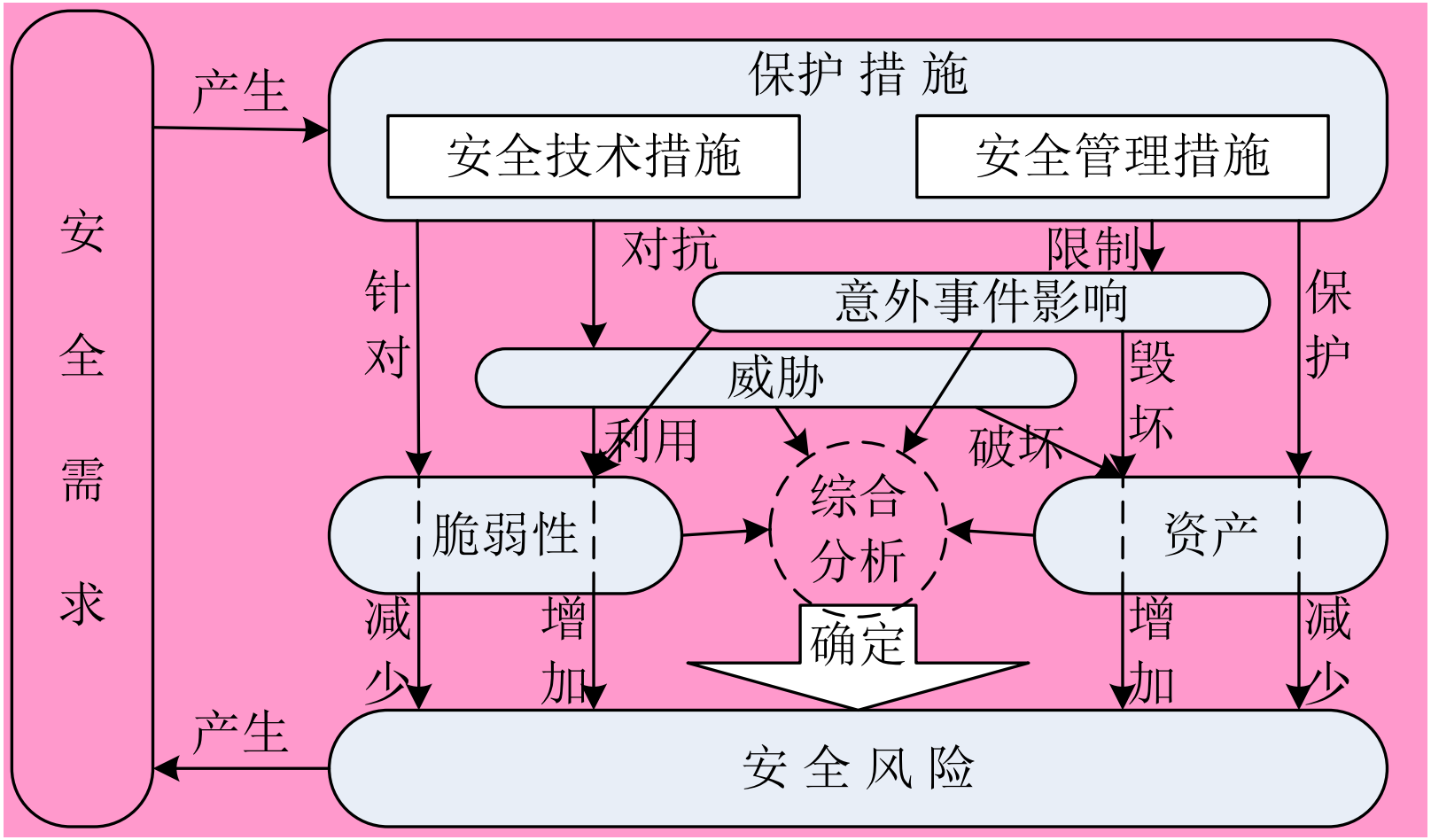
第5章 信息安全风险评估

信息安全工程与实践

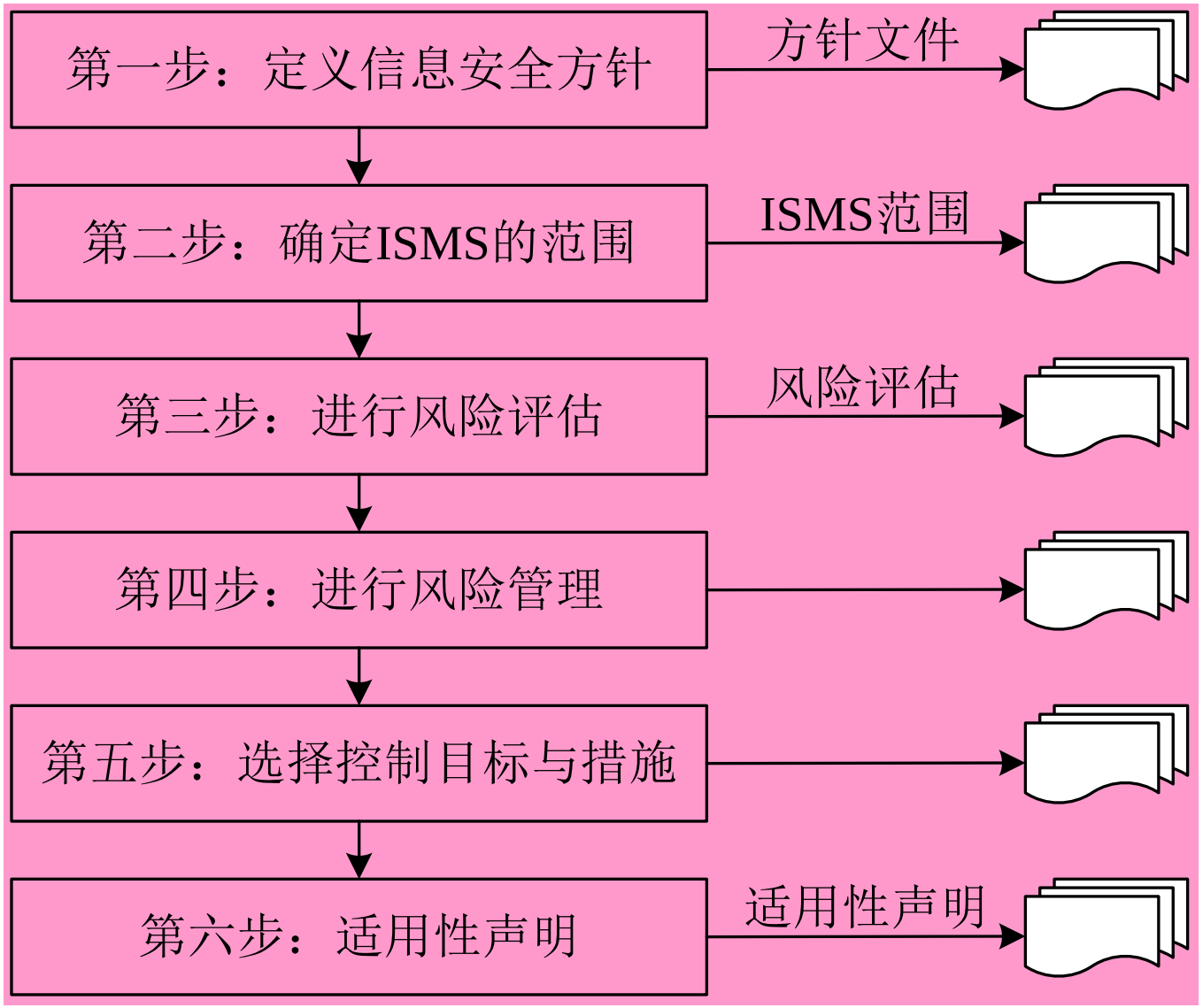
- 本章学习目标
  - **了解风险评估的意义。**
  - **明确风险评估的基本过程。**
  - **学习并熟练使用对风险评估要素的评估方法。**
  - **掌握风险值的计算算法。**

