第3章 合规性与风险评估

信息安全管理

主讲 李章兵

内容

- 3.1 企业合规性
- 3.2 信息安全风险与相关要素
- 3.3 风险要素的识别与评估
- 3.4 风险评估方法与标准
- 3.5 信息安全风险评估流程
- 3.6 风险分析与处理

- 作业

教学目标

- 本章的重点是
  - 企业合规性
  - 风险要素与关系
  - 风险计算与评估

3.1 企业合规性

- 当今企业管理的发展趋势
  - 合规管理、业务管理与财务管理并称企业管理的三大支柱
  - 合规管理是内控的重要方面，也是风险管理的关键环节。
  - 政策要求企业必须做到知识产权合规、反垄断合规、环保合规。
- 信息安全管理的趋势
  - 将安全管理、系统管理、存储管理与合规政策融为一体形成企业信息安全管理框架

3.1 企业合规性

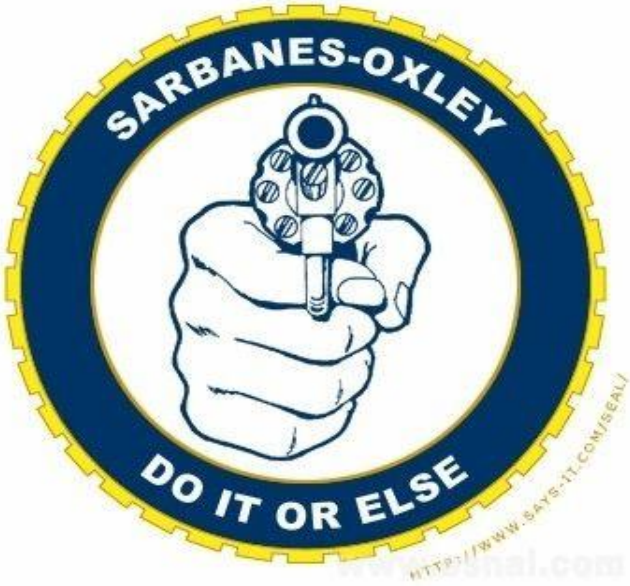
- 合规规范包括：
  - 央企：法律法规、监管规定、行业准则和企业章程、规章制度以及国际条约、规则等。
  - 外企：法律法规、国际条约、监管规定、行业准则、商业惯例、道德规范和企业依法制定的章程及规章制度。

3.1 企业合规性

- 美国萨班斯法案（SOX）2002
  - 上市公司要求
    - 针对产生财务交易的所有作业流程，都做到能见度、透明度、控制、通信、风险管理和欺诈防范，且必须详细记录到可追查交易源头。
    - 所有上市公司都必须加强和建立有效的内部控制框架，以确保上市公司遵守证券法律和提高公司披露信息的准确性和可靠性。
  - 财务流程
    - 是由IT系统驱动，IT和财务关联紧密，财务信息操作上的任何漏洞，都可能被IT系统出卖。
    - 企业风险管理与内部控制的工作中，60%在财务控制上，而40%是在IT控制上的。
  - SOX法案在合规方面也要求企业必须落实到对IT的有效管理控制上来。

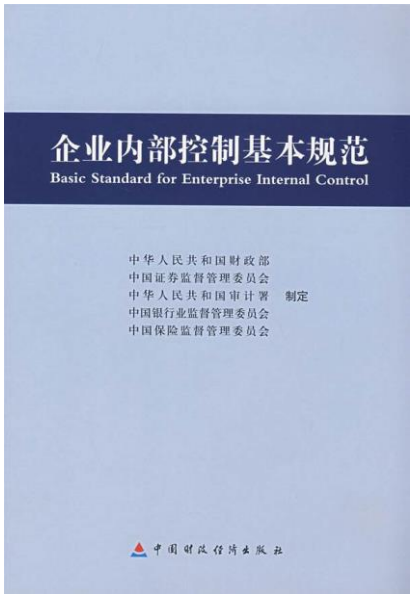
3.1 企业合规性

- SOX法案对IT内控合规管理要求主要有两个方面：
  - 一是IT应用控制（IT Application Control）
    - 对业务流程所依赖的IT系统进行某些控制，其中特别是针对支持财务报告的特定IT应用。
  - 二是IT一般控制（IT Generally Control）
    - 对于支撑公司运作的IT基础技术架构平台进行有效管理控制。
    - 主要是针对基本的IT基础设施控制，包括物理和逻辑网络安全、数据库管理、系统开发、变更控制、灾难恢复等，并由IT部门全程参与公司SOX法案合规管理项目。



3.1 企业合规性

- 我国《企业内部控制基本规范》要求
  - 企业应当建立重大风险预警机制和突发事件应急处理机制，明确风险预警标准；
  - 对可能发生的重大风险或突发事件，制定应急预案、明确责任人员、规范处置程序，确保突发事件得到及时妥善处理。
  - 企业实现的内控是以战略为导向的全面内控，但该规范包括的范围相当广泛。
  - 由于所有的业务都可能产生数据，如何确保数据的及时收集、准确与完整性都离不开IT系统的支撑。
  - IT部门将渐渐承担主角，成为保证财务报告内部控制有效性的基础。



3.1 企业合规性

- 企业内部控制的六大要点
  - 1.不相容职务分离控制；
  - 2.授权审批控制；
  - 3.财产保护控制；
  - 4.会计系统控制；
  - 5.发挥管理信息系统的作用；
  - 6.强化全面预算管理。
- 合规关键点
  - 如何把IT内控与企业内控管理统一起来
  - 在内控合规方面，IT就是一个最佳的突破口。
  - 保证财务报告内部控制有效性的基础。

3.1 企业合规性

- 合规性（compliance）
  - ISO/IEC 17799规定：合规性指“符合法律要求；安全策略和技术合规性的检查；系统审查相关事项”等要求。
  - 使企业经营活动与法律、管治及内部规则保持一致。
    - 1.规制：即遵守企业所在国和经营所在国的相关法律法规和行业准则；
    - 2.规则：即遵守企业内部规章制度，包括企业价值观、商业行为准则；
    - 3.规范：即遵守企业内部的规范流程，包括职业道德规范。

3.1 企业合规性

- 合规管理
  - 是指以有效防控合规风险为目的，以企业和员工经营管理行为为对象，开展包括制度制定、风险识别、合规审查、风险应对、责任追究、考核评价、合规培训等有组织、有计划的管理活动。
  - 企业通过制定合规政策，按照外部法规的要求统一制定并持续修改内部规范，监督内部规范的执行，以实现增强内部控制，对违规行为进行早期预警，防范、化解、控制合规风险的一整套管理活动和机制。
  - 目的就是通过建立一套机制，使公司能够有效识别、评估、监测合规风险，主动避免违法违规行为发生，从而免受法律制裁或财务、声誉等方面的损失，防范操作风险。

3.1 企业合规性

- 合规风险
  - 指企业及其员工因不合规行为，引发法律责任、受到相关处罚、造成经济或声誉损失以及其他负面影响的可能性。
  - 指企业合规义务的不合规发生的可能性和后果（我国《合规管理体系指南》（GB/T 35770-2017）第2.12条），是企业违反合规规范可能导致的制裁、处罚、财产损失和声誉损失风险。
    - 风险是指影响其总体或部门生产经营目标的不确定性。
    - 合规义务是企业追求商业行为价值观水平的综合反映。是企业主动承担或承诺的责任和标准。

3.1 企业合规性

- 合规风险影响
  - 法律影响：可用于针对未遵守规定的组织的法规和法律，可能导致罚款、监禁、产品扣押、处罚或禁止。
  - 财务影响：影响企业盈利、丧失投资者信心、股价或潜在未来盈利的结果。
  - 声誉影响：通过不良公关影响客户对一品牌认知的结果降低了员工信心或客户信任。
  - 业务影响：影响企业经营能力的因素，如工厂关闭或贸易禁运。
- 常见的合规风险类型
  - 影响大多数业务的运营方面：监管和政治不确定性、数据保护、利益冲突、市场风险、行为风险、贪污、质量。
- 评估合规风险
  - 通过使用资源并定义角色来实现：收集跨职能输入、杠杆数据、界定职责、持续修订

3.1 企业合规性

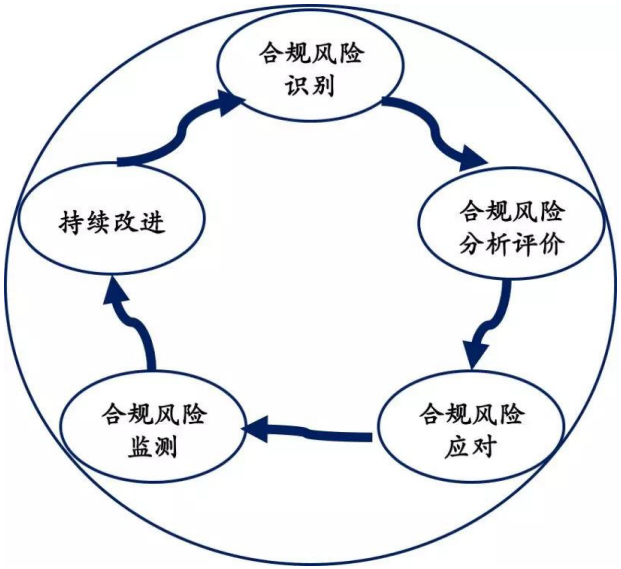
- 合规风险识别（《合规管理体系指南》第3.6条）
  - 是发现、收集、确认、描述合规风险以及整理和储存合规风险信息的过程，包括对风险根源、风险成因、风险事件及潜在后果的识别。
  - 合规风险识别是合规风险管理的首要步骤、前提和基础。
  - 根据合规规范对企业经营管理的各个领域进行合规风险排查，甄别、收集、确认和描述合规风险点，根据涉及的合规规范与合规风险发生的业务领域进行分类和整理，制作矩阵合规风险清单。

