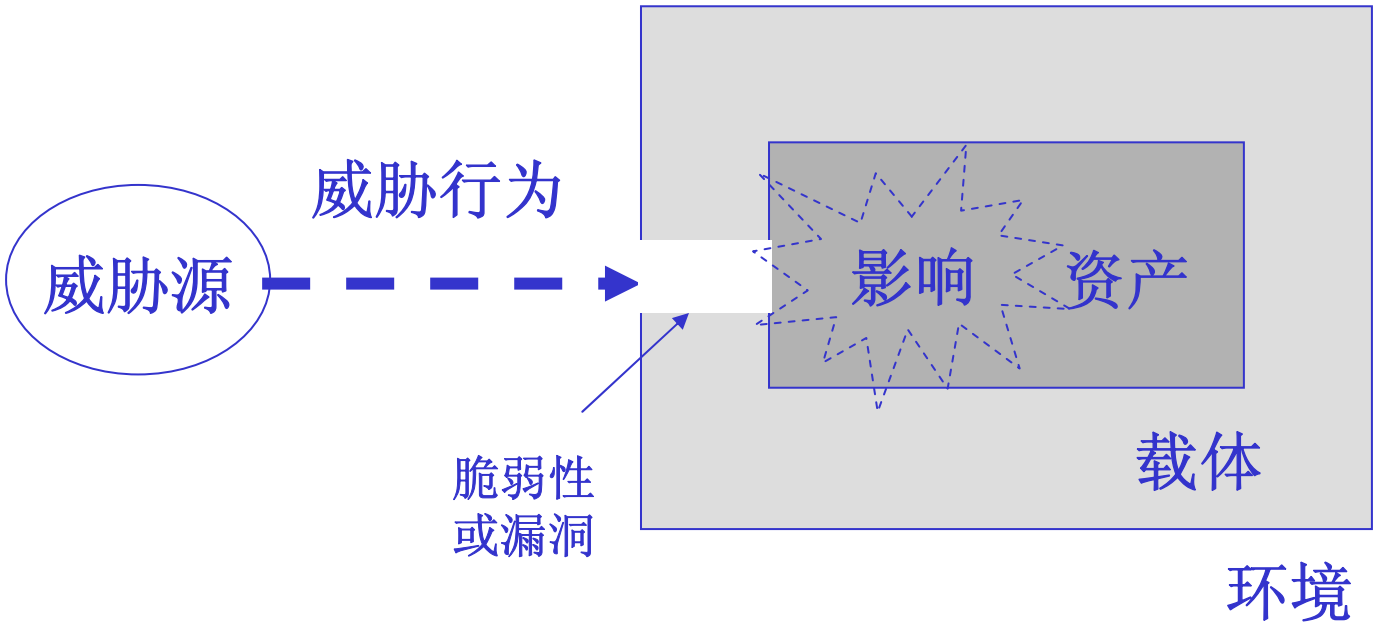
信息安全风险评估模型

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

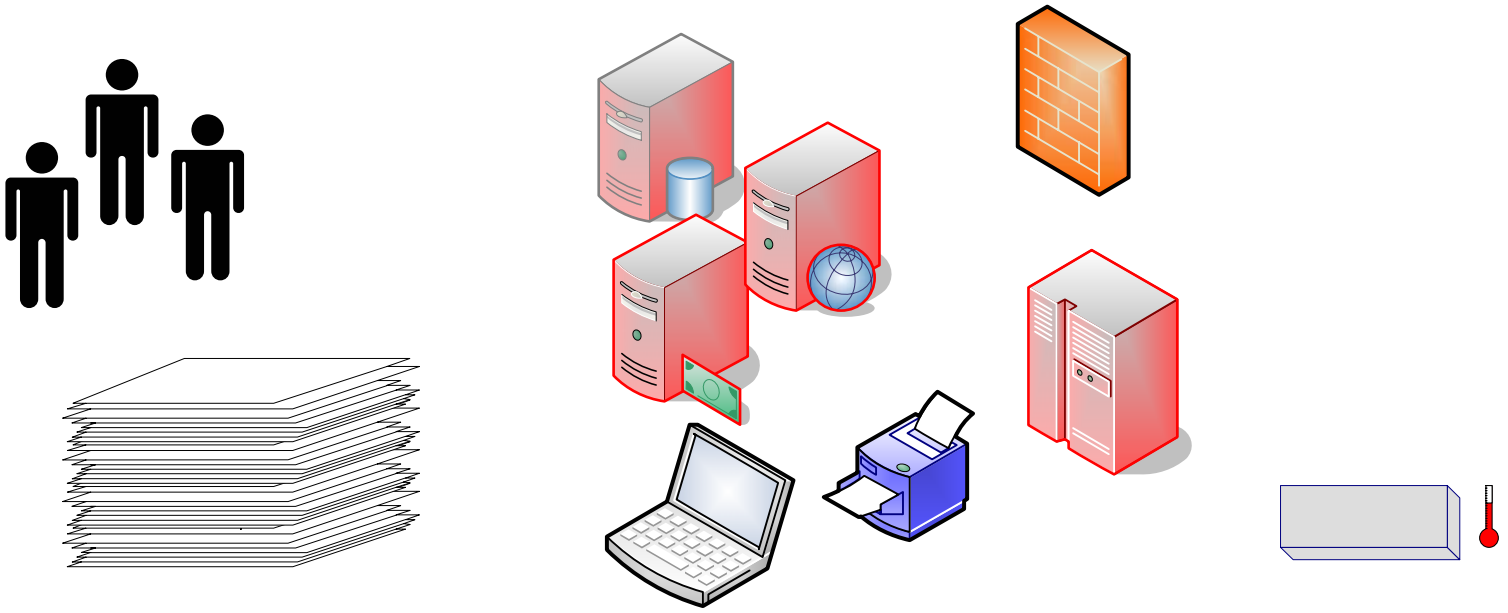
风险的定义

