

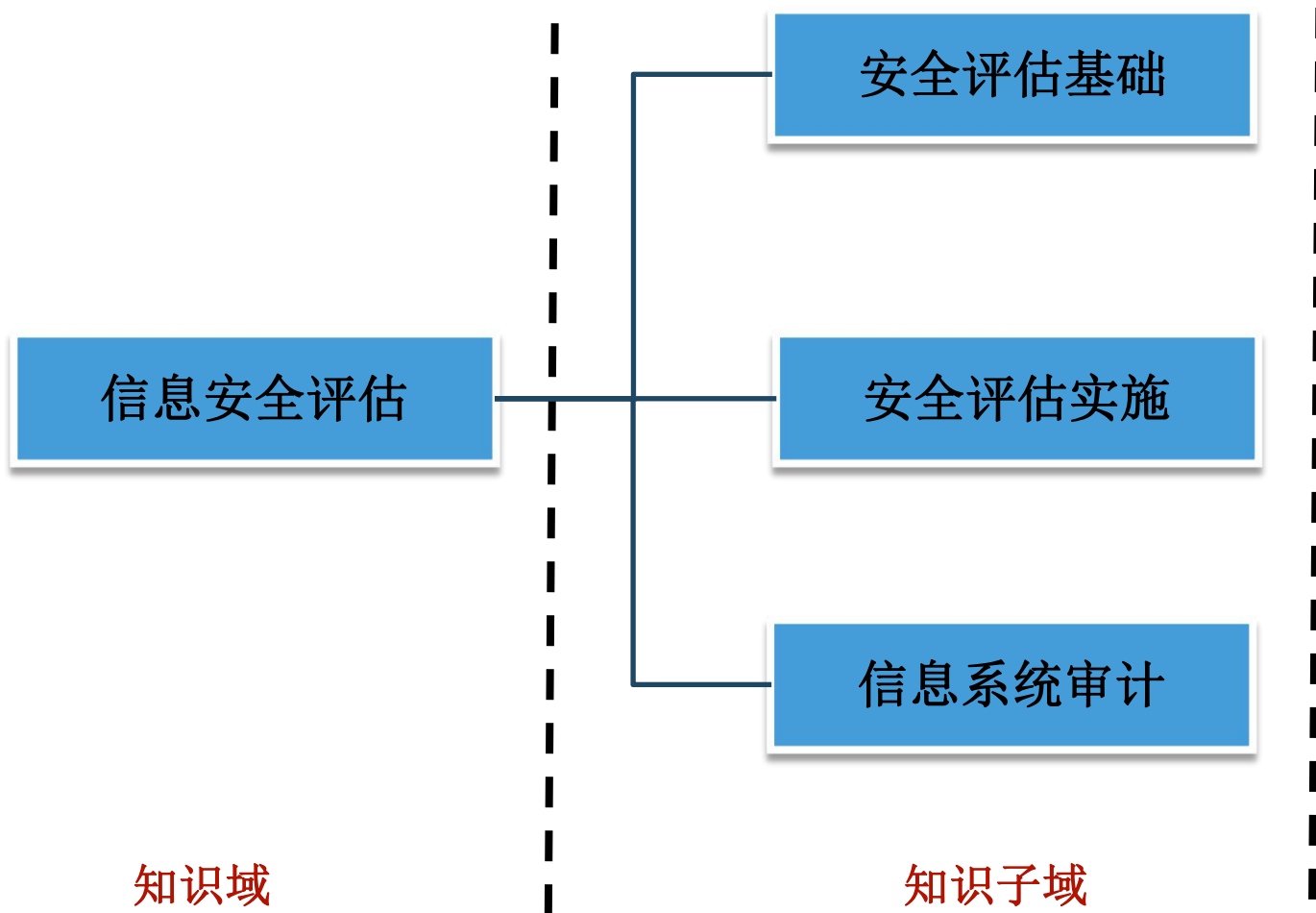
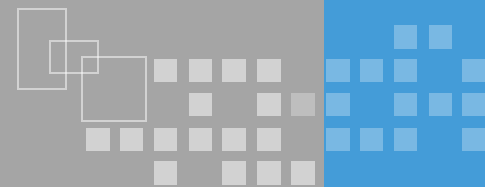


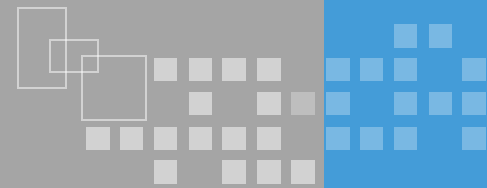
信息安全评估

版本：4.2

齐文振 河南信安世纪

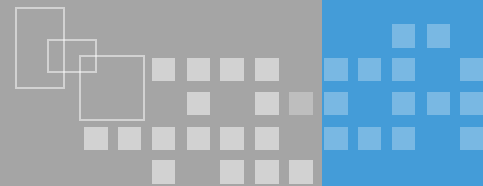
课程内容





❖ 安全评估概念

- 了解安全评估的定义、价值、风险评估工作内容及安全评估工具类型；
- 了解安全评估标准的发展；



❖ 什么是安全评估

- 针对事物潜在影响正常执行其职能的行为产生干扰或者破坏的因素进行识别、评价的过程

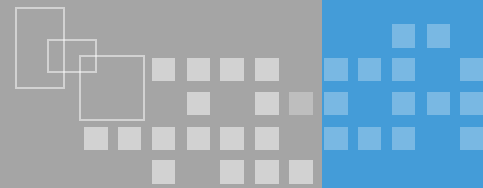
❖ 对安全评估的理解

- 狭义
- 广义

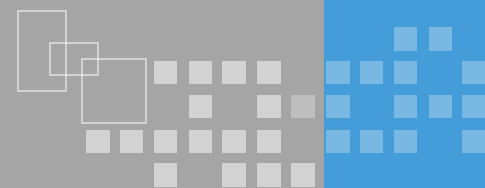
风险评估是确定安全需求的重要途径！



- ❖ 确定保护的对象（保护资产）是什么？它们直接和间接价值？
- ❖ 资产面临哪些潜在威胁？导致威胁的问题所在？威胁发生的可能性有多大？
- ❖ 资产中存在哪里弱点可能会被威胁所利用？利用的容易程序又如何？
- ❖ 一旦威胁事件发生，组织会遭受怎样的损失或者面临怎样的负面影响？
- ❖ 组织应该采取怎样的安全措施才能将风险带来的损失降低到最低程序。



- ❖ 安全建设的起点和基础
- ❖ 信息安全建设和管理的科学方法
- ❖ 倡导适度安全
- ❖ 保护网络空间安全的核心要素和重要手段



❖ 风险评估与管理工具

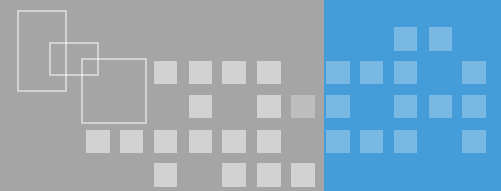
- 一套集成了风险评估各类知识和判据的管理信息系统，以规范风险评估的过程和操作方法；或者是用于收集评估所需要的数据和资料，基于专家经验，对输入输出进行模型分析

❖ 系统基础平台风险评估工具

- 主要用于对信息系统的主要部件（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

❖ 风险评估辅助工具

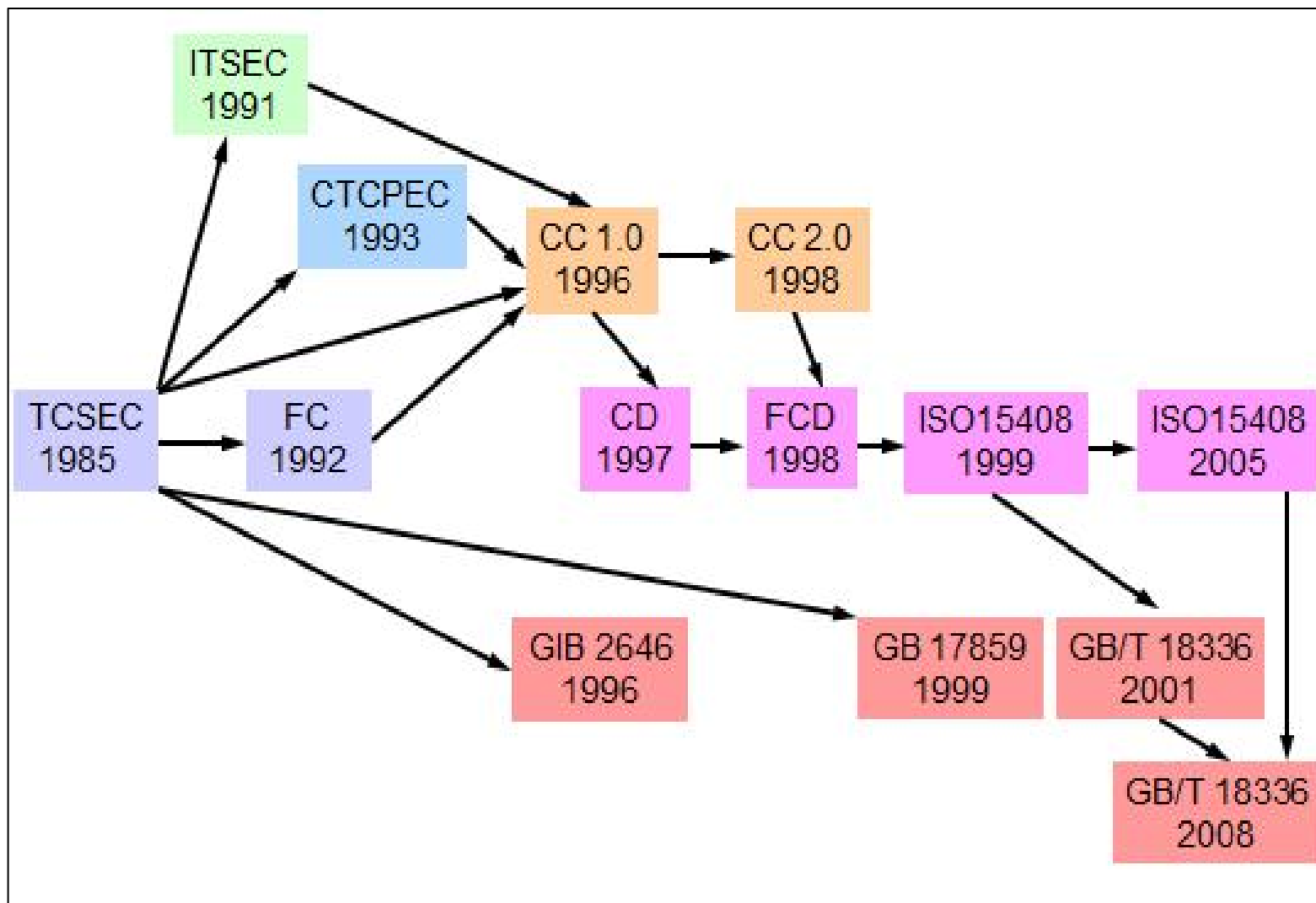
- 实现对数据的采集、现状分析和趋势分析等单项功能，为风险评估各要素的赋值、定级提供依据