基础知识（第五章）



信息系统的主要安全因素之间的关系

基础知识（第五章）


第一步：定义信息安全方针
方针文件
第二步：确定ISMS的范围
ISMS范围
第三步：进行风险评估
风险评估
第四步：进行风险管理
第五步：选择控制目标与措施
第六步：适用性声明
适用性声明

5.1 信息安全风险评估基础

信息安全风险评估：

是参照风险评估标准和管理规范，对信息系统的资产价值、潜在威胁、薄弱环节、已采取的防护措施等进行分析，判断安全事件发生的概率以及可能造成的损失，提出风险管理措施的过程。

- 风险评估的最终目的是帮助选择安全防护措施，将风险降低到可接受的程度，提高信息安全保障能力。
- 风险评估是信息安全管理体系的核心环节，是信息安全保障体系建设过程中的重要评价方法和决策机制。

5.1 信息安全风险评估基础

信息安全风险评估的制度化和规范化

- 美国的SP 800系列、英国的BS 7799《信息安全管理指南》、德国联邦信息安全办公室《IT基线保护手册》、日本的ISMS《安全管理系统评估制度》等。

5.1 信息安全风险评估基础

信息安全风险评估的制度化和规范化

✦我国:

- 在2004年3月启动信息安全风险评估指南和风险管理指南等标准的编制工作。
- 2005年完成《信息安全评估指南》和《信息安全管理指南》的征求意见稿。
- 2006年完成《信息安全评估指南》送审稿，并分别于2007年和2009年通过了国家标准化管理委员会的审查批准成为国家标准，即GB/T 20984-2007《信息安全风险评估规范》和GB/Z 24364-2009《信息安全风险管理指南》。

5.1 信息安全风险评估基础

信息安全风险评估的目标

- 了解信息系统的体系结构和管理水平，以及可能存在的安全隐患。
- 了解信息系统所提供的服务及可能存在的安全问题。
- 了解其他应用系统与此信息系统的接口及其相应的安全问题。
- 网络攻击和电子欺骗的模拟检测及预防。
- 找出目前的安全控制措施与安全需求的差距，并为其改进提供参考。

5.1 信息安全风险评估基础

信息安全风险评估的原则

- 风险评估的原则：
  - 可控性原则：人员、工具、项目过程可控。
  - 可靠性原则：根据标准和规定，有据可查。
  - 完整性原则：全面。
  - 最小影响原则：不影响组织的正常业务。
  - 时间与成本有效原则：平衡合理。
  - 保密原则。

5.1 信息安全风险评估基础

信息安全风险评估的原则

- 风险评估是建立信息安全风险管理策略的基础。
- 有利于建立信息安全风险意识、重视信息安全问题。
- 有助于管理者对系统资源和运行状况的了解，明确系统存在的弱点。
- 在设计阶段考虑风险评估，确认潜在损失。明确安全需求，事先控制比事后控制更节省成本。

5.1 信息安全风险评估基础

信息安全风险评估的制度化和规范化

✦我国:

- 在2004年3月启动信息安全风险评估指南和风险管理指南等标准的编制工作。
- 2005年完成《信息安全评估指南》和《信息安全管理指南》的征求意见稿。
- 2006年完成《信息安全评估指南》送审稿，并分别于2007年和2009年通过了国家标准化管理委员会的审查批准成为国家标准，即GB/T 20984-2007《信息安全风险评估规范》和GB/Z 24364-2009《信息安全风险管理指南》。

5.1 信息安全风险评估基础

信息安全风险评估的意义

- 一是更准确地认识风险。
- 二是保证目标规划的合理性和计划的可行性。
- 三是合理选择风险对策，形成最佳风险对策组合。

5.2 信息安全风险评估因素

- 风险评估是组织进一步确定信息安全需求和改进信息安全策略的**重要途径**，属于组织ISMS策划的**过程**。
- 信息系统是信息安全风险评估的对象，信息安全风险评估的基本要素主要包括：**资产、威胁、脆弱性、安全风险、影响、安全控制措施**以及**安全需求**。

5.2 信息安全风险评估因素

风险评估的相关因素1——资产

- **资产**:有价值的信息或资源，是策略保护的对象。
- 资产安全特性的三个要素：信息资产的**机密性、完整性和可用性。**
- 资产能够以多种形式存在，包括有形的或无形的、硬件或软件、文档或代码，以及服务或形象等诸多表现形式。

5.2 信息安全风险评估因素

风险评估的相关因素1——资产

- 资产分类方法

软件	系统软件、应用软件、源程序
硬件	系统和外围设备、安全设备、其他技术设备等
服务	信息服务、网络通信服务、办公服务、其他技术服务
流程	包括IT和业务标准流程、IT和业务敏感流程
数据	在传输、处理和存储状态的各种信息资料
文档	纸质的各种文件、传真、财务报告、发展计划、合同等
人员	掌握重要信息和核心业务的人员、其他可以访问信息资产的组织外用户
其他	企业形象与声誉、客户关系等

5.2 信息安全风险评估因素

风险评估的相关因素2——威胁

- **威胁**:潜在的可能导致信息安全风险事件并对组织及资产造成损害的因素。
- 威胁必须利用资产固有的脆弱性才能完成对资产的损害，它可能来自人为或非人为的、可能是故意或无意的、可能是来自环境的。

5.2 信息安全风险评估因素

风险评估的相关因素2——威胁

- 威胁分类方法

软硬件故障	设备硬件故障、存储介质故障、通讯链路中断、软件缺陷等
物理环境影响	对系统正常运行造成影响的物理环境问题和自然灾害
物理攻击	通过物理的接触造成对软件、硬件或数据的破坏
恶意代码	在计算机系统上能执行恶意任务的程序代码
越权或滥用	对信息、系统、网络和网络服务的非授权访问、滥用权限
网络攻击	利用工具和技术通过网络对信息系统进行攻击和入侵
泄密	信息泄露给不应了解的人
篡改	非法修改信息，破坏信息的完整性
抵赖	否认收到的信息或所进行过的操作和交易等
管理不到位	安全管理无法落实或不到位
无作为性失误	应该执行而没有执行相应操作，或无意执行了错误操作等