- **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]

资产定义

■资产

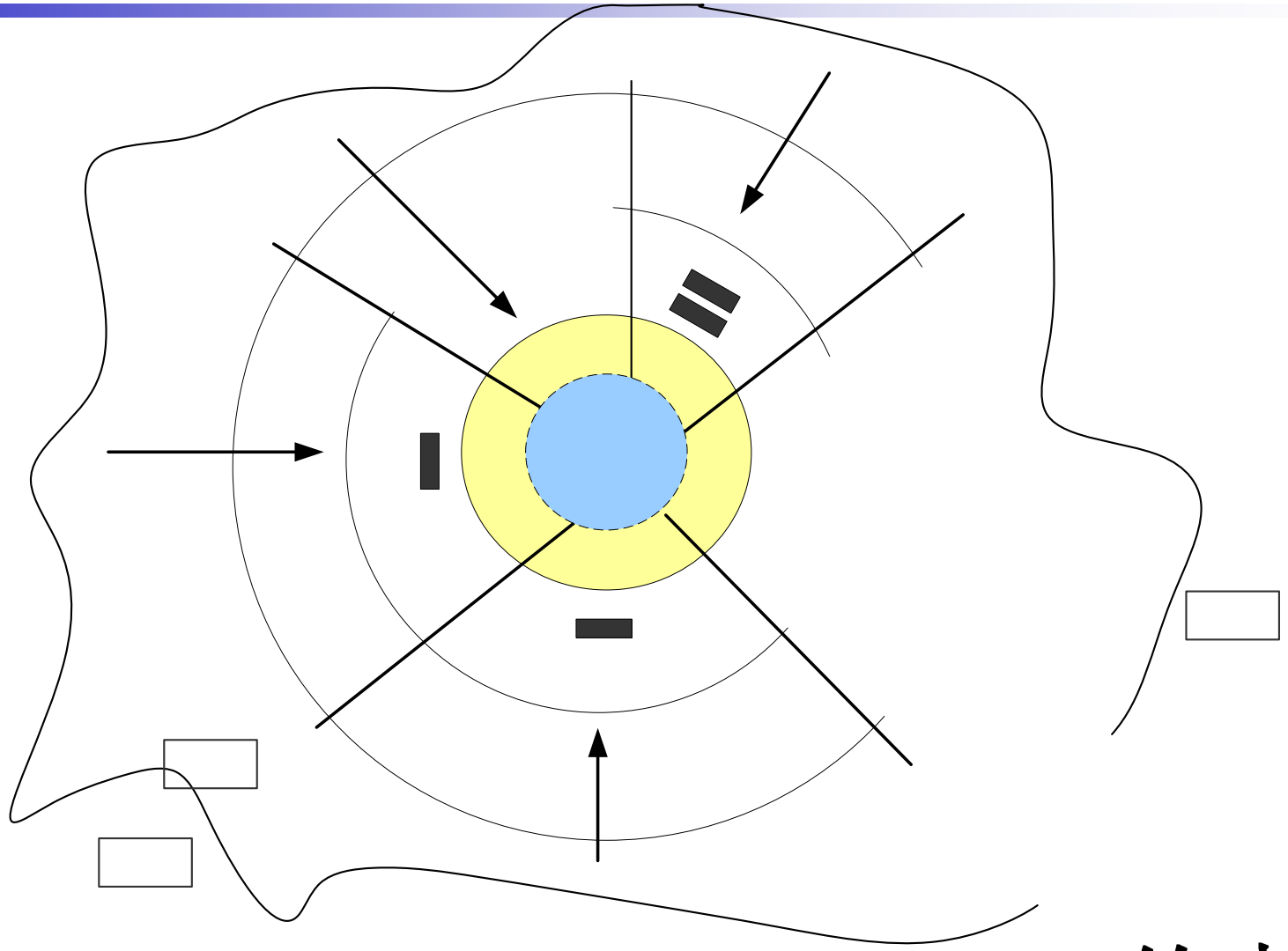
– 任何对组织有价值的事物。[ISO/IEC13335-1:2004]