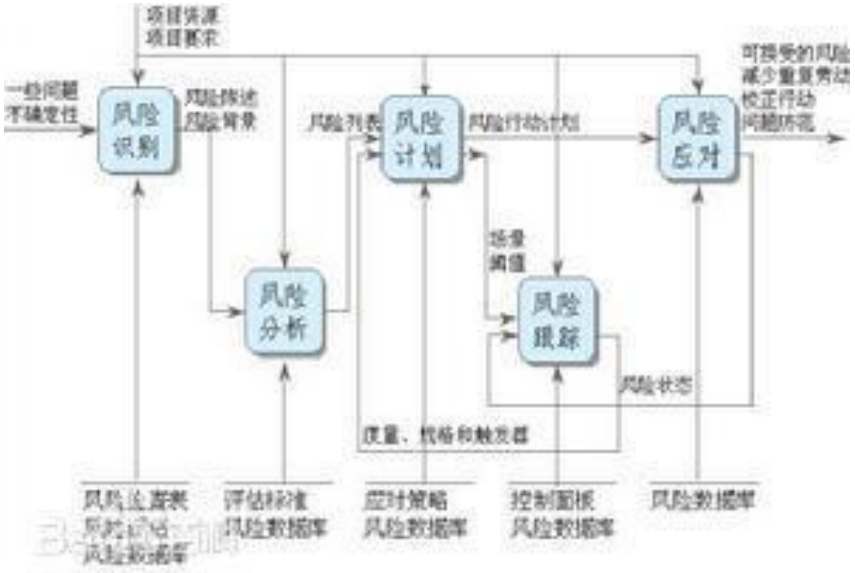
3.1 企业合规性

- RPN（Risk Priority Number）的SOD风险系数评估法
  - 对风险进行评估和打分，确定合规风险系数的高低。每一方面分为1到10个等级。
    - 风险的严重程度（Severity）
    - 发生的可能性和频率（Occurrence）
    - 可探测度（Detection）
  - 严重程度高于8分，或者RPN三个方面的乘积高于100分，说明其风险系数很高，系重大合规风险。

3.1 企业合规性

- 企业合规信息安全
  - 随着信息安全设施的逐渐完善，企业对安全管理提出了更高的要求。
  - 企业从单纯采购安全产品或安全集成项目演化到一体化的集中信息安全管理的趋势日益明显，将安全管理、系统管理、存储管理与合规政策融为一体形成企业信息安全管理框架是当今企业管理的发展趋势。



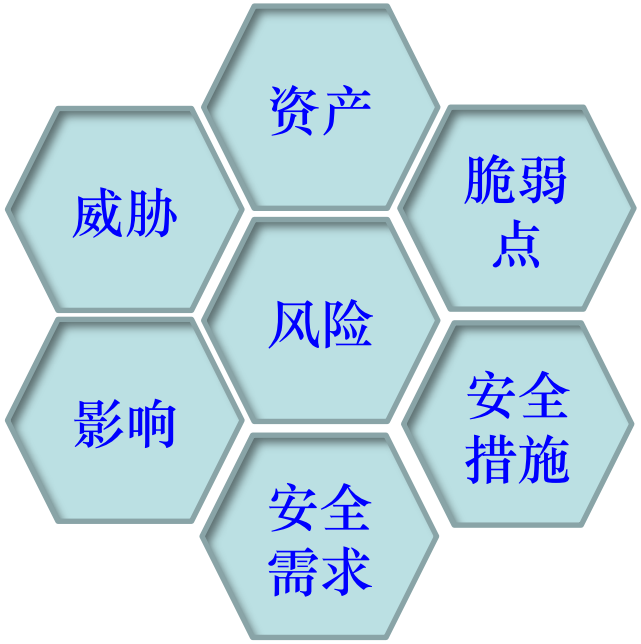


3.2 信息安全风险与相关要素

- 1. 风险
  - 信息安全风险是指威胁利用一个或一组资产的脆弱点导致组织受损的潜在性，并以威胁利用脆弱点造成的一系列不期望发生的事件（或称为安全事件）来体现。(ISO/IEC 13335-1)
  - 资产、威胁、脆弱点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，缺一不可。
    - 没有资产，威胁就没有攻击或损害的对象；
    - 没有威胁，尽管资产很有价值，脆弱点很严重，安全事件也不会发生；
    - 系统没有脆弱点，威胁就没有可利用的环节，安全事件也不会发生。

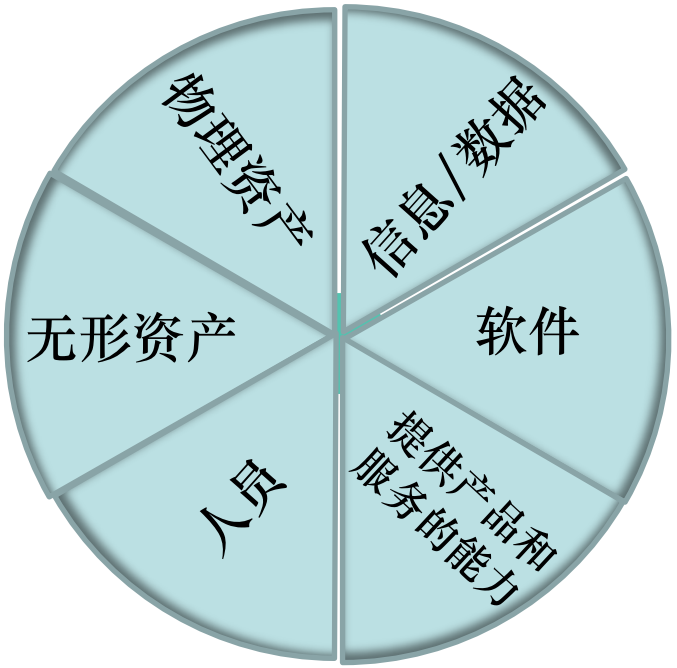
3.2 信息安全风险与相关要素

- 1. 风险
  - 风险可以形式化表示为：R=(A, T, V)
    - 其中R表示风险、A表示资产、T表示威胁、V表示脆弱点。



3.2 信息安全风险与相关要素

- 2. 风险评估相关要素
- (1).资产
  - 指任何对组织有价值的东西（根据ISO/IEC 13335-1）
  - 资产形式：以多种形式存在，有无形的、有形的
  - 信息资产
    - 指对组织具有价值的信息资源，是安全策略保护的对象。（我国的《信息安全风险评估指南》）
    - 根据资产的表现形式，可将信息资产分为数据、软件、硬件、文档、服务、人员等类。



3.2 信息安全风险与相关要素

- 2. 风险评估相关要素
  - 信息资产分类

分类	实例
数据	源代码，数据库数据，系统文档等
软件	系统软件，应用软件，源程序
硬件	网络设备，计算机设备，存储设备，传输线路，保障设备，其他电子设备
服务	办公服务，网络服务，信息服务
文档	纸质的各种文件，传真，电报，财务报告，发展计划等
人员	掌握重要信息和核心业务的人员，如主机维护主管等
其他	企业形象，客户关系等

3.2 信息安全风险与相关要素

- 2.风险评估相关要素
  - (2).威胁
    - 可能对资产或组织造成损害的潜在原因
    - 威胁有潜力导致不期望的事件发生
  - 不期望发生的事件
    - 可能对系统或组织及其资产造成损害的信息安全威胁
    - 可能是蓄意的对信息系统和服务所处理信息的直接或间接攻击
    - 也可能是偶发事件

3.2 信息安全风险与相关要素

- 2. 风险评估相关要素
  - (2).威胁—根据威胁源分类
    - 自然威胁：指自然界的不可抗力导致的威胁
    - 环境威胁：指信息系统运行环境中出现的重大灾害或事故所带来的威胁
    - 系统威胁：指系统软硬件故障所引发的威胁
    - 人员威胁：包含内部人员与外部人员，由于内部人员熟悉系统的运行规则，内部人员的威胁更为严重
      - 人员威胁根据威胁的动机又可分为恶意和无意两种
      - 威胁行为都可能对信息系统构成严重的损害，两者都应该予以重视

3.2 信息安全风险与相关要素

- **威胁分类：** 根据威胁源的不同分为：

自然威胁

环境威胁

系统威胁

人员威胁

3.2 信息安全风险与相关要素

- 2. 风险评估相关要素
  - (2).威胁—根据威胁源表现形式

威胁源	常见表现形式
自然威胁	地震、飓风、火山、洪水、海啸 、泥石流、暴风雪 、雪崩 、雷电等
环境威胁	战争, 重大疫情, 恐怖主义, 供水电气故障、危险物质泄漏、污染等
系统威胁	网络故障, 硬件故障, 软件故障, 恶意代码等
外部人员	网络窃听, 拒绝服务攻击等, 系统入侵、身份仿冒、物理破坏、抵赖、篡改、泄密等
内部人员	未经授权信息发布和读写, 抵赖, 电子攻击、物理破坏、盗窃、越权滥用、误操作等

3.2 信息安全风险与相关要素

- 2. 风险评估相关要素
  - (3).脆弱点
    - 是一个或一组资产所具有的，可能被威胁利用对资产造成损害的薄弱环节。
      - 如操作系统存在漏洞、数据库的访问没有访问控制机制、系统机房任何人都可进入等等。
    - 脆弱点是资产本身存在的
    - 资产的脆弱点具有隐蔽性
      - 有些弱点只有在一定条件和环境下才能显现
      - 不正确的、起不到应有作用的或没有正确实施的安全措施本身就可能是一个脆弱点。

3.2 信息安全风险与相关要素

- 2. 风险评估相关要素
  - (3).脆弱点--
    - 隐蔽性使得脆弱点识别变得困难。
    - 威胁总是要利用资产的弱点才可能造成危害。
      - 如果没有相应的威胁出现，单纯的脆弱点本身不会对资产造成损害。
      - 如果系统足够强健，再严重的威胁也不会导致安全事件，并造成损失。

3.2 信息安全风险与相关要素

- 脆弱点按表现分为：
  - 技术脆弱点和管理脆弱点

技术脆弱点

是指信息系统在设计、实现、运行时在技术方面存在的缺陷或弱点。如：
安装杀毒软件或病毒库未及时升级；
操作系统或其他应用软件存在拒绝服务攻击漏洞；
数据完整性保护不够完善；
数据库访问控制机制不严格等。

管理脆弱点

指组织管理制度、流程等方面存在的缺陷或不足。如：
系统机房钥匙管理不严；
人员职责不清；
未及时注销离职人员对信息系统的访问权限等。

3.2 信息安全风险与相关要素

- 2. 风险评估相关要素
  - (4).影响
    - 是威胁利用资产的脆弱点导致不期望事件发生的后果。后果表现可能为：

直接形式

如物理介质或设备的破坏、人员的损伤、 直接的资金损失等。容易估计且损失较少

间接形式

如公司信用、形象受损、市场分额损失、法律责任等。难以估计且更为严重

3.2 信息安全风险与相关要素

- 1.风险评估相关要素
  - (5).安全需求
    - 是指为保证组织业务战略的正常运作而在安全措施方面提出的要求。
    - 安全需求：体现在技术、组织管理等多个方面。
      - 如关键数据或系统的机密性、可用性、完整性需求
      - 法律法规的符合性需求
      - 人员安全意识培训需求
      - 信息系统运行实时监控的需求等。

3.2 信息安全风险与相关要素

- 2. 风险评估相关要素
  - (6).安全措施
    - 安全措施是指为保护资产、抵御威胁、减少脆弱点、限制不期望发生事件的影响、加速不期望发生事件的检测及响应而采取的各种实践、规程和机制的总称。
    - 有效安全：通常要求不同安全措施的结合，为资产提供多级的安全。
      - 例如，应用于计算机的访问控制机制应被审计控制、人员管理、培训和物理安全所支持。
    - 安全措施分已有的和未实施的
      - 已有的安全措施起作用时将减少安全风险

