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

§3 信息安全风险评估流程

§3.1 概述

§3.2 风险评估准备阶段

§3.3 资产识别与评估

§3.4 威胁识别与评估

§3.5 脆弱点识别与评估

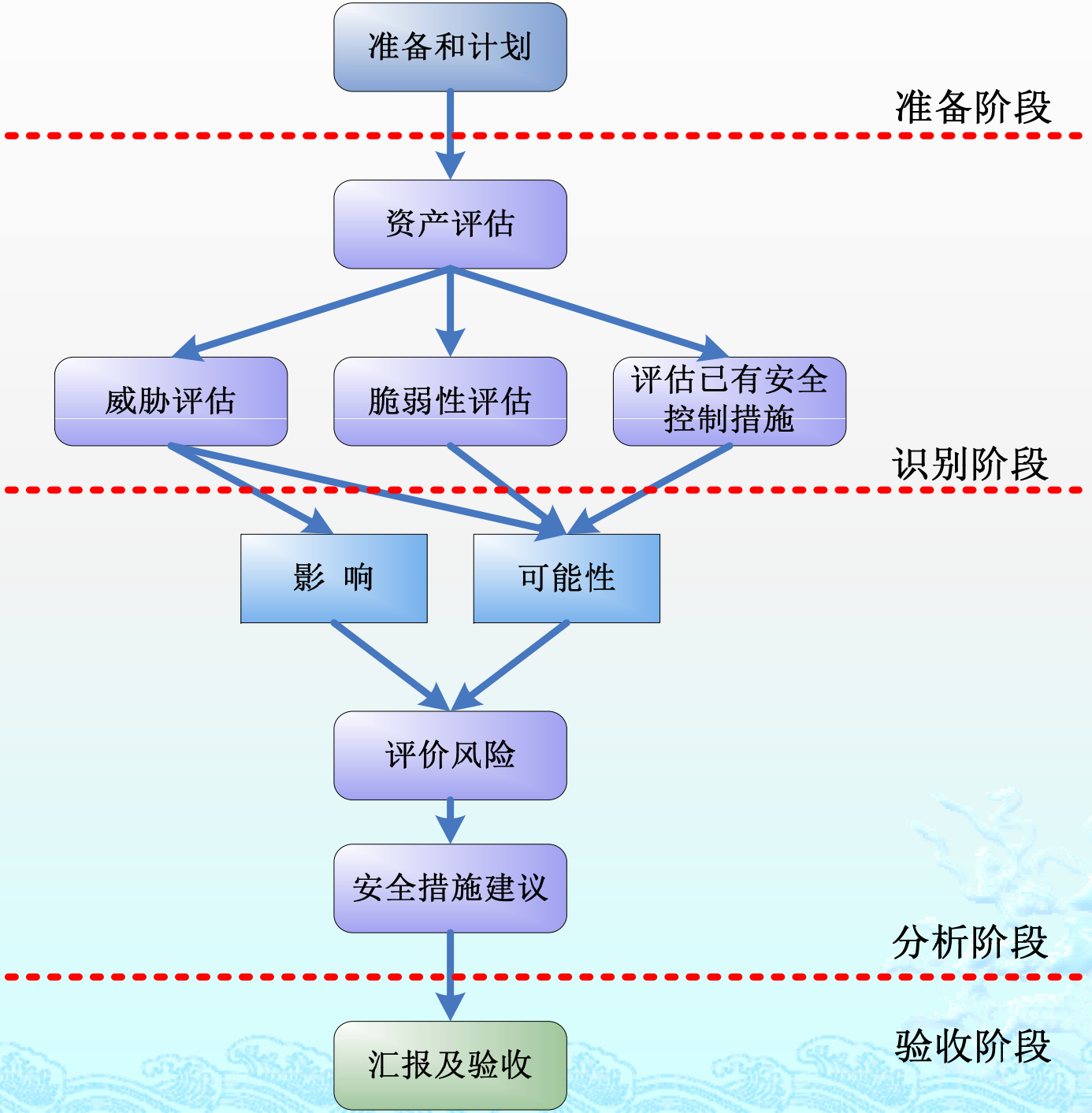
§3.6 已有安全措施的确认

§3.7 风险分析

§3.8 安全措施的选取

§3.9 风险评估文件和记录

§3 信息安全风险评估流程



§3.1 评估流程概述

一般流程

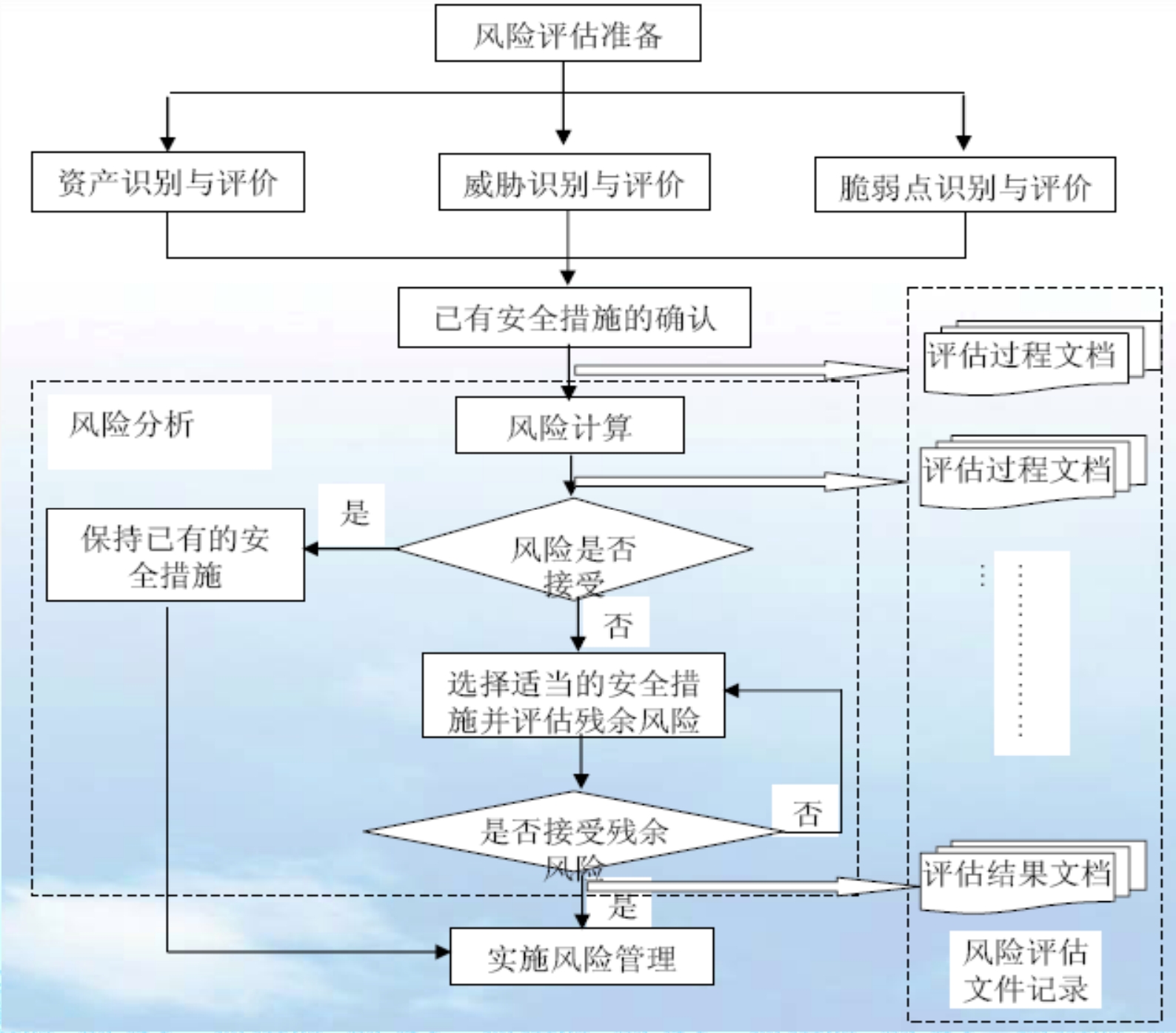
- 围绕资产、威胁、脆弱点识别与评估展开，并进一步分析不期望事件发生的可能性及其对组织的影响，最后考虑如何选取合适的安全措施，把安全风险降低到可以接受的程度

§3.1 评估流程概述

- 四个阶段
  - 风险评估准备
  - 风险识别：资产/威胁/脆弱点的识别
  - 风险评价：风险的影响分析、可能性分析以及风险的计算等，具体涉及到资产、威胁、脆弱点、当前安全措施的评价等
  - 风险处理：依据风险评估的结果选取适当的安全措施，将风险降低到可接受的程度

§3.1 评估流程概述

- 风险评估实施流程图



§3.2 风险评估准备阶段

主要工作

- 确定风险评估目标：风险评估的准备阶段应明确风险评估的目标，为风险评估的过程提供导向。
- 确定风险评估的对象和范围：对象可能是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。

§3.2 风险评估准备阶段

主要工作（续）

- 组建团队：组建适当的风险评估管理与实施团队，以支持整个过程的推进，如成立由管理层、相关业务骨干、IT技术人员等组成的风险评估小组。
- 选择方法：应考虑评估的目的、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：应得到组织的最高管理者的支持、批准，并对管理层和技术人员进行传达，应在组织范围就风险评估相关内容进行培训，以明确各有关人员的任务。