威胁与脆弱性定义

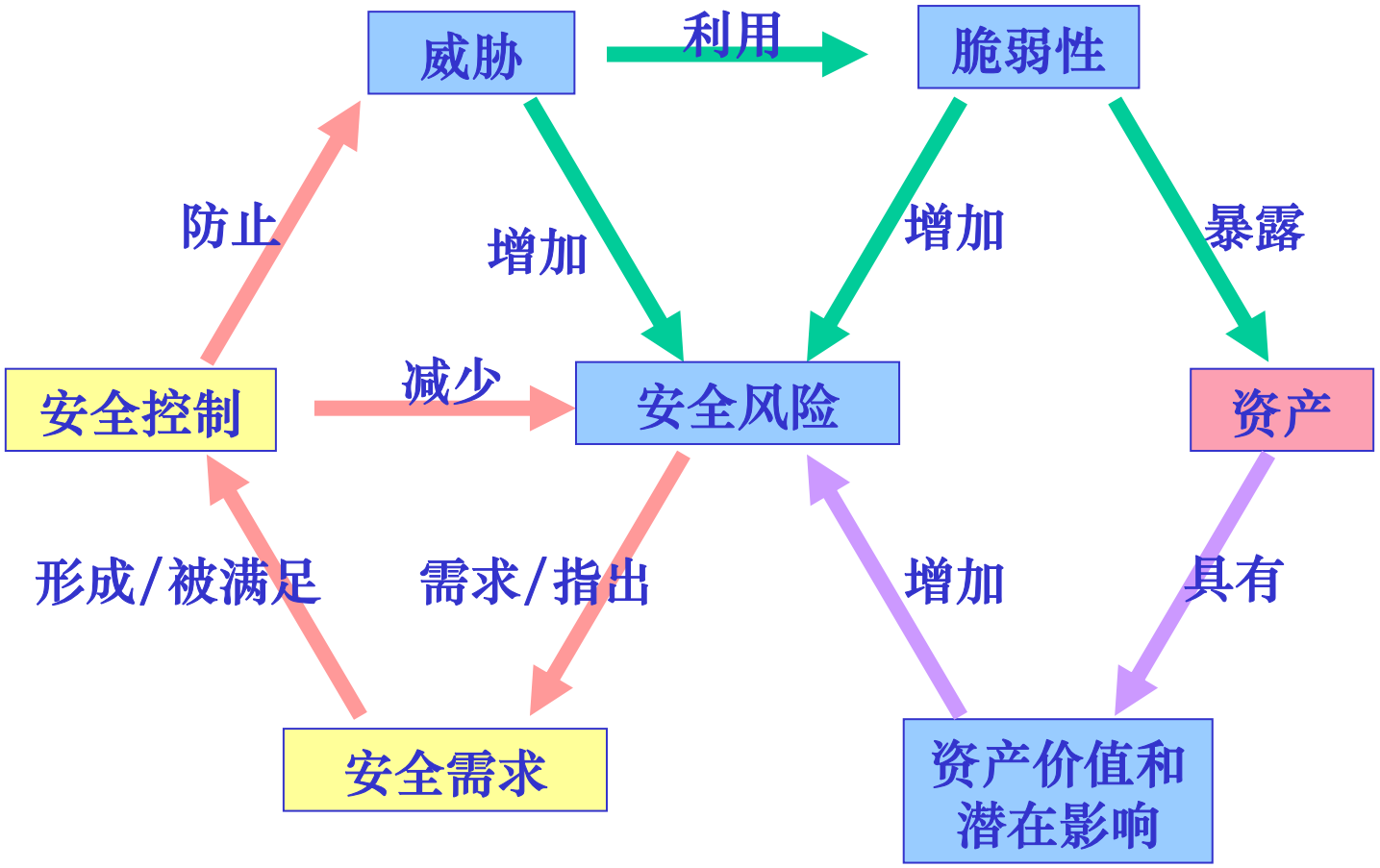
- **威胁　threat**
  - 非预期事件的潜在原因，这些事件可能对系统或组织的造成损害 [ISO/IEC TR 13335-1：2004] 。
- **脆弱性　vulnerability**
  - 可能会被一个或多个威胁所利用的一个或一组资产的弱点 [ISO/IEC TR 13335-1：2004] 。

