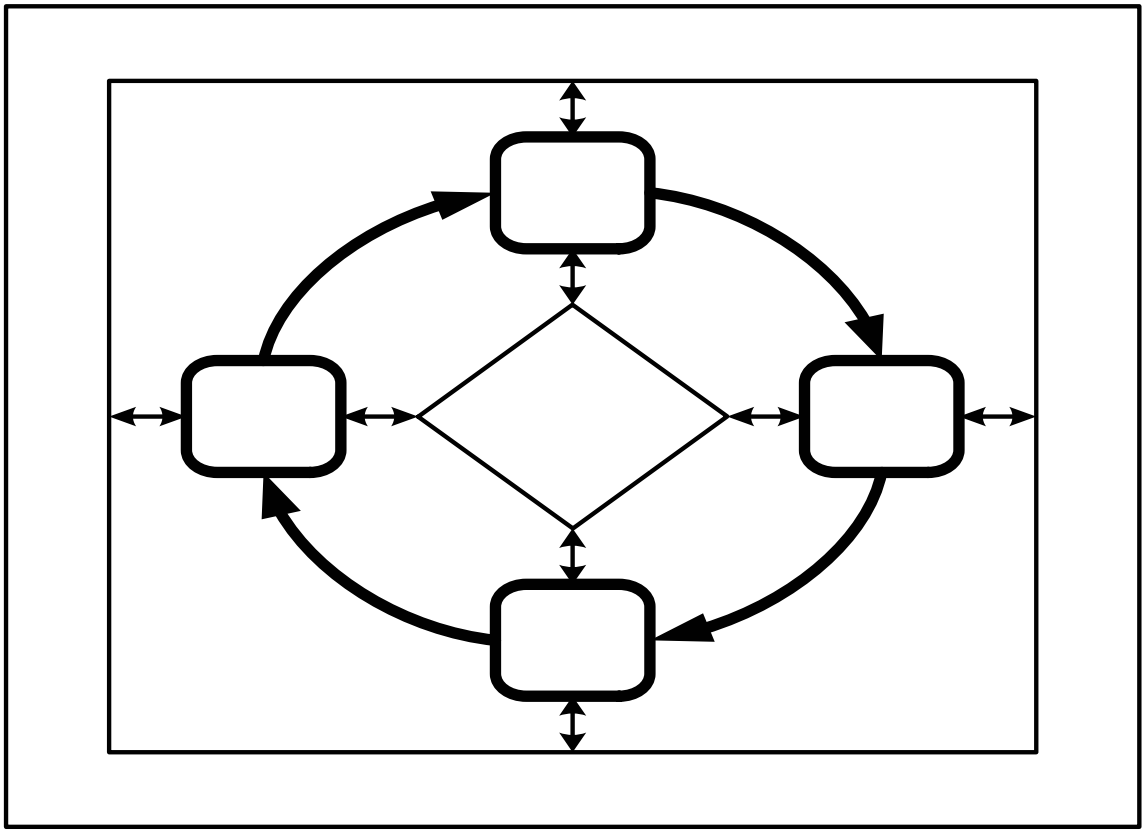
风险管理与信息安全工程

- 信息安全工程处处都体现风险管理的思想
- 风险管理过程不是信息安全工程过程的全部