❖ 安全评估标准

- 了解TCSEC基本目标和要求、分级等概念；
- 了解ITSEC标准的适用范围、功能准则和评估准则的级别；
- 了解ISO 15408标准的适用范围、作用和使用中的局限性；
- 了解GB/T 18336结构、作用及评估的过程；
- 理解评估对象（TOE）、保护轮廓（PP）、安全目标（ST）、评估保证级（EAL）等关键概念；
- 了解信息安全等级测评的作用和过程。

安全评估标准



- ❖ 美国政府国防部（DoD）标准，为评估计算机系统内置的计算机安全功能的有效性设定了基本要求
 - 国家安全局的国家计算机安全中心（NCSC）于1983年发布，1985年更新，作为国防部彩虹系列出版物的核心，TCSEC经常被称为橙皮书。
 - TCSEC已被2005年最初公布的国际标准《通用准则（CC）》所取代。

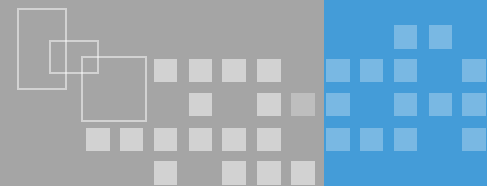
❖ 基本目标和要求

- 策略
- 问责
- 保证
- 文档

❖ 分级

- D-最小保护
- C-选择保护（C1、C2）
- B-强制保护（B1、B2、B3）
- A-验证保护（A1）

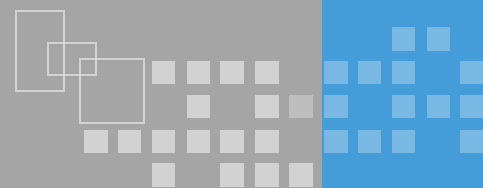
TCSEC	
D	最小保护
C	自主保护
C1	--自主安全保护
C2	--受控访问保护
B	强制保护
B1	--标签安全
B2	--结构化保护
B3	--安全域
A	验证保护
A1	--验证设计



- ❖ 以超越TCSEC为目的，将安全概念分为功能与功能评估两部分
- ❖ 功能准则：在测定上分F1-F10共10级
 - 1—5级对应于TCSEC的D到A
 - 6—10级加上了以下概念：
 - F6：数据和程序的完整性 F7：系统可用性
 - F8：数据通信完整性 F9：数据通信保密性
 - F10：包括机密性和完整性的网络安全
- ❖ 评估准则：分为6级：
 - E1：测试 E2：配置控制和可控的分配
 - E3：能访问详细设计和源码 E4：详细的脆弱性分析
 - E5：设计与源码明显对应 E6：设计与源码在形式上一致。

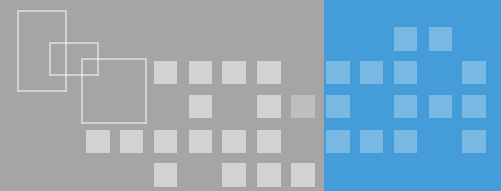
FC（联邦（最低安全要求）评估准则）

- ❖ 美国信息技术安全联邦准则(FC)
 - 1992年12月公布，是对TCSEC的升级
 - 引入了“保护轮廓（PP）”这一重要概念
- ❖ 保护轮廓包括
 - 功能部分
 - 开发保证部分
 - 测评部分
- ❖ 分级方式与TCSEC不同，吸取了ITSEC、CTCPEC中的优点
- ❖ 供美国政府用，民用和商用。

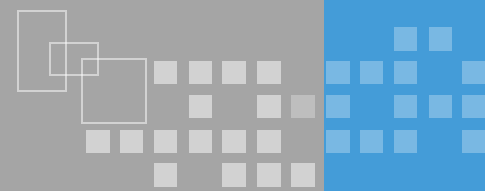


- ❖ 目前最全面的信息技术安全评估准则
- ❖ 主要思想和框架取自ITSEC和FC，充分突出“保护轮廓”，将评估过程分“功能”和“保证”两部分
- ❖ CC强调将安全的功能与保障分离，并将功能需求分为九类63族，将保障分为七类29族。

国际标准组织于1999年批准CC标准以“ISO/IEC 15408-1999”编号正式列入国际标准系列！



- ❖ 我国在2008年等同采用《ISO/IEC 15408: 2005 信息技术-安全技术-信息技术安全评估标准》形成的国家标准，标准编号为GB/T 18336
- ❖ 结构
 - GB/T 18336. 1-2008 简介和一般模型
 - 定义了IT 安全评估的一般概念和原理，并提出了评估的一般模型
 - GB/T 18336. 2-2008 安全功能要求
 - 建立一系列功能组件作为表达TOE功能要求的标准方法
 - GB/T 18336. 3-2008 安全保证要求
 - 建立一系列保证组件作为表达TOE保证要求的标准方法



❖ TOE（评估对象）的客户

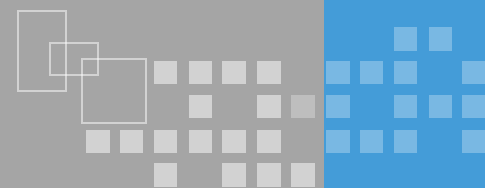
- CC从写作安排上确保评估满足用户的需求，因为这是评估过程的根本目的和理由。

❖ TOE的开发者

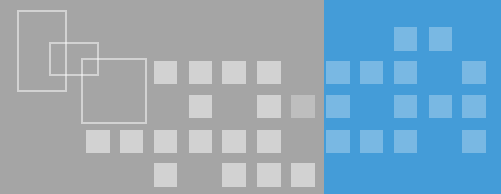
- 为开发者在准备和协助评估产品或系统以及确定每种产品和系统要满足的安全需求方面提供支持。

❖ TOE的评估者

- CC 包含评估者判定TOE 与其安全需求一致时所使用的准则。



- ❖ 评估对象 (Target of Evaluation, T0E)
 - 作为评估主体 (产品、系统、子系统等) 的IT产品及系统以及相关的指导性文档。
- ❖ 保护轮廓 (PP)
 - 满足特定用户需求的、一类T0E的、一组与实现无关的安全要求。
- ❖ 安全目标 (Security Target, ST)
 - 作为指定的T0E评估基础的一组安全要求和规范。



❖ 功能

- 规范IT产品和系统的安全行为，应做的事。
- 结构：类、族、组件

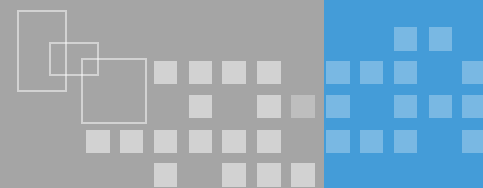
❖ 保证

- 实体达到其安全性目的的信任基础，是对功能产生信心的方法

❖ 包

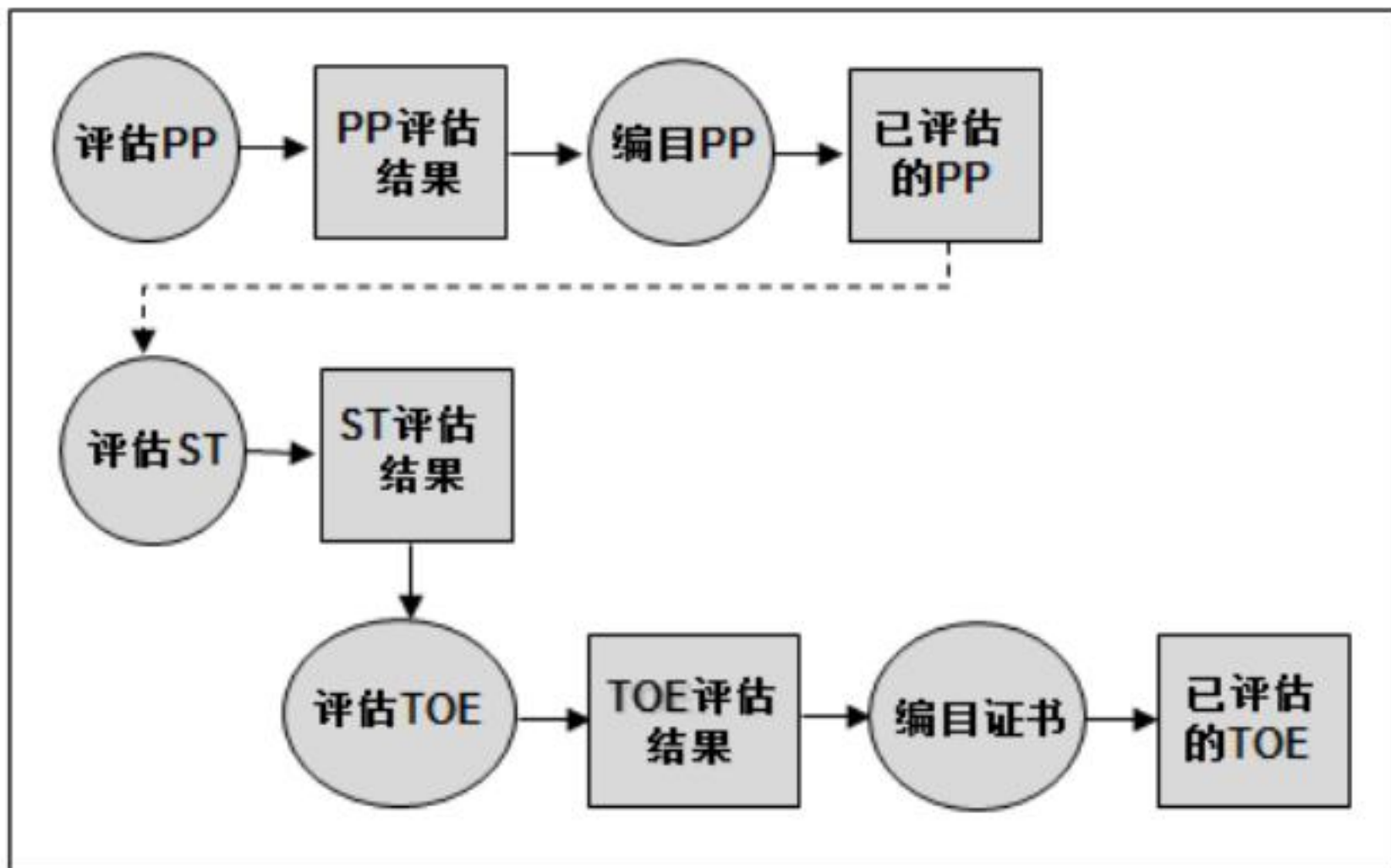
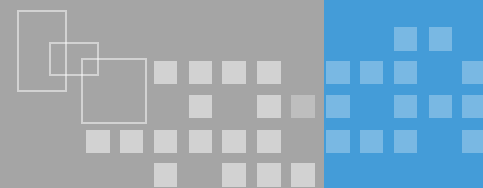
- 为满足一组确定的安全目的而组合在一起的，一组可重用的功能或保证组件

