



信息安全导论

第十三章 信息安全管理与 信息安全法规

黄 珂



温故

- 信息安全等级保护综述
- 等级保护的设计与应用
- 信息系统安全工程
- 系统安全工程-能力成熟度模型（SSE-CMM）



知新

- 信息安全管理概述
- 信息安全管理体系
- 信息安全风险评估
- 我国信息安全的法律体系
- 我国信息安全标准化体系



本章内容概要

- 信息安全管理概述
- 信息安全管理体系
- 信息安全风险评估
- 我国信息安全的法律体系
- 我国信息安全标准化体系



概述

- 信息安全管理控制措施与信息安全技术控制措施一起构成了信息安全防护措施的全部
 - 管理与技术并重
 - 特别是信息安全管理标准的制定



什么是管理

- 管住原则，理出思路
 - 原则：规章制度
 - 思路：事先的组织、规划以及实施过程中的协调和事后的评估、总结
 - 管理的核心要点
 - 管理的主体：明确谁来管
 - 管理的客体：管什么
 - 管理手段：怎么管
 - 管理效果：管的怎样
- 访问控制三要素
- 主体
- 客体
- 访问控制策略
- 审计
- 访问控制的三个基本面之一



什么是信息安全管理

- 将“管理”的概念应用到信息安全领域
- 信息安全管理是把分散的信息安全技术因素和人的因素，通过策略、规则协调调整合成为一体，服务于信息安全的目标
- 信息安全管理的层次划分
 - 根据管理主体、管理对象要素的不同
 - 国家层次的信息安全管理
 - 组织层面的信息安全管理



信息安全管理的特点

- 宏观化
 - 信息化的互联、互通、互操作特点
 - 如何定义信息边疆？如何捍卫信息边界？
 - 如何整合安全防御资源？
- 微观化
 - 现代信息系统的复杂性，需要微观信息安全管理
 - 人如何操作技术的规范尺度，是发挥人的因素和技术因素的桥梁
- 宏观管理是对微观管理的指导和约束，微观管理是对宏观管理的贯彻和落实，二者紧密相关，互为依托，缺一不可



信息安全管理的重要性

- 三分技术，七分管理

—据有关部门统计，在所有的计算机安全事件中，
越有52%是人为因素造成的，25%是由火灾、水灾
等自然灾害引起的，技术错误占10%，组织内部
人员作案占10%，仅有3%左右是由外部不法人员
攻击造成的

- 安全技术是信息安全的构筑材料，安全管理
是信息安全的黏合剂和催化剂



信息安全管理的范畴

- 制定信息安全政策
- 风险评估
- 控制目标与方式选择
 - 安全方针策略、组织安全、资产分类与控制、人员安全、物理与环境安全、通信与操作安全、访问控制、系统开发与维护、业务持续性管理、符合法律法规要求
- 制定规范的操作流程
- 对员工进行安全意识培训

保证组织信息资产的安全与业务的连续性



国外信息安全管理相关标准

- BS 7799 标准
- ISO/IEC 17799 标准
- ISO/IEC 2700X 系列标准
- IT 安全管理指南 (ISO/IEC TR 13335)
- 信息及相关技术控制目标 (COBIT)
- IT 服务流程管理 (ITIL)



BS 7799标准 (1/2)

- 英国标准协会 (BSI) 制定的信息安全管理体
系标准
 - 保障信息的保密性、完整性和可用性
 - BS 7799-1:1999 《信息安全管理实用规则》
 - 为第二部分的具体实施提供了指南
 - BS 7799-2:2002 《信息管理体系规范》
 - BS 7799涵盖了所有的信息安全议题
 - 从2000年到2005年，全球将近2000家组织获得了BS 7799-2认证，中国有将近20家单位获得此认证



BS 7799标准 (2/2)

- BS 7799-1
 - 组织建立并实施信息安全管理的一个指导性准则
- BS 7799-2
 - 引用了PDCA模型，将信息管理体系分解成风险评估、安全设计与执行、安全管理和再评估4个子过程
 - 提出了建立信息管理体系的步骤
 - 定义信息安全政策、定义ISMS的范围、进行信息安全风险评估、信息安全风险管理、确定控制目标和选择控制措施、准备信息安全适用性声明