3.2 信息安全风险与相关要素

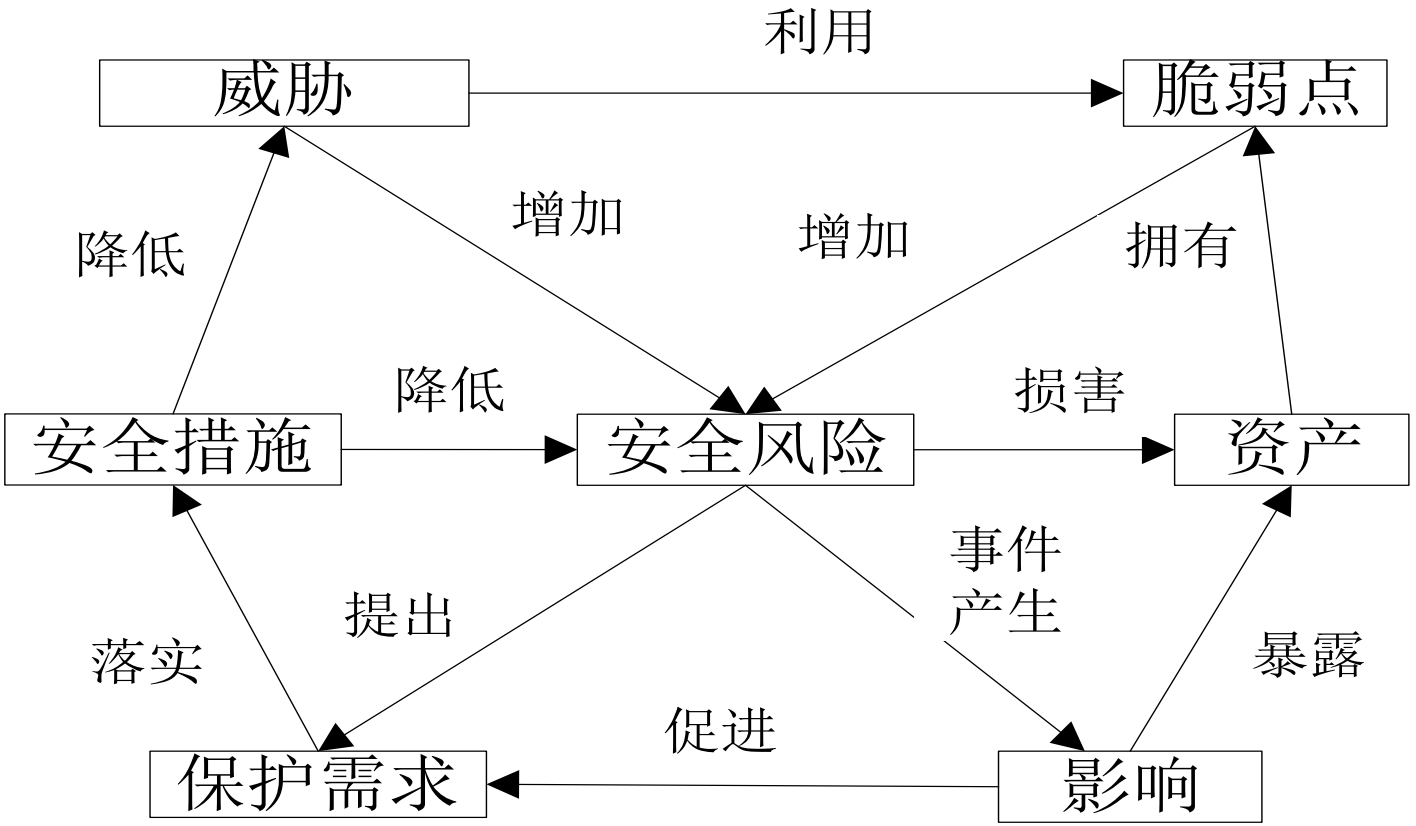
- 1.风险评估相关要素
  - (6).安全措施
    - 安全措施功能
      - 保护、震慑、检测、限制、纠正、恢复、监视、安全意识等。
    - 安全措施的实施领域
      - 物理环境、技术领域、人员、管理等
    - 可用的安全措施
      - 访问控制机制、防病毒软件、加密机制、数字签名、防火墙、监视与分析工具、冗余电力供应、信息备份等。

3.2 信息安全风险与相关要素

- 3.各风险要素的相互间关系
  - 威胁利用脆弱点将导致安全风险的产生；
  - 资产具有价值，并对组织业务有一定影响，资产价值及影响越大则其面临的风险越大；
  - 安全措施能抵御威胁、减少脆弱点，因而能减小安全风险；
  - 风险的存在及对风险的认识导出保护需求，保护需求通过安全措施来满足或实现。

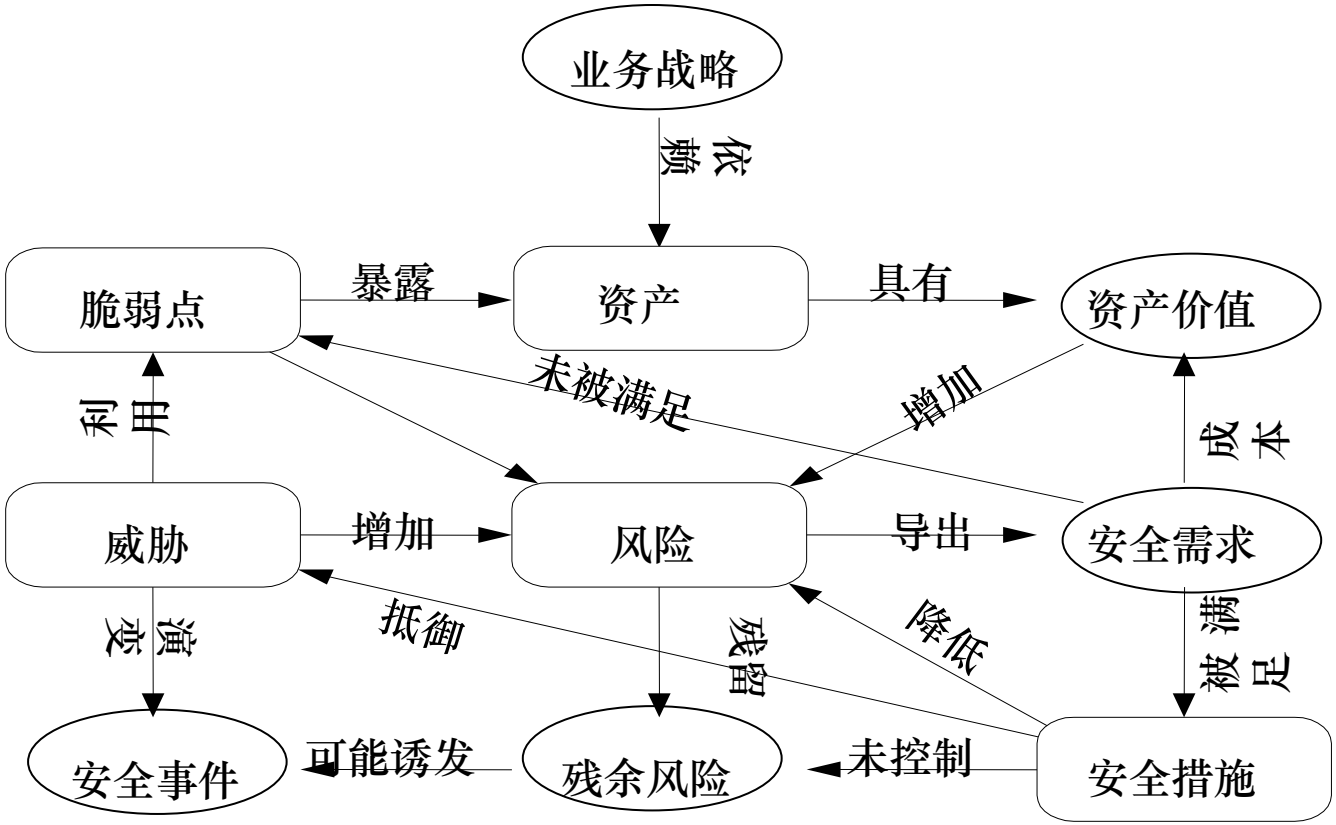
3.2 信息安全风险与相关要素

- **3.各风险要素的相互间关系**
  - **ISO/IEC 13335-1中风险要素及其相互关系**



3.2 信息安全风险与相关要素

- 3.各风险要素的相互间关系
  - 我国《信息安全风险评估指南》风险要素关系模型



3.3 风险要素的识别与评估

- 1.资产识别
  - 资产识别是风险识别的必要环节。
  - 任务：对确定的评估对象所涉及或包含的资产进行详细的标识。注意分类(有无形的、有形的)和依赖关系。
  - 方法：访谈、现场调查、问卷、文档查阅等。
    - ISO17799列出了常见信息资产有：
      - 数据与文档：数据库和数据文件、系统文件、用户手册、培训材料、运行与支持程序、业务持续性计划、应急安排
      - 书面文件：合同、指南、企业文件、包含重要业务结果的文件。
      - 软件资产：应用软件、系统软件、开发工具和实用程序
      - 物理资产：计算机、通讯设备、磁介质（磁盘与磁带），其他技术设备（供电设备、空调设备）、家具、办公场所
      - 人员：员工、客户
      - 企业形象与声誉
      - 服务：计算和通讯服务，其他技术服务（供热、照明、电力、空调）

3.3 风险要素的识别与评估

- 1.资产识别
  - 资产清单：列出资产清单是资产识别的关键
    - 27001-2013资产清单表
      - 其中子类别还可以细分为多级

27001-2013资产识别评价表										
编制:			审批:				日期:			
序号	类别	子类别	资产名称	资产编号	数量	所属部门	用途	位置	责任人	是否重要
	人员									
	设备									
	环境	办公楼								
	环境	家具								
	声誉									
	服务									
	文档									
	数据									
	软件									

3.3 风险要素的识别与评估

- 2.资产评估
  - 资产的评价是对资产的价值或重要程度进行评估
    - 资产本身的货币价值是资产价值的体现
    - 更重要的是资产对组织关键业务的顺利开展乃至组织目标实现的重要程度。
  - 多数情况下只能以定性的形式评价
    - 多数资产不能以货币形式的价值来衡量，评价很难以定量；
    - 依据重要程度的不同划分等级，具体划分应根据具体问题决定
    - 5级划分方法为：非常重要、重要、比较重要、不太重要、不重要
    - 定量赋值等级划分：可赋以相应的定量值，如：5、4、3、2、1。