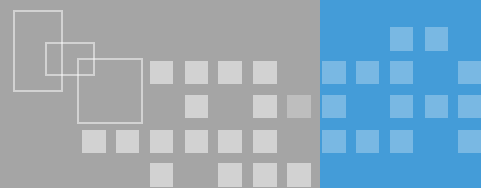
评估保证级别（EAL）



保证类	保证族	评估保证级别（EAL）的保证组件						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
配置管理	ACM_AUI				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	
分发与操作	ADO_DEI		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
开发	ADV_FSP	1	1	1	2	3	3	4
	ADV_HID		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_IID				1	1	2	3
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
指导性文件	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
生命周期支持	AIC_DVS			1	1	1	2	2
	AIC_FLR							
	AIC_ICD				1	2	2	3
	AIC_IAT				1	2	3	3
测试	ATF_COV		1	2	2	2	3	3
	ATF_DPT			1	1	2	2	3
	ATF_FUD		1	1	1	1	2	2
	ATF_IND	1	2	2	2	2	2	3
脆弱性评定	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

评估流程





❖ CC的意义

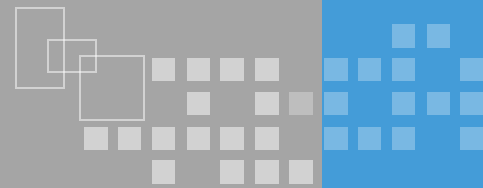
- 通过评估有助于增强用户对于IT产品的安全信心
- 促进IT产品和系统的安全性
- 消除重复的评估

❖ 优势

- 国际标准化组织统一现有多项准则的努力结果；
- 已有安全准则的总结和兼容，是目前最全面的评价准则；
- 通用的表达方式，便于理解
- 灵活的架构，可以定义自己的要求扩展CC要求



- ❖ CC标准采用半形式化语言，比较难以理解；
- ❖ CC不包括那些与IT安全措施没有直接关联的、属于行政管理安全措施的评估准则，即该标准并不关注于组织、人员、环境、设备、网络等方面的具体的安全措施；
- ❖ CC重点关注人为的威胁，对于其他威胁源并没有考虑；
- ❖ 并不针对IT安全性的物理方面的评估（如电磁干扰）；
- ❖ CC并不涉及评估方法学；
- ❖ CC不包括密码算法固有质量的评估。

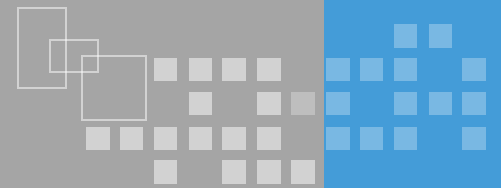


❖ 信息系统安全等级测评重要性

- 检测评估信息系统安全等级保护状况是否达到相应等级基本要求的过程
- 落实信息安全等级保护制度的重要环节

❖ 等级测评过程

- 测评准备活动
- 方案编制活动
- 现场测评活动
- 分析与报告编制活动

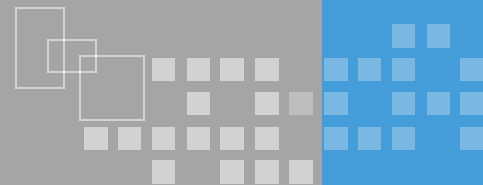


❖ 风险评估相关要素

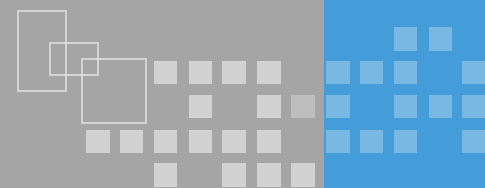
- 理解资产、威胁、脆弱性、安全风险、安全措施、残余风险等风险评估相关要素及相互关系。

❖ 风险评估途径与方法

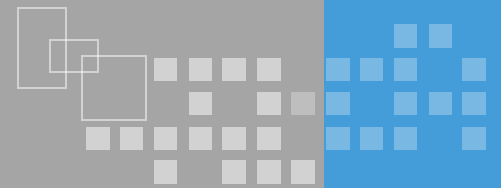
- 了解基线评估等风险评估途径及自评估、检查评估等风险评估方法；
- 了解基于知识的评估，理解定性评估、定量评估的概念及区别并掌握定量分析中量化风险的方法。



- ❖ 构成风险评估的资产是建立对组织具有价值的信息或资源，是安全策略保护的对象。
- ❖ 风险评估中资产的价值不是以资产的经济价值来衡量，而是由资产在这三个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。



- ❖ 可能导致对系统或组织危害的不希望事故潜在起因。
- ❖ 威胁可以通过威胁主体、资源、动机、途径等多种属性来描述。引起风险的外因
- ❖ 造成威胁的因素
 - 人为因素和环境因素。
- ❖ 根据威胁的动机，
 - 人为因素又可分为恶意和非恶意两种。
 - 环境因素包括自然界不可抗的因素和其它物理因素。



- ❖ 可能被威胁所利用的资产或若干资产的薄弱环节。
- ❖ 脆弱性是资产本身存在的，如果没有被相应的威胁利用，单纯的脆弱性本身不会对资产造成损害。
- ❖ 威胁总是要利用资产的脆弱性才可能造成危害。

❖ 信息安全风险

- 人为或自然的威胁利用信息系统及其管理体系中存在的脆弱性导致安全事件的发生及其对组织造成的影响。
- 信息安全风险只考虑那些对组织有负面影响的事件

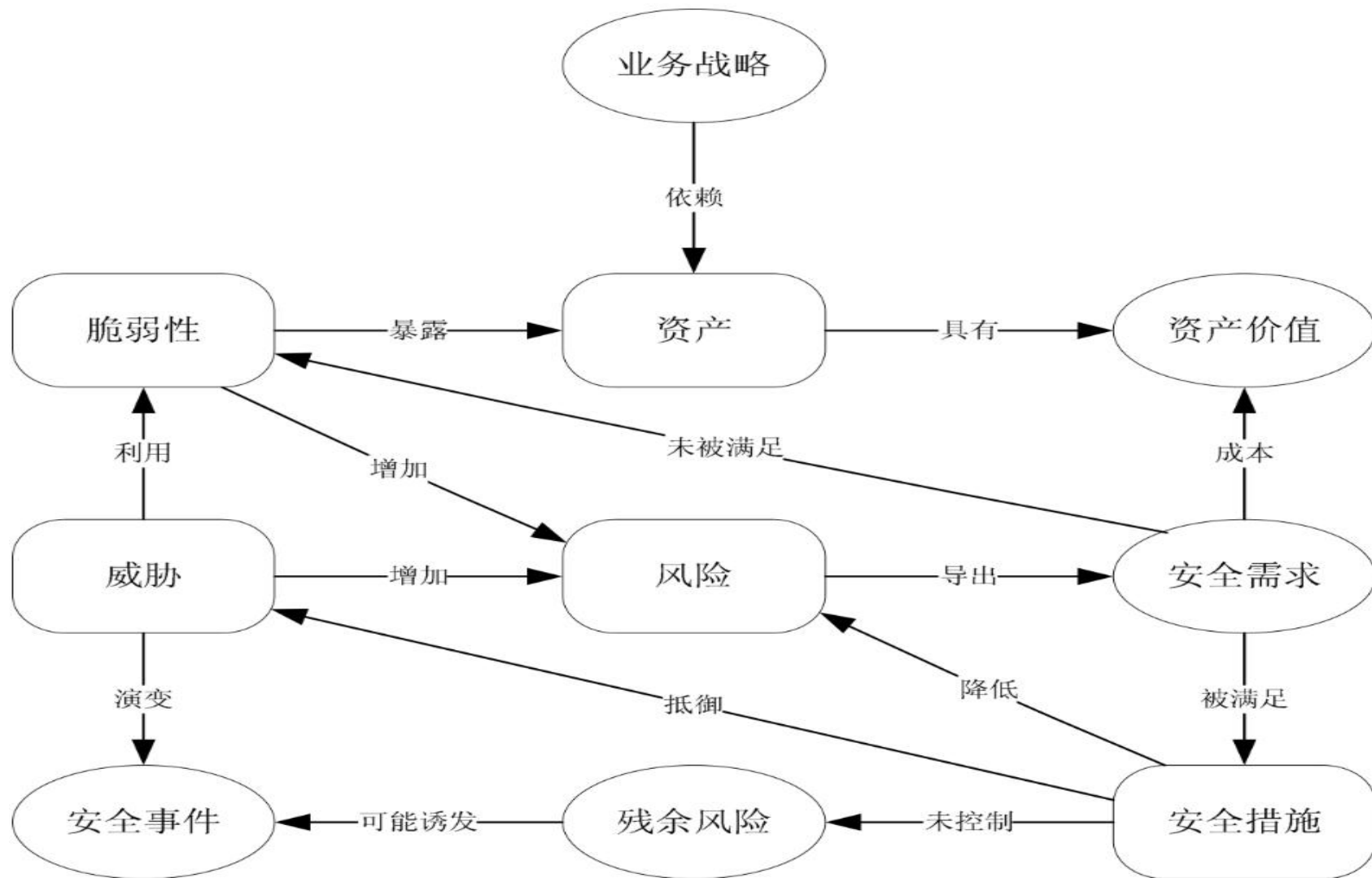
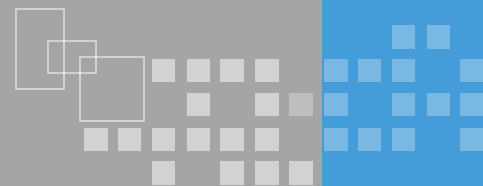
❖ 安全措施