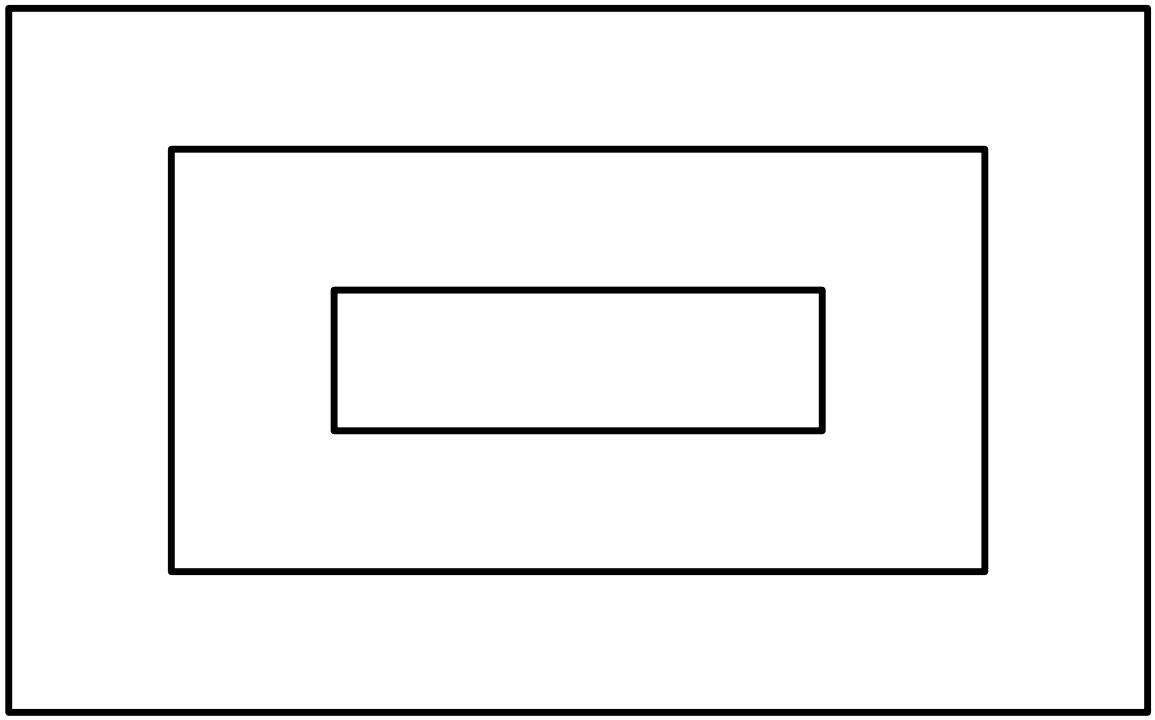
中国　风险管理过程

—— 范红　　国家信息中心信息安全研究与服务中心

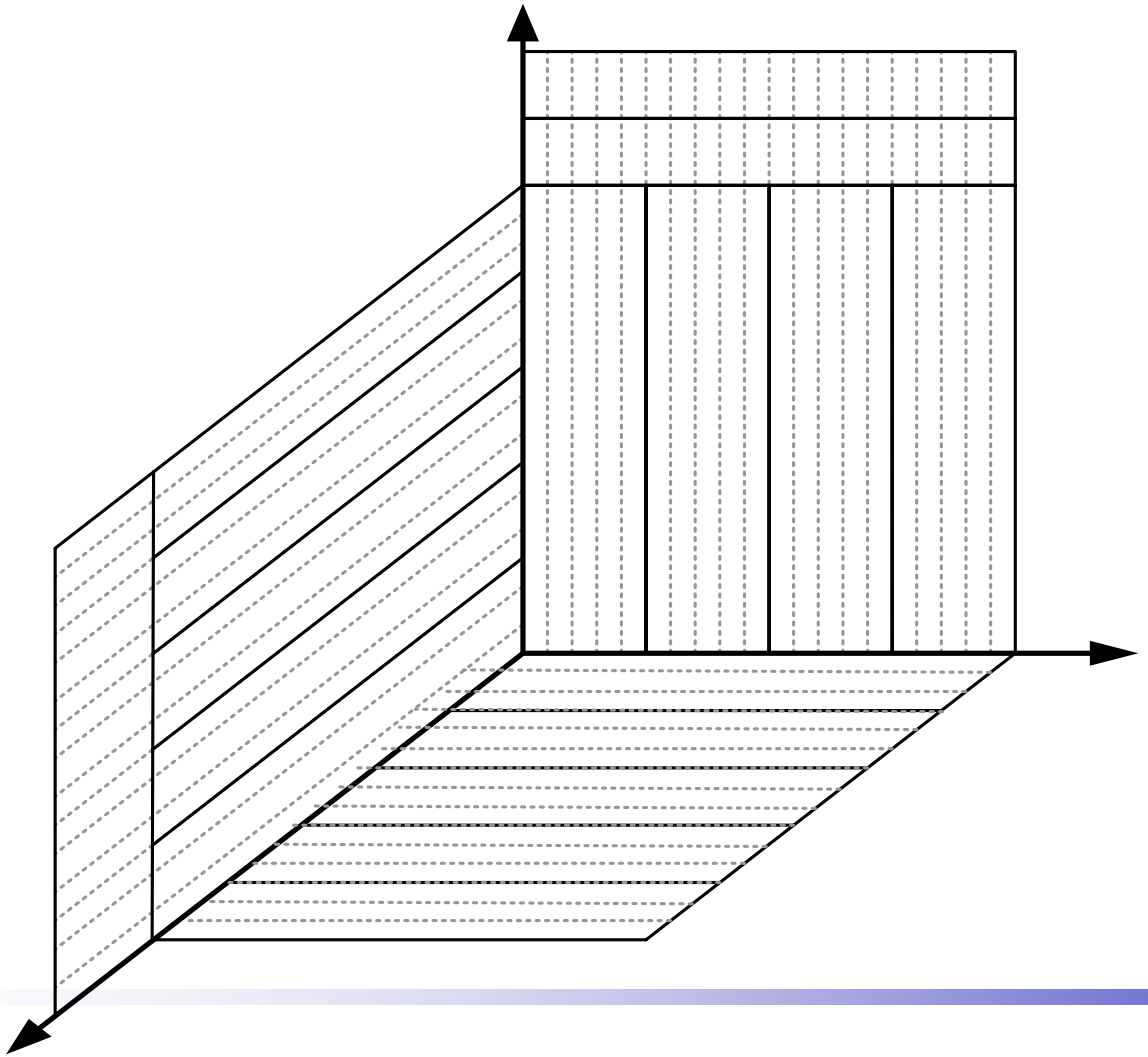