各要素之间相互关系（ISO/IEC13335）

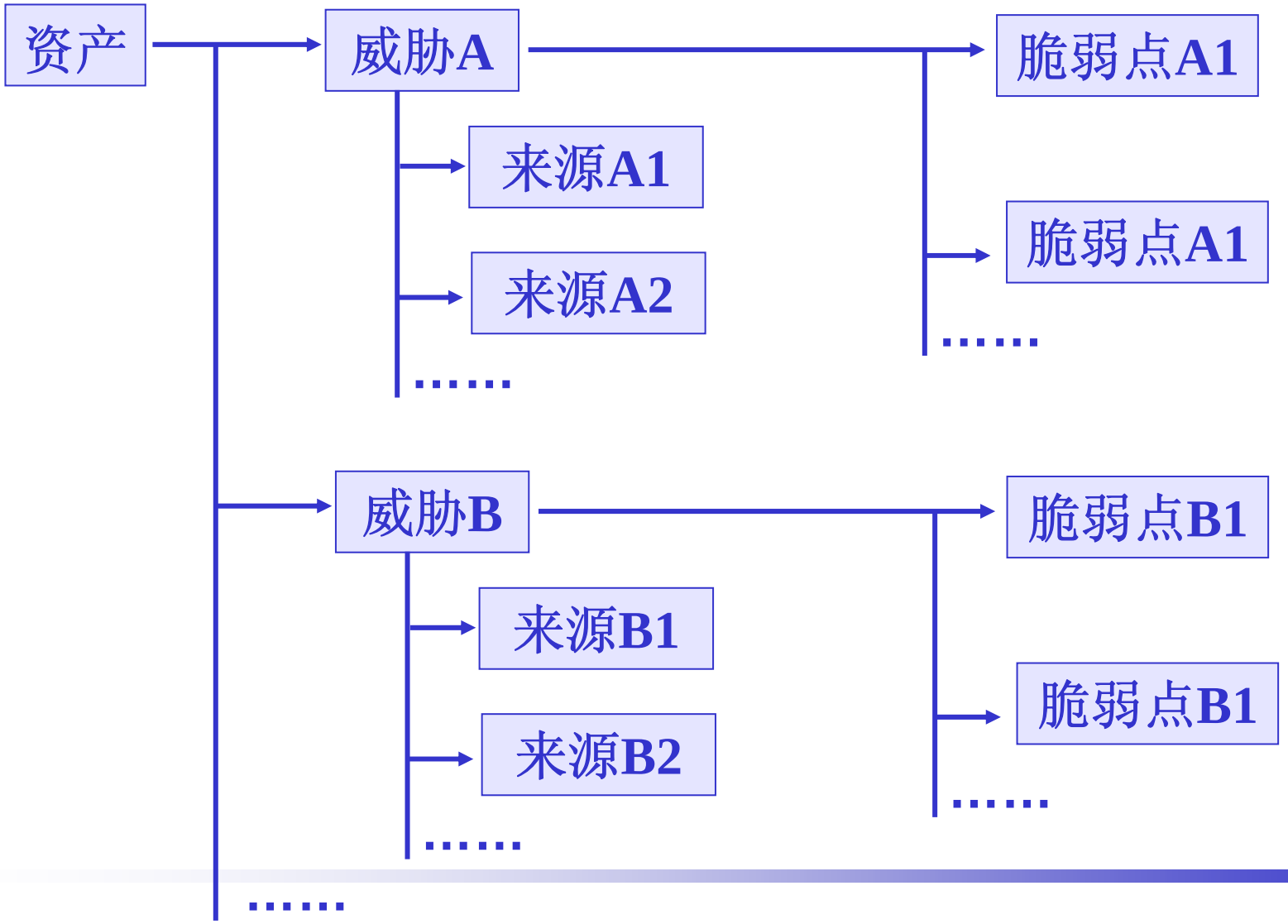


约束

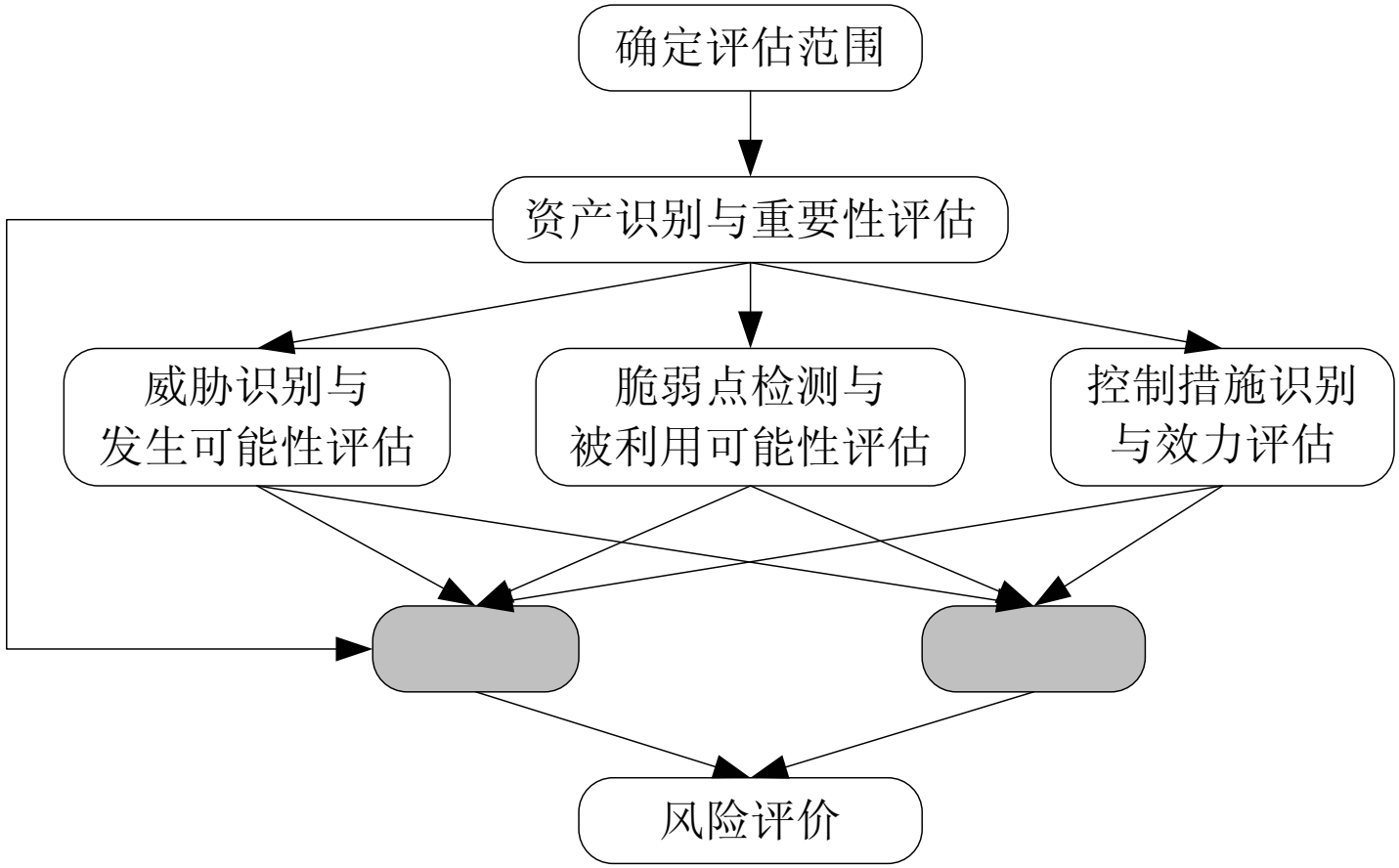
风险分析的理论关系


威胁
利用
脆弱性
防止
增加
增加
暴露
安全控制
减少
安全风险
资产
形成/被满足
需求/指出
增加
具有
安全需求
资产价值和
潜在影响

风险分析应考虑的对应关系



风险评估的一般过程


确定评估范围
资产识别与重要性评估
威胁识别与
发生可能性评估
脆弱点检测与
被利用可能性评估
控制措施识别
与效力评估
风险评价

风险评估应考虑的因素

- 信息资产及其价值
- 对这些资产的威胁，以及它们发生的可能性
- 脆弱点，以及它们别利用的可能性和造成的后果
- 已有的安全控制措施

一般的风险计算模型

- 风险是潜在损失 I 及其发生可能性 P_{TV} 的函数
- 风险概率 P_{TV} 是威胁在信息系统中实际发生的概率，因此风险概率是威胁发生概率 P_T 及脆弱点被利用概率 P_V 的函数
- 潜在损失 I 是资产相对价值 V 和 价值损失程度 C_L 的函数（C_L是一个小于等于1 大于0的系数）

信息安全风险评估方法

评估方法的不同分类

- 技术评估与整体评估
- 基于知识的评估和基于模型的评估
- 定性评估与定量评估

定性风险评估