3.3 风险要素的识别与评估

- 2.资产评估
  - 分级原则：按分值进行等级分类

赋值	标识	定义
5	极高	包含组织最重要的秘密，关系未来发展的前途命运，对组织根本利益有着决定性影响，如果泄漏会造成灾难性的损害
4	高	包含组织的重要秘密，其泄露会使组织的安全和利益遭受严重损害
3	中等	包含组织的一般性秘密，其泄露会使组织的安全和利益受到损害
2	低	包含仅能在组织内部或在组织某一部门内部公的信息，向外扩散有可能对组织的利益造成损害
1	极低	包含可对社会公开的信息，公用的信息处理设备和系统资源等

3.3 风险要素的识别与评估

- 2.资产评估
  - 资产的重要程度
    - 通常信息资产的机密性、完整性、可用性、可审计性和不可抵赖性等是评价资产的安全属性。
      - 资产的价值可由资产在这些安全属性上的达成程度或者其安全属性未达成时所造成的影响程度来决定的。
      - 先分别对资产在以上各方面的重要程度进行评估，然后通过一定的方法进行综合，可得资产的综合价值。
      - 一般只考虑信息资产的基本属性。

3.3 风险要素的识别与评估

- 2.资产评估
  - 资产重要性计算
    - 若资产在机密性、完整性、可用性、可审计性和不可抵赖性的赋值分别记为VAc、VAi、VAa、VAac、VAn , 综合价值记为VA, 综合的方法可以是：
      - 最大原则：VA=max{VAc, VAi, VAa VAac、VAn }。
      - 加权原则：
      - VA= Ac*Wc+VAi*Wi+VAa*Wa+VAacC*Wac+VAn*Wn 。
        - 信息资产的机密性、完整性、可用性、可审计性和不可抵赖性对应的重要性赋予一非负的权值Wc、Wi、Wa Wac、Wn
    - 资产的每种属性都可以用等级赋值
      - 用5、4、3、2、1表示：极高、高、中等、低、可忽略

3.3 风险要素的识别与评估

- 2.资产评估
  - 资产评价表

27001-2013资产识别评价表													
编制:			审批:					日期:					
资产								重要性					
序号	类别	子类别	资产名称	用途	位置	所属部门	责任人	保密性	可用性	完整性	合规性	综合值	重要等级
	人员							5	5	5	5	20	5
	设备											15	5
	环境	办公楼										16	5
	环境	家具											4
	声誉												4
	服务												3
	文档												5
	数据												5
	软件												

3.3 风险要素的识别与评估

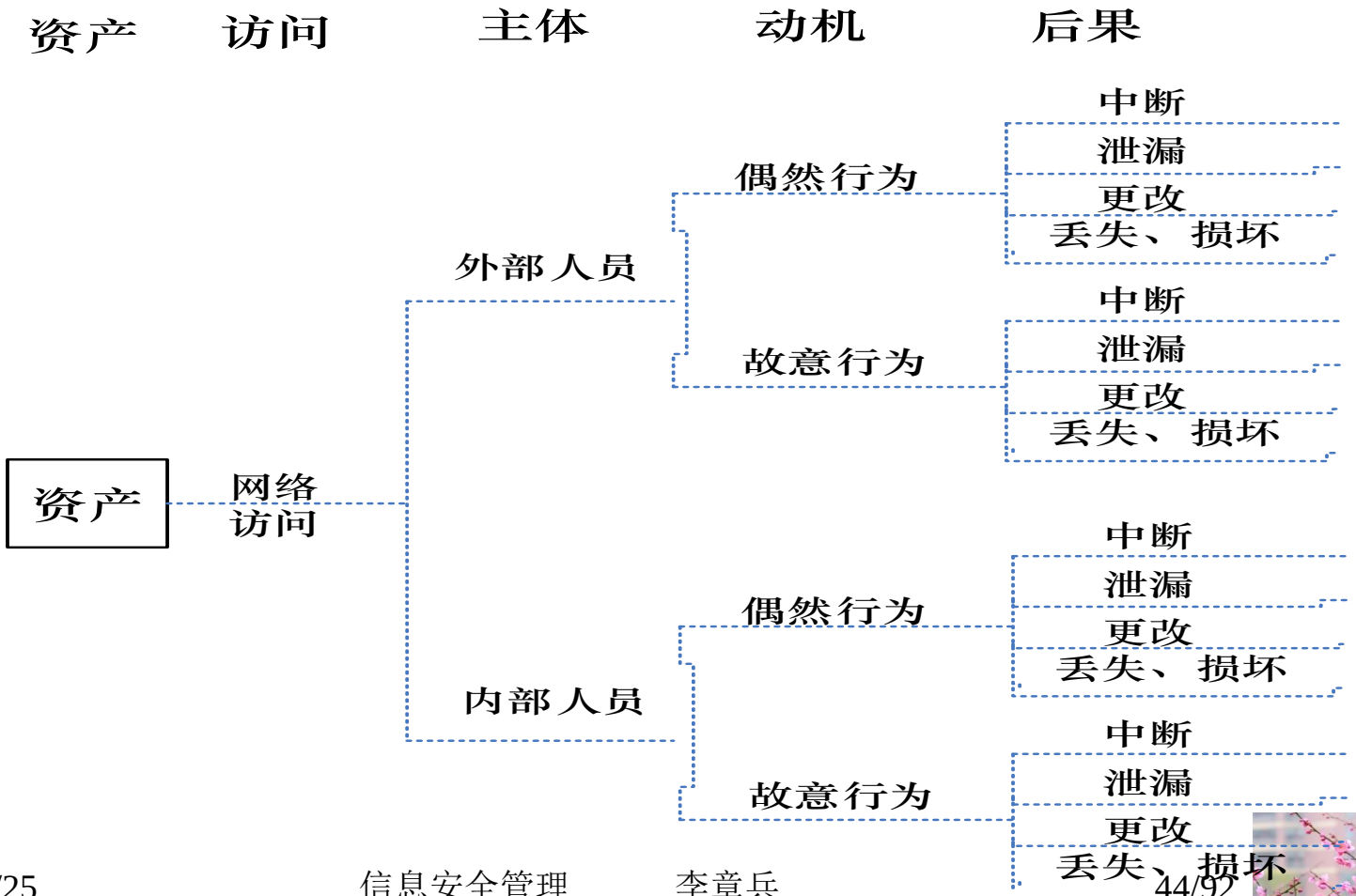
- **3. 威胁识别**
  - 威胁是构成风险的必要组成部分，因而威胁识别是风险识别的必要环节
  - 任务：对组织资产面临的威胁进行全面的标识。
    - 威胁识别可从威胁源进行分析；
    - 根据有关标准、组织所提供的威胁参考目录进行分析。
  - 威胁分类
    - 德国的《IT基线保护手册》将威胁分为五大类
      - 每类威胁有详细列举和说明，是威胁识别的重要参考
    - 分别是：不可抗力、组织缺陷、人员错误、技术错误、故意行为。
      - 每种类型威胁具体包含几十到一百多种威胁

3.3 风险要素的识别与评估

- **3. 威胁识别**
  - **OCTAVE威胁识别与分析**
    - 通过建立威胁配置文件，文件包括**5**个属性
      - 资产（**assert**）、访问**(access)**、主体**(actor)**、动机**(motive)**、后果**(outcome)**。
      - 人类利用网络访问对资产的威胁及系统故障对资产的威胁，其配置文件分别对应的威胁树：

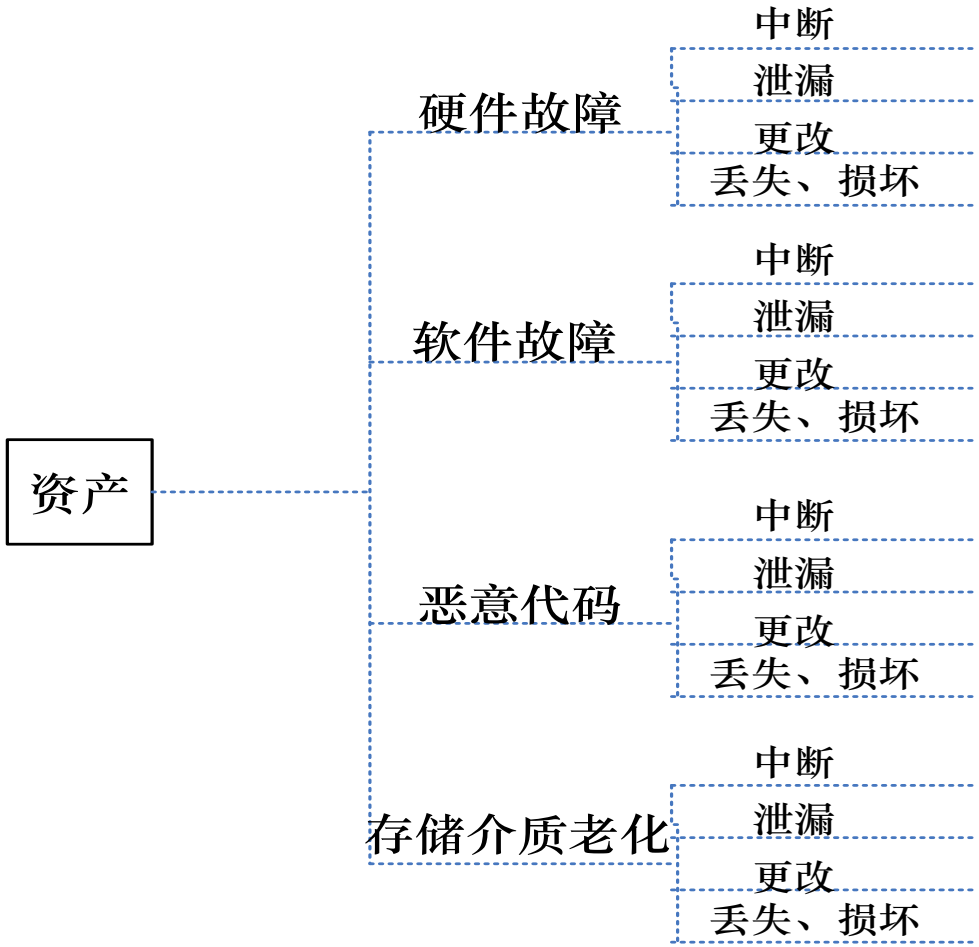
3.3 风险要素的识别与评估

- **3. 威胁识别**
  - 人类利用网络访问的威胁树



3.3 风险要素的识别与评估

- **3. 威胁识别**
  - 系统故障威胁树



3.3 风险要素的识别与评估

- 4. 威胁评估
  - 威胁频率与破坏力统计
    - (1) 以往安全事件报告中出现过的威胁、威胁出现频率、破坏力的统计；
    - (2) 实际环境中通过检测工具以及各种日志发现的威胁及其频率的统计；
    - (3) 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出现频率及其破坏力的统计。
  - 威胁评估的结果一般都是定性的
    - 威胁综合值=频率*破坏力
    - 破坏力即威胁后果对系统及组织业务的影响。

