第二章 信息安全风险评估（上）

本章提纲

§1 概述

§2 风险评估策略

§3 风险评估流程

§4 风险评估方法

§5 风险评估案例

§1 概述

§1.1 信息安全风险评估相关要素

§1.2 信息安全风险评估

§1.3 风险要素相互间的关系

§1.1 信息安全风险评估相关要素

- 资产
- 威胁
- 脆弱点
- 风险
- 影响
- 安全措施
- 安全需求

资产

第一种定义

根据ISO/IEC 13335-1，资产是指任何对组织有价值的东西，包括：

- 物理资产（如计算机硬件，通讯设施，建筑物）
- 信息/数据（如文件，数据库）；软件
- 提供产品和服务的能力；人员
- 无形资产（如信誉，形象）

资产

- 第二种定义

我国的《信息安全风险评估指南》认为，资产是指对组织具有价值的信息资源，是安全策略保护的对象。它能够以多种形式（即表现形式）存在，有无形的、有形的，有硬件、软件，有文档、代码，也有服务、形象等。

基于表现形式的资产分类

分类	示例
数据	存在信息媒介上的各种数据资料，包括源代码、数据库数据、系统文档、运行管理规程、计划、报告、用户手册等
软件	系统软件：操作系统、语言包、工具软件、各种库等 应用软件：外部购买的应用软件，外包开发的应用软件等 源程序：各种共享源代码、可执行程序、自行或合作开发的各种程序等
硬件	网络设备：路由器、网关、交换机等 计算机设备：大型机、服务器、工作站、台式计算机、移动计算机等 存储设备：磁带机、磁盘阵列等 移动存储设备：磁带、光盘、软盘、U盘、移动硬盘等 传输线路：光纤、双绞线等 保障设备：动力保障设备（UPS、变电设备等）、空调、保险柜、文件柜、门禁、消防设施等 安全保障设备：防火墙、入侵检测系统、身份验证等 其他电子设备：打印机、复印机、扫描仪、传真机等
服务	办公服务：为提高效率而开发的管理信息系统（MIS），它包括各种内部配置管理、文件流转管理等服务 网络服务：各种网络设备、设施提供的网络连接服务 信息服务：对外依赖该系统开展服务而取得业务收入的服务
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、网络维护主管及应用项目经理及网络研发人员等
其它	企业形象，客户关系等

资产

两种定义之比较

- 两种定义基本上是一致的，所包含的内容也基本是一致的，主要的区别在于后者把资产限定在“信息资源”范围内，这是基于信息安全风险评估应用特殊性的考虑，信息安全风险评估应重点分析信息资产面临的风险。
- 从具体分类明细看，后者还是包含了其他内容，如保障设备、人员、企业形象、客户关系等，这些未必都能视为信息资产。

威胁

定义

- 威胁指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发生的事件发生，该事件可能对系统或组织及其资产造成损害。这些损害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。

威胁的分类

- 根据威胁源的不同，威胁可分为：
  - 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

威胁的分类

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、其他
环境威胁	火灾 、战争、重大疫情 、恐怖主义、供电故障、供水故障 、其他公共设施中断 、危险物质泄漏、重大事故（如交通工具碰撞等）、污染、温度或湿度、其他
系统威胁	网络故障、硬件故障 、软件故障 、恶意代码、存储介质的老化 、其他
外部人员	网络窃听、拒绝服务攻击、用户身份仿冒、系统入侵、盗窃、物理破坏、信息篡改、泄密、抵赖、其他。
内部人员	未经授权信息发布、未经授权的信息读写、抵赖、电子攻击（如利用系统漏洞提升权限）、物理破坏（系统或存储介质损坏）、盗窃、越权或滥用、误操作