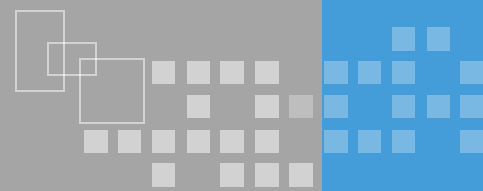
- 保护资产、抵御威胁、减少脆弱性、降低安全事件的影响，以及打击信息犯罪而实施的各种实践、规程和机制。

❖ 残余风险

- 采取了安全措施后，信息系统仍然可能存在的风险

风险评估要素之间关系





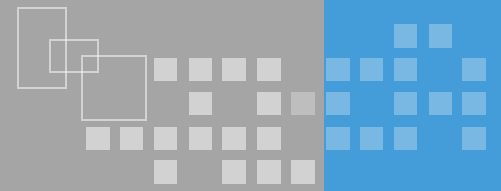
❖ 风险评估途径

- 基线评估
- 详细评估
- 组合评估

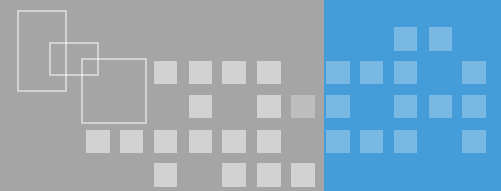
❖ 风险评估方式

- 自评估：由组织自身发起，组织自己实施或委托第三方实施
- 检查评估：由被评估组织的上级主管机关或业务主管机关发起

风险评估的常用方法

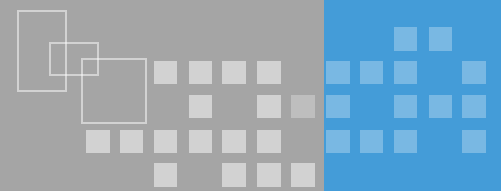


- ❖ 定量分析
- ❖ 定性分析
- ❖ 半定量分析



❖ 基本概念

- 暴露因子 (Exposure Factor, EF) : 特定威胁对特定资产靠损失的百分比, 或者说损失的程度。
- 单一预期损失 (single Loss Expectancy, SLE) : 也称作SOC (Single Occurrence Costs), 即特定威胁可能造成的潜在损失总量
- 年度预期损失 (Annualized Loss Expectancy, ALE) : 或者称作EAC (Estimated Annual Cost), 表示特定资产在一年内遭受损失的预期值

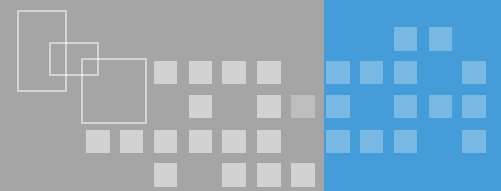


❖ 概念的关系

- 首先，识别资产并为资产赋值
- 通过威胁和弱点评估，评价特定威胁作用于特定资产所造成的影响，即EF（取值在0%~100%之间）
- 计算特定威胁发生的频率，即ARO
- 计算资产的SLE；
- 计算资产的ALE；

❖ 定量风险分析的一种方法就是计算年度损失预期值（ALE）。计算公式如下：

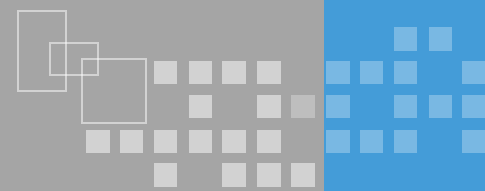
- 年度损失预期值（ALE） = SLE x 年度发生率（ARO）
- 单次损失预期值（SLE） = 暴露因素（EF） x 资产价值（AV）



❖ 定量评估计算案例

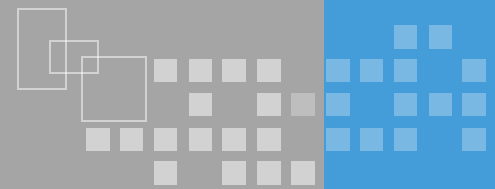
- 计算由于人员疏忽或设备老化对一个计算机机房所造成火灾的风险。
- 假设：
 - 组织在3年前计算机机房资产价值100万，当年曾经发生过一次火灾导致损失10万；
 - 组织目前计算机机房资产价值为1000万；
 - 经过和当地消防部门沟通以及组织历史安全事件记录发现，组织所在地及周边在5年来发生过3次火灾；
 - 该组织额定的财务投资收益比是30%
- 由上述条件可计算风险组织的年度预期损失及ROSI，为组织提供一个良好的风险管理财务清单

风险评估常用方法-定量分析



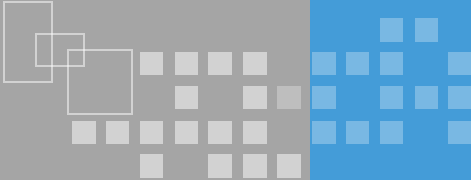
- ❖ 根据历史数据获得EF：
 - $10\text{万} \div 100\text{万} \times 100\% = 10\%$
- ❖ 根据EF计算目前组织的SLE
 - $1000\text{万} \times 10\% = 100\text{万}$
- ❖ 根据历史数据中ARO计算ALE
 - $100\text{万} \times (3 \div 5) = 60\text{万}$
- ❖ 此时获得年度预期损失值，组织需根据该损失衡量风险可接受度，如果风险不可接受则需进一步计算风险的处置成本及安全收益；
 - $ROSI = (\text{实施控制前的ALE}) - (\text{实施控制后的ALE}) - (\text{年控制成本})$
- ❖ 组织定义安全目标，假如组织希望火灾发生后对组织的损失降低70%，则，实施控制后的ALE应为：
 - $60\text{万} \times (1 - 70\%) = 18\text{万}$
 - 年控制成本 = $(60 - 18) \times 30\% = 12.6\text{万}$
 - 则： $ROSI = 60 - 18 - 12.8 = 29.4\text{万}$
- ❖ 至此，组织通过年投入12.6万获得每年29.4万的安全投资收益

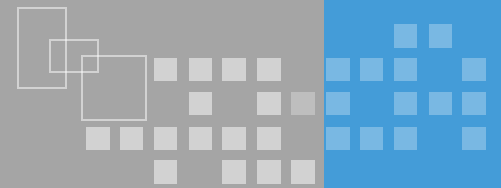
风险评估常用方法-定性分析



- ❖ 目前采用最为广泛的一种方法
- ❖ 带有很强的主观性，往往凭借分析者的经验和直觉，或者业界的标准和惯例，为风险管理诸要素的大小或高低程度定性分级

可能性	影响				
	可以忽略 1	较小 2	中等 3	较大 4	灾难性 5
A（几乎肯定）	H	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

- 
- ❖ 在风险评估中进行定量的后果分析时，如果采用年度风险损失值（ALE, annualized loss expectancy）的方法进行计算，应当使用以下哪个公式？
 - ❖ A. SLE （单次损失预期值） \times ARO （年度发生率）；
 - ❖ B. ARO （年度发生率） \times EF （暴漏因子）；
 - ❖ C. SLE （单次损失预期值） \times EF （暴漏因子） \times ARO （年度发生率）；
 - ❖ D. ARO （年度发生率） \times SLE （单次损失预期值） $- EF$ （暴漏因子）



❖ 风险评估的基本过程

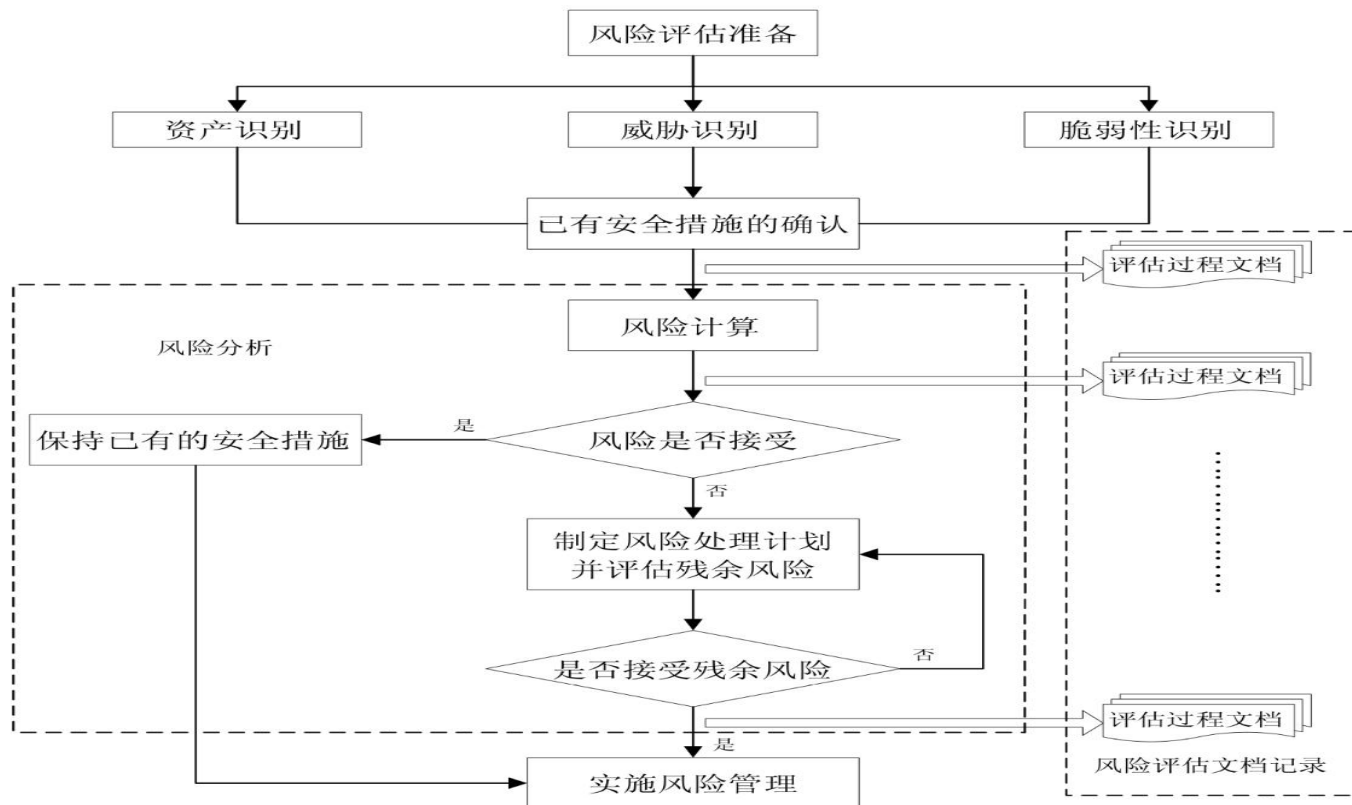
- 了解风险评估基本过程；
- 理解风险评估准备工作内容；
- 掌握风险识别中资产的赋值方法；
- 理解风险分析的方法；
- 了解风险结果判定、风险处理计划、残余风险评估等阶段工作内容。