ISO/IEC 17799标准

- 2000年12月，BS 7799-1《信息安全管理实用规则》被国际标准化组织（ISO）正式批准成为国际标准，编号为ISO/IEC 17799
 - ISO/IEC 17799的最新版本是ISO/IEC 17799:2005
 - 对原有的11个控制进行了修改，保留了116个原有控制，增加了17个新的控制（共计133个控制），增加了8个新的控制目标（共计39个控制目标），5个控制目标进行了重新调整



ISO/IEC 2700X 系列标准

- 2005年10月，BS 7799-2《信息安全管理规范》成功升级为国际标准，编号为：
ISO/IEC 27001
 - ISO/IEC 27001是信息管理体系（ISMS）的规范说明
 - ISO/IEC 17799则同时被国际标准化组织重新编号为ISO/IEC 27002



IT安全管理指南 (ISO/IEC TR 13335)

- ISO/IEC 13335 《IT安全管理指南》新版称做“信息和通信技术安全管理”，它是由ISO/IEC 制定的技术报告，是一个信息安全管理方面的指导性标准
 - 目的：有效实施IT安全管理提供建议和支持
 - 特点：强调以风险管理为核心的信息安全管理



信息及相关技术控制目标 (COBIT)

- 国际上通用的信息系统审计标准
—Control Objectives for Information and related Technology
- COBIT以组织的业务目标为核心，为组织提供其所需的信息，同时，平衡在信息技术领域的投资与风险，把握技术发展带来的机会，以达到利益最大化，机会资本化，获取竞争优势



IT服务流程管理 (ITIL)

- 信息技术基础设施库ITIL是由英国政府的中央计算机和通信机构（CCTA）提出的，是由英国商务部（OGC）负责维护的一套IT服务管理标准
 - Information Technology Infrastructure Library
 - 通过描述IT的关键的10个核心流程的目标、活动、输入、输出以及各个流程之间的关系，为IT服务管理领域确立了一套最佳实践方法
 - 到20世纪90年代中期，ITIL已经成为世界服务管理领域事实上的标准，IT著名厂商IBM、HP、CA根据ITIL都提出了自己的服务管理模型
 - 与ISO/IEC 27001相比，ITIL关注面更为广泛，而且更侧重于具体的实施流程



我国信息安全管理相关标准

- 全国信息安全标准化技术委员会内，第7工作组（WG7）主要负责研究和制定适用于涉密和敏感领域之外的安全保障的通用安全管理方法、安全控制措施以及安全支撑和服务等方面的标准、规范及指南。目前我国已正式转化的信息安全管理国际标准有：
 - GB/T 19716-2005《信息技术 信息安全管理实用规则》
(修改采用国际标准ISO/IEC 17799:2000)
 - GB/T 19715.1-2005《信息技术 IT安全管理指南第1部分：IT安全概念和模型》
(等同采用ISO/IEC TR 13335-1:1996)
 - GB/T 19715.2-2005《信息技术 IT安全管理指南第2部分：管理和规划安全》
(等同采用ISO/IEC TR 13335-2:1997)
 - ...



从ISO/IEC 27002标准看信息安全管理控制措施

- (1) 信息安全方针
- (2) 信息安全组织
- (3) 资产管理
- (4) 人力资源安全
- (5) 物理和环境安全
- (6) 通信和操作管理
- (7) 访问控制
- (8) 信息系统获取、开发和维护
- (9) 信息安全事件管理
- (10) 业务连续性管理
- (11) 符合性



信息安全方针

- Information Security Policy

- 描述组织具有哪些重要的信息资产，并说明这些资产如何被保护的一个计划

- 目的

- 对组织中成员阐明 (HOW to do)

- 如何使用组织中的信息系统资源

- 如何处理敏感信息

- 如何采用安全技术产品

- 用户在使用信息时应当承担的责任

- 有所为，有所不为 (WHAT to do)

- 详细描述员工的安全意识与技能要求

- 列出被组织禁止的行为



信息安全组织

- 内部组织
 - 攘外必先安内
 - 清晰的内部组织说明、可证实的承诺、明确的信息安全职责分配及确认
- 外部各方
 - 组织的被外部各方访问、处理、管理或与外部进行通信的信息和信息处理设施的安全
 - 不同安全域的等级安全保护