3.3 风险要素的识别与评估

- **4. 威胁评估**
  - 我国的《信息安全风险评估指南》威胁分级
    - 威胁频率等级划分为五级，分别代表威胁出现的频率的高低。等级数值越大，威胁出现的频率越高。如表：

等级	标识	定义
5	很高	威胁出现的频率很高，在大多数情况下几乎不可避免或者可以证实经常发生过
4	高	威胁出现的频率较高，在大多数情况下很有可能会发生或者可以证实多次发生过
3	中	威胁出现的频率中等，在某种情况下可能会发生或被证实曾经发生过
2	低	威胁出现的频率较小，一般不太可能发生，也没有被证实发生过
1	很低	威胁几乎不可能发生，仅可能在非常罕见和例外的情况下发生

3.3 风险要素的识别与评估

- **4. 威胁评估**
  - 威胁评估列表：同一资产可能有多个威胁

27001-2013威胁识别评价表												
编制:			审批:			日期:						
资产						威胁						
序号	类别	子类别	资产名称	用途	所属部门	威胁类别	威胁名称	威胁主体	频率	后果	综合值	等级
	人员					人员		人员		受伤	5	4
	设备					人员	破坏			丢失	8	5
	环境	办公楼				自然	故障				4	3
	环境	家具				自然						3
	声誉					技术	攻击					4
	服务					技术		系统		中断		3
	文档									更改		5
	数据									泄露		5
	软件											

3.3 风险要素的识别与评估

- 5. 脆弱点识别
  - 资产脆弱点的特点
    - 弱点是资产本身存在的；
    - 单纯的弱点本身不会对资产造成损害；
    - 威胁总是要利用资产的弱点才可能造成危害；
    - 资产脆弱点具有隐蔽性。
      - 有些弱点只有在一定条件和环境下才能显现，这是脆弱点识别中最为困难的部分。
      - 脆弱点识别时的数据应来自于资产的所有者、使用者，以及相关业务领域的专家和软硬件方面的专业等人员。
      - 需要注意的是，不正确的、起不到应有作用的或没有正确实施的安全措施本身就可能是一个弱点。

3.3 风险要素的识别与评估

- 5. 脆弱点识别
  - 针对每一项需要保护的资产，找出可能被威胁利用的弱点(主要从技术和管理两个方面)，并对脆弱点的严重程度进行评估。
    - 技术脆弱点：与具体技术相关
    - 管理脆弱点：与技术活动和管理环境相关
  - 主要识别方法
    - 问卷调查、工具检测、人工核查、文档查阅、渗透性测试等。
  - 实施识别脆弱点的技术或管理标准
    - 对物理环境的脆弱点识别可以参照《GB/T 9361－2000 计算机场地安全要求》中的技术指标实施；
    - 对操作系统、数据库可以参照《GB 17859－1999 计算机信息系统安全保护等级划分准则》中的技术指标实施。
    - 管理脆弱点识别方面可以参照《ISO/IEC 17799-2005 Code of practice for information security management》的要求对安全管理制度及其执行情况进行检查，发现管理漏洞和不足。
    - 技术脆弱点涉及物理层、网络层、系统层、应用层等各个层面的安全问题

3.3 风险要素的识别与评估

- 5. 脆弱点识别
  - 脆弱点识别参考表

类型	识别对象	识别内容
技术脆弱点	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进行识别。
	服务器（含操作系统）	从物理保护、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（初始化）、注册表加固、网络安全、系统管理等方面进行识别。
	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进行识别。
	数据库	从补丁安装、鉴别机制、口令机制、访问控制、网络和服务设置、备份恢复机制、审计机制等方面进行识别。
	应用系统	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、密码保护等方面进行识别。
管理脆弱点	技术管理	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、业务连续性。
	组织管理	安全策略、组织安全、资产分类与控制、人员安全、符合性

3.3 风险要素的识别与评估

- 6. 脆弱点评估
  - 是对脆弱点被利用后对资产损害程度、技术实现的难易程度、弱点流行程度进行评估；也可是对利用后资产的损害程度、被利用的可能性分别评估；然后以一定方式综合。
    - 脆弱点综合值=利用损害程度*流行度/技术难度
    - 脆弱点综合值=利用损害程度*利用可能性
  - 评估的结果
    - 一般都是定性等级划分形式，综合的标识脆弱点的严重程度。
    - 若很多弱点反映的是同一方面的问题，应综合考虑这些脆弱点，最终确定这一方面的脆弱点严重程度。

3.3 风险要素的识别与评估

- **6. 脆弱点评估**
  - 我国的《信息安全风险评估指南》
    - 依据脆弱点被利用后，对资产造成的危害程度来评估
    - 将脆弱点严重程度的等级划分为五级，分别代表资产脆弱点严重程度的高低。等级数值越大，脆弱点严重程度越高。

等级	标识	定义
5	极严重	如果被威胁利用，将对资产造成完全损害
4	严重	如果被威胁利用，将对资产造成重大损害
3	中等	如果被威胁利用，将对资产造成一般损害
2	一般	如果被威胁利用，将对资产造成较小损害
1	低	如果被威胁利用，将对资产造成的损害可以忽略

3.3 风险要素的识别与评估

- **6. 脆弱点评估**
  - **脆弱点列表：同一资产可能有多个脆弱点**

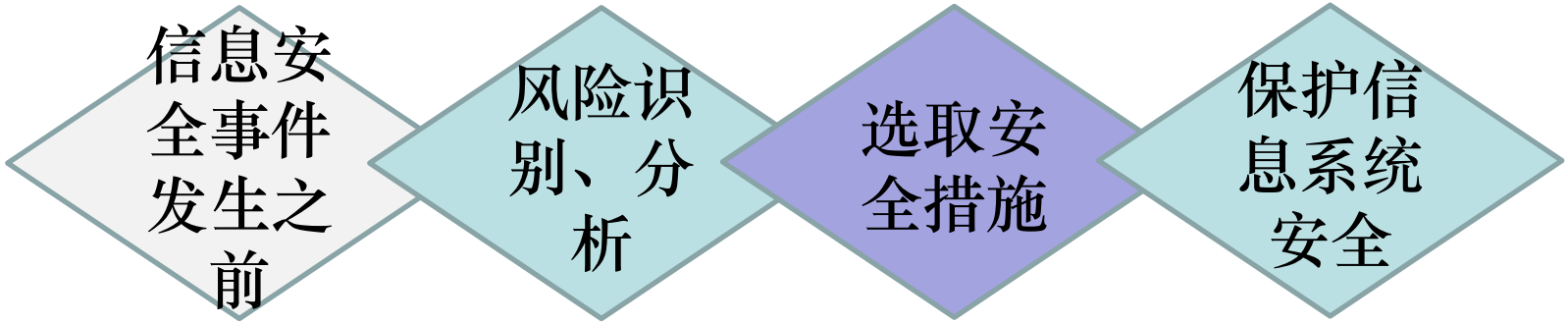
27001-2013脆弱点识别评价表												
编制:			审批:			日期:						
资产						脆弱点(综合值=利用可能*流行度*损害后果)						
序号	类别	子类别	资产名称	用途	所属部门	脆弱类别	利用可能	隐蔽性	流行度	利用后果	综合值	等级
	人员					管理		高		受伤	5	4
	设备					管理	高			丢失	8	5
	环境	办公楼				管理	中				4	3
	环境	家具				管理						4
	声誉					技术	一般					4
	服务					技术		高		中断		3
	文档									更改		5
	数据									泄露		5
	软件											

3.4 风险评估方法与标准

- 1.风险评估（Risk Assessment）
  - 在风险事件发生之前或之后（但还没有结束），该事件给人们的生活、生命、财产等各个方面造成的影响和损失的可能性进行量化评估的工作。
  - 风险评估就是量化测评某一事件或事物带来的影响或损失的可能程度。
  - 风险评估的目标
    - 是满足组织业务持续发展在安全方面的需要, 或符合相关方的要求, 或遵守法律法规的规定等。

3.4 风险评估方法与标准

- 1. 风险评估
  - 基本思路和目的
    - 不期望事件发生的可能性依赖于资产对于潜在攻击者的吸引力、威胁出现的可能性以及脆弱点被利用的难易程度。
    - 根据风险评估的结果来识别和选择安全措施，将风险降低到可接受的水平。



3.4 风险评估方法与标准

- 1.风险评估
  - 主要任务
    - 识别评估对象面临的各种风险
    - 评估风险概率和可能带来的负面影响
    - 确定组织承受风险的能力
    - 确定风险消减和控制的优先等级
    - 推荐风险消减对策

3.4 风险评估方法与标准

- 1. 风险评估
  - 信息安全风险评估：对信息资产（即某事件或事物所具有的信息集）所面临的威胁、存在的弱点、造成的影响，以及三者综合作用所带来风险的可能性的评估。
  - 依据：有关信息安全技术与管理标准
  - 评价对象：信息系统及由其处理的、传输和存储的信息资产的安全属性（机密性、完整性和可用性）
  - 风险估计：资产面临的威胁以及威胁利用脆弱点导致安全事件的可能性
  - 影响推测：结合安全事件所涉及的资产价值来判断安全事件一旦发生对组织造成的影响

3.4 风险评估方法与标准

- 2.风险评估方法
  - 基线风险评估、详细风险评估、综合风险评估
- (1)基线风险评估
  - 基线：一种在测量、计算或定位中的基本参照。
  - 安全基线
    - 类比于“木桶理论”，是安全木桶的最短板，或者是信息系统的最低安全要求。
    - 计算机安全基线：微软安全体系中对如何配置和管理计算机的详细描述。
    - 安全基线的元素包括：
      - 服务和应用程序设置、操作系统组件的配置、权限和权利分配、管理规则。

3.4 风险评估方法与标准

- (1)基线风险评估
  - 基线风险评估方法
    - 根据组织的实际情况，对信息系统进行基线安全检查，得出基本的安全需求，通过选择并实施标准的安全措施来消减和控制风险。
  - 安全基线标准
    - 在诸多标准规范中规定的一组安全控制措施或者惯例，适用于特定环境下的所有系统。
      - 国际标准和国家标准，例如ISO 17799、ISO 13335；
      - 行业标准或推荐，例如德国联邦安全局的《IT 基线保护手册》；
      - 来自其他有类似商务目标和规模的组织的惯例。

3.4 风险评估方法与标准

- **(1)基线风险评估**
  - 优点：
    - 只需要最少数量的资源，并且花费更少的时间和努力；
    - 很多系统可以采用相同或相似的基线防护措施而不需要太多的努力。
  - 缺点：
    - 基线水平难以设置
      - 不同组织信息系统千差万别，威胁时刻都在变化，很难制定全面的、具有广泛适用性的安全基线
      - 组织自行建立安全基线成本很高。
    - 风险评估不全面，不透彻，且不易处理变更
      - 如系统升级、业务变更
    - 没有全面、统一的、能符合组织目标的、值得信赖的安全基线，因而基线评估方法开展并不普遍。