❖ 风险评估文档

- 了解风险评估文档化工作的重要性及对文档的相关要求；

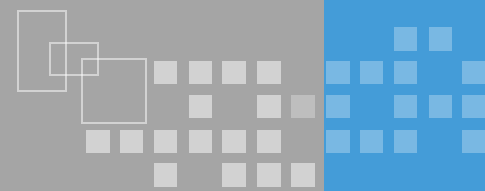
风险评估的基本过程

❖ 风险评估是组织确定信息安全需求的过程，包括资产识别与评价、威胁和弱点评估、控制措施评估、风险认定在内的一系列活动。





- ❖ 风险评估准备是整个风险评估过程有效性的保证
 - 组织实施风险评估是一种战略性的考虑，其结果将受到组织的业务战略、业务流程、安全需求、系统规模和结构等方面的影响。
- ❖ 风险评估准备工作
 - 确定风险评估的目标
 - 确定风险评估的范围
 - 组建适当的评估管理与实施团队
 - 进行系统调研
 - 确定评估依据和方法
 - 制定风险评估方案
 - 获得最高管理者对风险评估工作的支持

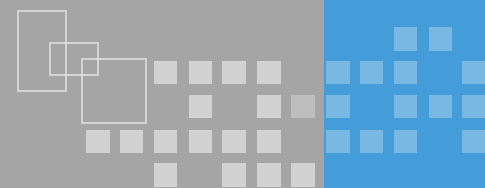


❖ 确定风险评估的目标

- 根据满足组织业务持续发展在安全方面的需要、法律法规的规定等内容，识别现有信息系统及管理上的不足，以及可能造成的风险大小。

❖ 确定风险评估的范围

- 风险评估范围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信息系统、关键业务流程、与客户知识产权相关的系统或部门等。

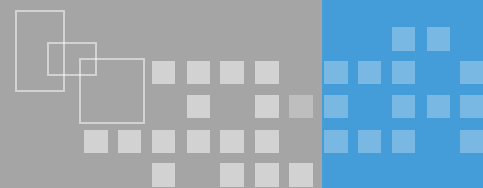


❖ 组建适当的评估管理与实施团队

- 风险评估实施团队，由管理层、相关业务骨干、IT技术等人员组成风险评估小组。
- 评估实施团队应做好评估前的表格、文档、检测工具等各项准备工作，进行风险评估技术培训和保密教育，制定风险评估过程管理相关规定。

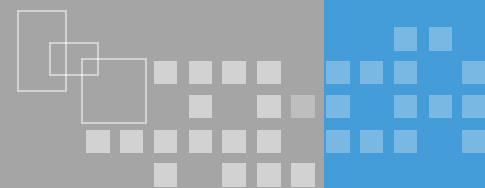
❖ 进行系统调研；

- 系统调研是确定被评估对象的过程，风险评估小组应进行充分的系统调研，为风险评估依据和方法的选择、评估内容的实施奠定基础。
- 调研内容至少应包括：业务战略及管理制度；主要的业务功能和要求；网络结构与网络环境，包括内部连接和外部连接；系统边界；主要的硬件、软件；数据和信息；系统和数据的敏感性；支持和使用系统的人员。
- 系统调研可以采取问卷调查、现场面谈相结合的方式进行。



❖ 确定评估依据和方法

- 根据系统调研结果，确定评估依据和评估方法。
- 评估依据包括（但不仅限于）：现有国际标准、国家标准、行业标准；行业主管机关的业务系统的要求和制度；系统安全保护等级要求；系统互联单位的安全要求；系统本身的实时性或性能要求等。
- 据组织机构自身的业务特点、信息系统特点，选择适当的风险分析方法并加以明确，如定性风险分析、定量风险分析，或是半定量风险分析。
- 根据评估依据，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计算方法，并依据业务实施对系统安全运行的需求，确定相关的判断依据，使之能够与组织环境和安全要求相适应。

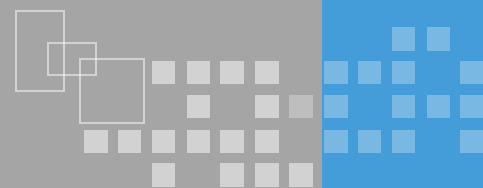


❖ 制定风险评估方案

- 风险评估方案的目的是为后面的风险评估实施活动提供一个总体计划，用于指导实施方开展后续工作。
- 风险评估方案的内容一般包括（但不仅限于）：
 - 团队组织：包括评估团队成员、组织结构、角色、责任等内容；
 - 工作计划：风险评估各阶段的工作计划，包括工作内容、工作形式、工作成果等内容；
 - 时间进度安排：项目实施的时间进度安排。

❖ 获得最高管理者对风险评估工作的支持

- 上述所有内容确定后，应形成较为完整的风险评估实施方案，得到组织最高管理者的支持、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，以明确有关人员在风险评估中的任务。



❖ 资产分类、分级、形态及资产价值评估

❖ 资产分类

- 数据、软件、硬件、服务、人员、其他（（ GB/T 20984 《信息安全风险评估规范》 ） ）

❖ 资产形态

- 有形资产、无形资产

❖ 资产分级

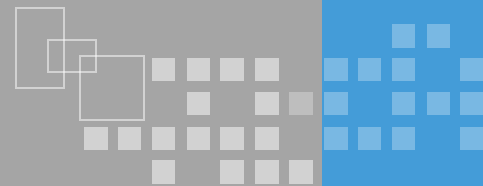
- 保密性分级、完整性分级、可用性分级
- 资产重要性分级



❖ 制定资产重要性分级准则

- 依据资产价值大小对资产的重要性划分不同的等级。资产价值依据资产在保密性、完整性和可用性上的赋值等级，经过综合评定得出。

赋值	重要性等级	定义
5	很高	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
4	高	重要，其安全属性破坏后可能对组织造成比较严重的损失
3	中	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
2	低	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	很低	不重要，其安全属性破坏后对组织造成很小的损失，甚至忽略不计

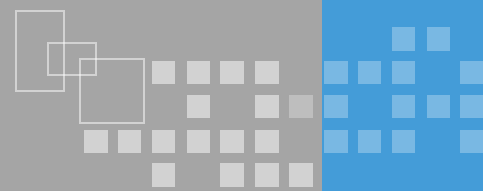


❖ 威胁类型

- 自然因素、人为因素

❖ 威胁频率级别

赋值	威胁出现频率级别	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；或可以证实经常发生过
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；或可以证实多次发生过
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；仅可能在非常罕见和例外的情况下发生