资产管理

- 资产负责
 - 所有资产都是可核查的，并且有指定的责任人
- 信息分类
 - 遵循等级安全保护原则，依照信息资产的不同价值属性和存在特点
 - 存在的弱点、面临的威胁、需要进行的保护和安全控制差异
 - 组织的价值、法律要求、敏感性和关键性



人力资源安全

- 任用前
 - 确保员工、合同方和第三方用户了解其责任并认可其角色，减少盗窃、滥用或设施误用风险
- 任用中
 - 确保员工、合同方和第三方用户知晓威胁，明确权责，照章办事
- 任用的终止和变更
 - 设备归还和访问控制授权取消



物理和环境安全

- 安全区域
 - 界定安全边界
 - 严把物理访问出入口
 - 设定公共访问和交接区并落实物理访问控制
 - 内部安全保护（办公室、房间和设施）
- 设备安全
 - 目标是防止资产流失
 - 有形资产和物理设备所承载的无形资产
 - 人为损害和非人为损害
 - 设备安置、使用、传输、处置及再利用等设备生命周期完整保护



通信和操作管理

- 操作规程和职责
- 第三方服务交付管理
- 系统规划与验收
- 防范恶意和移动代码
- 备份
- 网络安全管理
- 介质处理
- 信息交换
- 电子商务服务
- 监视



访问控制

- 访问控制的业务要求
- 用户访问管理
- 用户责任
- 网络访问控制
- 操作系统访问控制
- 应用和信息访问控制
- 移动计算和远程工作



信息系统获取、开发和维护

- 信息系统的安全要求
- 应用中的正确处理
 - 系统安全、软件安全开发生命周期管理
- 密码控制
- 系统文件的安全
- 开发和支持过程中的安全
- 技术脆弱性管理



信息安全事件管理

- 报告信息安全事件和弱点
 - CVE、NVD、CNVD等漏洞分类和报告标准
- 信息安全隐患管理和改进



业务连续性管理

- 防止业务活动中断

- 通过预防性和恢复性措施相结合，将灾难和安全事故造成的影响降低到可以接受的水平
- 对灾难事故、安全故障和服务损失所造成的结果进行分析
- 制定并实施紧急事件处理计划，确保能够在要求的时间内恢复业务流程，并应当保持这种计划，使之成为其他管理程序的一部分
- 业务连续性管理还应当包括相关的管理测试来识别并减小风险、限制毁灭性事件的后果、确保重要操作及时恢复



符合性

- 与法律法规要求的符合性
- 与安全策略、标准以及技术要求的符合性
 - 最佳实践原则
- 信息系统审计考虑



本章内容概要

- 信息安全管理概述
- 信息安全管理体系
- 信息安全风险评估
- 我国信息安全的法律体系
- 我国信息安全标准化体系



引言

- 信息安全管理体ISMS
 - Information Security Management System
 - 组织基于业务风险方法，建立、实施、运行、监视、评审、保持和改进信息安全的体系，是一个组织的整个管理体系的一部分，它包括组织结构、方针策略、规划活动、职责、实践、规程、过程和资源
 - 以ISO/IEC 2700X为基础，建立ISMS已经成为很多组织开展信息系统安全建设的基本方法