§3.2 风险评估准备阶段

主要工作（续）

- 准备相关的评估工具：为保证风险评估的顺利进行，需要相应的评估工具支持，如信息收集工具、数据及文档管理工具。

✓ 信息收集工具包括漏洞扫描工具、渗透性测试工具等

✓ 数据及文档管理工具主要用来收集和管理评估所需要的数据和资料，并根据需要的格式生成各种报表，帮助决策。

§3.3 资产识别与评估

资产识别

- 资产识别的任务：对确定的评估对象所涉及的资产进行详细的标识。
- 资产识别的方法：访谈、现场调查、问卷、文档查阅等。
- 资产识别过程中要特别注意无形资产的遗漏，同时还应注意不同资产间的相互依赖关系，关系紧密的资产可作为一个整体来考虑，同一中类型的资产也应放在一起考虑。

§3.3 资产识别与评估

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。
- 资产评价常以定性的形式进行，依据重要程度的不同划分等级，具体划分为多少级应根据具体问题具体分析，如5级划分方法为：非常重要、重要、比较重要、不太重要、不重要等，对这些定性值也可赋以相应的定量值，如：5、4、3、2、1。

§3.3 资产识别与评估

资产评估：综合价值

- 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所评价资产的安全属性。信息安全风险评估中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。可以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。

§3.3 资产识别与评估

- 综合价值计算方法1：最大原则
  - 资产价值在机密性、完整性、可用性、可审计性和不可抵赖性方面不是均衡的，在某个方面可能大，某个方面可能小，最大原则是取最大的那个方面的赋值作为综合评价值，即

$$VA = \max\{ VA_c, VA_i, VA_a , VA_{ac}, VA_n \}$$

  - ✓ 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VA_c、VA_i、VA_a、VA_{ac}、VA_n,综合价值记为VA

§3.3 资产识别与评估

综合价值计算方法2：加权原则

- 根据机密性、完整性、可用性、可审计性和不可抵赖性保护对组织业务开展影响的大小，分别赋予非负权值 W_c、W_i、W_a、W_{ac}、W_n（$W_c+W_i+W_a+W_{ac}+W_n=1$），综合价值由加权求得：

$$VA = VA_c*W_c+VA_i*W_i+VA_a*W_a+VA_{ac}*W_{ac}+VA_n*W_n$$

§3.3 资产识别与评估

- **资产评估：**我国《信息安全风险评估指南》推荐方法
  - 先对资产在机密性、完整性、可用性三个方面分别进行定性赋值，然后通过一定的方法进行综合，所使用的综合方法基本属于最大原则。
  - 以下是所给出的机密性赋值表。

资产机密性赋值表

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开的信息，向外扩散有可能对组织的利益造成损害
1	可忽略	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

§3.4 威胁识别与评估

威胁识别

- 威胁识别的任务是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，也可根据有关标准、组织所提供的威胁参考目录进行分析。

§3.4 威胁识别与评估

威胁分类

- 德国的《IT基线保护手册》将威胁分为五大类，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，手册分别对每类威胁进行了详细列举和说明，因而是威胁识别的重要参考。

§3.4 威胁识别与评估

威胁配置文件

- OCTAVE则通过建立威胁配置文件来进行威胁识别与分析，威胁配置文件包括5个属性，分别是：资产（assert）、访问(access)、主体(actor)、动机(motive)、后果(outcome)。

§3.4 威胁识别与评估

- 人类利用网络访问的威胁树

- 系统故障威胁树


资产
主体
后果
资产
硬件故障
软件故障
恶意代码
存储介质老化
中断
泄漏
更改
丢失、损坏
中断
泄漏
更改
丢失、损坏
中断
泄漏
更改
丢失、损坏
中断
泄漏
更改
丢失、损坏

§3.4 威胁识别与评估

- **威胁评估**：以下三方面内容，对威胁评估很有帮助：
  - 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；
  - 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；
  - 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 。

§3.4 威胁识别与评估

威胁评估结果

- 威胁评估的结果一般都是定性的，我国的《信息安全风险评估指南》将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。如下页表中所示。

§3.4 威胁识别与评估

➢ 威胁评估结果

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

§3.5 脆弱点识别与评估

脆弱点识别

- 脆弱点识别主要从技术和管理两个方面进行
- 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。
- 管理脆弱点又可分为技术管理和组织管理两方面，前者与具体技术活动相关，后者与管理环境相关。

§3.5 脆弱点识别与评估

- 我国的《信息安全风险评估指南》列举了不同对象的脆弱点识别内容参考

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

§3.5 脆弱点识别与评估

脆弱点识别

- 脆弱点识别将针对每一项需要保护的资产，找出可能被威胁利用的弱点，并对脆弱点的严重程度进行评估。
- 脆弱点识别方法主要有：问卷调查、工具检测、人工核查、文档查阅、渗透性测试等。

§3.5 脆弱点识别与评估

脆弱点评估

- 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，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。也可以对脆弱点被利用后对资产的损害程度以及被利用的可能性分别评估，然后以一定方式综合。

§3.5 脆弱点识别与评估

- 脆弱点分级
  - 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，将脆弱点严重程度的等级划分为五级