WannaCry勒索危机

学院网信处也发布紧急通知：

各部门：

近期国内多所院校出现ONION勒索软件感染情况，磁盘文件会被病毒加密为.onion后缀，只有支付高额赎金才能解密恢复文件，对学习资料和个人数据了造成严重损失。

该勒索软件目前主要利用Windows系统的445端口进行传播，是不法分子利用NSA黑客武器库泄漏的“永恒之蓝”所发起的攻击事件。只要用户开机连网，不法分子就能远程在电脑和服务器中植入勒索软件、远程控制木马、虚拟货币挖矿机等恶意程序。

该漏洞在微软的安全公告中被标记为严重漏洞，影响到几乎所有版本的Windows系统，请尽快安装补丁，地址：https://technet.microsoft.com/zh-cn/library/security/MS17-010

请使用Windows系统的老师和同学尽快将系统更新至最新状态，并尽量使用移动硬盘等设备将重要文件离线备份。对于XP、2003等微软已不再提供支持的系统，可以使用360发布的“NSA武器库免疫工具”检测系统是否存在漏洞，并关闭受到漏洞影响的端口，以避免遭到勒索软件等病毒的侵害。免疫工具下载地址：http://dl.360safe.com/nsa/nsatool.exe。

网信处

2017年5月13日

“永恒之蓝”传播的勒索病毒以ONION和WNCRY两个家族为主，受害机器的磁盘文件会被篡改为相应的后缀，图片、文档、视频、压缩包等各类资料都无法正常打开，只有支付赎金才能解密恢复。这两类勒索病毒，勒索金额分别是5个比特币和300美元，折合人民币分别为5万多元和2000多元。

脆弱点

- 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。威胁总是要利用资产的脆弱点才可能造成危害。
- 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，这是脆弱点识别中最为困难的部分。

脆弱点的分类

- **技术脆弱点**
  - 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
  - 例如：安装杀毒软件或病毒库未及时升级，数据库访问控制机制不严格
- **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
  - 例如：系统机房钥匙管理不严、人员职责不清等

风险

定义

- 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。

风险三要素之间的关系

- 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。

风险的形式化表示

$$R = (A, T, V)$$

其中：R 表示风险、A 表示资产、T 表示威胁、V 表示脆弱点。

影响

定义

- 威胁利用资产的脆弱点导致不期望发生事件的后果。

  这些后果可能表现为：

  - ✓ 直接形式，如物理介质或设备的破坏、人员的损伤等
  - ✓ 间接的损失，如公司信用、形象受损、市场分额损失等

影响

- 直接/间接损失

  - 在信息安全领域，直接的损失往往容易估计且损失较小，间接的损失难以估计且常常比直接损失更为严重。

  - 如某公司信息系统中一路由器因雷击而破坏，其直接的损失表现为路由器本身的价值、修复所需的人力物力等；而间接损失则较为复杂，由于路由器不能正常工作，信息系统不能提供正常的服务，导致公司业务量的损失、企业形象的损失等，若该路由器为金融、电力、军事等重要部门提供服务，其间接损失更为巨大。

安全措施

定义

- 安全措施指为保护资产、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。

安全措施

理解

- 有效的安全通常要求不同安全措施的结合以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

理解

- 安全措施可能实现一个或多个下列功能：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包括：物理环境、技术领域、人员、管理等。
- 可用的安全措施包括：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。

安全需求

- 含义

安全需求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。

- 体现

安全需求可体现在技术、组织管理等多个方面。如关键数据或系统的的机密性/可用性/完整性、人员安全意识培训、系统运行实时监控的需求等。

§1.2 信息安全风险评估

基本思路

- 在信息安全事件发生之前，通过有效的手段对组织面临的信息安全风险进行识别、分析，并在此基础上选取相应的安全措施，将组织面临的信息安全风险控制在可接受范围内，以此达到保护信息系统安全的目的。

