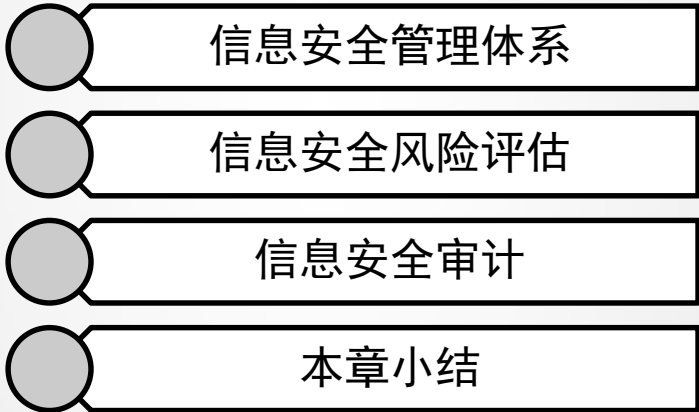


## 第12章 信息安全管理与审计



信息安全管理体系

信息安全风险评估

信息安全审计

本章小结

# 信息安全管理体系



# 信息安全管理需求



信息系统是人机交互系统



应对风险需要人为的管理过程



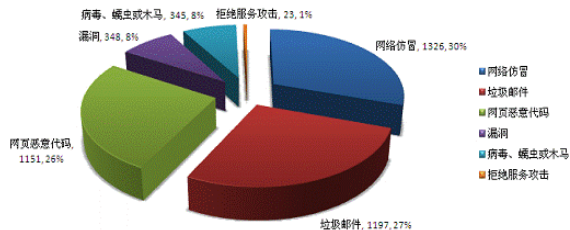
设备的有效利用是人为的管理过程

# 三分技术，七分管理

- 据有关统计，信息安全事件中大约有70%以上的问题都是由于管理方面的原因造成的。

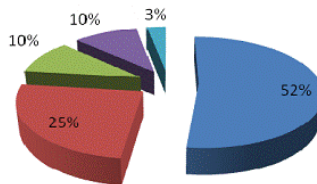
2007年网络安全事件类型分布

CNERT/CC



计算机安全事件

■ 人为因素 ■ 自然灾害 ■ 技术错误  
■ 组织内部人员作案 ■ 外部不法人员攻击



数据来源  
CNCERT/CC

# 信息安全工程

- 信息安全需要对信息系统的各个环节进行统一的综合考虑、规划和架构，并需要兼顾组织内外不断变化的发生的变化。
- 木桶原理：信息系统安全水平将由与信息安全有关的所有环节中**最薄弱**的环节所决定
- 要实现信息安全目标，一个组织必须使构成安全防范体系的这只“木桶”的所有木板都达到一定的长度。

要实现良好的信息安全，需要信息安全技术和信息安全管理有效地配合

# 信息安全工程

## ■ 信息安全技术层面

- 建设安全的主机系统和安全的网络系统，包括物理层安全、系统层安全、网络层安全和应用层安全等
- 配备一定的安全产品，如数据加密产品、数据存储备份产品、系统容错产品、防病毒产品、安全网关产品等

## ■ 信息安全管理层面

- 构建信息安全管理体系统

# 信息安全管理

- 信息安全管理(Information Security Management)的概念没有统一的定义。
- **信息安全管理**：组织为了实现信息安全目标和信息资产保护，用来指导和管理各种控制信息安全风险的、一组相互协调的活动。

要实现组织中信息的安全性、高效性和动态性管理，就需要依据**信息安全管理模型**和**信息安全管理标准**构建**信息安全管理**体系

# 信息安全管理体系

- 信息安全管理体系(Information Security Management System, ISMS)
  - 组织以信息安全风险评估为基础的系统化、程序化和文件化的管理体系，包括建立、实施、运行、监视、评审、保持和改进信息安全等一系列的管理活动。
- ISMS是整个管理体系的一部分。