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

§3.6 已有安全措施的确认

安全措施

- **预防性安全措施**可以降低威胁利用脆弱点导致安全事件发生的可能性。这通过两个方面的作用实现，（1）减少威胁出现的频率，如通过安全培训可以减少无意行为导致安全事件出现的频率；（2）减少脆弱点，如及时对硬件设备定期检查能够减少系统的技术脆弱点等。
- **保护性安全措施**可以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。

§3.6 已有安全措施的确认

- 该步骤的主要任务：对当前信息系统所采用的安全措施进行标识，并对其预期功能、有效性进行分析。
- 对已采取的安全措施进行确认，至少有两个方面的意义
  - 有助于对当前信息系统面临的风险进行分析，由于安全措施能够减少安全事件发生的可能性及影响，对当前安全措施进行分析与确认，是资产评估、威胁评估、脆弱点评估的有益补充，其结果可用于后面的风险分析；
  - 通过对当前安全措施的确认，分析其有效性，对有效的安全措施继续保持，以避免不必要的工作和费用，防止安全措施的重复实施。对于确认为不适当的安全措施应核实是否应被取消，或者用更合适的安全措施替代，这有助于随后进行的安全措施的选取。

§3.7 风险分析

概念

- 风险分析就是利用资产、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，对资产面临的风险进行分析。
- 由于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，风险的大小是由安全事件造成的影响以及其发生的可能性来决定，风险分析的主要任务就是分析当前环境下，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。

§3.7 风险分析

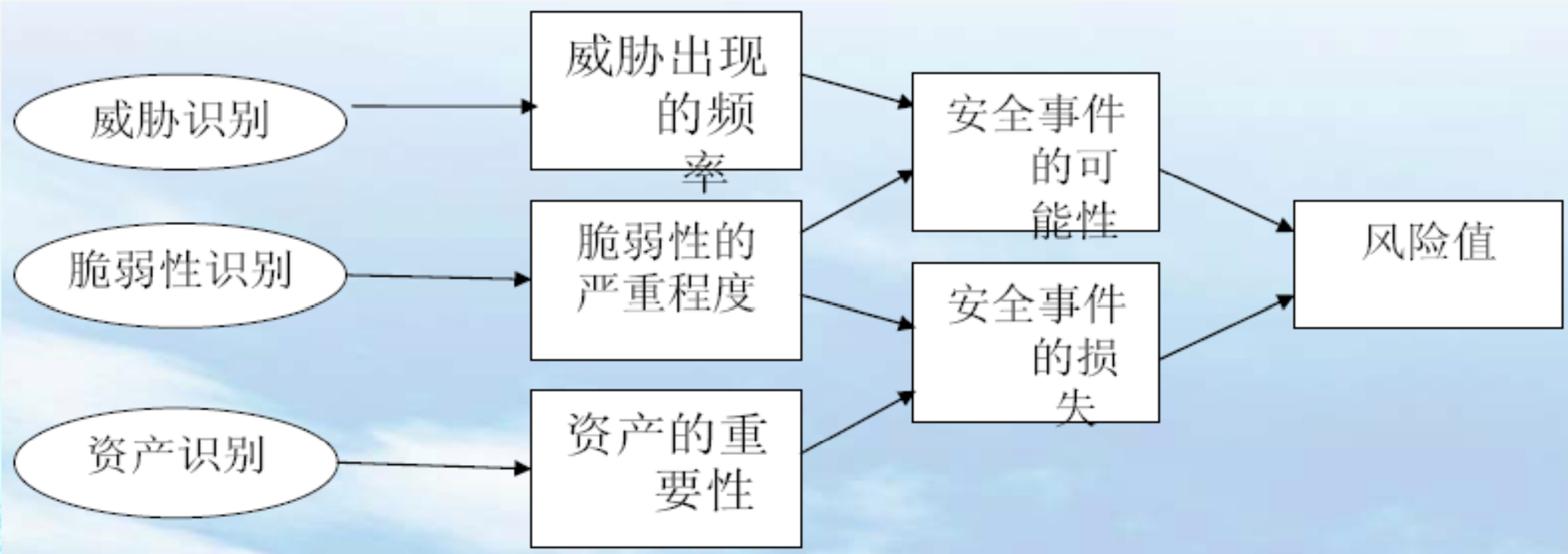
风险计算

- 风险的形式化表示：R=(A,T,V)
- 风险值由A、T、V的取值决定，是它们的函数，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，但表达式难给出。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)。

§3.7 风险分析

风险计算

- 我国的《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，其风险分析流程如图所示，相应的，风险值 VR = R(A, T, V) = R(L(T, V), F(A, V))



§3.7 风险分析

- 影响分析，安全事件对组织的影响体现在：
  - 直接经济损失：风险事件可能引发直接的经济损失
  - 物理资产的损坏：物理资产损坏的经济损失也很容易计算，可用更新或修复该物理资产的花费来度量
  - 业务影响：如业务中断，可用“单位时间损失×修复所需时间＋修复代价”可将业务影响表示为经济损失。业务影响还包括经营业绩影响、市场影响等