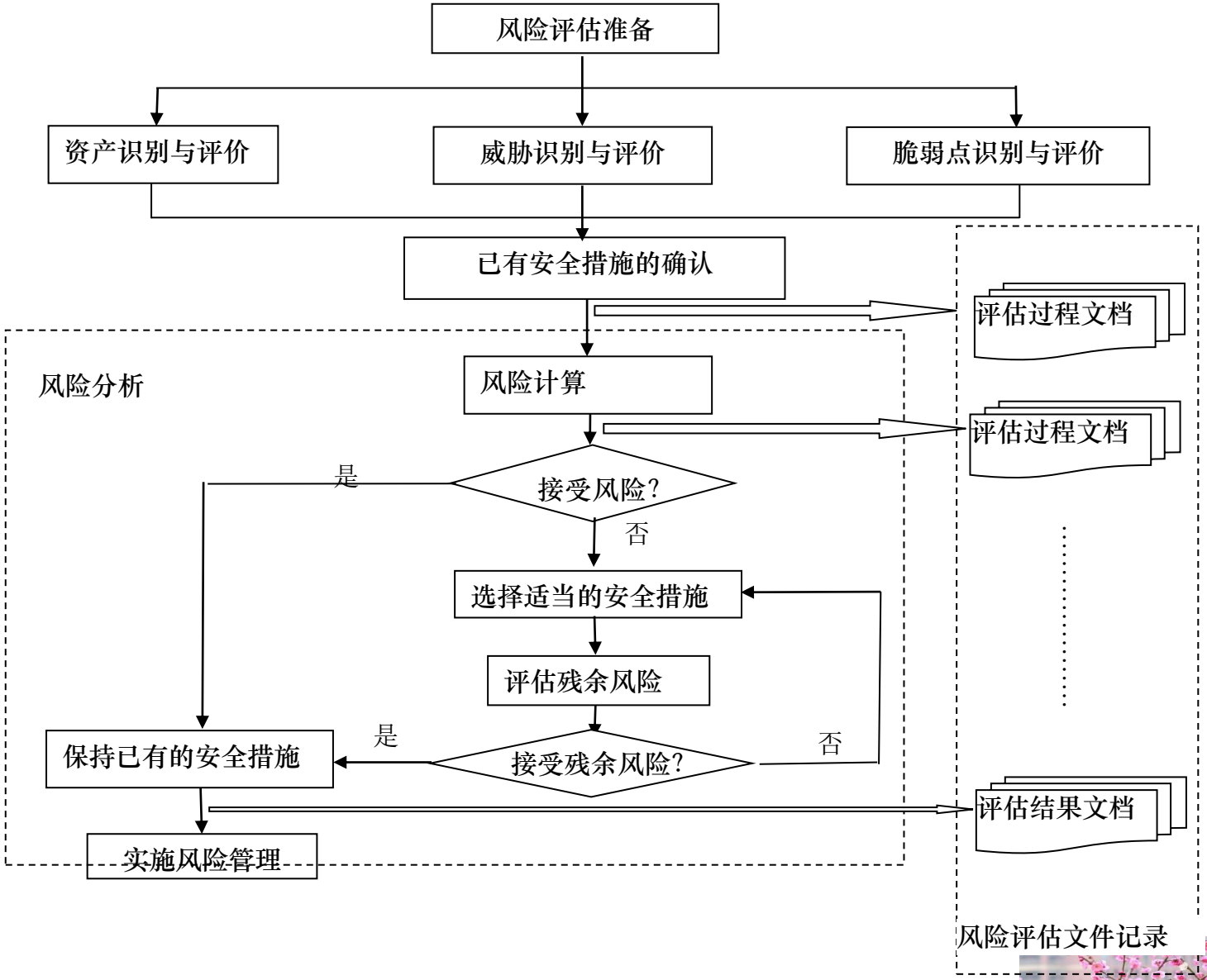
3.4 风险评估方法与标准

- **(2).详细风险评估**
  - **概念**
    - 详细风险评估要求对资产、威胁和脆弱点进行详细识别和评价
    - 评估可能引起风险的水平：通过不期望事件的潜在负面业务影响评估及其发生的可能性来完成。
    - 根据风险评估的结果来识别和选择安全措施，将风险降低到可接受的水平。
  - **不期望事件**
    - 可能表现为直接形式，如直接的经济损失；
    - 也可能表现为间接的影响，如法律责任、公司信誉等。
    - 发生的可能性依赖于资产对于潜在攻击者的吸引力、威胁出现的可能性以及脆弱点被利用的难易程度。

3.4 风险评估方法与标准

- (2)详细风险评估
  - 流程
    - (1) 风险评估准备阶段
    - (2) 资产识别与评估
    - (3) 威胁识别与评估
    - (4) 脆弱点识别与评估
    - (5)已有安全措施的确认
    - (6)风险分析
    - (7)安全措施的选取
    - (8)风险评估文件和记录

详细风险评估流程


风险评估准备
资产识别与评价
威胁识别与评价
脆弱点识别与评价
已有安全措施的确认
评估过程文档
风险分析
风险计算
评估过程文档
是
接受风险?
否
选择适当的安全措施
评估残余风险
是
保持已有的安全措施
接受残余风险?
否
评估结果文档
实施风险管理
风险评估文件记录

3.4 风险评估方法与标准

- **(2)详细风险评估**
  - 优点
    - 有可能为所有系统识别出适当的安全措施
    - 详细分析的结果可用于安全变更管理
  - 缺点
    - 需要更多的时间、努力和专业知识。

3.4 风险评估方法与标准

- (3)综合风险评估
  - 概述
    - 基线风险评估耗费资源少、周期短、操作简单, 但不够准确, 适合一般环境的评估;
    - 详细风险评估准确而细致, 但耗费资源较多, 适合严格限定边界的较小范围内的评估。
    - 实际上, 组织多是采用二者结合的综合评估方式。

3.4 风险评估方法与标准

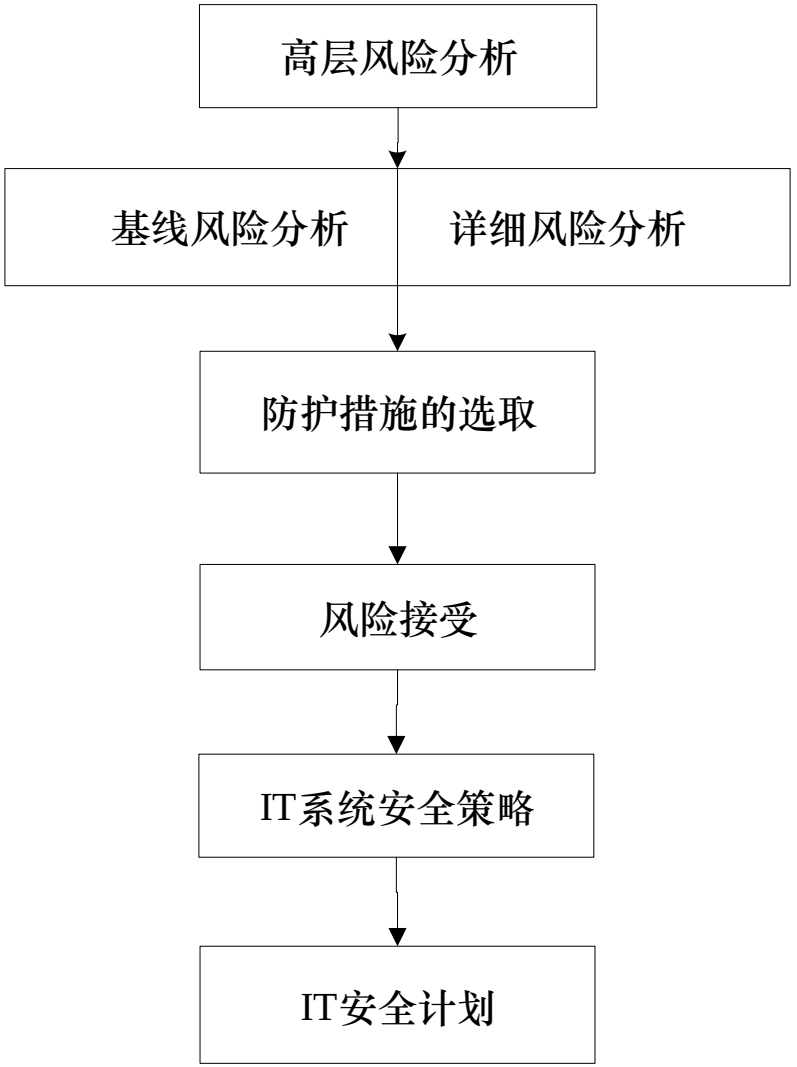
- (3)综合风险评估
  - 综合风险评估流程
    - 第一步：高层风险分析
      - 确定每个IT系统所采用的风险分析方法（基线或详细风险分析）
      - 考虑IT系统及其处理信息的业务价值、组织业务角度的风险
      - 实施风险分析
    - 第二步：依据基线或详细风险分析结果选取相应安全措施
      - 考虑信息系统的残余风险是否在可接受范围内
      - 如不可接受的风险则需要加强安全措施，必要时再评估。
    - 第三步：IT系统安全策略
      - IT系统安全策略是前面各阶段评估结果的结晶，包括系统安全目标、系统边界、系统资产、威胁、脆弱点、所选取的安全措施、安全措施选取的原因、费用估计等。
    - 第四步：IT安全计划
      - IT安全计划：可接受的安全风险的安全措施实施。

3.4 风险评估方法与标准

- (3)综合风险评估
  - 优点
    - 节省了评估所耗费的资源，又能确保获得一个全面系统的评估结果
    - 组织的资源和资金能够应用到最能发挥作用的地方，具有高风险的信息系统能够被预先关注。
  - 缺点
    - 如果初步的高级风险分析不够准确，某些本来需要详细评估的系统也许会被忽略，最终导致某些严重的风险未被发现。

3.4 风险评估方法与标准

- (3)综合风险评估
  - 综合风险评估流程
    - ISO/IEC 13335-3提出



3.4 风险评估方法与标准

- 3.风险评估标准
  - 详细风险评估标准
    - AS/NZS 4360
    - NISTSP800-30
    - OCTAVE
    - 我国的《信息安全风险评估指南》