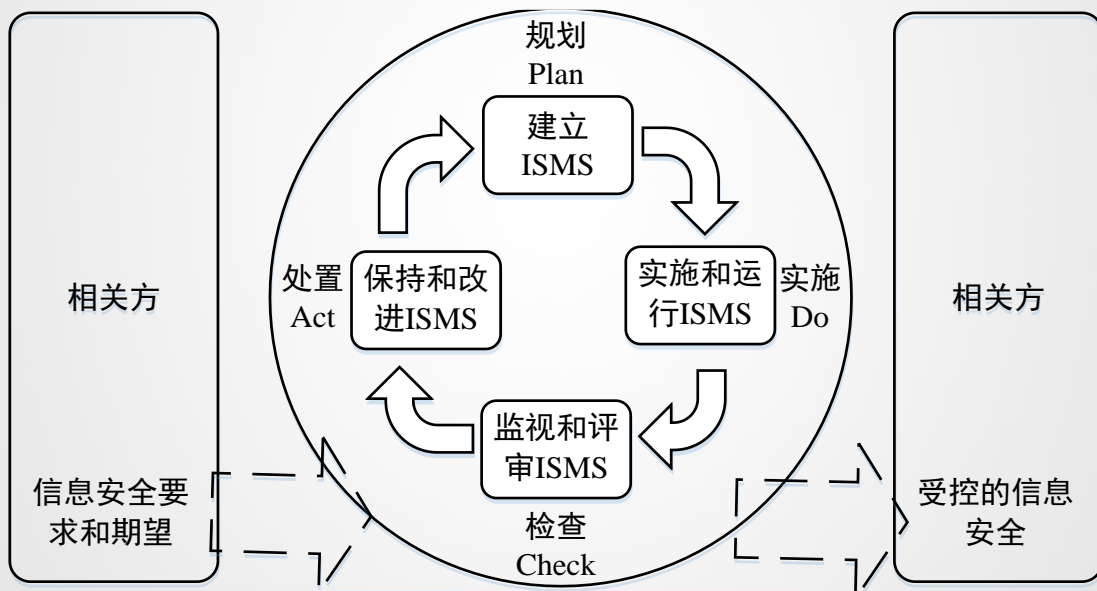
ISMS的建立是基于组织，立足于信息安全风险评估，体现以预防为主的思想，并且是全过程和动态控制。



# 信息安全管理体系

- **BS7799-2《信息安全管理体系规范》**：详细说明了建立、实施和维护信息安全管理体系的要求。
- **BS7799-2**的修订版本**BS7799-2: 2002**中引入了**PDCA(Plan-Do-Check-Action)过程方法**，用于建立、实施和持续改进ISMS。
  - PDCA循环又称“戴明环”，由美国质量管理专家Edwards Deming博士在20世纪50年代提出，是全面质量管理所应遵循的科学程序。
  - **PDCA强调应将业务过程看作连续的反馈循环**，在反馈循环的过程中识别需要改进的部分，以使过程得到持续的改进，质量得到螺旋式上升。

# 应用于ISMS过程的PDCA模型



# 信息安全管理体系统建流程



# 信息安全管理体系功能

- 强化员工的信息安全意识，规范组织的信息安全行为。
- 对组织的关键信息资产进行全面系统的保护，维持竞争优势。
- 在信息系统受到侵袭时，确保业务持续开展并将损失降到最低程度。
- 使组织的生意伙伴和客户对组织充满信心。
- 使组织定期地考虑新的威胁和脆弱点，并对系统进行更新和控制。
- 促使管理层坚持贯彻信息安全保障体系。

# 信息安全管理标准

- BS7799
- 信息和相关技术控制目标(Control Objective for Information and related Technology, COBIT)
- ISO/IEC13335
- GB17895-1999
- ...