- 使用最广泛，多依据组织面临威胁、脆弱点和控制措施等元素来决定安全风险等级
- 在评估中使用相对的等级划分，如：高，中，低
- 典型的定性风险评估方法包括
  - 过程危害分析（process hazard analysis）
  - 检查表分析（checklist analysis）
  - 失误模式与影响分析（FMEA）
  - 故障树分析（FTA）
  - 危害与可操作性分析（HazOp）

定量风险评估

- 量化两个基本元素：
  - 威胁事件发生的概率和可能造成的损失

威胁事件发生的概率 ✖ 可能造成的损失 = 年预期损失 (ALE)

  - 理论上根据ALE来计算威胁事件的风险等级，并作出相应的决策

定量风险评估的几个相关的因素

- 资产估价
- 计算单一预期损失 (SLE)
- 年发生率 (ARO)
- 年预期损失 (ALE) 的值
- 成本控制
- 确定安全投资收益 (ROSI)

资产估价

- 主观估计
- 资产的帐面价值
- 资产对于组织业务的重要性
  - 需要建立针对的评估标准
- 计算因素
  - 对于您的组织该资产所具有的总价值
  - 资产损失对财务的直接影响
  - 损失该资产的间接业务影响

对于您的组织该资产所具有的总价值

- 从财务上计算或估算资产价值。 考虑这样一个简单示例，一个通常每周七天、每天 24 小时运行，平均每小时从客户订单获得 2000 元收入的电子商务网站临时中断的影响。 您可以自信地宣布该网站的年销售收入为 17,520,000 元。