5.2 信息安全风险评估因素

风险评估的相关因素3——脆弱性

- **脆弱性**:也被称为弱点评估，是信息安全风险评估中的重要内容。
- 弱点是资产本身具有的，是与信息资产有关的造成风险的内因。
- 弱点是资产本身固有的，但它本身不会造成损失，它只是一种可能被威胁利用而造成损失的条件或环境。
- 脆弱性分为技术脆弱性和管理脆弱性。

5.2 信息安全风险评估因素

风险评估的相关因素3——脆弱性

- 脆弱性分类方法

技术脆弱性	未安装杀病毒软件	能发生系统信息被病毒侵害
	使用口令不当	能导致系统信息的非授权访问
	无保护的外网连接	能破坏联网系统中存储与处理信息的安全性
管理脆弱性	安全培训不足	能造成用户缺乏足够的安全意识，或产生用户错误
	机房钥匙管理不严	能形成资产的直接丢失或物理损害等
	离职人员权限未撤消	能引起泄密或业务活动受到损害

5.2 信息安全风险评估因素

风险评估的相关因素4——安全风险

- **安全风险:**威胁可以利用体系的脆弱性，从而直接或间接造成资产损害，导致一系列不期望发生的安全事件。
- 资产、威胁和脆弱性都是信息安全风险的**基本要素**，是信息安全风险存在的基本条件。
  - 资产是威胁攻击或损害的对象，威胁只能找到系统的脆弱性，将其作为可利用的切入点，才能触发安全事件。

$$R = f(a, t, v)$$

其中R表示安全风险，a表示资产，t表示威胁，v表示脆弱性。

5.2 信息安全风险评估因素

风险评估的相关因素5——影响

- **影响**:资产是威胁攻击或损害的对象，威胁只能找到系统的脆弱性，将其作为可利用的切入点，才能触发安全事件。
- 影响的后果表现形式：
  - **直接形式**：如物理介质或设备的损坏、人员的损伤、资金的损失等。
  - **间接形式**：如公司信用和名誉受损、市场份额减少、承担法律责任等

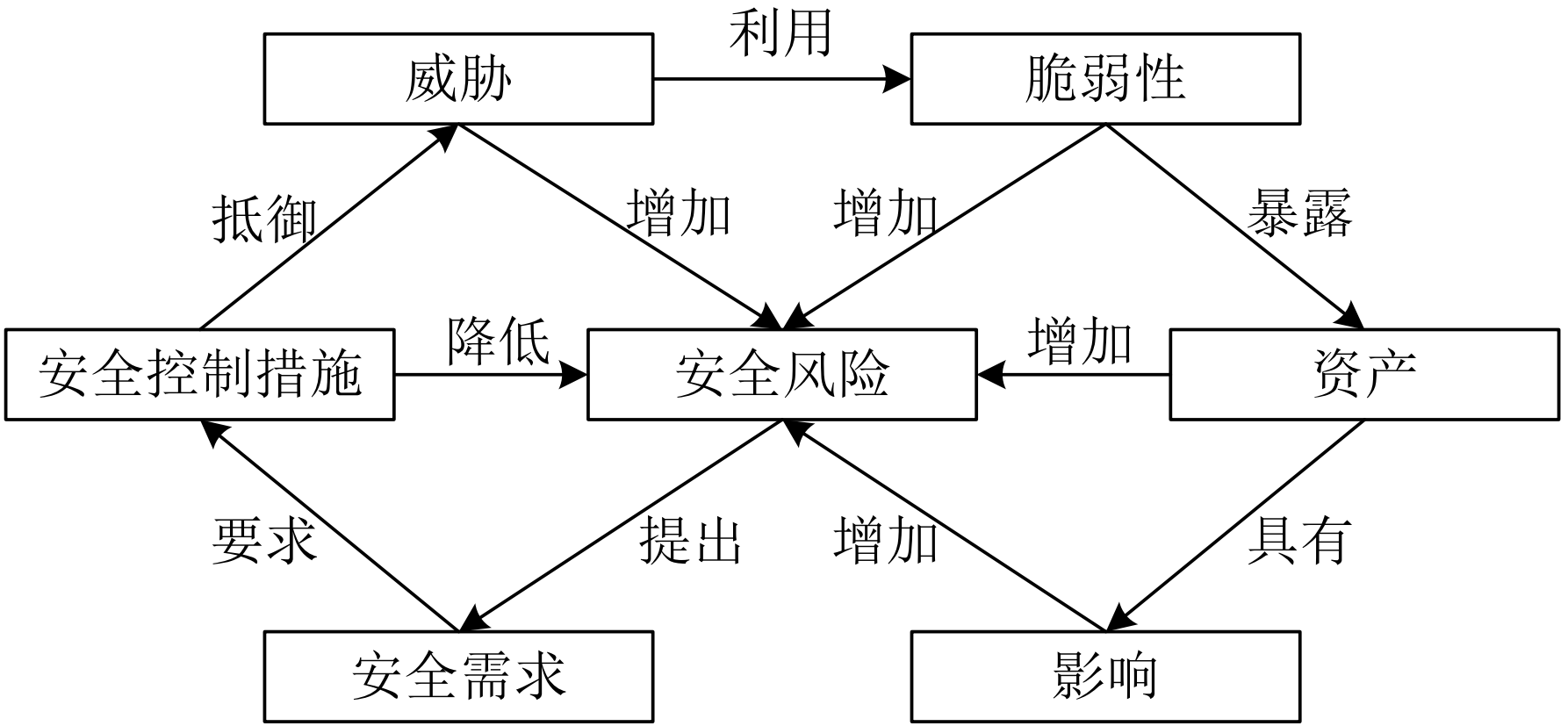
5.2 信息安全风险评估因素

风险评估的相关因素7——安全需求

- **安全需求**:为保证组织正常运作而在安全控制措施方面所提出的要求。
- 安全需求来源于以下三个方面:
  - 风险评估的要求。
  - 法律、法规和合同的要求。
  - 业务规则、业务目标和业务信息处理的要求。