# BS7799

- BS7799是由英国BSI/DISC的BDD/2信息安全管理委员会指导下完成的，是当前国际公认的信息安全实施标准。
- 旨在为一个组织提供用来制定安全标准、实施有效安全管理的通用要素，并不涉及“怎么做”的细节。
- 是制定一个机构自己标准的出发点，因此适用于各种产业和组织。其演化发展过程如下图。



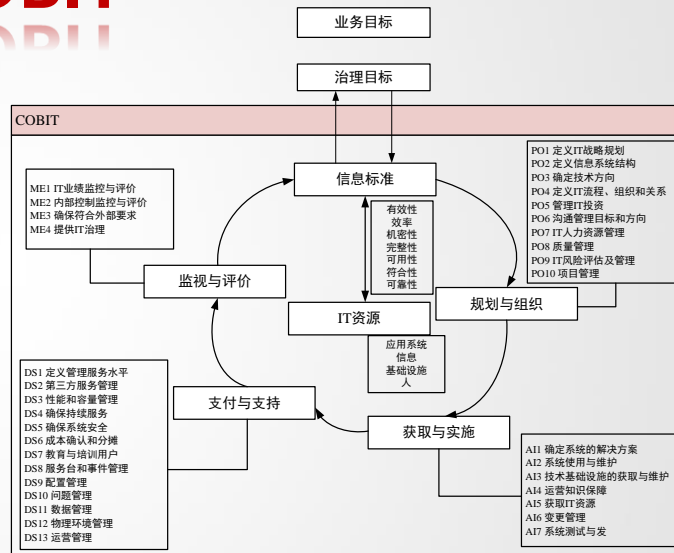
# BS7799

## ■ BS7799发展后分为两部分

- **ISO/IEC 27001: 2005 《信息技术-安全技术-信息安全管理-要求》**
  - 主要讨论了以PDCA过程方法建设ISMS以及ISMS评估的内容。
  - 该标准详细的说明了建立、实施、监视和维护ISMS的具体任务和要求，指出实施机构应该遵循的风险评估标准。
- **ISO/IEC 27002: 2005 《信息技术-安全技术-信息安全控制实用规则》**
  - 标准包含有11项管理内容，133条安全控制措施。
  - 作为组织基于ISO/IEC 27001实施ISMS的过程中选择控制措施时的参考，或作为组织实施通用信息安全控制措施时的指南文件，或开发组织自身的信息安全管理指南。

# COBIT

- COBIT是目前国际上通用的安全与信息技术管理和控制标准
- 它在业务风险、控制需要和技术问题之间架起了一座桥梁，可以辅助管理层进行IT治理，指导组织有效利用信息资源，有效地管理与信息相关的风险。
- COBIT共分为4个域，34个高级控制目标和318个详细控制目标。





# ISO/IEC13335

- ISO/IEC13335是国际标准《IT安全管理指南》(Guidelines for the Management of IT Security, GMITS)
  - ISO/IEC13335-1:1996《IT安全的概念与模型》（被ISO/IEC 13335-1:2004《信息和通信技术安全管理的概念和模型》替代）
  - ISO/IEC13335-2:1997《IT安全管理与规划》
  - ISO/IEC13335-3:1998《IT安全管理技术》
  - ISO/IEC13335-4:2000《防护措施的选择》
  - ISO/IEC13335-5:2001《网络安全管理指南》

# GB17895-1999

GB17895-1999

- GB17895-1999《计算机信息系统安全保护等级划分准则》标准由我国公安部主持制定、国家质量技术监督局1999年发布，2001年1月1日起施行。
- 计算机信息系统安全保护等级被划分为5个级别
  - 用户自主保护级
  - 系统审计保护级
  - 安全标记保护级
  - 结构化保护级
  - 访问验证保护级