风险管理的内容和过程



信息安全风险管理的范围和对象



三维结构关系



微软提出的风险管理过程

Microsoft Solutions Framework

– MSF 风险管理过程包含六个逻辑阶段（识别、分析、计划、跟踪、控制和学习）

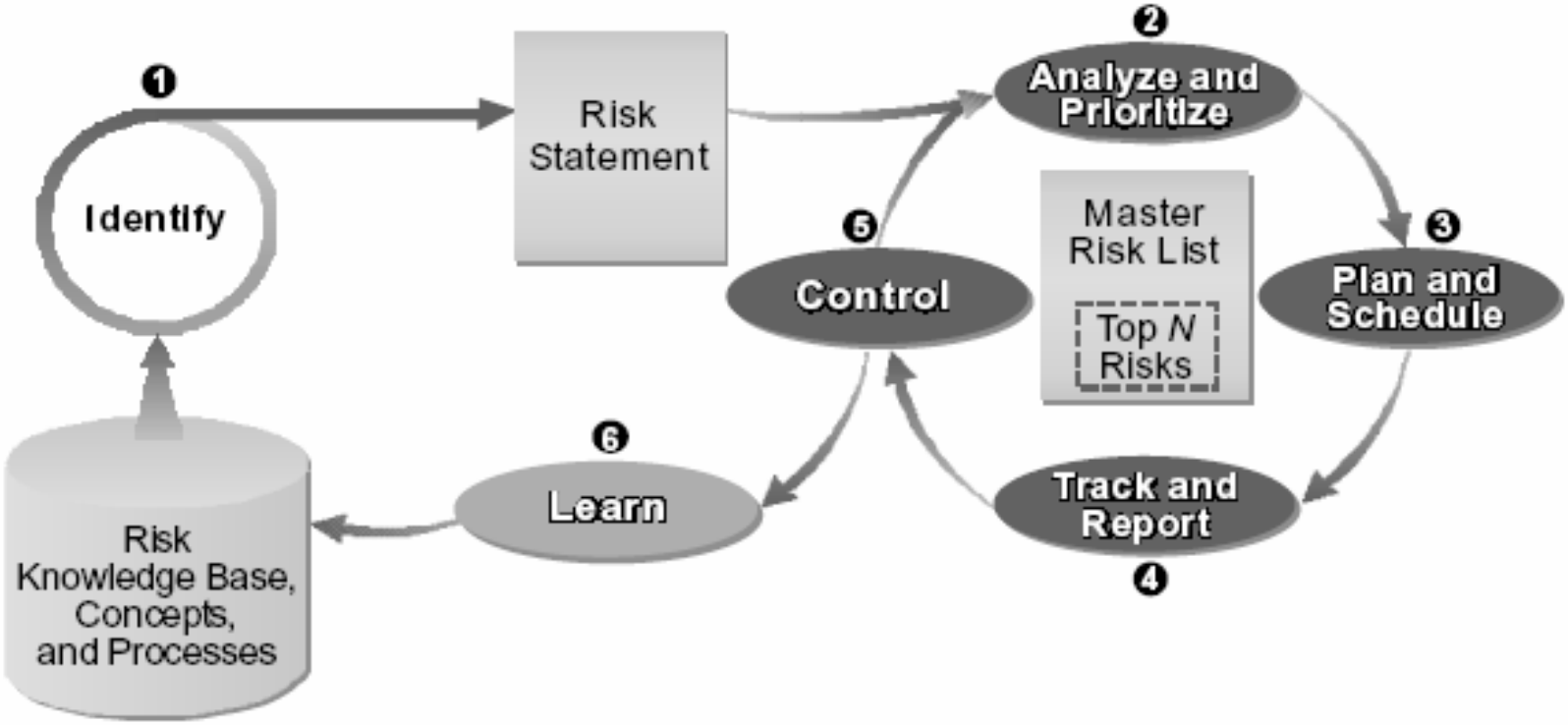
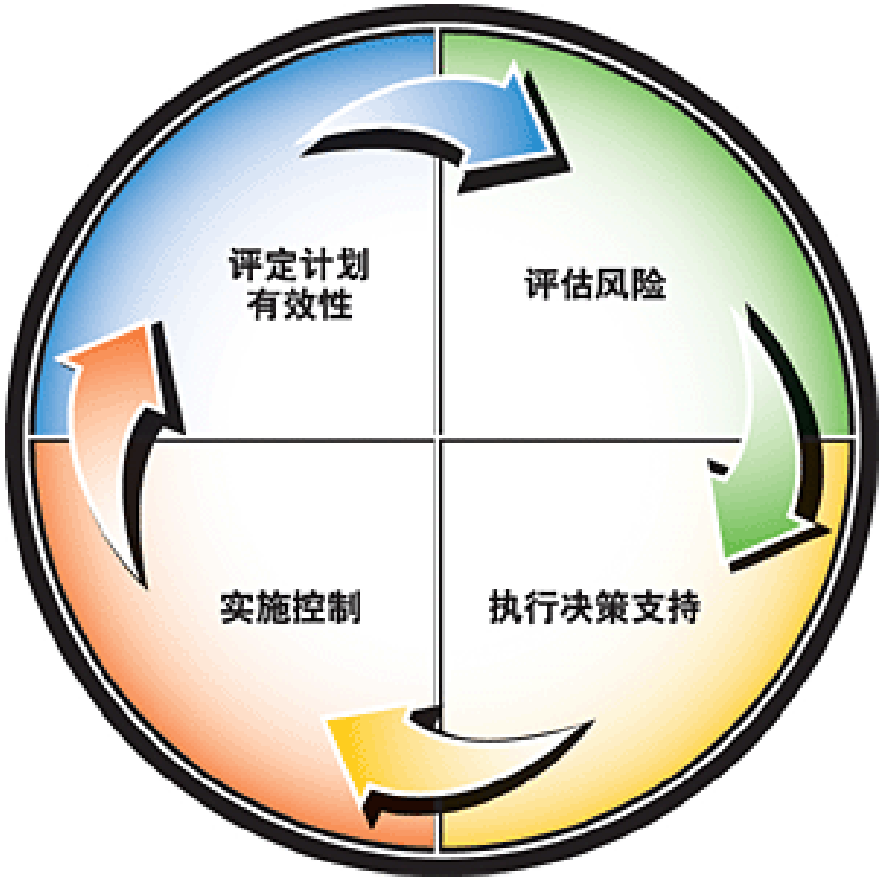