§3.7 风险分析

- 影响分析，安全事件对组织的影响体现在：
  - 法律责任：如由于安全故障导致机密信息的未授权发布、未能履行合同规定的义务或违反有关法律、规章制度的规定，这些可用由于应承担应有的法律责任可能支付赔偿金额来表示经济损失。
  - 人员安全危害：风险事件可能对人员安全构成危害，甚至危及到生命，这类损失很难用货币衡量。
  - 组织信誉、形象损失：风险事件可能导致组织信誉、形象受损，这类损失很难用直接的经济损失来估计，应通过一定的方式计算潜在的经济损失，如由于信誉受损，可能导致市场份额损失、与外部关系受损等，市场份额损失可以转化为经济损失，与外界各方关系的损失可通过分析关系重建的花费、由于关系受损给业务开展带来的额外花费等因素来估计。

§3.7 风险分析

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、安全措施的效能等。
- 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、人员故意行为等。不同类型的安全事件，其可能性影响因素也有点不同。

§3.8 安全措施的选取

- 风险评估的目的不仅是获取组织面临的有关风险信息，更重要的是采取适当的措施将安全风险控制在可接受的范围内。
- 如前所述，安全措施可以降低安全事件造成的影响，也可以降低安全事件发生的可能性，在对组织面临的安全风险有全面认识后，应根据风险的性质选取合适的安全措施，并对对可能的残余风险进行分析，直到残余风险为可接受风险为止。

§3.9 风险评估文件和记录

- 风险评估文件包括在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，包括：
  - 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，清单中应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；

§3.9 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；
- 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，并通过对残余风险的评价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

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

§4 风险评估方法

§4.1 风险矩阵测量法

§4.2 威胁分级计算法

§4.3 风险综合评价法

§4.1 风险矩阵测量法

基本方法

- 事先建立资产价值、威胁等级和脆弱点等级的一个对应矩阵，预先确定风险等级。然后根据不同资产的赋值从矩阵中确定不同的风险。资产风险判别矩阵（见教材 P50）。
- 对于每一资产的风险，都将考虑资产价值、威胁等级和脆弱点等级。

§4 风险评估方法

§4.1 风险矩阵测量法

§4.2 威胁分级计算法

§4.3 风险综合评价法

§4.2 威胁分级计算法

基本方法

- 直接考虑威胁、威胁导致的安全事件对资产产生的影响以及威胁导致安全事件发生的可能性来确定风险。
- 首先确定威胁导致的安全事件对资产产生的影响，可用等级来表示。识别威胁的过程可以通过两种方法完成。一是准备威胁列表，让系统所有者去选择相应资产的威胁，或由评估团队的人员识别相关的威胁，进行分析和归类。

§4.2 威胁分级计算法

基本方法

- 然后评价威胁导致安全事件发生的可能性。在确定影响值和可能性之后，计算风险值。风险的计算方法，可以是影响值与可能性之积，也可以是之和，或利用前面所述的效用函数来计算，具体算法由用户来定。在本例中，风险的测量采用两值的乘积，如表所示。

§4.2 威胁分级计算法

- 举例

资产	威胁描述	影响（资产）值	威胁发生可能性(c)	风险测度	风险等级划分
某个资产	威胁A	5	2	10	2
	威胁B	2	4	8	3
	威胁C	3	5	15	1
	威胁D	1	3	3	5
	威胁E	4	1	4	4
	威胁F	2	4	8	3

§4 风险评估方法

§4.1 风险矩阵测量法

§4.2 威胁分级计算法

§4.3 风险综合评价法

§4.3 风险综合评价法

基本原理

- 这种方法中风险由威胁导致的安全事件发生的可能性、对资产的影响程度以及已经存在的控制措施三个方面来确定。与风险矩阵法和威胁分级法不同，本方法将控制措施的采用引入风险的评价之中。
- 在这种方法中，识别威胁的类型是很重要的。从资产的识别开始，接着识别威胁以及对应安全事件发生的可能性。然后对威胁造成的影响进行分析，在这里对威胁的影响进行了分类型的考虑。比如对人员的影响、对财产的影响、对业务的影响，将以上各值相加添入数值表中。比如，本例中将可能性分为5级：1—5；影响也分为5级：1—5。在可能性和影响确定后，计算总的影响值。本例中采用加法。
- 最后分析是否采用了能够减小威胁的控制措施。这种控制措施包括从内部建立的和从外部保障的，并确定它们的有效性，对其赋值。本例中将控制措施的有效性有小到大分为5个等级，1—5。在此基础上再求出总值，即风险值，本例采用“影响值—控制措施赋值”来计算。