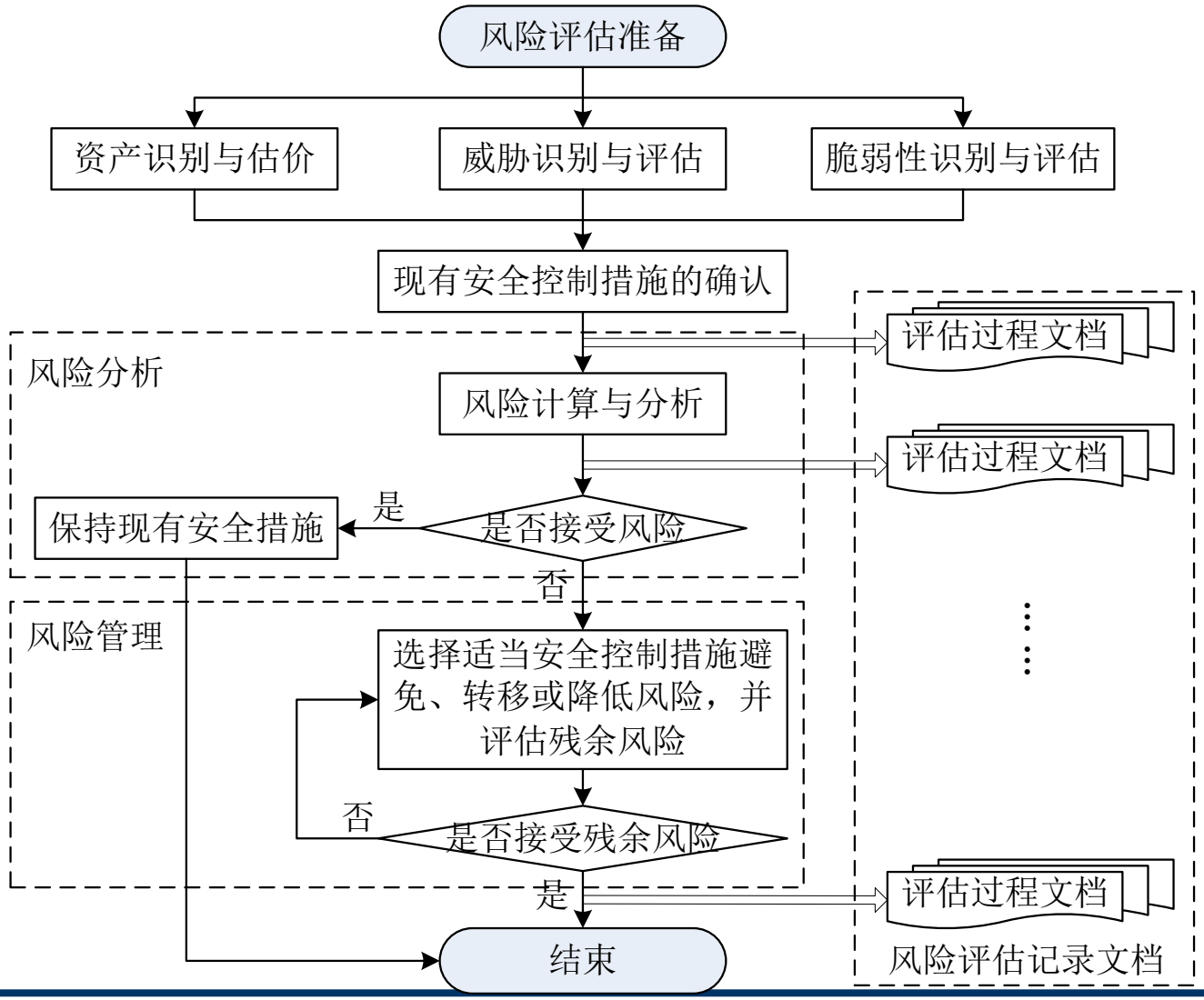
5.2 信息安全风险评估因素

各个风险因素之间的关系



5.3 信息安全风险评估过程

信息安全风险评估的过程



5.3 信息安全风险评估过程

风险评估准备

- **风险评估准备,**是整个风险评估过程有效性的**保证。**应做好以下准备工作:
  - 确定信息安全风险评估的目标。
  - 确定信息安全风险评估的范围。
  - 组建适当的评估管理与实施团队。
  - 进行系统调研。
  - 确定信息安全风险评估的依据和方法。制定信息安全风险评估方案。
  - 获得最高管理者对信息安全风险评估工作的支持。

5.3 信息安全风险评估过程

- 识别并评估资产
  - 在信息安全风险评估的过程中，应清晰地识别其所有的信息安全的基本要素，不能遗漏，划入风险评估范围和边界内的每一项都应该被确认和评估。

5.3 信息安全风险评估过程

识别并评估资产

✦资产识别

- 资产识别,是风险识别的必要环节，其任务是对评估对象所涉及的资产进行详细的标识，并建立资产清单。
- 主要方法有访谈、现场
  - 识别软件和硬件。
  - 识别服务、流程、数据、文档、人员和其他。

名称、IP地址、MAC地址、资产类型、产品序列号、、制造商、型号或编号、版本号、物理位置、逻辑位置、控制实体等

姓名/ID/职位、入职时间、技能

服务的描述、类型、功能、提供者、面向的对象、满足服务的附加条件

流程的描述、能、相关的软/硬件/网络要参考资料的存位置、更新数的存储位置

数据的类别、数据结构及范围、所有者/创建者/管理者、存储位置、备份流程

文档的描述、名称、密级、制定时间、制定者/管理者

5.3 信息安全风险评估过程

识别并评估资产

✦ 资产定级

- 资产清单，必须反映每一项信息资产的敏感度和安全等级，并根据这些属性对资产制定一项分类方案，同时确定分类对组织的风险评估计划是否有意义。
- 可参考的资产分类方案：
  - ✓ 按机密性分类、按完整性分类、按可用性分类。
- 每一种分类方案中可按从低到高的要求进行级别标识，即对每一项分类都指明特定的信息资产的保护等级。

5.3 信息安全风险评估过程

识别并评估资产

✦ 评价资产的价值

- 提出以下问题帮助确定资产的影响力和资产的价值：
  - ✓ 哪种信息资产对组织的成功最为重要？
  - ✓ 哪种信息资产能带来最大收益？
  - ✓ 哪种信息资产的更新花费最多？
  - ✓ 哪种信息资产的保护费用最昂贵？
  - ✓ 哪种信息资产的损失、损坏或暴露出缺陷最易造成麻烦，或导致损失？

5.3 信息安全风险评估过程

识别并评估威胁

✦ 威胁识别

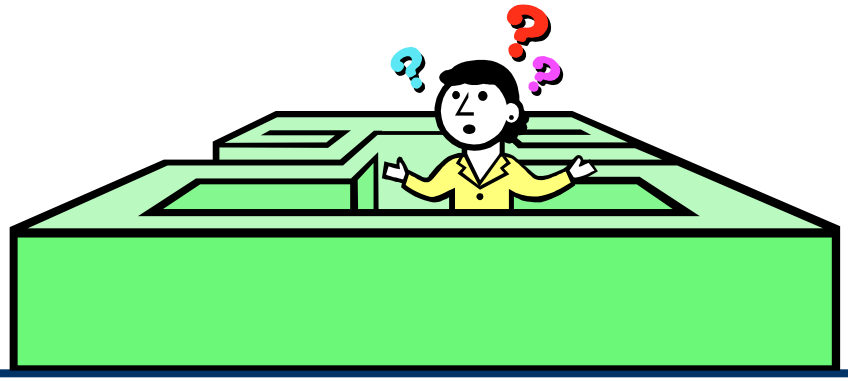
- 威胁识别的任务是对资产面临的威胁进行全面的标识。
- 威胁的有关信息可以从信息安全管理体系的参与人员和相关业务流程处收集获得。
  - ✓ 典型的，一项资产可能受到多个威胁的影响，而一个威胁可能作用于不同的资产。
- 威胁源可能有多个，主要来源于环境因素与人为因素。
- 威胁识别活动中，可能会用到的方法有以下几种：IDS 采样分析、日志分析、人员访谈、人工分析、安全策略文档分析、安全审计等。