Figure 4: MSF Risk Management Process

《安全风险管理指南》



– 安全风险管理方法提供了一种前瞻性的方法，可帮助各种规模的组织响应他们所在的环境以及法律挑战提出的要求。 正式的风险管理流程让企业能够以最具有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，更好地管理风险。

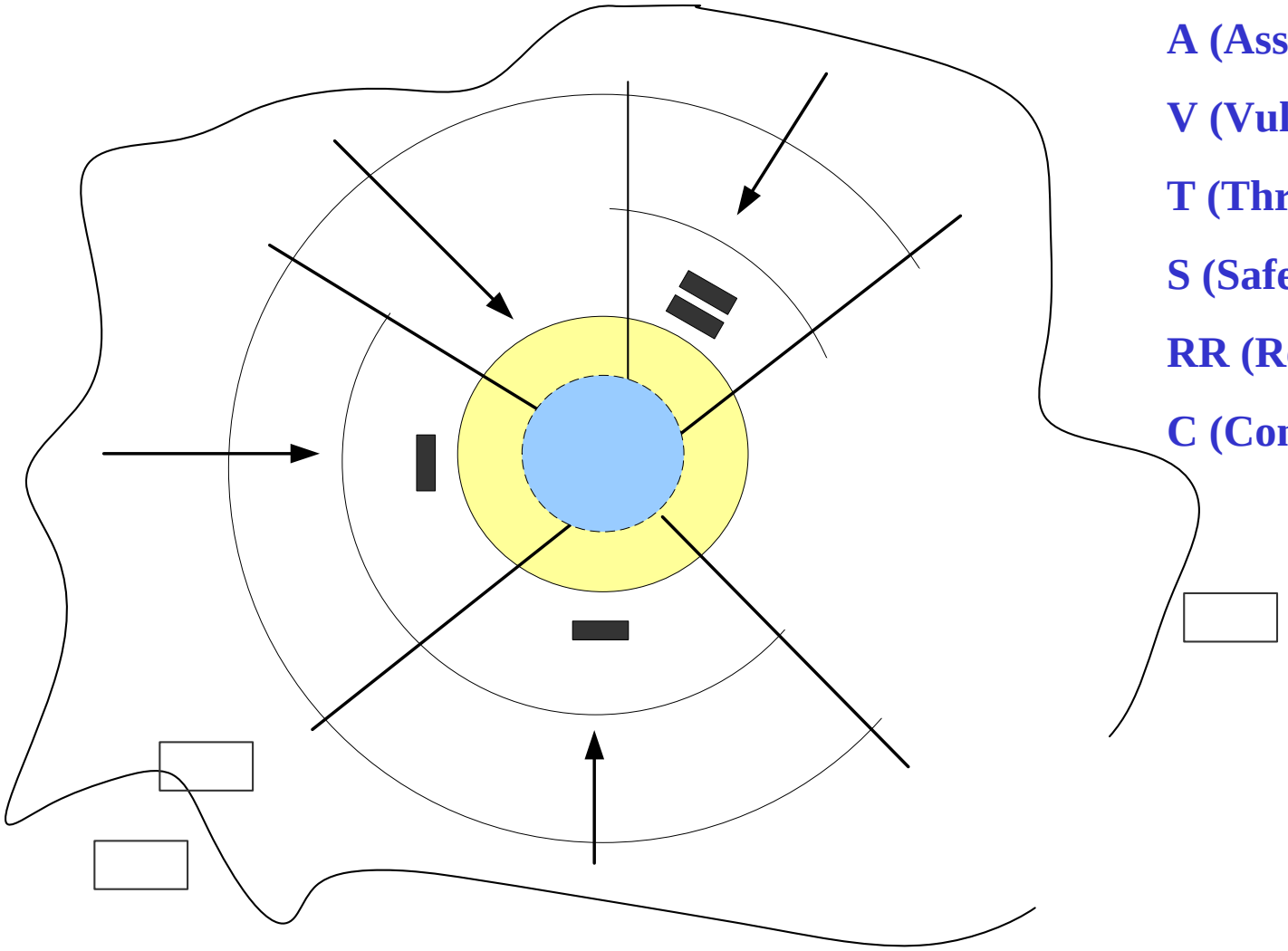
风险管理过程

- 评估风险
  - 综合了定性和定量风险评估方法，给出一份相对较短的经过详细检查的最重要风险列表。
- 实施决策支持
  - 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的安全筹划指导委员会
- 实施控制
  - 缓解方案所有者实际实施控制解决方案
- 评定计划有效性
  - 用于验证控制措施实际提供预期的保护程度，并观察环境变化

如何理解风险评估与风险管理

- 风险评估是否存在唯一正确的结果?
- 风险评估是否是一劳永逸的事情?
- 风险评估就是漏洞扫描?
- 风险评估是IT部门的事，与其他部门无关?
- 风险管理就是要实现最大的安全?
- 要满足安全需求是不是一定需要风险管理?

安全要素与其相互关系（ISO/IEC13335）



A (Asset) 资产

V (Vulnerability) 脆弱性

T (Threat) 威胁

S (Safeguard) 保护措施

RR (Residual Risk) 残余风险