§1.2 信息安全风险评估

含义（广义）

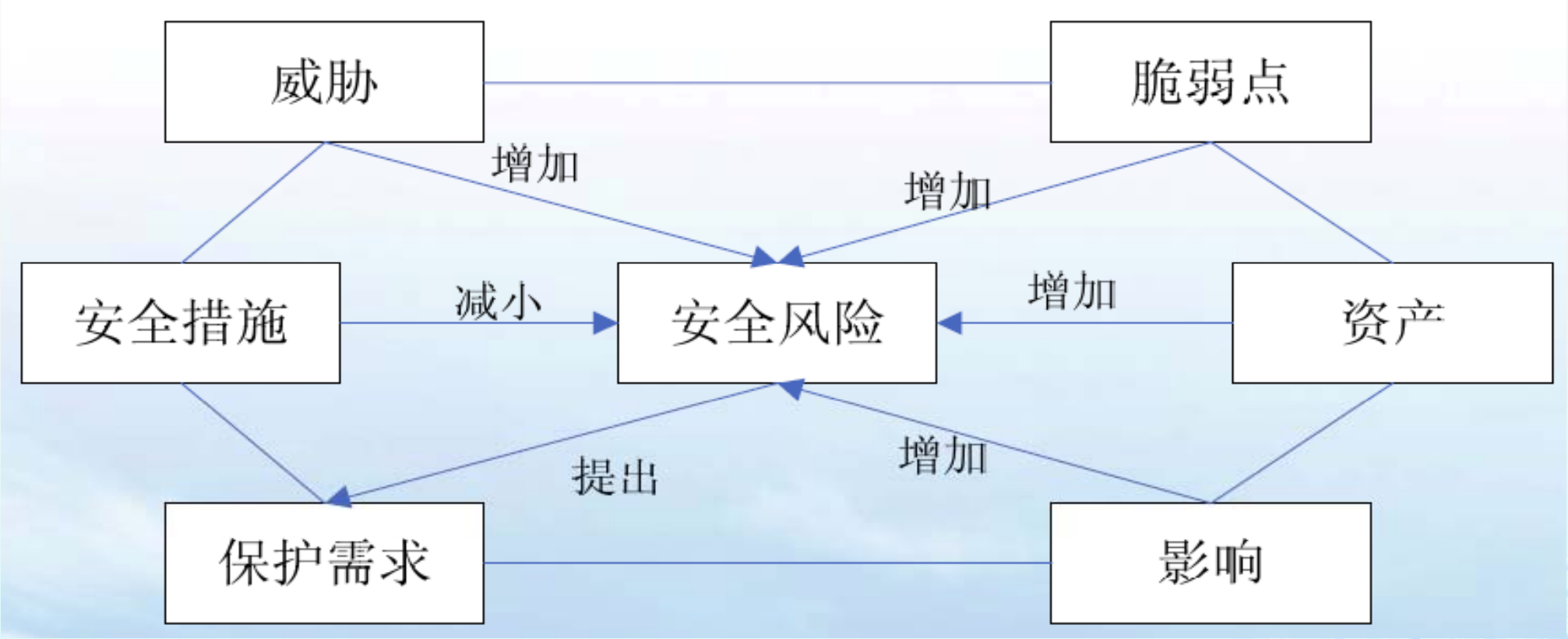
- 指依据有关信息安全技术与管理标准，对信息系统及由其处理、传输和存储的信息的机密性、完整性和可用性等安全属性进行评价的过程。
- 它要评估资产面临的威胁以及威胁利用脆弱点导致安全事件的可能性，并结合安全事件所涉及的资产价值来判断安全事件一旦发生对组织造成的影响。

§1.2 信息安全风险评估

- 含义（狭义）
  - 狭义的风险评估包括：评估前准备、资产识别与评估、威胁识别与评估、脆弱点识别与评估、当前安全措施的识别与评估、风险分析以及根据风险评估的结果选取适当的安全措施以降低风险的过程。