资产损失对财务的直接影响

- 如果有意简化示例并假定网站每小时的收益不变，同样的网站停用六个小时，则计算出的暴露系数为每年 0.000685%。 资产年价值乘以暴露百分比，可以预测此时直接损失是 12,000 元。 事实上，大多数电子商务网站视每天的不同时段、星期几、季节、营销活动和其他因素而有不同的收益率。 此外某些客户可能找到更喜欢从其进行购买的备选网站，因此网站可能会永久性地失去一些用户。 如果要进行精确计算并考虑所有潜在类型的损失，则计算收入损失实际上相当复杂。

损失该资产的间接业务影响

- 在此示例中，公司估计将花费 10,000 元的广告费用，以抵消该事件造成的负面影响。 此外，公司也估计损失年销售额的 1%，即 17,520 元。 通过组合额外的广告支出和年销售收入损失，可以预计本案例的间接总损失为 27,520 元。

SLE

- **SLE 指发生一次风险引起的收入损失总额。**
  - SLE 是分配给单个事件的金额，代表一个具体威胁利用漏洞时公司将面临的潜在损失。（SLE 类似于定性风险分析的影响。）
  - 通过将资产价值与暴露系数相乘 (EF) 计算出 SLE。暴露系数表示成为现实的威胁对某个资产造成的损失百分比。 如果一个网站的资产价值为 150,000 元，一场大火造成的损害占其价值的 25%，此时 SLE 为 37,500 元。 然而这是一个尽量简化的示例；可能还需要考虑其他支出。