3.4 风险评估方法与标准

- 3.风险评估标准
  - AS/NZS 4360-澳大利亚 /新西兰风险管理标准
    - AS/NZS 4360是ISO9000 系列的补充件
    - 应用于与一个组织所有活动相关的风险管理之中，具有极广泛的适用性；
    - 为各种类型组织提供了一套通用的风险管理模式和总体框架。
    - 有一套辅助性的标准与其相辅相成，更增加了实用性和广泛适用性。
    - 把分析风险背景放在第一步，将风险管理的目标与组织目标以及各利益相关方的要求整合在一起；
    - 强调风险沟通，充分发挥团队精神，调动各方面的积极性，为风险管理成功创造了良好的环境。

3.4 风险评估方法与标准

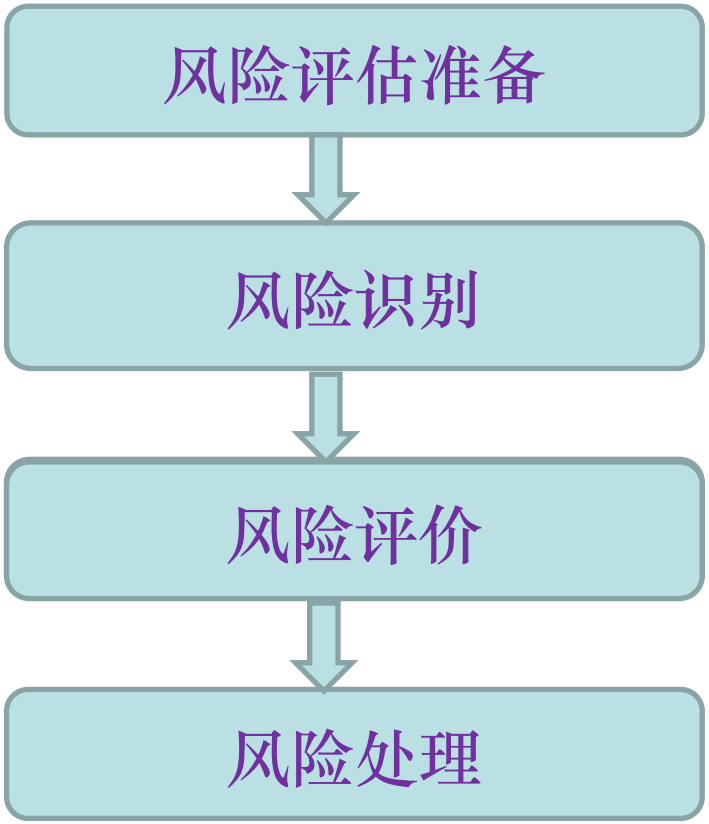
- 3.风险评估标准
  - NIST SP800-30
    - SP800系列特别报告书
      - 美国国家标准和技术学会NIST信息技术实验室(ITL)
      - 在计算机安全领域与业界、政府和学术组织协同工作的报告
    - NISTSP800-30《IT 系统风险管理指南》
      - 描述了风险管理方法
      - 结合系统发展生命周期的各个阶段, 说明风险管理过程与系统授权过程的紧密联系；
      - 提出了风险评估的方法论和一般原则；
      - 基本采用3级定义法，分级定义言简意赅；
      - 适合初步开展风险评估的组织使用。

3.4 风险评估方法与标准

- **3.风险评估标准**
  - **OCTAVE可操作的关键威胁、资产和弱点评估**
    - **Operational Critical Threat, Asset, Vulnerability Evaluation**
    - **一种信息安全风险评估的方法.**
      - 由美国卡耐基.梅隆大学CERT协调中心开发
        - » 软件工程研究所下属
      - 它由一系列循序渐进的讨论会组成, 每个讨论会都需要其参与者之间的交流和沟通。
      - 理清复杂的组织问题和技术问题, 了解安全问题, 改善组织的安全状况并解决信息安全风险。
    - **OCTAVE的基本原则:**
      - 自主、适应度量 、已定义的过程、连续过程的基础
    - **OCTAVE包括两种具体方法:**
      - 面向大型组织的**OCTAVE Method**
      - 面向小型组织的**OCTAVE-S**

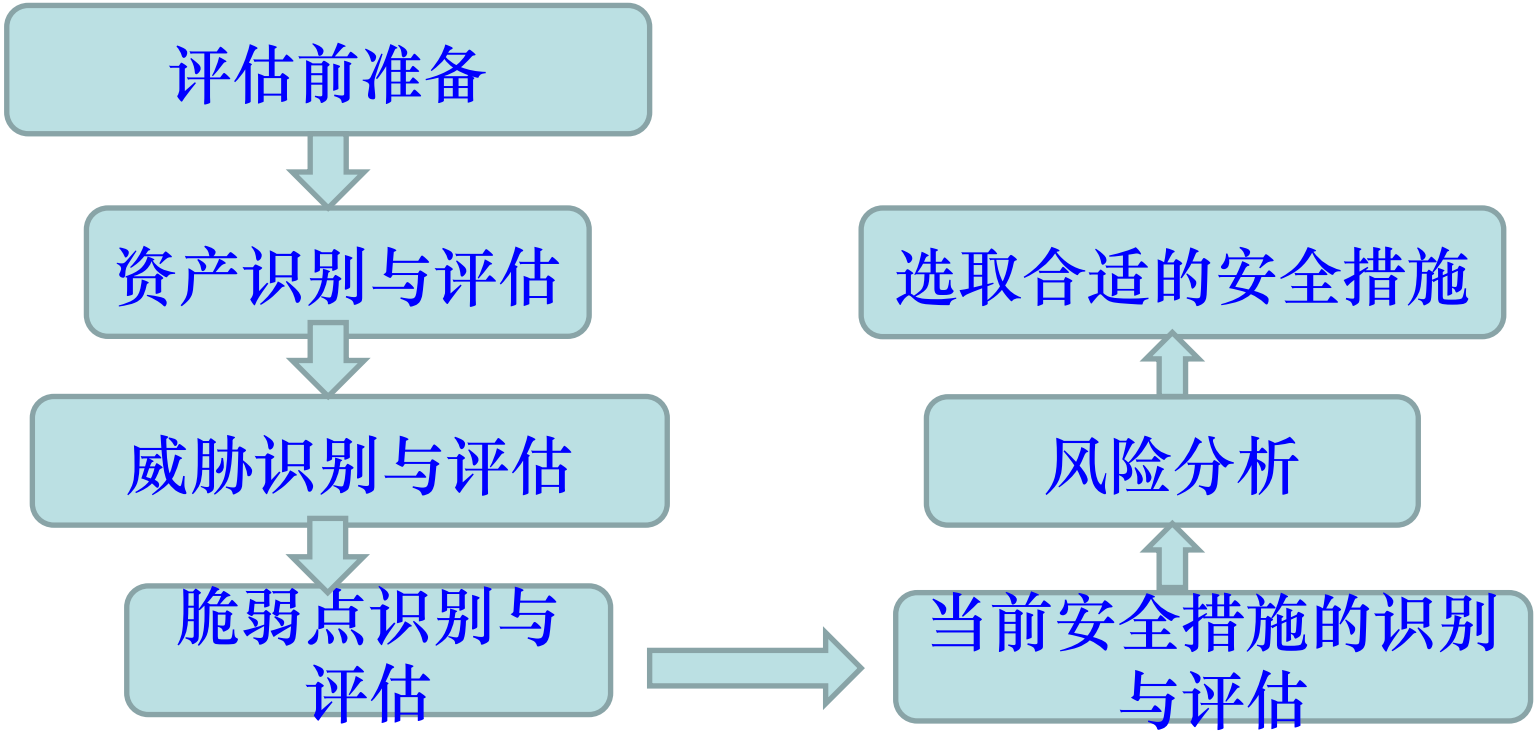
3.5 信息安全风险评估流程

- 1.风险评估流程
  - 具体流程有一定的差异
    - 都是围绕资产、威胁、脆弱点识别与评估展开；
    - 进一步分析不期望事件发生的可能性及其对组织的影响；
    - 最后考虑如何选取合适的安全措施，把安全风险降低到可以接受的程度。
  - 总体流程可分为四个阶段



3.5 信息安全风险评估流程

- 1. 风险评估总体流程
  - 狭义的风险评估流程



3.5 信息安全风险评估流程

- 2.信息安全风险评估策略
  - 不同的组织有不同的安全需求和安全战略，风险评估的操作范围可以是整个组织，也可以是组织中的某一部门，或者独立的信息系统、特定系统组件和服务。
  - 影响风险评估进展的某些因素，包括评估时间、力度、展开幅度和深度，都应与组织的环境和安全要求相符合。
  - 组织应该针对不同的情况来选择恰当的风险评估方法。常见的风险评估方法有三种：
    - 基线风险评估方法
    - 详细风险评估方法
    - 综合风险评估方法

3.5 信息安全风险评估流程

- **3.风险评估的准备**
  - 是整个风险评估过程有效性的保证。主要工作:
    - 确定风险评估目标
      - 明确目标(业务需求与合规性),为风险评估的过程提供导向
      - 信息系统是重要的资产，维持竞争优势、获利能力、法规要求和组织形象，是威胁的主要目标
      - 满足组织业务持续发展在安全方面的需要, 或符合相关方的要求, 或遵守法律法规的规定等。
    - 确定风险评估的对象和范围
      - 完成风险评估的前提
      - 对象：组织全部的信息及与信息处理相关的各类资产、管理机构, 也可能是某个独立的系统, 关键业务流程, 与客户知识产权相关的系统或部门等。
    - 组建团队（人员素质）
      - 由管理层、相关业务骨干、IT技术人员等组成风险评估小组。

3.5 信息安全风险评估流程

- 3.风险评估的准备
  - 选择方法（具体的风险判断方法）
    - 考虑评估的目的、范围、时间、效果、人员素质等因素来选择具体的风险判断方法，使之能够与组织环境和安全要求相适应。
  - 获得支持
    - 组织的最高管理者的支持、批准；
    - 对管理层和技术人员进行传达；
    - 在组织范围就风险评估相关内容进行培训，明确各有关人员的风险评估任务。
  - 准备相关的评估工具
    - 评估工具：信息收集与渗透测试工具、数据及文档管理工具
    - 主要是漏洞扫描、渗透测试等工具

3.5 信息安全风险评估流程

- 4.已有安全措施的确认
  - 已有安全措施可以分为两种：
    - 预防性安全措施和保护性安全措施

预防性安全措施

降低威胁利用脆弱点导致安全事件发生的可能性。

保护性安全措施

减少因安全事件发生对信息系统造成的影响，如业务持续性计划。

3.5 信息安全风险评估流程

- 5.风险评估文件和记录
- 整个风险评估过程中产生的评估过程文档和评估结果文档：
  - 风险评估计划
    - 阐述风险评估的目标、范围、团队、评估方法、评估结果的形式和实施进度等；
  - 风险评估程序
    - 明确评估的目的、职责、过程、相关的文件要求，并且准备实施评估需要的文档；
  - 资产识别清单
    - 根据组织在风险评估程序文件中所确定的资产分类方法进行资产识别，形成资产识别清单，明确各资产的责任人/部门；
  - 重要资产清单
    - 根据资产识别和赋值的结果，形成重要资产列表，包括重要资产名称、描述、类型、重要程度、责任人/部门等；