§1.3 风险要素相互关系

- 关系图（ISO/IEC 13335-1）



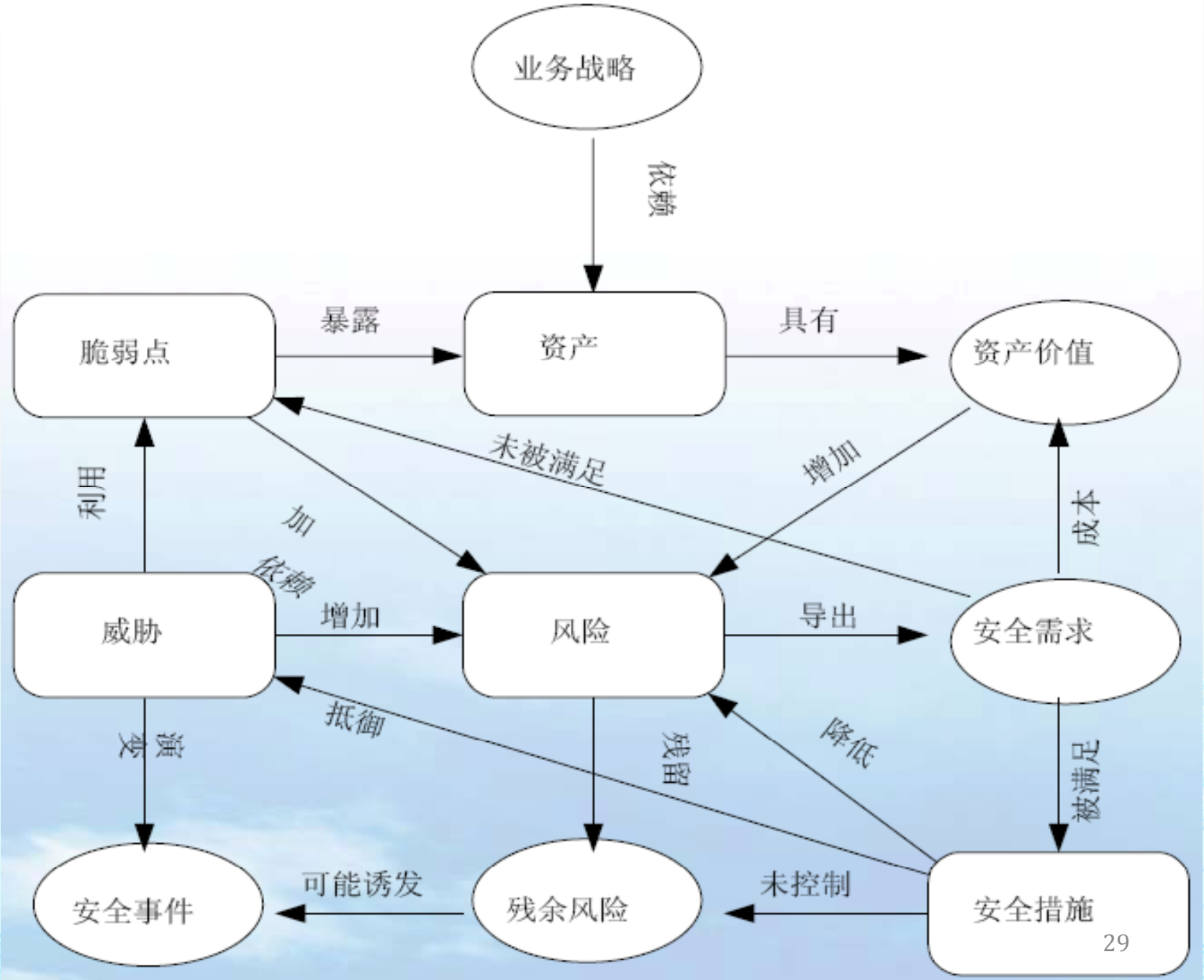
§1.3 风险要素相互关系

主要表现

- 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。

§1.3 风险要素相互关系

- （经我国）扩展后的风险要素关系模型



§1.3 风险要素相互关系

关系描述

- 业务战略依赖资产去实现；
- 资产是有价值的，组织的业务战略对资产的依赖度越高，资产价值就越大；
- 资产价值越大则其面临的风险越大；
- 风险是由威胁引发的，资产面临的威胁越多则风险越大，并可能演变成安全事件；
- 弱点越多，威胁利用脆弱点导致安全事件的可能性越大；
- 脆弱点是未被满足的安全需求，威胁要通过利用脆弱点来危害资产，从而形成风险；
- 风险的存在及对风险的认识导出安全需求；