C (Constrains) 约束

约束

威胁

利用风险评估知道了什么?

- 面临什么威胁?
- 这些威胁对组织业务的潜在影响如何?
- 系统中存在哪些技术隐患?
- 组织管理上存在哪些薄弱环节?
- 产生这些问题的原因是什么?
- 目前运行状况是否满足系统的安全需求?

风险评估的作用和目的

- 了解和评价信息安全现状
- 提出信息系统的安全需求
- 选择最佳的风险控制措施
- 建立信息安全管理体系
- 制订有效的安全策略

风险评估过程

计划准备与确定评估范围

识别风险

1) 识别范围内的资产及资产所有者；
2) 识别资产的威胁；
3) 识别可能被威胁利用的脆弱点；
4) 识别资产保密性、完整性、可用性损失的影响。

分析并评价风险

1) 评估安全失效可能导致的组织业务影响，考虑因资产保密性、完整性、可用性的损失而导致的后果；
2) 根据资产的主要威胁、脆弱性、有关的影响以及已经实施的安全控制，评估安全失效发生的现实可能性；
3) 估计风险的等级 ；
4) 根据已建立的准则，判断风险是否可接受或需要处理。

—— ISO/IEC 27001:2005

风险接受准则

- 风险接受准则表示了在规定的时间内或某一行为阶段中可接受的总体风险等级，应尽可能的反映出安全需求和目标
- 必须参考
  - 工程中的安全性要求
  - 公认的安全标准和行为准则
  - 自身活动和相关事故中的经验
- 分类
  - 风险矩阵
  - ALARP原则
  - 风险比较准则

ALARP原则

- ALARP——最低合理可行原则（as low as reasonably practicable）