ARO

- **ARO 是一年中风险发生的次数，应合理预估该数字。**
  - 做出这些估计相当困难；只有极少的实际数据可供使用。 迄今为止收集的数据成为少数财产保险公司持有的私有信息。 为了估计 ARO，请利用以往的经验并请教风险管理专家以及安全和业务顾问。 ARO 类似于定性风险分析的可能性，其范围从 0 （从不）至 100%（始终）。

ALE

- **ALE 是您的组织不采取任何减轻风险的措施在一年中可能损失的总金额。**
  - SLE 乘以 ARO 即可计算出该值。 ALE 类似于定量风险分析的相对级别。
  - 例如，如果此同一公司的网络场发生的火灾导致 37,500 元的损失，而火灾发生的可能性（或 ARO）的值为 0.1（表示每十年发生一次），则这种情况下的 ALE 值为 3,750 元（37,500 元 x 0.1 = 3,750 元）。

ALE（续）

- ALE 提供了一个价值，您的组织可以使用它来预算建立一种控制或安全措施以阻止此类损害 — 在本例中是每年 3,750 元或更少 — 并提供足够级别的保护需要多少成本。 为了知道需要花费多少钱来避免威胁的潜在后果的影响，量化风险的实际可能性和威胁造成的损失（以货币尺度计量）是重要的。

确定控制成本

- 确定控制成本要求精确估计
  - 购买
  - 测试
  - 部署
  - 操作
  - 维护

  各个控制措施所需的成本。

安全投资收益 (ROSI)

- **(实施控制前的 ALE） – （实施控制后的 ALE） – （年控制成本）= ROSI**
  - 例如，攻击者对 Web 服务器的威胁的 ALE 为 12,000 元，在实施了建议的安全措施后，估计 ALE 为 3,000 元。 安全措施每年的维护与操作成本为 650 元，因此，ROSI 为每年 8,350 元，如以下表达式所示：12,000 元 - 3,000 元 - 650 元 = 8,350 元。

定量风险分析的结果

- 分配给资产的货币值
- 详细的重要威胁列表
- 每个威胁发生的可能性
- 在 12 个月内每项危险对公司的潜在损失
- 推荐的安全措施、控制措施和行为

定性风险评估

- 评估相对的等级大小
  - 风险发生的可能性大小判断
  - 风险发生的后果/影响大小判断
- 通过矩阵对应的方式

可能性判断因素

- 威胁源的动机和能力
- 脆弱性的性质
- 安全控制的存在和有效性

可能性分级示例

- 1—不会发生，或者发生的概率很低（如每年最多发生一次的）
- 2—每个月都可能发生的
- 3—每天或每周都可能发生的

后果/影响判断

- 分析角度
  - 分析对业务的影响
  - 评估资产的关键性
  - 数据关键性
  - 数据敏感性
- 可分安全性的不同方面分析
  - 例如：保密性，完整性，可用性等

例

低：4-6；

中：7-9；

高：10-12；

与关键业务相关性				完整性								
				低			中			高		
				可用性			可用性			可用性		
				低	中	高	低	中	高	低	中	高
与关键业务相关性	低	保密性	低	4	5	6	5	6	7	6	7	8
			中	5	6	7	6	7	8	7	8	9
			高	6	7	8	7	8	9	8	9	10
	中	保密性	低	5	6	7	6	7	8	7	8	9
			中	6	7	8	7	8	9	8	9	10
			高	7	8	9	8	9	10	9	10	11
	高	保密性	低	6	7	8	7	8	9	8	9	10
			中	7	8	9	8	9	10	9	10	11
			高	8	9	10	9	10	11	10	11	12