5.3 信息安全风险评估过程

识别并评估威胁

✦ 威胁评估

- 威胁评估是对威胁出现的频率和强度进行评估，是风险评估的重要环节。
- 提出以下问题帮助理解威胁及其对资产的潜在影响：
  - ✓ 当前哪些威胁对组织的信息资产产生了威胁？
  - ✓ 哪种威胁会对组织的信息资产带来最严重的危害？



5.3 信息安全风险评估过程

识别并评估威胁

✦ 威胁评估

- ➢ 识别出威胁的原因、目标后，要根据经验和有关统计数据来分析威胁出现的频率、强度和破坏力，考虑：
  - ✓ 根据经验和统计规律，估计出威胁多长时间发生一次，即威胁发生的频度。
  - ✓ 研究攻击者的动机、需具备的能力、所需的资源、资产的吸引力的大小和脆弱性程度，是否有预谋的威胁。
  - ✓ 近一两年来国际组织发布的对于整个社会或特定行业的威胁及其频率统计，以及发布的威胁预警。
  - ✓ 研究地理因素，如是否靠近化工厂、是否处于极端天气高发区等。

5.3 信息安全风险评估过程

识别并评估威胁

✦ 威胁评估

➢ 威胁评估的结果一般都是定性的。GB/T 20984—2007《信息安全风险评估规范》将威胁频度等级划分为五级。

等 级	标 识	定 义
5	很高	出现的频率很高(或≥1次/周);或在大多数情况下几乎不可避免;或可证实经常发生过
4	高	出现的频率较高(或≥1次/月);或在大多数情况下很有可能会发生;或可证实多次发生过
3	中	出现的频率中等(或>1次/半年);或在某种情况下可能会发生;或被证实曾经发生过
2	低	出现的频率较小;或一般不太可能发生;或没有被证实发生过
1	很低	威胁几乎不可能发生;或可能在非常罕见和例外的情况下发生

5.3 信息安全风险评估过程

识别并评估脆弱性

✦ 脆弱性识别

- 脆弱性可以从技术和管理两个方面进行分类，涉及物理层、网络层、系统层、应用层、管理层等各个层面的安全问题。
  - ✓ 在技术脆弱性评估方面主要是通过远程和本地两种方式进行系统扫描、对网络设备和主机进行人工抽查。
- 脆弱性识别所采用的方法主要有：问卷调查、人员问询、工具扫描、手动检查、文档审查、渗透测试等。

5.3 信息安全风险评估过程

识别并评估脆弱性

✦ 脆弱性识别

类 型	识别对象	识 别 内 容
技术脆弱性	物理环境	从机房场地、机房防火、机房供配电、机房防静电、机房接地与防雷、电磁防护、通信线路的保护、机房区域防护、机房设备管理等方面识别
	网络结构	从网络结构设计、边界保护、外部访问控制策略、内部访问控制策略、网络设备安全配置等方面识别
	系统软件	从补丁安装、物理保护、用户帐号、口令策略、资源共享、事件审计、访问控制、新系统配置、注册表加固、网络安全、系统管理等方面识别
	应用中间件	从协议安全、交易完整性、数据完整性等方面识别
	应用系统	从审计机制、审计存储、访问控制策略、数据完整性、通信、鉴别机制、密码保护等方面识别
管理脆弱性	技术管理	从物理和环境安全、通信与操作管理、访问控制、系统开发与维护、业务持续性等方面识别
	组织管理	从安全策略、组织安全、资产分类与控制、人员安全、符合性等方面识别

5.3 信息安全风险评估过程

识别并评估脆弱性

✦ 脆弱性评估

- 根据对资产的损害程度、技术实现的难易程度、弱点的流行程度，采用等级区分方式对已识别的脆弱性的严重程度进行赋值评估。
- 衡量资产的脆弱性还应参考技术管理和组织管理脆弱性的严重程度。
- 脆弱性严重程度可以进行等级化，等级代表资产脆弱性严重程度的高低。等级越高，脆弱性的程度越高。

5.3 信息安全风险评估过程

识别并评估脆弱性

✦ 脆弱性评估

➢ 脆弱性评估的结果一般也是定性的。GB/T 20984—2007《信息安全风险评估规范》将脆弱性严重程度划分为5级。

等 级	标 识	定 义
5	很高	如果被威胁利用，将对资产造成完全损害
4	高	如果被威胁利用，将对资产造成重大损害
3	中	如果被威胁利用，将对资产造成一般损害
2	低	如果被威胁利用，将对资产造成较小损害
1	很低	如果被威胁利用，将对资产造成的损害可以忽略

5.3 信息安全风险评估过程

确定安全控制措施

- 安全控制措施可以分为**预防性安全控制措施**、**检查性安全控制措施**和**纠正性安全控制措施**。
- 安全控制措施的确认应评估其有效性，即是否真正地降低了系统的脆弱性，抵御了威胁。
  - 有效的安全控制措施：继续保持。
  - 不适当的安全控制措施：取消、修正或替代。