§4.3 风险综合评价法

- 实例

威胁类型	可能性	对人的影响	对财产的影响	对业务的影响	影响值	已采用的控制措施		风险度量
						内部	外部	
威胁A	4	1	1	2	8	2	2	4

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

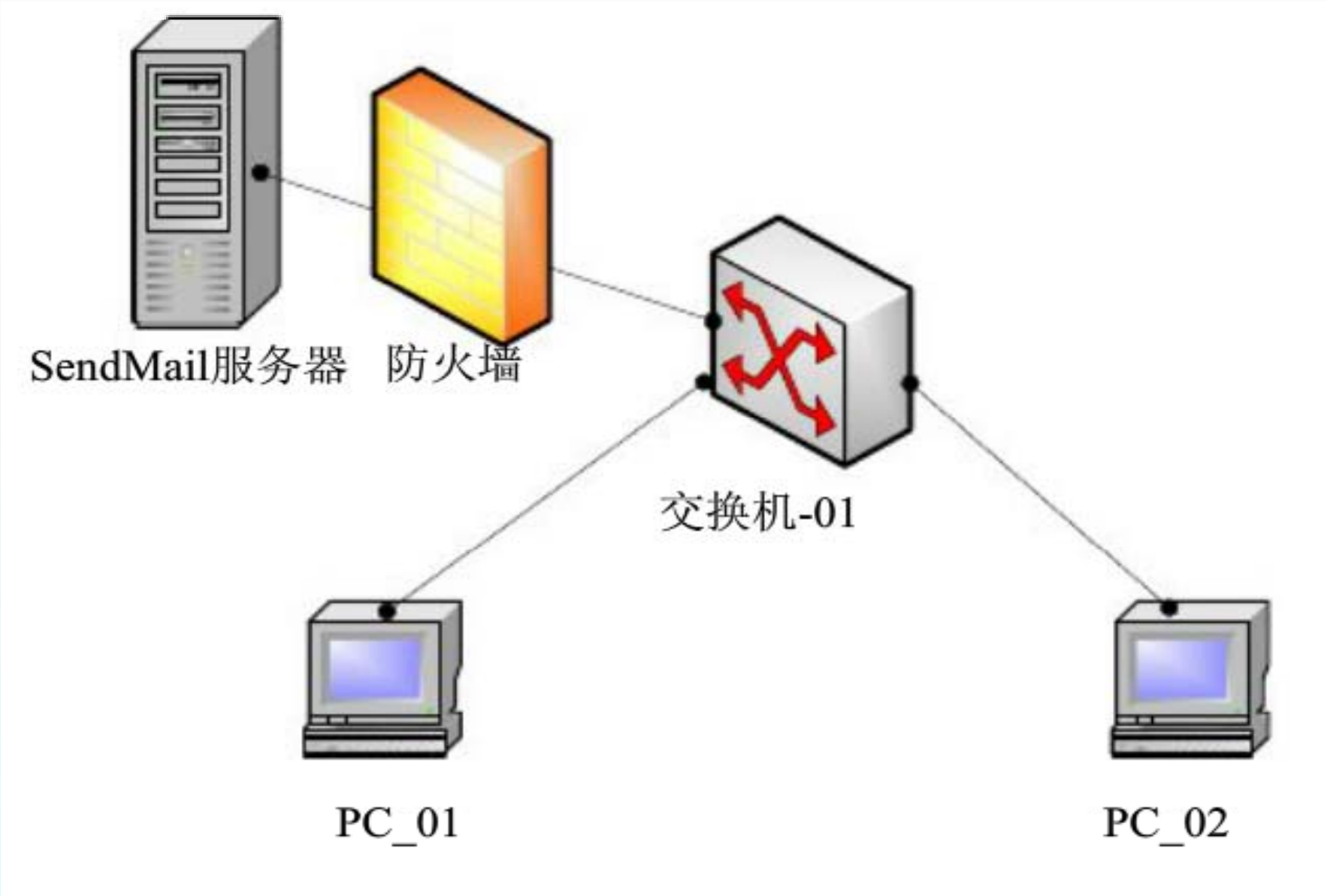
§5 风险评估案例

案例一：术语理解

- A公司的主机数据库由于存在XX漏洞，然后攻击者B利用此漏洞对主机数据库进行了攻击，造成A公司业务中断3天。（一次安全事件）
  - ✓ 风险：数据库被攻击者攻击；
  - ✓ 资产：主机数据库；
  - ✓ 威胁：攻击者B；
  - ✓ 弱点：XX漏洞；
  - ✓ 影响：业务中断3天；
- 部分提供风险评估业务的网络安全公司：启明星辰、绿盟科技等

案例二：某电子邮件系统的资产评估

Mail系统网络拓扑结构



业务识别

- 电子邮件系统作为全系统的通信基础设施，为各种业务提供通用的通信平台。
- 发文、收文、信息服务、档案管理、会议管理

资产识别与分类

- 硬件资产清单

资产编号	资产名称	责任人	资产描述
ASSET_01	Mail Server	A	Mail 服务器，软件版本为 SendMail v8.9.3
ASSET_02	Fire Wall_01	B	防火墙，软件版本为 IPTables v1.2.11
ASSET_03	Switch_01	B	骨干交换机
ASSET_04	PC_01	C	用户终端
ASSET_05	PC_02	D	用户终端