第一级 自主安全保护

自主访问控制
身份鉴别
完整性保护

第二级 审计安全保护

自主访问控制
身份鉴别
完整性保护

系统审计
客体重用

第三级 强制安全保护

自主访问控制
身份鉴别
完整性保护

系统审计
客体重用

强制访问控制
标记

第四级 结构化保护

自主访问控制
身份鉴别
完整性保护

系统审计
客体重用

强制访问控制
标记

隐蔽通道分析
--------

可信路径
------

第五级 访问验证保护级

自主访问控制
身份鉴别
完整性保护

系统审计
客体重用

强制访问控制
标记

隐蔽通道分析
--------

可信路径
------

可信恢复
------

# 信息安全风险评估

# 信息安全风险评估

- 信息安全风险评估概念
- 信息安全风险评估组成要素
- 信息安全风险评估流程
- 信息安全风险评估方法
- 信息安全风险评估工具

# 信息安全风险

- 风险(Risk): 一定条件下和一定时期内可能发生的不利事件发生的可能性。
- 目前, 信息安全风险没有统一的定义
  - 澳大利亚/新西兰国家标准AS/NZS4360
    - 信息安全风险指对目标产生影响的某种事件发生的可能性, 可以用后果和可能性来衡量。
  - ISO/IEC13335-1标准
    - 信息安全风险是指某个给定的威胁利用单个或一组资产的脆弱点造成资产受损的潜在可能性。
  - GB/T20984-2013 《信息安全风险评估规范》
    - 信息安全风险是指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点导致安全事件的发生及其对组织造成的影响。

# 信息安全风险评估

- 一般而言，信息安全风险可表现为威胁(Threats)、脆弱点(Vulnerabilities)和资产(Asset)之间的相互作用。

$$Risk = Threats + Vulnerabilities + Asset$$

- GB/T20984-2013 《信息安全风险评估规范》

风险会随着任一因素的增加而增大，减少而减少

- 信息安全风险评估是指依据有关信息安全技术与管理标准，对信息系统及其处理、传输和存储的信息的**保密性、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**。

# 信息安全风险评估组成要素

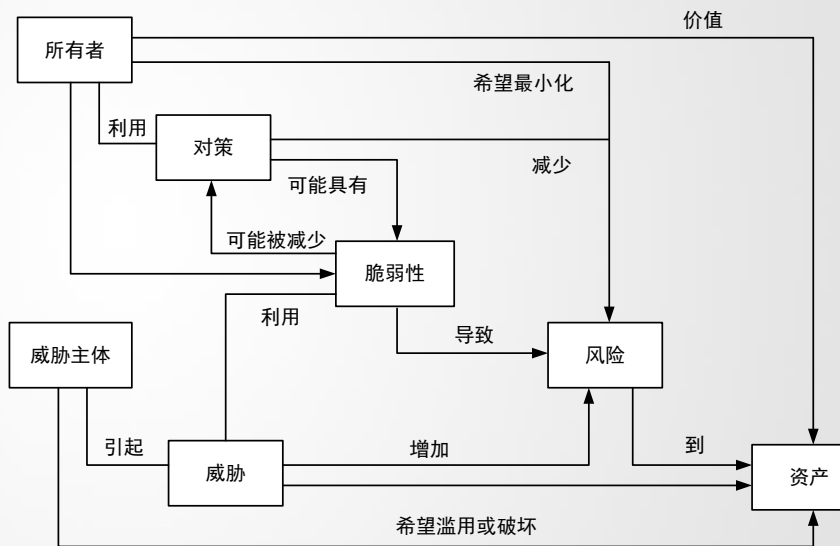
## ■ CC标准

- 1993年，美国，加拿大同欧洲四国组成六国七方，共同制定了国际通用的评估准则CC(Common Criteria)
- 目的是建立一个各国都能接受的通用的信息安全产品和系统的安全性评价标准。
- 在1996年颁布了CC1.0版，1998年颁布了CC2.0版
- 1999年，ISO接纳CC2.0版为ISO/IEC 15408草案，并命名为信息技术-安全技术-IT安全性评估准则，并于同年正式发布国际标准ISO/IEC15408 CC2.1版