§1.3 风险要素相互关系

关系描述

- 安全需求可通过安全措施得以满足，需要结合资产价值考虑实施成本；
- 安全措施可抵御威胁，降低安全事件的发生的可能性，并减少影响；
- 风险不可能也没有必要降为零，在实施了安全措施后还会有残留下来的风险。有些残余风险来自于安全措施可能不当或无效,在以后需要继续控制，而有些残余风险则是在综合考虑了安全成本与效益后未控制的风险，是可以被接受的；
- 残余风险应受到密切监视，它可能会在将来诱发新的安全事件。

§2 信息安全风险评估策略

§2.1 基线风险评估

§2.2 详细风险评估

§2.3 综合风险评估

§2.1 基线风险评估

含义

- 基线风险评估要求组织根据自己的实际情况，对信息系统进行基线安全检查（将现有的安全措施与安全基线规定的措施进行比较，找出其中的差距），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。
- 所谓的安全基线，是在诸多标准规范中规定的一组安全控制措施或者惯例，这些措施和惯例适用于特定环境下的所有系统，可以满足基本的安全需求，能使系统达到一定的安全防护水平。

§2.1 基线风险评估

- 安全基线的选择（资源）
  - 国际/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。

§2.1 基线风险评估

- 优点
  - 风险分析和每个防护措施的实施管理只需要最少数量的资源，并且在选择防护措施时花费更少的时间和努力；
  - 如果组织的大量系统都在普通环境下运行并且如果安全需要类似，那么很多系统都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。

§2.1 基线风险评估

- 缺点
  - 基线水平难以设置，如果基线水平设置的过高，有些IT系统可能会有过高的安全等级；如果基线水平设置的过低，有些IT系统可能会缺少安全，导致更高层次的暴露；
  - 风险评估不全面、不透彻，且不易处理变更。例如，如果一个系统升级了，就很难评估原来的基线防护措施是否充分。

§2.1 基线风险评估

综合评价

- 由于不同组织信息系统千差万别，信息系统的威胁时刻都在变化，很难制定全面的、具有广泛适用性的安全基线，而组织自行建立安全基线成本很高。
- 目前还没有全面、统一的、能符合组织目标的、值得信赖的安全基线，该评估策略开展并不普遍。

§2.2 详细风险评估

含义

- 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，并对可能引起风险的水平进行评估，这通过不期望事件的潜在负面业务影响评估和他们发生的可能性来完成。
- 不期望事件可能表现为直接形式，如直接的经济损失，如物理设备的破坏；也可能表现为间接的影响，如法律责任、公司信誉及形象的损失等。
- 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。