5.3 信息安全风险评估过程

风险分析

✦计算公式

➢ $R = R(A, T, V)\text{-}Rc = R(P(T, V), I(Ve, Sz)) - Rc$

R ——安全风险

A ——资产

T ——威胁

V ——脆弱性

可简化为：

$$R = R(P(T, V), I(Ve, Sz))$$

Rc ——已有控制所所减少的风险

Ve ——安全事件所作用的资产价值

Sz ——脆弱性严重程度

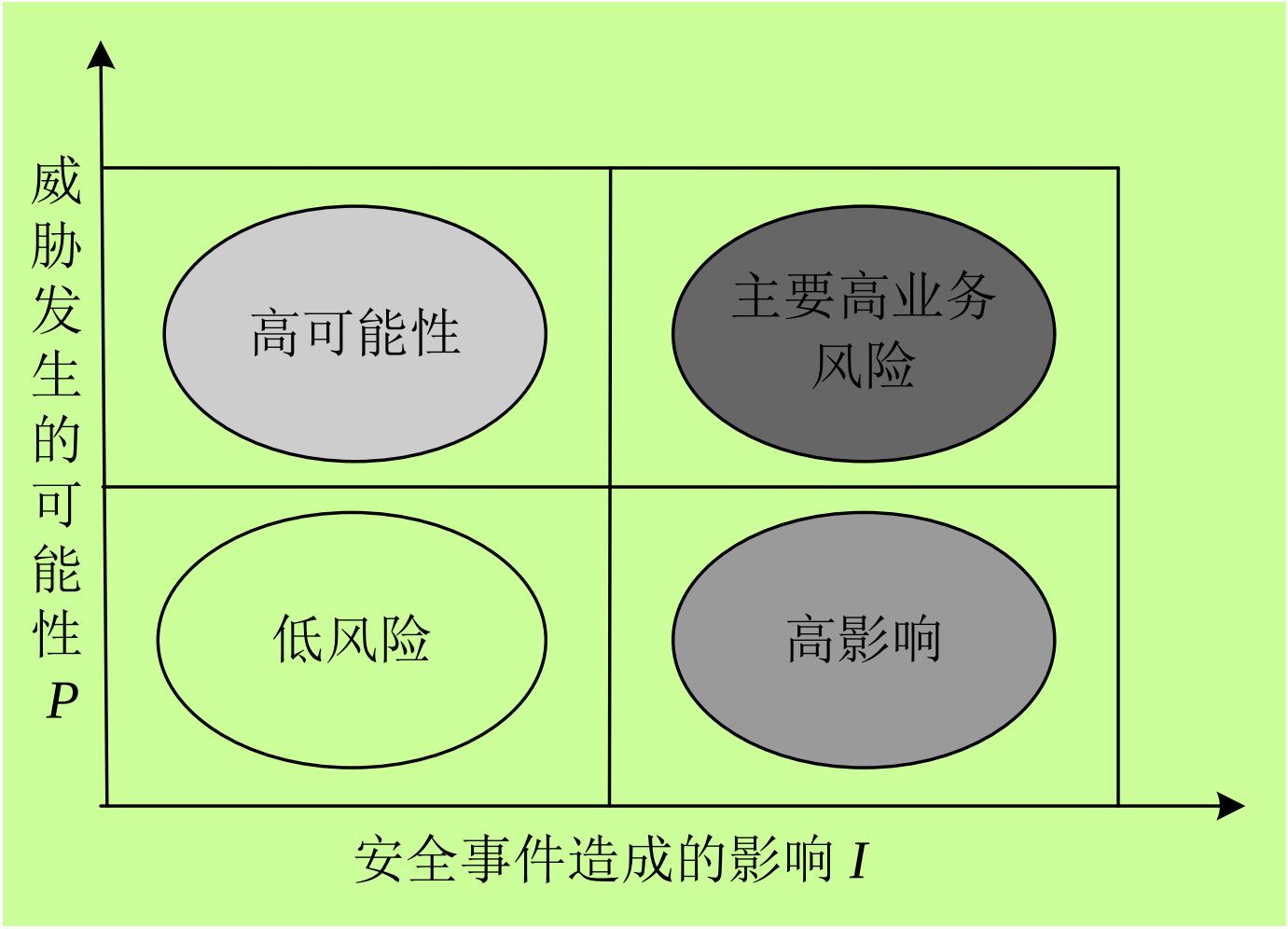
P ——威胁利用资产的脆弱性导致安全事件的可能性

I ——安全事件发生后造成的影响

5.3 信息安全风险评估过程

风险分析

✦ 函数图



5.3 信息安全风险评估过程

风险处理

✦安全控制措施的选择

- ➢ 当选择安全控制措施时，要考虑以下因素：
  - ✓ 控制的成本费用：安全平衡原则。
  - ✓ 控制的可用性。
  - ✓ 已存在的控制：补充、兼容。
  - ✓ 控制功能的范围和强度。

✦ 最终结果只能是降低风险到可接受的水平，或做出正式的管理决策接受风险，其目的是为了控制风险。

✦ 控制风险的方法：避免风险、转移风险、降低风险和接受风险。

5.3 信息安全风险评估过程

风险处理

✦ 风险规避

- 通过不使用面临风险的资产来避免风险。
- 风险规避通常在无法接受风险的损失，又难以通过控制措施降低风险的情况下使用。
- 通过以下方式进行规避：

✓ 政策的应用。

✓ 培训和教育的应用。

✓ 打击威胁。

✓ 实施安全技术。

5.3 信息安全风险评估过程

风险处理

✦转移风险

- 通过将面临风险的资产或其价值进行安全转移来避免或降低风险。
- 通常只有当风险不能被降低或避免、且被第三方（被转嫁方）接受时才被采用。
- 转移风险，是一种风险控制方法，是组织在无法避免风险时，或者减少风险很困难，成本也很高时，将风险转向其他的资产、过程或组织。
- ✓ 可通过修改配置模型、执行项目外包并完善合同、购买保险等方式实现。

5.3 信息安全风险评估过程

风险处理

✦降低风险

- 降低风险，是一种风险控制方法，主要是通过实施各种预防和应急响应计划来减少因脆弱性而带来的攻击对资产的损害。
- 主要包括：
  - ✓ 事件响应计划。
  - ✓ 灾难恢复计划。
  - ✓ 业务持续性计划。

5.3 信息安全风险评估过程

风险处理

✦ 接受风险

- 接受风险是一个对残余风险进行确认和评价的过程。
- 当完成了以下工作，接受风险才是一项正确的战略：
  - ✓ 确定影响信息资产的风险等级。
  - ✓ 评估发生威胁和产生脆弱性的可能性。
  - ✓ 近似地计算了该类攻击每年发生的几率。
  - ✓ 估计攻击所造成的潜在损失。
  - ✓ 进行了全面的成本-效益分析。
  - ✓ 评估使用的每一项安全控制措施。

5.3 信息安全风险评估过程

风险评估记录文档

- 风险评估方案。
- 风险评估程序。
- 资产识别清单。
- 重要资产清单。
- 威胁列表。
- 脆弱性列表。
- 已有安全控制措施确认表。
- 风险评估报告。
- 风险处理计划。
- 风险评估记录。

文档档发布前是得到批准的

文档的更改和修订状态是可识别的

文档的分发得到适当的控制

防止作废文档的非预期使用

规定文档的标识、存储、保护、检索、保存期限以及处置所需的控制

5.4 风险计算算法

风险计算方法

- 将风险要素按照组合方式使用具体的计算方法进行计算，即可得到风险值。
- 风险值计算涉及的要素一般为资产、威胁和脆弱性，即由威胁和脆弱性确定安全事件发生的可能性，由资产和脆弱性确定安全事件的影响，以及由安全事件发生的可能性和安全事件的影响来确定风险值。
- 常用的计算方法为矩阵法和相乘法。

5.4 风险计算算法

风险计算方法

- **假设：有以下信息系统中资产面临威胁利用脆弱性的情况。**
- **共有两项重要资产：A_1和A_2；**
  - ✓ 资产A_1面临两个主要威胁T_1和T_2；资产A_2面临一个主要威胁T_3；
  - ✓ 威胁T_1可以利用资产A_1存在的一个脆弱性V_1；
  - ✓ 威胁T_2可以利用资产A_1存在的一个脆弱性V_2；
  - ✓ 威胁T_3可以利用资产A_2存在的一个脆弱性V_3；
  - ✓ 资产价值分别是：资产$A_1=2$，资产$A_2=4$；
  - ✓ 威胁发生的频率分别是：威胁$T_1=2$，威胁$T_2=4$，威胁$T_3=3$；
  - ✓ 脆弱性严重程度分别是：脆弱性$V_1=3$，脆弱性$V_2=5$，脆弱性$V_3=4$。