❖ 脆弱性识别与威胁识别是何关系？

- 验证：以资产为对象，对威胁识别进行验证

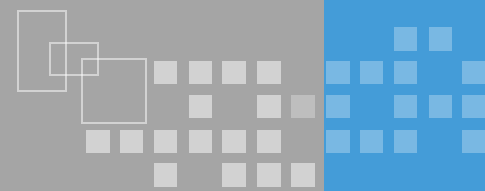
❖ 脆弱性识别的难点是什么？

- 三性：隐蔽性、欺骗性、复杂性

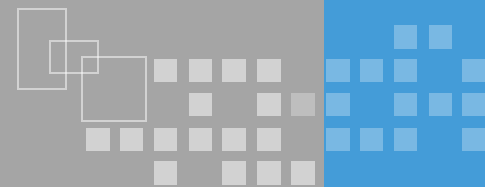
❖ 脆弱性识别的方法有哪些？

赋值	脆弱性严重程度级别	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

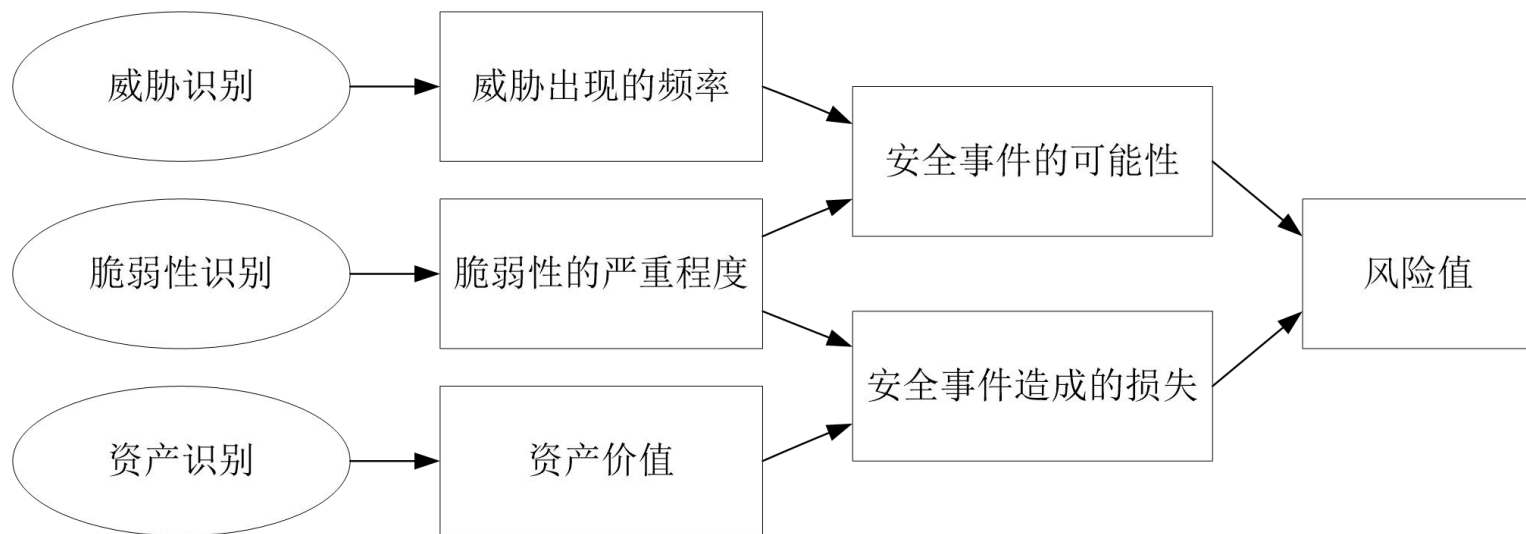
确认已有的控制措施



- ❖ 依据三个报告
 - 《信息系统的描述报告》、《信息系统的分析报息告》和《信系统的安全要求报告》
- ❖ 确认已有的安全措施，包括：
 - 技术层面（物理平台、系统平台、网络平台和应用平台）的安全功能
 - 组织层面（组织结构、岗位和人员）的安全控制
 - 管理层面（策略、规章和制度）的安全对策
 - 形成《已有安全措施列表》。
- ❖ 控制措施类型
 - 预防性、检测性和纠正性
- ❖ 在识别脆弱性的同时，评估人员应对已采取的安全措施的有效性进行确认。安全措施的确应评估其有效性，对有效的安全措施继续保持，以避免不必要的工作和费用，防止重复实施。

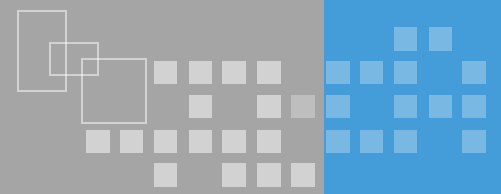


❖ GB/T 20984-2007 《信息安全风险评估规范》 给出信息安全风险分析思路



$$\text{风险值} = R(A, T, V) = R(L(T, V), F(Ia, Va))$$

- R表示安全风险计算函数
- A表示资产
- T表示威胁
- V表示脆弱性
- Ia表示安全事件所作用的资产价值
- Va表示脆弱性严重程度
- L表示威胁利用资产的脆弱性导致安全事件的可能性
- F表示安全事件发生后造成的损失



❖ 计算安全事件发生的可能性

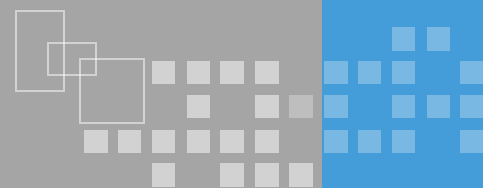
- 安全事件的可能性= L (威胁出现频率, 脆弱性) = $L(T, V)$

❖ 计算安全事件发生后造成的损失

- 安全事件造成的损失= F (资产价值, 脆弱性严重程度) = $F(Ia, Va)$

❖ 计算风险值

- 风险值= R (安全事件的可能性, 安全事件造成的损失) = $R(L(T, V), F(Ia, Va))$



❖ 评估风险的等级

- 评估风险的等级依据《风险计算报告》，根据已经制定的风险分级准则，对所有风险计算结果进行等级处理，形成《风险程度等级列表》。

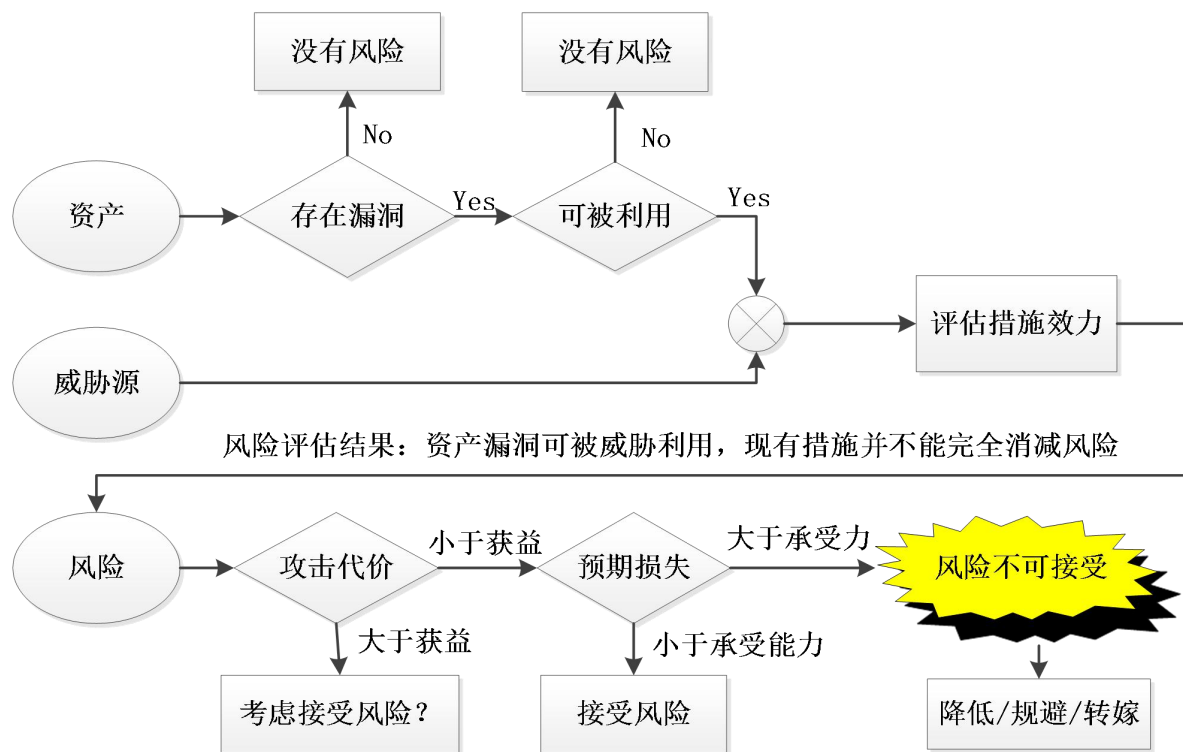
❖ 综合评估风险状况

- 汇总各项输出文档和《风险程度等级列表》，综合评价风险状况，形成《风险评估报告》

等级	取值范围	名称	描述
H	25, 20	高风险	最高等级的风险，需要立即采取应对措施。不可接受。
S	12, 15, 16	严重风险	需要高级管理层注意。不可接受
M	6, 8, 9, 10	中等风险	必须规定管理责任。通常需要综合考虑取舍。
L	1, 2, 3, 4, 5	低风险	可以通过例行程序来处理。可接受。

❖ 对不可接受的风险应根据导致该风险的脆弱性制定风险处理计划

- 管理措施
- 技术措施

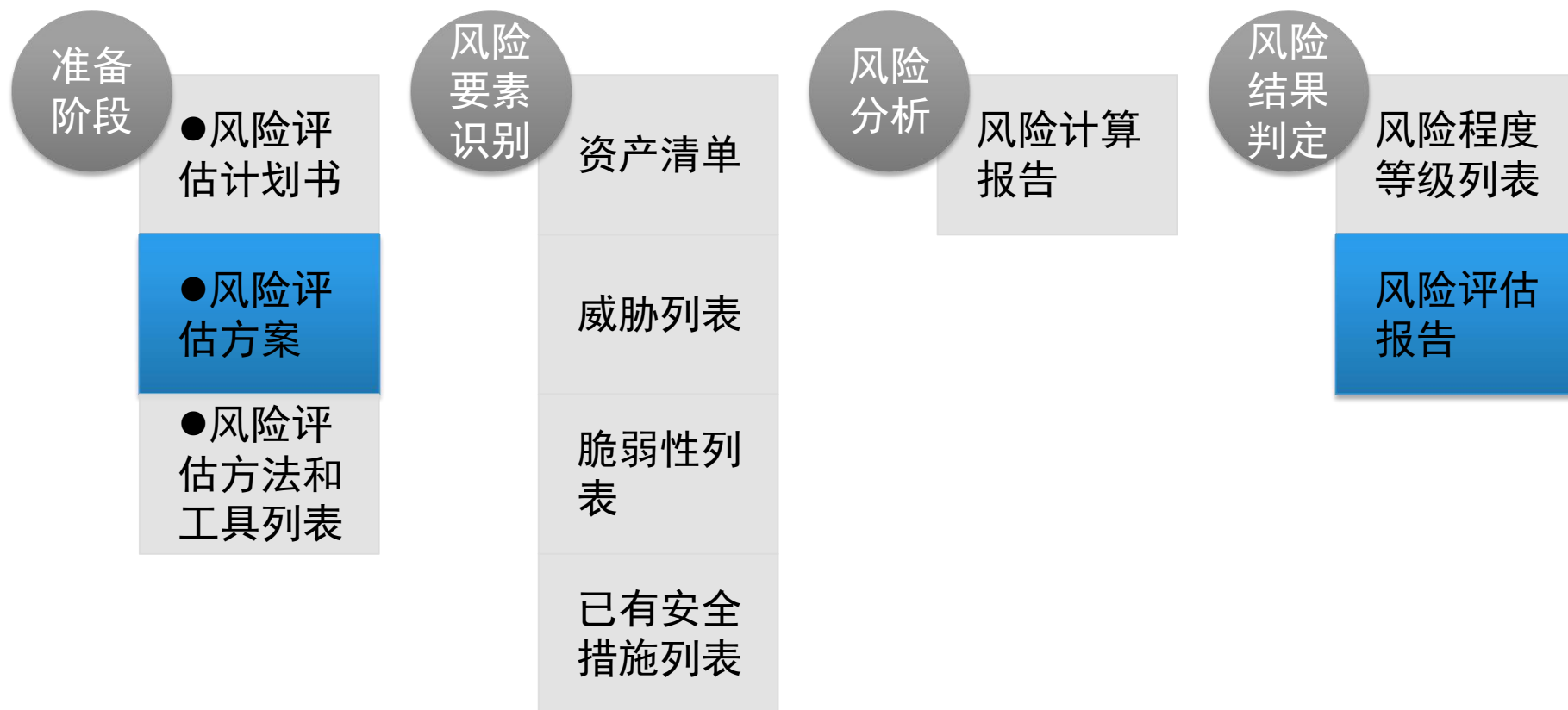
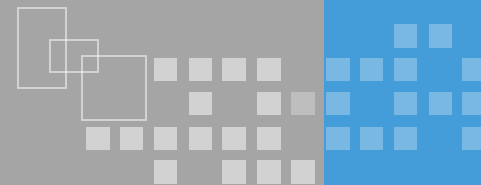