§2.2 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

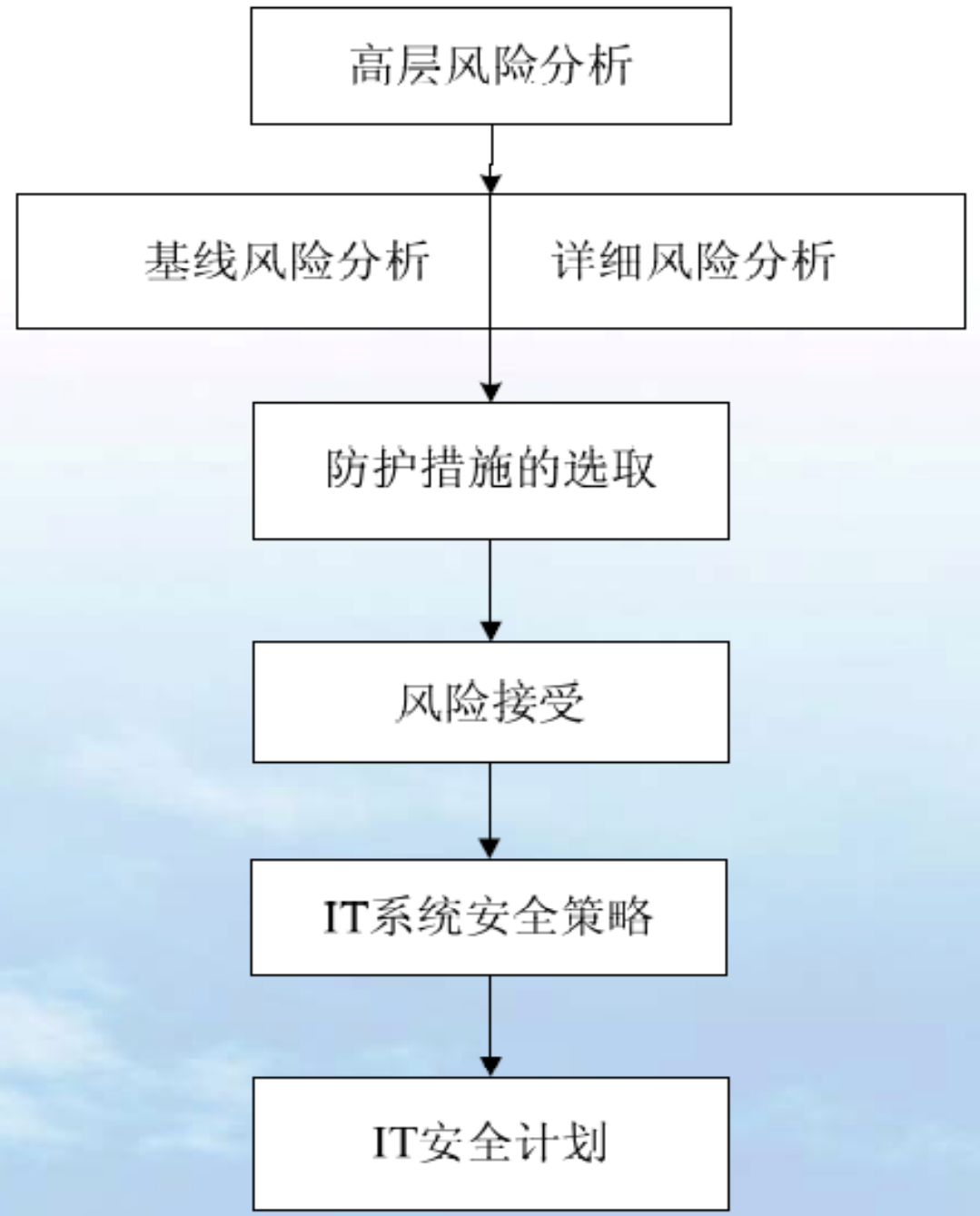
- 目前，世界各国推出的风险评估方法多属于这一类，如AS/NZS 4360、NISTSP800-30、OCTAVE以及我国的《信息安全风险评估指南》中所提供的方法。

§2.3 综合风险评估

- 动机（由来）
  - 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。因而实践当中，组织多是采用二者结合的综合评估方式。

§2.3 综合风险评估

- 综合风险评估框架（实施流程）



§2.3 综合风险评估

- 确定每个IT系统所采用的风险分析方法（基线/详细）
- 依据基线风险分析与详细风险分析的结果选取相应的安全措施，并检查上述安全措施实施后，信息系统的残余风险是否在可接受范围内，对不可接受的风险需要进一步加强安全措施，必要时应采取再评估。
- 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。
- IT安全计划则处理如何去实施所选取的安全措施。

§2.3 综合风险评估

- 优点
  - 结合基线和详细风险评估的优势，既节省了评估所耗费的资源，又能确保获得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。