3.5 信息安全风险评估流程

- **5.风险评估文件和记录**
  - 威胁列表
    - 根据威胁识别和赋值的结果，形成威胁列表，包括威胁名称、种类、来源、动机及出现的频率等；
  - 脆弱点列表
    - 根据脆弱点识别和赋值的结果，形成脆弱点列表，包括脆弱点名称、描述、类型及严重程度等；
  - 已有安全措施确认表
    - 根据已采取的安全措施确认的结果，形成已有安全措施确认表，包括已有安全措施名称、类型、功能描述及实施效果等；
  - 风险评估报告
    - 对整个风险评估过程和结果进行总结，详细说明被评估对象，风险评估方法，资产、威胁、脆弱点的识别结果，风险分析、风险统计和结论等内容；

3.5 信息安全风险评估流程

- 5.风险评估文件和记录
  - 风险处理计划
    - 对评估结果中不可接受的风险制定风险处理计划；
    - 选择适当的控制目标及安全措施；
    - 明确责任、进度、资源；
    - 评价残余风险，确保所选择安全措施的有效性；
  - 风险评估记录
    - 根据组织的风险评估程序文件，记录对重要资产的风险评估过程。

3.6 风险分析与处理

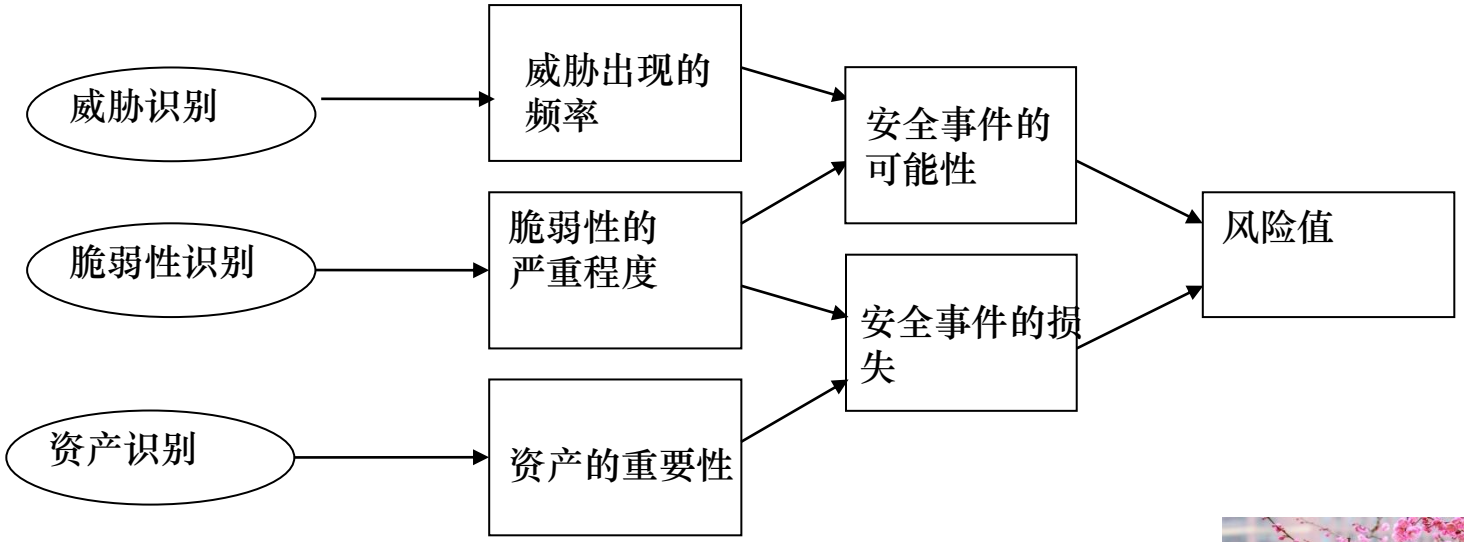
- 1.风险分析
  - 利用资产、威胁、脆弱点识别与评估结果以及已有安全措施的确认与分析结果，分析资产面临的风险。
  - 主要任务：
    - 分析当前环境下，安全事件发生的可能性以及造成的影响，然后利用一定的方法计算风险。
      - 安全风险总是以威胁利用脆弱点导致一系列安全事件的形式体现出来；
  - 风险的大小
    - 由安全事件造成的影响以及其发生的可能性来决定

3.6 风险分析与处理

- 风险计算
  - 风险可形式化的表示为R=(A, T, V), 其中R表示风险、A表示资产、T表示威胁、V表示脆弱点。相应的风险值由A、T、V的取值决定, 是它们的函数, 可以表示为：
  - VR=R(A, T, V)=R(L(A, T, V), F(A, T, V))
    - 其中, L(A, T, V)、F(A, T, V)分别表示对应安全事件发生的可能性及影响, 它们也都是资产、威胁、脆弱点的函数, 但其表达式很难给出。
    - 而风险则可表示为可能性L和影响F的函数, 简单的处理就是将安全事件发生的可能性L与安全事件的影响F相乘得到风险值, 实际就是平均损失,
    - 即VR= L(A, T, V)×F(A, T, V)。

3.6 风险分析与处理

- **2.我国的风险分析流程**
  - 《信息安全风险评估指南》在风险分析方面采用了简化的处理方法, 如图所示,
  - 相应的, 风险值**VR=R（A, T, V）= R(L(T, V), F(Ia, Va))**



3.6 风险分析与处理

- **2.我国的风险分析流程**
  - 安全事件可能性分析
    - 安全事件发生的可能性的因素有：

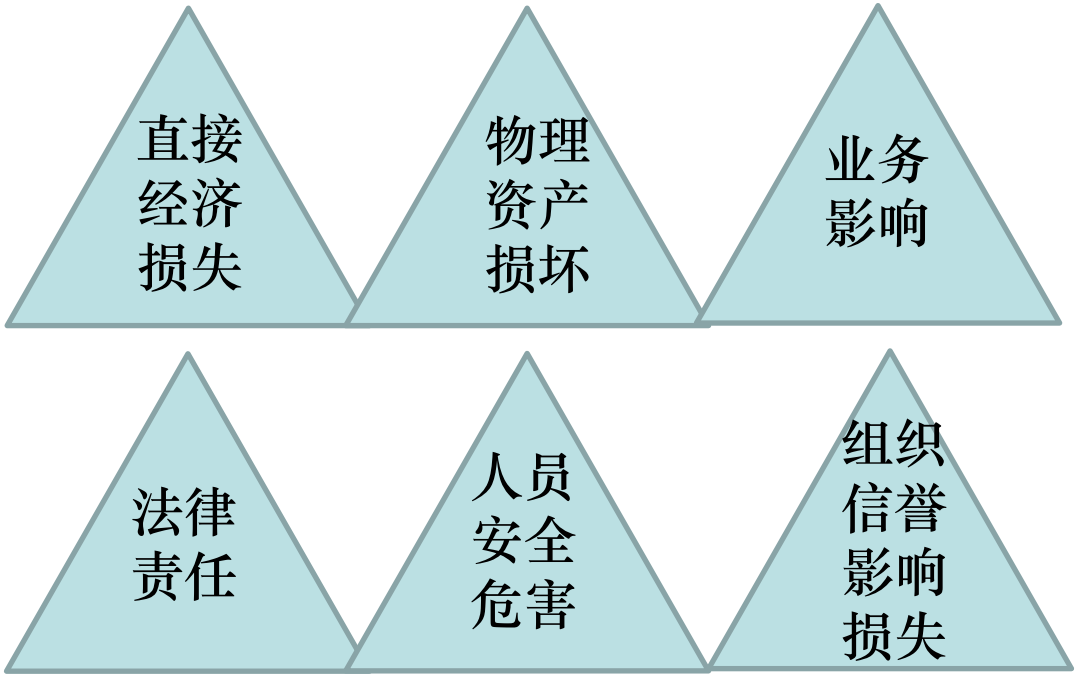
资产吸引力	威胁出现的可能性
脆弱点的属性	安全措施的效能
…	…

- 根据威胁源的分类，引起安全事件发生的原因可能是

自然灾害	环境及系统威胁
人员无意行为	人员故意行为
…	…

3.6 风险分析与处理

- **2.我国的风险分析流程**
  - 安全事件对组织的影响可体现在以下方面：



3.6 风险分析与处理

- 3.风险分析意义
  - 有助于对当前信息系统面临的风险进行分析
  - 确认并分析当前安全措施的有效性
    - 确认当前安全措施，是资产评估、威胁评估、脆弱点评估的有益补充，可用于后面的风险分析；
    - 分析当前安全措施的有效性,对保持整改替代意义
      - 保持有效的安全措施，以避免不必要的工作和费用，防止安全措施的重复实施；
      - 核实取消确认为不适当的安全措施应；
      - 选取更合适的安全措施替代。

3.6 风险分析与处理

- **4.风险处理**
  - 根据风险分析结果和组织的安全战略，提出新的安全需求，选取适当的安全措施，将安全风险控制在可接受的范围内。
    - 风险评估的目的就是获取组织面临的有关风险信息，采取适当的措施将安全风险控制在可接受的范围内。
  - **(1)提出新的安全需求**
    - 根据现有风险和安全战略目标，提出符合战略目标的新安全需求。

3.6 风险分析与处理

- 4.风险处理
  - (2)安全措施的选取
    - 全面认识组织面临的安全风险，根据风险的性质选取合适的安全措施；
      - 降低安全事件造成的影响；
      - 降低安全事件发生的可能性。
  - (3)分析残余风险是否可接受
    - 对采取新的安全措施后可能的残余风险进行分析，不可接收则重复步骤(1)；
    - 直到残余风险为可接受风险为止。

小结

- 信息安全风险评估概念
- 信息安全风险评估策略
- 信息安全风险评估流程
- 信息安全风险评估方法

作业

- 1. 名词解释
  - 风险；资产；威胁；脆弱点；安全措施、影响。
- 2. 信息资产可以分为哪几类？请分别举出一两个例子说明
- 3. 威胁源有哪些？其常见表现形式分别是什么？
- 4. 如何评估资产、威胁和脆弱点？如何计算风险？
- 5.什么是信息安全风险评估？它由哪些基本步骤组成？风险评估流程中主要包括哪些活动？
- 6. 风险评估方法分为哪几种？其优缺点分别是什么？
- 7. 请写出风险计算公式，并解释其中各项所代表的含义。
- 8. 风险评估文件由哪些主要文档组成？
- 9. 常用的综合评价方法有哪些，试进行比较。
- 10. 常用的定性与定量的风险分析方法有哪些？各有什么特点？