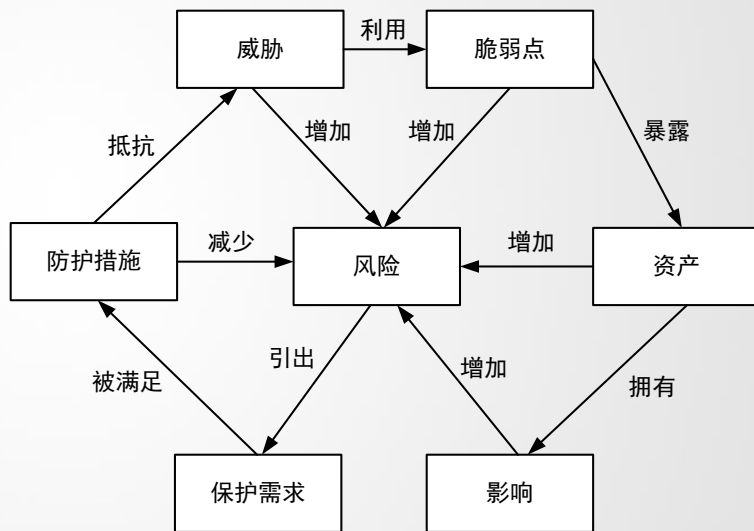
# 信息安全风险评估组成要素

- CC标准主要有三部分构成
  - 简介和一般模型
  - 安全功能要求
  - 安全保障要求
- 信息安全风险构成要素
  - 威胁、风险、脆弱点、资产、对策等关键风险要素
  - 提出了所有者和威胁主体的概念



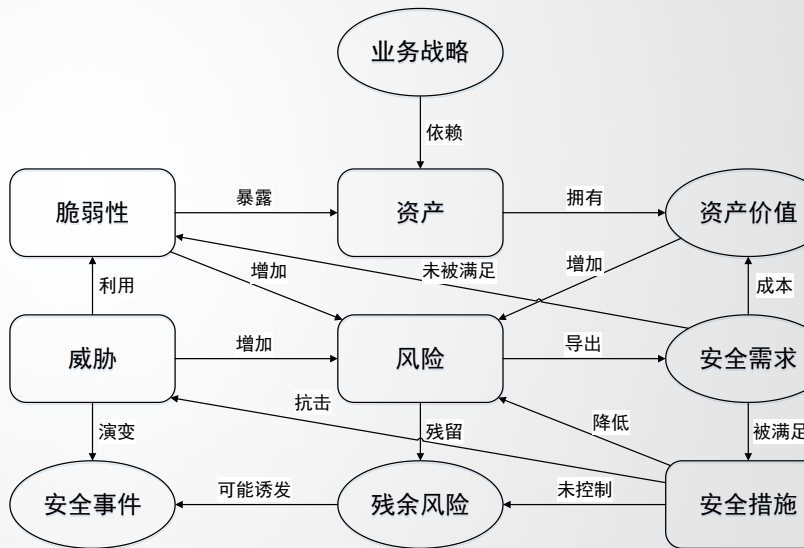
# 信息安全风险评估组成要素

- ISO13335标准
- ISO/IEC13335是信息安全管理方面的指导性标准。
- ISO/IEC13335-1以风险为中心，确定了资产、威胁、脆弱点、影响、风险、防护措施为信息安全风险的要素，并描述了它们之间的关系。



# 信息安全风险评估组成要素

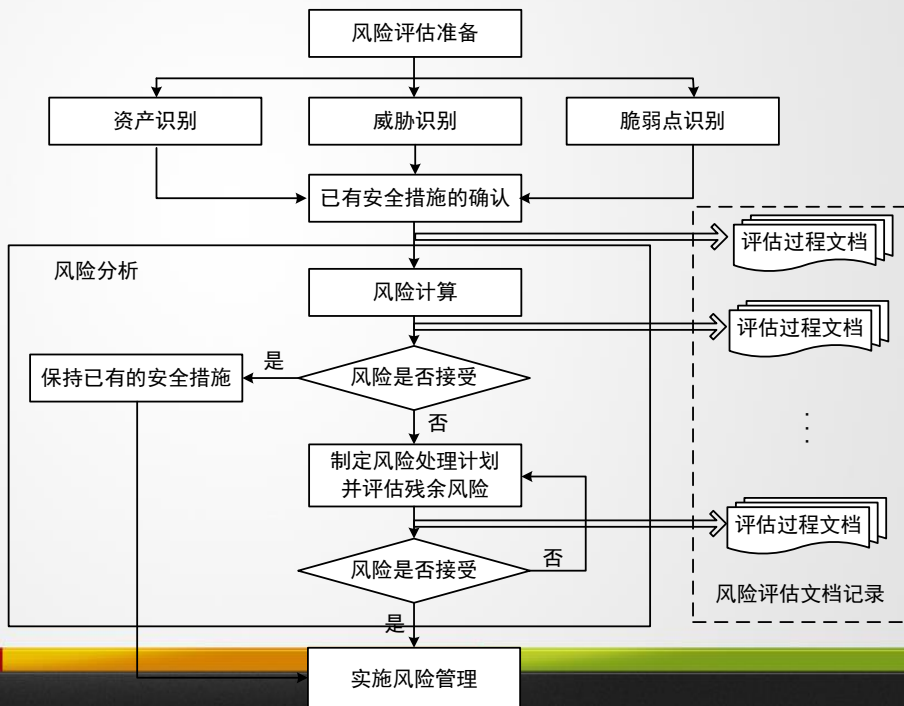
- GB/T20984-2007 标准《信息安全风险评估规范》
- 风险评估围绕着资产、威胁、脆弱性和安全措施这些基本要素展开。
- 在基本要素的评估过程中，充分考虑业务战略、资产价值、安全需求、安全事件、残余风险等与这些基本要素相关的各类属性。