资产识别与分类

- 文档和数据资产清单

资产编号	资产名称	责任人	资产描述
ASSET_06	人员档案	E	机构人员档案数据
ASSET_07	电子文档数据	E	OA 系统中的电子文件

资产识别与分类

- 制度资产清单

资产编号	资产名称	责任人	资产描述
ASSET_08	安全管理制度	E	机房安全管理制度等
ASSET_09	备份制度	E	系统备份制度

资产识别与分类

- 人员资产清单

资产编号	资产名称	责任人	资产描述
ASSET_10	杨肖	A	系统管理员
ASSET_11	石丹	B	网络管理员
ASSET_12	孙悦	C	普通用户
ASSET_13	万黎	D	普通用户
ASSET_14	王玉龙	E	档案和数据管理员，制度实施者

安全需求分析

- 资产识别记录表格（以**ASSET_01** 为例，人工访谈）

资产识别活动信息			
日期	2007-7-2	起止时间	2007-7-4
访谈者	A	访谈对象及说明	系统管理员
地点说明	640		
记录信息			
所属类别	硬件资产		
资产名称	Mail Server	资产编号	ASSET_01
IP 地址	59.64.156.193	物理位置	机房
功能描述	接收和发送电子邮件		
机密性要求	很高		
完整性要求	很高		
可用性要求	很高		
重要程度	很高		
安全控制措施	防火墙		
负责人	A		
备注			

资产赋值

- 资产CIA三性等级表

资产编号	资产名称	机密性	完整性	可用性
ASSET_01	Mail Server	5	5	5
ASSET_02	Fair Wall_01	5	5	5
ASSET_03	Switch_01	5	5	5
ASSET_04	PC_01	2	2	2
ASSET_05	PC_02	2	2	2
ASSET_06	人员档案	5	5	2
ASSET_07	电子文档数据	5	5	3
ASSET_08	安全管理制度	1	4	4
ASSET_09	备份制度	1	4	4
ASSET_10	A	5	3	2
ASSET_11	B	5	3	2
ASSET_12	C	1	3	2
ASSET_13	D	1	3	2
ASSET_14	E	1	3	2

资产赋值

资产价值计算

资产价值应依据资产在机密性、完整性和可用性上的赋值等级，经过综合评定得出，根据本系统的业务特点，采取相乘法决定资产的价值，计算公式如下，其中：v 表示资产价值，x 表示机密性，y 表示完整性，z 表示可用性。$v=\sqrt{z*\sqrt{x*y}}$

资产等级划分：资产重要性程度判别准则

资产价值	资产等级	资产等级值	描述
(4.2, 5]	很高	5	非常重要，其安全属性破坏后可能对组织造成非常严重的损失
(3.4, 4.2]	高	4	重要，其安全属性破坏后可能对组织造成比较严重的损失
(2.6, 3.4]	中等	3	比较重要，其安全属性破坏后可能对组织造成中等程度的损失
(1.8, 2.6]	低	2	不太重要，其安全属性破坏后可能对组织造成较低的损失
(1, 1.8]	很低	1	不重要，其安全属性破坏后可能对组织造成很小的损失，甚至忽略不计

资产赋值

资产价值表

资产编号	资产名称	资产价值	资产等级	资产等级值
ASSET_01	Mail Server	5	很高	5
ASSET_02	Fair Wall_01	5	很高	5
ASSET_03	Switch_01	5	很高	5
ASSET_04	PC_01	2	低	2
ASSET_05	PC_02	2	低	2
ASSET_06	人员档案	3.2	中	3
ASSET_07	电子文档数据	3.9	高	4
ASSET_08	安全管理制度	2.8	中	3
ASSET_19	备份制度	2.8	中	3
ASSET_10	A	2.8	中	3
ASSET_11	B	2.8	中	3
ASSET_12	C	2.4	低	2
ASSET_13	D	2.4	低	2
ASSET_14	E	2.8	中	3

案例三：多媒体教学系统

§5 案例三

§5.1 案例介绍

§5.2 资产识别与评估

§5.3 威胁识别与评估

§5.4 脆弱点识别与评估

§5.5 风险分析与等级划分

§5.6 安全措施的选取

§5.1 案例介绍

- 多媒体教学系统是学校常用的信息系统，它为课堂教学提供信息化平台。本节以多媒体教学系统这一简单信息系统为例讲述详细风险评估的实施过程。
- 对多媒体教学系统，其安全需求主要表现为系统的可用性，而完整性、机密性安全需求很低，通常不会涉及到，因而风险评估主要围绕系统的可用性展开，风险评估的目的是通过分析系统面临的影响系统可用性的安全风险，并选取相应的安全措施降低风险。