5.4 风险计算算法

风险计算方法

✦矩阵法

➢ 矩阵法概述

- ✓ 矩阵法主要适用在由两个要素值确定一个要素值时。
- ✓ 首先需要确定二维计算矩阵，然后将两个元素的值在矩阵中进行比对，行列交叉处即为所确定的计算结果，即：

$$z = f(x, y)$$

5.4 风险计算算法

风险计算方法

✦矩阵法

➢ 矩阵法计算示例

- 计算资产风险值

这里以资产 A_1 为例使用矩阵法计算其风险值

计算安全事件发生的可能性。威胁发生频率：威胁 T_2=4；脆弱性严重程度：脆弱性 V_2=5。

5.4 风险计算算法

- 计算资产风险值

首先根据矩阵法原理，构建安全事件发生可能性的矩阵。

脆弱性严重程度 威胁发生频率	1	2	3	4	5
1	2	4	7	10	13
2	3	6	10	13	16
3	5	9	12	16	19
4	7	11	14	18	22
5	8	12	17	20	25

由矩阵可确定安全事件发生的可能性为22

5.4 风险计算算法

- 计算资产风险值

在构建风险矩阵前，先对安全事件发生的可能性进行等级划分。

安全事件发生可能性的值	1～5	6～11	12～16	17～21	22～25
发生可能性的等级	1	2	3	4	5

可知安全事件发生可能性的等级为5

5.4 风险计算算法

- 计算资产风险值

计算安全事件的影响。

资产价值：资产 A_1=2；脆弱性严重程度：脆弱性 V_2=5。先根据矩阵法原理，构建安全事件影响的矩阵

脆弱性严重程度 资产价值	1	2	3	4	5
1	2	4	7	11	14
2	3	6	9	13	16
3	5	9	12	16	19
4	7	11	14	18	22
5	9	12	17	21	25

可知安全事件的影响值为16

5.4 风险计算算法

- 计算资产风险值

此时安全事件影响等级为3；综合前两项的计算风险值。

此时，已计算出：安全事件发生可能性=5，安全事件的影响=3。

同样，可根据矩阵法原理，构建风险矩阵。

安全事件发生可能性安全事件影响	1	2	3	4	5
1	3	6	9	12	16
2	5	7	10	13	18
3	7	9	12	16	21
4	9	11	15	20	23
5	10	12	17	22	25

由矩阵可确定风险值为21。

5.4 风险计算算法

- 获得结果

先确定风险等级划分的标准。

风险值	1～5	6～12	13～17	18～22	23～25
风险等级	1	2	3	4	5

以此类推，可计算出两个重要资产的其他风险值，并确定出各自的风险等级结果。

资产	威胁	脆弱性	风险值	风险等级
资产A1	威胁T1	脆弱性V1	7	2
	威胁T2	脆弱性V2	21	4
资产A2	威胁T3	脆弱性V3	15	3

5.5 典型风险评估算法

风险评估算法

- 从计算方法上来看，有定性的方法、定量的方法和半定量的方法；从实施手段来区分，有基于树的技术及动态系统的技术等。

方法	优点	缺点
定性	简易的计算方式；不必精确算出资产价值；不需得到量化的威胁发生率；非技术或非安全背景的员工也能轻易参与；流程和报告形式比较有弹性	本质上是非常主观的；对关键资产的财务价值评估参考性较低；缺乏对风险降低的成本分析
定量	结果建立在独立客观的程序或量化指标上；大部分的工作集中在制定资产价值和减缓可能风险；主要目的是做成本效益的审核	风险计算方法复杂；需要自动化工具及相当的基础知识；投入大；个人难以执行

5.5 典型风险评估算法

OCTAVE法

- 由美国卡耐基·梅隆大学软件工程研究所下属的CERT协调中心开发的用以定义一种系统的、组织范围内的评估信息安全风险的方法。
- 着眼于组织自身并识别出组织所需保护的对象，明确它为什么存在风险，然后开发出技术和实践相结合的解决方案。
- **核心**是**自主原则**。
- 明确定义了所有评估环节的具体实施及输出。

5.5 典型风险评估算法

OCTAVE法

- OCTAVE方法的评估过程和相应的输出结果表。

评估过程	输出	
第一阶段	产生组织机构数据的输出	信息系统的资产列表
		关键资产的安全需求列表
		关键资产的威胁列表
		现有安全措施的列表
		当前组织机构及其系统的管理方面的脆弱点
第二阶段	产生技术数据的输出	输出组织机构的关键组件列表
		现有技术上的脆弱性
第三阶段	产生风险分析和降低数据的输出	输出关键资产的风险报告
		确定风险大小
		制定保护策略
		降低风险的计划