# 信息安全风险评估流程

## ■ 我国的GB/T20984-2007标准《信息安全风险评估规范》

- 风险评估准备
- 资产识别
- 威胁识别
- 脆弱点识别
- 已有安全措施的确认
- 风险分析
- 风险评估文档记录



# 风险评估准备

- 确定风险评估的目标
- 确定风险评估的对象与范围
- 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

# 资产识别

## ■ 资产分类

- 根据资产的表现形式，可将资产分为物理资产、信息资产、软件资产、服务以及无形资产等方面。

## ■ 资产赋值：对资产的价值或重要程度进行评估

- 一般地，资产的价值可由资产在安全属性上的达成程度或其他安全属性未达成时所造成的影响程度来决定，可分为对**保密性、完整性、可用性**三个方面的赋值。
- 在此基础上，经过**综合评定**得到资产重要性等级。
  - 加权平均原则、最大化原则等

# 威胁识别

## ■ 威胁识别

➤ 根据威胁来源，威胁可分为环境威胁和人为威胁。

- 环境威胁：自然界不可抗力威胁和其它物理因素威胁
- 人为威胁：恶意和非恶意

## ■ 威胁赋值

➤ 对威胁出现的频率进行等级化处理，不同等级分别代表威胁出现的频率的高低。

- 以往安全事件报告中出现过的威胁、威胁的频率、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频率及其破坏力的统计。

# 脆弱点识别

## ■ 脆弱点识别

### ➤ 技术和管理

- 技术脆弱点：物理层、网络层、系统层、应用层等
- 管理脆弱点：技术管理和组织管理

## ■ 脆弱点赋值

- ### ➤ 一般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、弱点流程序度进行评估，然后以定性等级划分形式，综合给出脆弱点的严重程度。



# 已有安全措施的确认真

## ■ 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：
  - 减少威胁出现的频率：培训、惩罚等
  - 减少脆弱点：打补丁、定期检查等

## ■ 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：
  - 业务持续性计划。

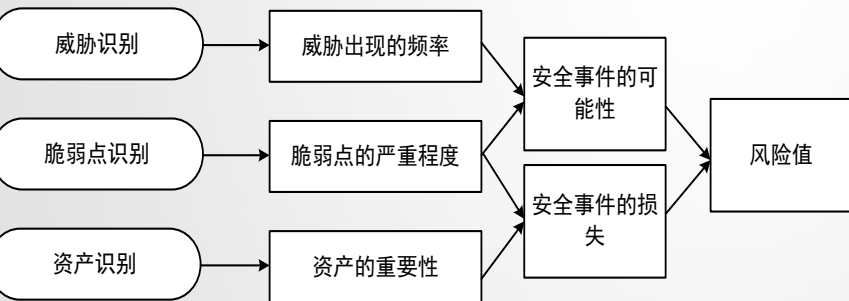
# 风险分析

- 该阶段主要完成风险计算、风险处理计划、残余风险评估三个方面的内容。
- 在风险计算方面，主要通过综合安全事件所作用的资产价值及脆弱点的严重程度，判断安全事件造成的损失对组织的影响，即得到安全风险。
- 在风险处理计划方面，主要完成对不可接受的风险的处理工作。
  - 风险处理计划中应明确采取的弥补脆弱点的安全措施、预期效果、实施条件、进度安排、责任部门等。
- 在残余风险评估方面，主要用来评估在安全措施实施后，残余风险是否降低到可以接受的水平。若仍然不满足风险水平的要求，则需要进一步调整风险处理计划，增加相应的安全措施。