§5.2 资产识别与评估

资产类别	名称	关键程度	
硬件	多媒体电脑	高	4
	投影仪	高	4
	控制台	中	3
	供电设备	高	4
	投影幕	低	2
	空调	中	3
	网络电缆及接口	低	2
软件	系统软件	中	3
	课件播放软件	中	3
	应用软件	中	3
	杀毒软件	低	2
信息	多媒体课件	低	2
	演示程序	低	2
人员	课室管理人员	中	3
	技术支持人员	中	3
	安全保卫人员	低	2

§5.3 威胁识别与评估

威胁类型	威胁表现形式	评估等级	
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	很低	1
环境威胁	供电中断	中	3
	火灾、供水故障、污染、极端温度或湿度	低	2
系统威胁	电脑、投影仪硬件故障	低	2
	网络故障	中	3
	系统软件、应用软件故障、课件播放软件故障	高	4
	恶意代码	很高	5
人员威胁	盗窃	高	4
	物理硬件故意破坏	中	3
	误操作	很高	5
	疾病或其他原因导致不能及时到岗	中	3

§5.4 脆弱点识别与评估

可能威胁	脆弱点	评估等级	
供电中断	没有备用电源	高	4
盗窃、物理破坏	安全保卫机制不健全	很高	5
疾病或其他原因导致不能及时到岗	课室钥匙管理人员无“备份”	高	4
	多媒体技术支持人员无“备份”	高	4
误操作	老师对多媒体课室使用注意事项不熟悉	很高	5
火灾	未部署防火设施	很高	5
极端温度及湿度	未安装空调及除湿设备	高	4
软件故障	软件的安装与卸载权限管理机制不严	高	4
恶意代码	杀毒软件不能及时升级	低	2
自然威胁	硬件物理保护不够	很高	5
硬件故障	硬件使用寿命有限或其他原因	高	4

§5.5 风险的影响分析

风险标识	资产	威胁	脆弱点	影响分析	影响等级	
R1	多媒体系统	供电中断	没有备用电源	系统无法使用	高	4
R2		误操作	老师对多媒体课室使用注意事项不熟悉	硬件损害或软件误删除	很高	5
R3		自然威胁	硬件物理保护不够	设备物理破坏	很高	5
R4	硬件	盗窃、物理破坏	安全保卫机制不健全	硬件被破坏或被盗	很高	5
R5		火灾	未部署防火设施	系统被烧毁	很高	5
R6		极端温度及湿度	未安装空调及除湿设备	系统使用不正常	中	3
R7		硬件故障	硬件使用寿命有限或其他原因	硬件不能正常使用	高	4
R8	软件	软件故障	软件的安装与卸载权限管理机制不严	所需软件被卸载，不能正常使用	高	4
R9		恶意代码	杀毒软件不能及时升级	系统运行很慢	低	2
R10	人员	疾病或其他原因导致不能及时到岗	钥匙管理人员不可达，无“备份”	多媒体课室门不能及时打开	高	4
R11			多媒体技术支持人员无“备份”	技术支持不能及时到位	中	3

§5.5 风险评估

风险标识	资产	威胁	影响评估	可能性评估	风险值	风险等级
R1	多媒体系统	供电中断	4	3	12	中
R2		误操作	5	5	25	很高
R3		自然威胁	5	1	5	低
R4	硬件	盗窃、物理破坏	5	4	20	很高
R5		火灾	5	2	10	中
R6		极端温度及湿度	3	2	6	低
R7		硬件故障	4	2	8	中
R8	软件	软件故障	4	4	16	高
R9		恶意代码	2	5	10	中
R10	人员	疾病或其他原因导致不能及时到岗	4	3	12	中
R11			3	3	9	中

§5.5 风险等级划分方法

风险			可能性				
			可忽略:1	低：2	中：3	高：4	极高：5
影响程度	极高	5	5	10	15	20	25
	高	4	4	8	12	16	20
	中	3	3	6	9	12	15
	低	2	2	4	6	8	10
	可忽略	1	1	2	3	4	5

§5.6 安全措施的选取

风险标识	资产	威胁	风险等级	安全措施
R1	多媒体系统	供电中断	中	配置备用电源
R2		误操作	很高	多媒体系统操作培训
R4	硬件	盗窃、物理破坏	很高	加强安全保卫工作
R5		火灾	中	配备灭火设备
R7		硬件故障	中	技术支持
R8	软件	软件故障	高	加强权限管理，采用系统“一键还原”机制。
R9		恶意代码	中	定期升级病毒库
R10	人员	疾病或其他原因导致不能及时到岗	中	配备多个人员备用
R11			中	配备多个人员备用

本章小结

§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

作业题

1. 名词解释：

   资产、威胁、脆弱点、风险、影响

2. 简述一般的风险评估流程。

3. 风险评估方法分哪几种？其优缺点分别是什么？

实践作业（1）

- （信息安全风险评估）案例分析交流与报告
  - ✓以分组汇报与讨论方式，针对任选的某一具体应用信息系统，开展信息安全风险评估，陈述完整的评估过程与方法，汇报并提交完整的评估文档与评估结果。