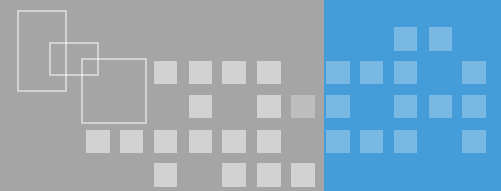


❖ 实施安全措施后对措施有效性进行再评估

- 在对于不可接受的风险选择适当安全措施后，为确保安全措施的有效性，可进行再评估，以判断实施安全措施后的残余风险是否已经降低到可接受的水平。
- 某些风险可能在选择了适当的安全措施后，残余风险的结果仍处于不可接受的风险范围内，应考虑是否接受此风险或进一步增加相应的安全措施

风险评估文档





❖ 审计原则与方法

- 了解信息系统审计职能、流程、内部控制及审计标准；

❖ 审计技术控制

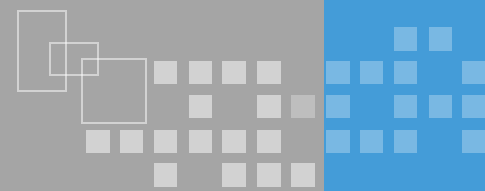
- 了解脆弱性措施、渗透测试等审计技术控制措施；

❖ 审计管理控制

- 了解账户管理、备份验证等审计管理控制措施；

❖ 审计报告

- 了解信息系统审计报告标准SAS70和SOC；



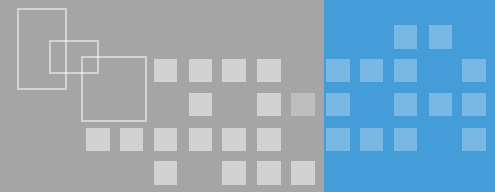
❖ 信息系统审计的定义

- 国家审计属的定义
- 国际信息系统和控制协会（ISACA）

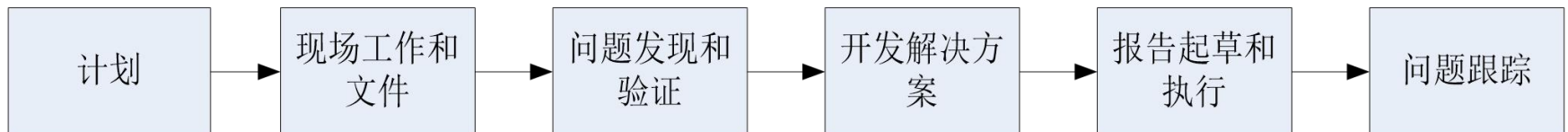
❖ 信息系统审计的作用

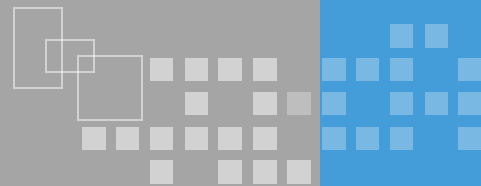
- 从审计目标看，信息系统审计主要是检查和促进被审计单位信息系统及其内部控制的真实性、正确性、完整性、安全性、可靠性和经济性等各类目标要素。
- 审计内容看，信息系统审计中的一般控制审计包括信息安全技术控制审计和信息安全管理控制审计。

信息系统审计工作流程

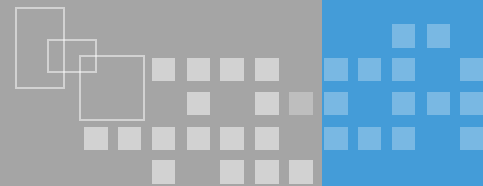


- ❖ 计划：确定审计的目标和范围
- ❖ 现场工作和文件：收集数据并进行访谈以帮助分析潜在风险
- ❖ 问题发现和验证：潜在问题清单并验证
- ❖ 开发解决方案：与客户合作制定解决每个问题的行动计划
- ❖ 报告起草和执行
- ❖ 问题跟踪

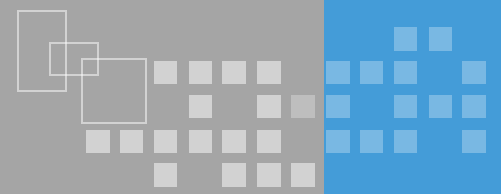




- ❖ 脆弱性测试
- ❖ 渗透测试
- ❖ 战争驾驶
- ❖ 其他漏洞类型
- ❖ 日志
- ❖ 合成交易
- ❖ 滥用案例测试
- ❖ 代码审查
- ❖ 接口测试



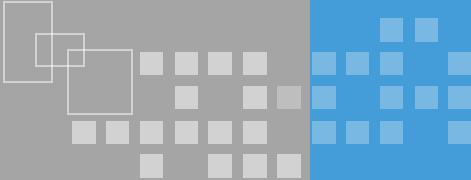
- ❖ 账户管理
- ❖ 备份验证
- ❖ 灾难恢复和业务连续性
- ❖ 安全培训和安全意识培训
- ❖ 关键绩效和风险指标

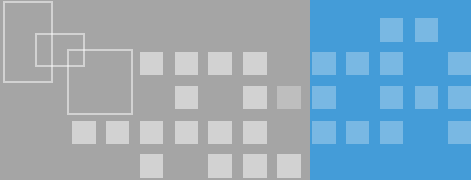


- ❖ 专业人员了解信息系统安全在更广泛的业务环境中的作用，并能够将其传达给技术和非技术观众
- ❖ SAS70
 - 由美国注册会计师协会（AICPA）制定的用于处理服务机构的审计标准
 - 提供了一套基于服务组织（如提供IT服务的服务组织）标准可以展示其内部控制的有效性
- ❖ SOC
 - 取代SAS 70并解决更广泛的特定用户需求，例如解决安全性，隐私和可用性问题



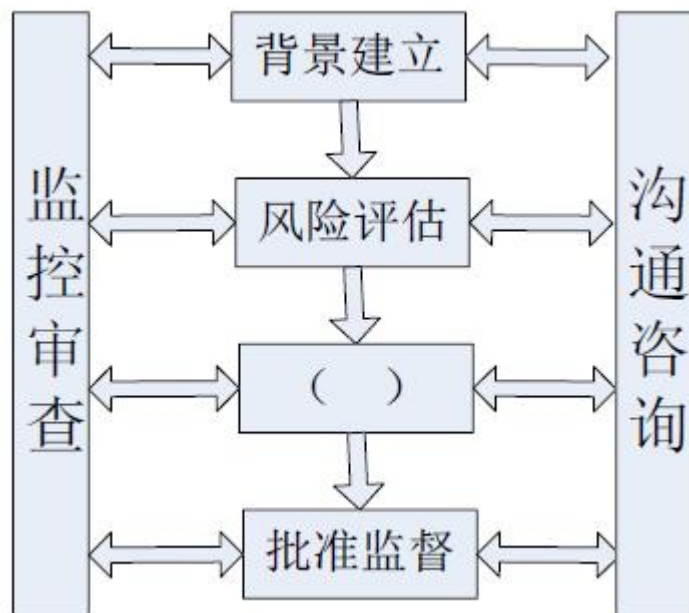
- ❖ 安全评估基础
 - 概念、作用、安全评估标准
- ❖ 安全评估实施
 - 威胁、脆弱性、资产等评估重要概念
 - 风险评估实施流程及方法
- ❖ 信息系统审计

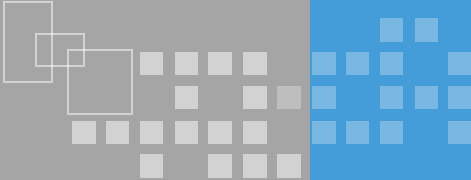
- 
- ❖ 小牛在对某公司的信息系统进行风险评估后，因考虑到该业务系统中部分涉及金融交易的功能模块风险太高，他建议该公司以放弃这个功能模块的方式来处理该风险。请问这种风险处置的方法是（）
- ❖ A. 降低风险
 - ❖ B. 规避风险
 - ❖ C. 转移风险
 - ❖ D. 放弃风险

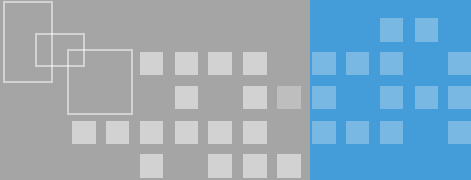
- 
- ❖ 残余风险是风险管理中的一个重要概念。在信息安全风险管理中，关于残余风险描述错误的是（）
 - ❖ A. 残余风险是采取了安全措施后，仍然可能存在的风险：一般来说，是在综合考虑了安全成本与效益后不去控制的风险
 - ❖ B. 残余风险应受到密切监视，它会随着时间的推移而发生变化，可能会在将来诱发新的安全事件
 - ❖ C. 实施风险处理时，应将残余风险清单告知信息系统所在组织的高管，使其了解残余风险的存在和可能造成的后果
 - ❖ D. 信息安全风险处理的主要准则是尽可能降低和控制信息安全风险，以最小残余风险值作为风险管理效果评估指标