# 风险计算

## ■ 风险值计算

$$\text{风险值} = R(A, T, V) = R[L(T, V) \times F(I_a, V_a)]$$



R: 风险函数

A: 资产

T: 威胁

V: 脆弱点

$I_a$ : 安全事件所作用的资产价值

$V_a$ : 脆弱点等级大小

L: 威胁利用资产的脆弱点而导致安全事件的可能性

F: 安全事件发生后造成的损失

# 风险评估文档记录

■ 主要记录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。

- 风险评价计划
- 风险评估程序
- 资产识别清单
- 重要资产清单
- 威胁列表
- 脆弱点列表
- 已有安全措施确认表
- 风险评估报告
- 风险处理计划
- 风险评估记录

# 信息安全风险评估方法

## ■ 定性分析方法

- 定性的评估分析方法是一种采用比较广泛的模糊分析方法。
- 主要依靠 *专家的知识*和*经验*、被评估对象的相关记录以及相关走访调查来对资源、威胁、脆弱点和现有的防范措施进行系统评估。
- 定性分析方法很多，包括小组讨论（如Delphi方法）、调查、人员访谈、问卷和检查列表等。。

## ■ 典型的定性分析方法

- 主观评分法
- 故障树分析法

# 信息安全风险评估方法

## ■ 定量分析方法

- 对构成风险的各个要素和潜在损失的水平赋以数值，进而来量化风险评估的整个过程和结果。

## ■ 典型的定量分析方法

- 决策树法
- 模糊综合评价法
- 层次分析法
- ...

# 信息安全风险评估方法

## ■ 定性和定量结合的分析方法

- 定性分析要求分析者具有一定的能力和经验，且分析基于主观性，其结果很难统一。
  - 定量分析依赖大量的统计数据，且分析基于客观，其结果很直观，容易理解。
- ## ■ 信息安全风险评估是一个复杂的过程，涉及多个因素、多个层面，具有不确定性，它是一个多约束条件下的多属性决策问题
- 有些要素的量化很容易，而有些却是很困难甚至是不可能的。
  - 如果单纯的使用定性或定量的方法，对风险有效的评估则是很难的。

# 信息安全风险评估工具

工具名称	COBRA	RA	CRAMM	@RISK	BDSS
组织/国家	C&A/Britain	BSI/Britain	CCTA/Britain	Palisade/America	The Integrated Risk Management Group/America
体系结构	C/S模式	单机版	单机版	单机版	单机版
采用方法	专家系统	过程式算法	过程式算法	专家系统	专家系统
定性/定量算法	定性/定量结合	定性/定量结合	定性/定量结合	定性/定量结合	定性/定量结合
数据采集形式	调查问卷	过程	过程	调查问卷	调查问卷
对使用人员的要求	不需要有风险评估的专业知识	依靠评估人的知识和经验	依靠评估人的知识和经验	不需要有风险评估的专业知识	不需要有风险评估的专业知识
结果输出形式	结果报告：风险等级与控制措施	风险等级与控制措施（基于BS7799提供的控制措施）	风险等级与控制措施（基于BS7799提供的控制措施）	决策支持信息	安全防护措施列表



# 信息安全审计

# 信息安全审计

## ✓ 审计 ( Audit )

### ✓ Audit 审计,查账

- ✓ an inspection of the accounting procedures and records by a trained accountant or CPA

### ✓ 审计

- ✓ 审计是对资料作出证据搜集及分析，以评估企业财务状况，然后就资料及一般公认准则之间的相关程度作出结论及报告。进行审计的人员必需有独立性及具相关专业知识。

## ✓ 信息安全审计

- 信息安全审计/IT审计/信息系统安全审计
- 审计应该是独立的，审计与信息安全的目标是一致的，而不是对立的。

## ✓ 信息安全与信息安全审计

- 信息安全其中一项必不可少的内容是IT审计
- IT审计主要针对的是信息安全，也包含其他内容
- 信息安全与IT审计有很大的重合点
- 要做好IT审计必须了解信息安全