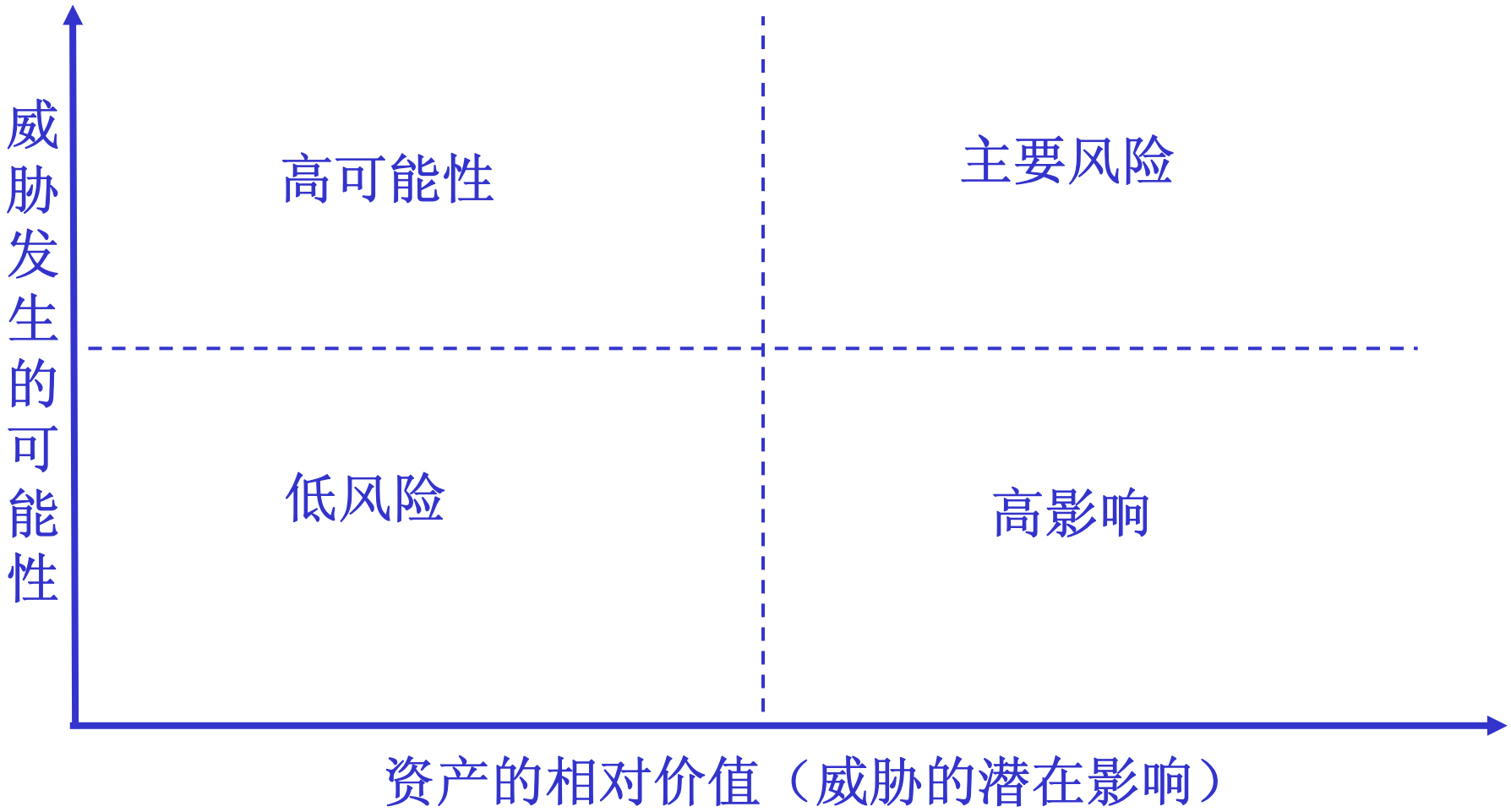
风险矩阵示例

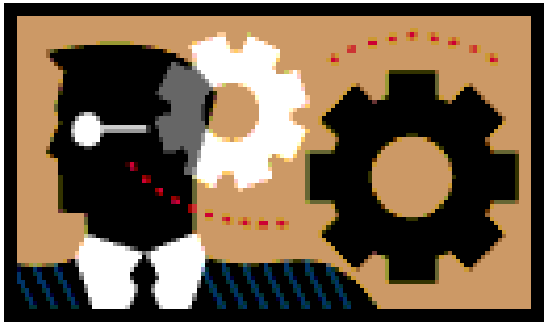
可能性	后果				
	可以忽略 1	较小 2	中等 3	较大 4	灾难性 5
A（几乎肯定）	M	H	E	E	E
B（很可能）	M	H	H	E	E
C（可能）	L	M	H	E	E
D（不太可能）	L	L	M	H	E
E（罕见）	L	L	M	H	H

注：风险的四个级别：

E：极度风险　H：高风险　M：中等风险　L：低风险

风险区域示意图





Q&A