❖ 我国标准《信息安全风险管理指南》（GB/Z24364）给出了信息安全风险管理的内容和过程，可以用下图来表示。图中空白处应该填写（）

- ❖ A. 风险计算
- ❖ B. 风险评价
- ❖ C. 风险预测
- ❖ D. 风险处理

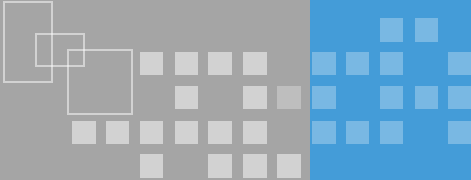


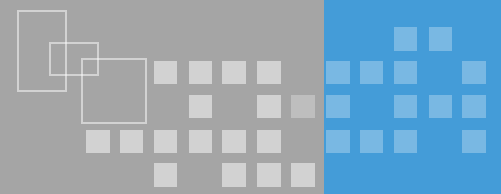
- 
- ❖ 降低风险（或减低风险）是指通过对面临风险的资产采取保护措施的方式来降低风险，下面哪个措施不属于降低风险的措施（）
 - ❖ A. 减少威胁源。采用法律的手段制按计算机犯罪，发挥法律的威慑作用，从而有效遏制威胁源的动机
 - ❖ B. 签订外包服务合同。将有技术难点、存在实现风险的任务通过签订外部合同的方式交予第三方公司完成，通过合同责任条款来应对风险
 - ❖ C. 减少脆弱性。及时给系统补丁，关闭无用的网络服务端口，从而减少系统的脆弱性，降低被利用的可能性
 - ❖ D. 减少威胁能力。采取身份认证措施，从而地址身份假冒这种威胁行为的能力。



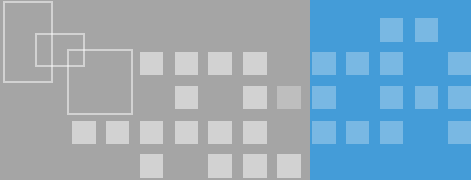
❖ 某单位在一次信息安全风险管理活动中，风险评估报告提出服务器 A 的 FTP 服务存在高风险漏洞。随后该单位在风险处理时选择了关闭 FTP 服务的处理措施。请问该措施属于哪种风险处理方式（）

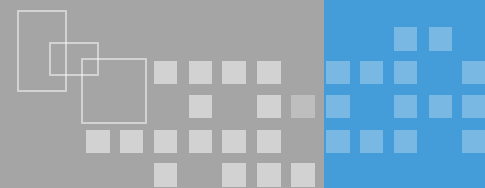
- ❖ A. 风险降低
- ❖ B. 风险规避
- ❖ C. 风险转移
- ❖ D. 风险接受

- 
- ❖ 小李在某单位是负责信息安全风险管理方面工作的部门领导，主要负责对所在行业的新人进行基本业务素质培训，一次培训的时候，小李主要负责讲解风险评估方法。请问小李的所述论点中错误的是哪项：
 - ❖ A. 风险评估方法包括：定性风险分析、定量风险分析以及半定量风险分析
 - ❖ B. 定性风险分析需要凭借分析者的经验和直觉或者业界的标准和惯例，因此具有随意性
 - ❖ C. 定量风险分析试图在计算风险评估与成本效益分析期间收集的各个组成部分的具体数字值因此更具有客观性
 - ❖ D. 半定量风险分析技术主要指在风险分析过程中综合使用定性和定量风险分析技术对风险要素的赋值方式，实现对风险各要素的度量数值化



- ❖ 信息安全风险评估是信息安全风险管理工作中的重要环节。在国家网络与信息安全协调小组发布的《关于开展信息安全风险评估工作的意见》（国信办[2006]5 号）中，风险评估分为自评估和检查评估两种形式，并对两种工作形势提出了有关工作原则和要求。下面选项中描述正确的是（）
- ❖ A. 信息安全风险评估应以自评估为主，自评估和检查评估相结合、互为补充
- ❖ B. 信息安全风险评估应以检查评估为主，自评估和检查评估相结合、互为补充
- ❖ C. 自评估和检查评估时相互排斥的，单位应慎重地从两种工作形式选择一个，并长期使用
- ❖ D. 自评估和检查评估是相互排斥的，无特殊理由的单位均应选择检查评估，以保证安全效果

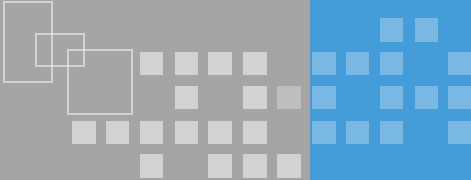
- 
- ❖ 信息安全风险评估师信息安全风险管理工作中的重要环节。在《关于开展信息安全风险评估工作的意见》（国信办[2006]5 号）中，指出了风险评估分为自评估和检查评估两种形式，并对两种工作形式提出了有关工作原则和要求。下面选项中描述错误的是（ ）
 - ❖ A. 自评估是由信息系统拥有、运营或使用单位发起的对本单位信息系统进行的风险评估
 - ❖ B. 检查评估是指信息系统上级管理部门组织的国家有关职能部门依法开展的风险评估
 - ❖ C. 信息安全风险评估应以自评估为主，自评估和检查评估相结合、互为补充
 - ❖ D. 自评估和检查评估是相互排斥的，单位应慎重地从两种工作形式选择一个， 并坚持使用

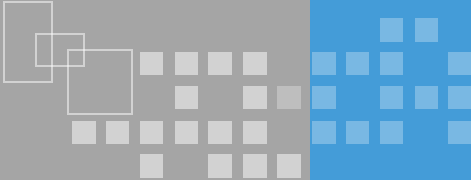


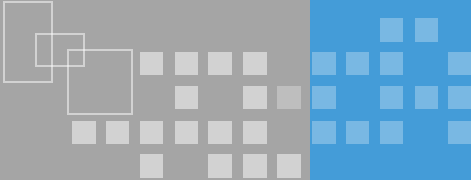
❖ 风险分析是风险评估工作中的一个重要内容，GB/T 20984-2007 在资料性附录中给出了一种矩阵法来计算信息安全风险大小，其中风险计算矩阵如下图所示。请为图中括号空白处选择合适的内容（）

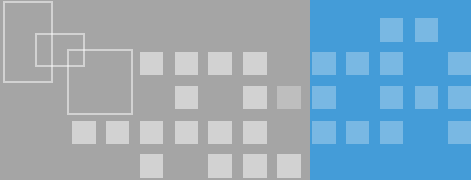
- ❖ A. 安全资产价值大小等级
- ❖ B. 脆弱性严重程度等级
- ❖ C. 安全风险隐患严重等级
- ❖ D. 安全事件造成损失大小

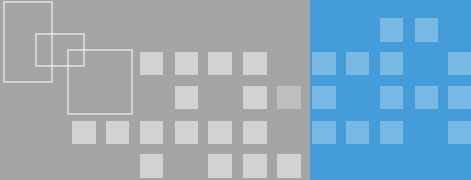
		安全事件发生可能性				
		1	2	3	4	5
()	1	3	6	9	12	16
	2	5	8	11	15	18
	3	6	7	13	17	21
	4	7	11	16	20	23
	5	9	14	20	23	25

- 
- ❖ 王工是某某单位的系统管理员，他在某次参加了单位组织的风险管理工作时，发现当前案例中共有两个重要资产：资产 A1 和资产 A2；其中资产 A1 面临两个主要威胁，威胁 T1 和威胁 T2；而资产 A2 面临一个主要威胁，威胁 T3；威胁 T1 可以利用的资产 A1 存在的两个脆弱性；脆弱性 V1 和脆弱性 V2；威胁 T2 可以利用的资产 A1 存在的三个脆弱性，脆弱性 V3、脆弱性 V4 和脆弱性 V5；威胁 T3 可以利用的资产 A2 存在的两个脆弱性；脆弱性 V6 和脆弱性 V7. 根据上述条件，请问：使用相乘法时，应该为资产 A1 计算几个风险值（）
- ❖ A. 2 B. 3 C. 5 D. 6

- 
- ❖ 公司甲做了很多政府网站安全项目，在为网游公司乙的网站设计安全保障方案时，借鉴以前项目经验，为乙设计了多重数据加密安全措施，但用户提出不需要这些加密措施，理由是影响了网站性能，使用户访问量受限。双方引起争议。下面说法哪个是错误的：
 - ❖ A. 乙对信息安全不重视，低估了黑客能力，不舍得花钱
 - ❖ B. 甲在需求分析阶段没有进行风险评估，所部属的加密针对性不足，造成浪费
 - ❖ C. 甲未充分考虑网游网站的业务与政府网站业务的区别
 - ❖ D. 乙要综合考虑业务、合规性和风险，与甲共同确定网站安全需求

- 
- ❖ 某单位在实施信息安全风险评估后，形成了若干文档，下面()中的文档不应属于风险评估中“风险评估准备”阶段输出的文档。
 - ❖ A. 《风险评估工作计划》，主要包括本次风险评估的目的、意义、范围、目标、组织结构、角色及职责、经费预算和进度安排等内容
 - ❖ B. 《风险评估方法和工具列表》。主要包括拟用的风险评估方法和测试评估工具等内容
 - ❖ C. 《已有安全措施列表》，主要包括经检查确认后的已有技术和管理各方面安全措施等内容
 - ❖ D. 《风险评估准则要求》，主要包括风险评估参考标准、采用的风险分析方法、风险计算方法、资产分类标准、资产分类准则等内容

- 
- ❖ 规范的实施流程和文档管理，是信息安全风险评估能否取得成果的重要基础。按照规范的风险评估实施流程，下面哪个文档应当是风险要素识别阶段的输出成果（ ）
 - ❖ A. 《风险评估方案》
 - ❖ B. 《需要保护的资产清单》
 - ❖ C. 《风险计算报告》
 - ❖ D. 《风险程度等级列表》

- 
- ❖ 关于风险要素识别阶段工作内容叙述错误的是：（ ）。
 - ❖ A. 资产识别是指对需要保护的资产和系统等进行识别和分类
 - ❖ B. 威胁识别是指识别与每项资产相关的可能威胁和漏洞及其发生的可能性
 - ❖ C. 脆弱性识别以资产为核心，针对每一项需要保护的资产，识别可能被威胁利用的弱点，并对脆弱性的严重程度进行评估
 - ❖ D. 确认已有的安全措施仅属于技术层面的工作，牵涉到具体方面包括：物理平台、系统平台、网络平台和应用平台



谢谢，请提问题！