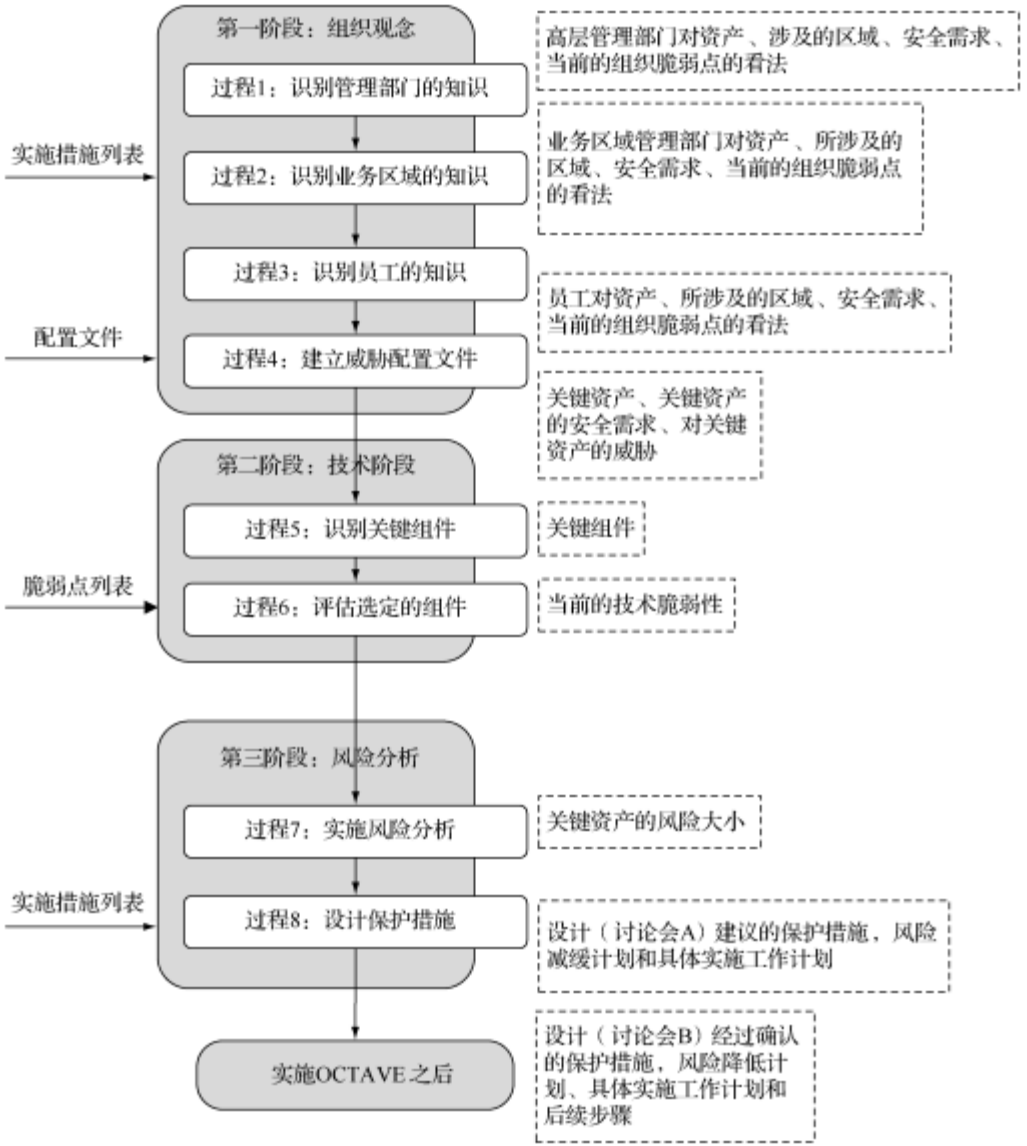
5.5 典型风险评估算法

层次分析法（AHP 法）

- 将与决策总是有关的元素分解成目标、准则、方案等层次，在此基础之上进行定性和定量分析的决策方法。
- 将一个复杂的多目标决策问题作为一个系统，将目标分解为多个目标或准则，进而分解为多指标（或准则、约束）的若干层次，通过定性指标模糊量化方法算出层次单排序（权数）和总排序，以作为目标（多指标）、多方案优化决策的系统方法

5.5 典型风险评估算法

层次分析法



5.6 风险评估工具

- **风险评估工具**是风险评估的辅助手段，是保证**风险评估结果可信度**的一个重要因素。
- 从功能应用角度和目标可分为**预防**、**检测**和**响应**。
- 根据在评估过程中的主要任务和作用原理的不同，分为：
  - 风险评估与管理工具。
  - 信息基础设施风险评估工具。
  - 风险评估辅助工具。

5.6 风险评估工具

✦ 风险评估与管理工具

- 是集成风险评估各类知识和判据的管理信息系统，以规范风险评估的过程和操作方法，或用于收集评估所需的数据和资料，基于专家经验，对I/O进行模型分析，并有针对性地提出风险控制措施。
- 根据实现方法不同，有3种：
  - ✓ 基于相关标准或指南的风险评估与管理工具：

    CRAMM、CC Toolbox、ASSET 等。
  - ✓ 基于知识的风险评估与管理工具：

    MSAT、COBRA等。
  - ✓ 基于定性或定量的模型算法的风险评估与管理工具：

    RA/SYS、CORA等。

5.6 风险评估工具

✦ 风险评估与管理工具——常见工具比较

工具	国家/组织	标准/方法	定性/定量	数据输入	结果输出
CRAMM	英国CCTA	BS 7799	定性/定量结合	过程	结果报告、风险等级、控制措施
ASSET	美国NIST	SP 800-26	定量	调查文件	决策支持信息
CC Toolbox	美国NIAP	CC	定性/定量结合	调查问卷	评估报告
COBRA	英国C&A系统安全公司	ISO 17799、专家知识	定性/定量结合	调查文件	结果报告、风险等级、控制措施
MSAT	美国Microsoft	专家知识	定性/定量结合	调查文件	风险管理措施与意见
RA/SYS	英国BSI	ISO 17799、过程式算法	定量	过程	风险等级、控制措施
CORA	国际安全技术公司	过程式算法	定性/定量结合	调查文件	决策支持信息

5.6 风险评估工具

✦ 信息基础设施风险评估工具

- 信息基础设施风险评估工具，主要用于对信息系统的主要部件（例如操作系统、数据库系统、网络设备等）的脆弱性进行分析，或实施基于脆弱性的攻击。
  - ✓ 脆弱性扫描工具：

    Nmap、X-scan、Nessus和Fluxay等。
  - ✓ 渗透性测试工具：

    Core Impact、Canvas和Metasploit等。

5.6 风险评估工具

✦ 风险评估辅助工具

➢ 在风险评估过程中，可以利用一些辅助性的工具和方法来收集评估所需要的数据和资料，帮助完成风险的现状分析和趋势分析。

- ✓ 检查列表。
- ✓ 入侵检测系统。
- ✓ 安全审计工具。
- ✓ 拓朴发现工具。
- ✓ 资产信息收集系统。
- ✓ 其他。

5.6 风险评估工具

✦ 风险评估工具的选择

➢ 选择与使用风险评估工具时应考虑：

- ✓ 所提供的依据、方法和功能应符合信息安全方针，并与风险评估的方法相适应。
- ✓ 在满足选择可靠的、成本有效的控制措施同时，能够对评估的结果形成清晰、无歧义、精确的报告。
- ✓ 提供数据收集、分析和输出功能，并保存和维护历史记录。
- ✓ 要与信息系统中的硬件和软件协调和兼容。
- ✓ 具有充分的使用培训和相关的帮助文件，保证相关工具的安装和使用过程的安全。

5.7风险评估案例

对XX学院官方网站进行信息安全风险评估

- 1．风险评估准备
- 2．资产识别与估价
- 3．威胁识别与评估
- 4．脆弱性识别与评估
- 5．风险计算与分析
- 6．风险管理与控制

小 结

1. 风险评估是用来了解信息系统的安全状况，估计威胁发生的可能性，计算因为脆弱性影响而受到攻击的潜在损失，并帮助选择安全防护控制措施，将风险降低到可接受的程度，提高信息安全保障能力。
2. 资产、威胁、脆弱性、安全风险、风险的影响、安全需求和已有的安全控制措施构成了风险评估的基本要素。
3. 风险评估过程分为四个阶段。
4. 风险值计算涉及资产、威胁和脆弱性，并由计算得出的安全事件发生的可能性和安全事件的影响来确定风险值。
5. 选择评估方法和工具时，应遵循相关原则。

作 业

1. 简述信息安全风险评估的概念、目的、原则以及意义。
2. 信息安全风险评估的核心要素是什么？它们之间有何关系?
3. 画出信息安全风险评估的流程图并简述其过程。
4. 风险计算的公式是什么？并解释公式中相关符号的含义。
5. 简述风险计算的过程。

作 业

6. 风险处理的过程中，选择安全控制措施时应该考虑哪些因素?

7. 风险评估文档包括哪些？简述并阐述文档内容。

8. 举例说明几个典型的信息安全风险评估算法。

9. 信息安全的风险评估工具有哪些？简述并举例说明。

10. 联系实际谈谈你对风险评估的看法。

实 验

实验二　网络信息系统风险评估