## ✓ 信息安全审计师

- ✓ 信息安全审计师，英文为Certified Information Security Professional - Auditor（简称CISP-Auditor），CISP-Auditor是中国信息安全测评中心在CISP现有人员资格认证注册工作的基础上，于2012年推出的又一项信息安全专业人员资格认证项目，是CISP家族的新成员，是国家对信息安全审计人员资质的最高认可。
- ✓ 要求：博士研究生；硕士研究生以上，具有1年工作经历；或本科毕业，具有2年工作经历；或大专毕业，具有4年工作经历。
- ✓ 知识体系结构共包括：信息安全保障、信息安全标准与法律法规、信息安全技术、信息安全管理、信息安全工程、信息安全审计概述、信息安全审计组织和实施、信息安全控制措施审计实务这八个知识类。

## SOX(Sarbanes-Oxley)法案

- ✓ 2002 年颁布的 Sarbanes-Oxley 法案的一些强制要求。
- ✓ 此法案要求上市公司的工作人员个人不仅对公司的财务报表负责，而且还需要负责设置恰当的控制措施，以确保报表的准确性。如果没有遵守这些规定，则需要负刑事责任，并会向公众公开以示惩罚。

## SOX(Sarbanes-Oxley)法案

- ✓ 尽管此法案不包含关于 IT、计算机或技术方面的内容，但是审计事务所还是已经将 IT 组织包括在其调查的范围之内。
- ✓ 这些事务所认为，SOX 不仅包括对财务进行恰当的控制；而且还包括如何保护股东资产。这些资产容易受到操作问题的影响，其中包括 IT 风险，如系统灾难、违犯安全，等等。

## SOX(Sarbanes-Oxley)法案

- ✓ 公司高级管理人员被判定行为不当的某些最臭名卓著的案例包括指使 IT 人员涉嫌操纵数据、修改程序和忽略基本系统控制，以便为财务报表和审计提供不正确的数据。
- ✓ 因此，是美国上市公司审计监督委员会要求公开审计的内容包括 IT 控制

# IT审计的要求

- ✓ IT审计是独立的IT审计师采用客观的标准对以计算机为核心的信息系统的整个生命周期内的相关的活动和产物进行完整、有效的检查和评估的过程。那么，为了保证审计结果的客观性和权威性，IT审计师必须采用一套公认的、权威的审计标准，作为实施IT审计的基本准则和实施依据。



# IT Audit 相关标准

- ✓ 目前在国际上较为流行的是美国的ISACA协会的审计标准。ISACA于1996年推出了用于“IT审计”的知识体系COBIT ( Control Objectives for Information and related Technology ) , 即信息系统和技术控制目标。作为IT治理的核心模型, COBIT包含34个信息技术过程控制, 并归集为4个控制域: IT规划和组织 ( Planning and Organization )、系统获得和实施 ( Acquisition and Implementation )、交付与支持 ( Delivery and Support ) , 以及信息系统运行性能监控 ( Monitoring )。目前, COBIT已成为国际公认的IT管理与控制标准。

# IT Audit

IT Audit

- ✓ **信息系统审计**是指根据公认的标准和指导规范对信息系统及其业务应用的效能、效率、安全性进行监测、评估和控制的过程, 以确认预定的业务目标得以实现。
- ✓ 信息系统审计其业务范围包括与信息系统有关的所有领域。

# 信息系统审计准则

中国内部审计协会

## 准则内容

- ✓ 内部审计具体准则第2203号——信息系统审计

[http://www.ciia.com.cn/docs/fg\\_xg\\_nszz/2013-08-28/1377650086885.html](http://www.ciia.com.cn/docs/fg_xg_nszz/2013-08-28/1377650086885.html)

- ✓ 分为7章28条

- ✓ **总则**、**一般原则**、审计计划、风险评估、信息系统审计的内容、  
信息系统审计的方法

- ✓ 自2014年1月1日起施行