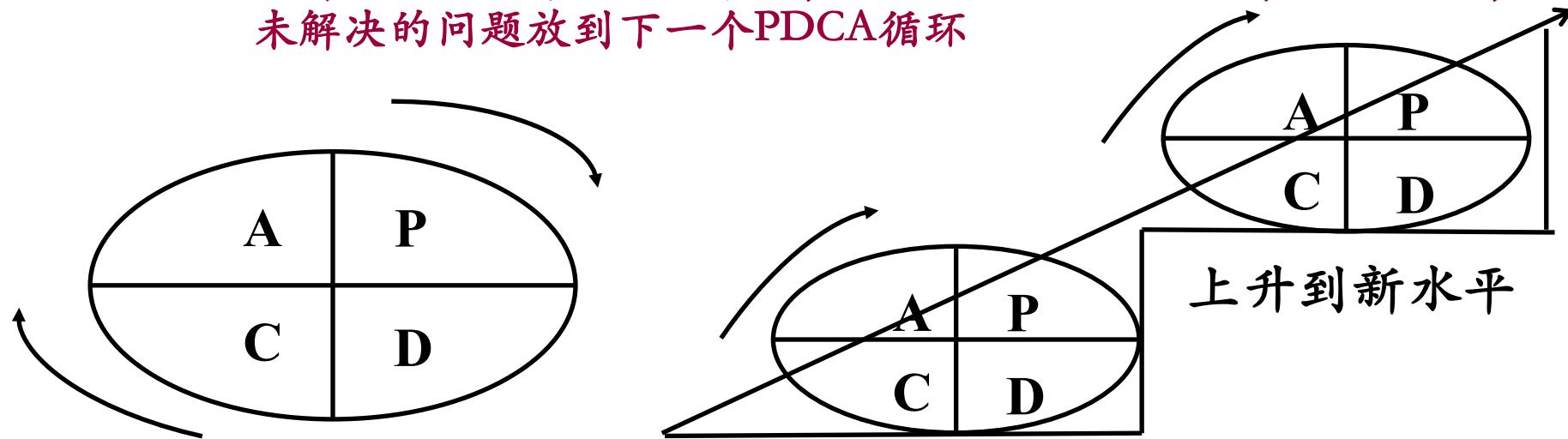


PDCA模型

- ISMS实施方法的核心理念——PDCA循环

- 美国质量管理专家戴明提出，所以又称为“戴明环”

- P (Plan) : 计划，确定方针和目标，确定活动计划
 - D (Do) : 实施，实际去做，实施计划中的内容
 - C (Check) : 检查，总结执行计划的结果，注意效果，找出问题
 - A (Action) : 行动，对总结检查的结果进行处理，成功的经验加以肯定并适当推广、标准化；失败的教训加以总结，以免重现；未解决的问题放到下一个PDCA循环





PDCA循环的特点

- 大环带小环
 - 企业和部门、小组之间的关系
- 阶梯式上升
 - 螺旋式上升和发展的
 - 每循环一次就解决一部分问题
 - 到了下一次循环，又有了新的目标和内容，更上一层楼
- 科学管理方法的综合应用
 - PDCA循环应用以质量控制七种工具为主的统计处理方法以及工业工程中工作研究的方法作为进行工作和发现问题的工具



PDCA之于ISMS

- 建立ISMS
- 实施和运行ISMS
- 监视和评审ISMS
- 保持和改进ISMS



建立ISMS





实施和运行ISMS

- **主要工作**
 - 建立一个有效的管理体系
 - 依据规定的方式、方法监控计划阶段所提的活动
 - 确保计划阶段未预料的影响和破坏被快速识别并得到适当管理
 - 分配适当的资源（人员、时间和资金）运行信息安全管理
体系以及所有的安全控制
 - 安排针对信息安全意识的培训，并检查意识培训的效果
 - 实施并保持已计划好的检测和响应机制
- **关键问题**
 - 保证资源、提供培训、提高安全意识
 - 风险管理



监视和评审ISMS

- 符合性检查
 - 方针、程序、标准与法律法规
- 主要工作
 - 执行监视程序和其他控制措施以快速检测处理结果中的错误
 - 评审信息安全管理体系建设的有效性、剩余风险和可接受风险的等级
 - 审核规定的安全程序是否适当、是否符合标准以及是否按照预期的目的进行工作
- 常用的检查措施主要有以下几种
 - 日常检查、自治程序
 - 学习其他组织好的经验
 - 信息安全管理体系建设审核
 - 管理评审、趋势分析



保持和改进ISMS

- 主要工作

- 测量信息安全管理体体系满足安全方针和目标方面的业绩
- 识别信息安全管理体体系的改进，并有效实施
- 采取适当的纠正和预防措施
- 沟通结果及活动，并与所有相关方磋商
- 必要时修订信息安全管理体体系
- 确保修订达到预期的目标

- 关键问题

- 不符合项的确定
- 纠正性措施
- 预防性措施



本章内容概要

- 信息安全管理概述
- 信息安全管理体系
- 信息安全风险评估
- 我国信息安全的法律体系
- 我国信息安全标准化体系

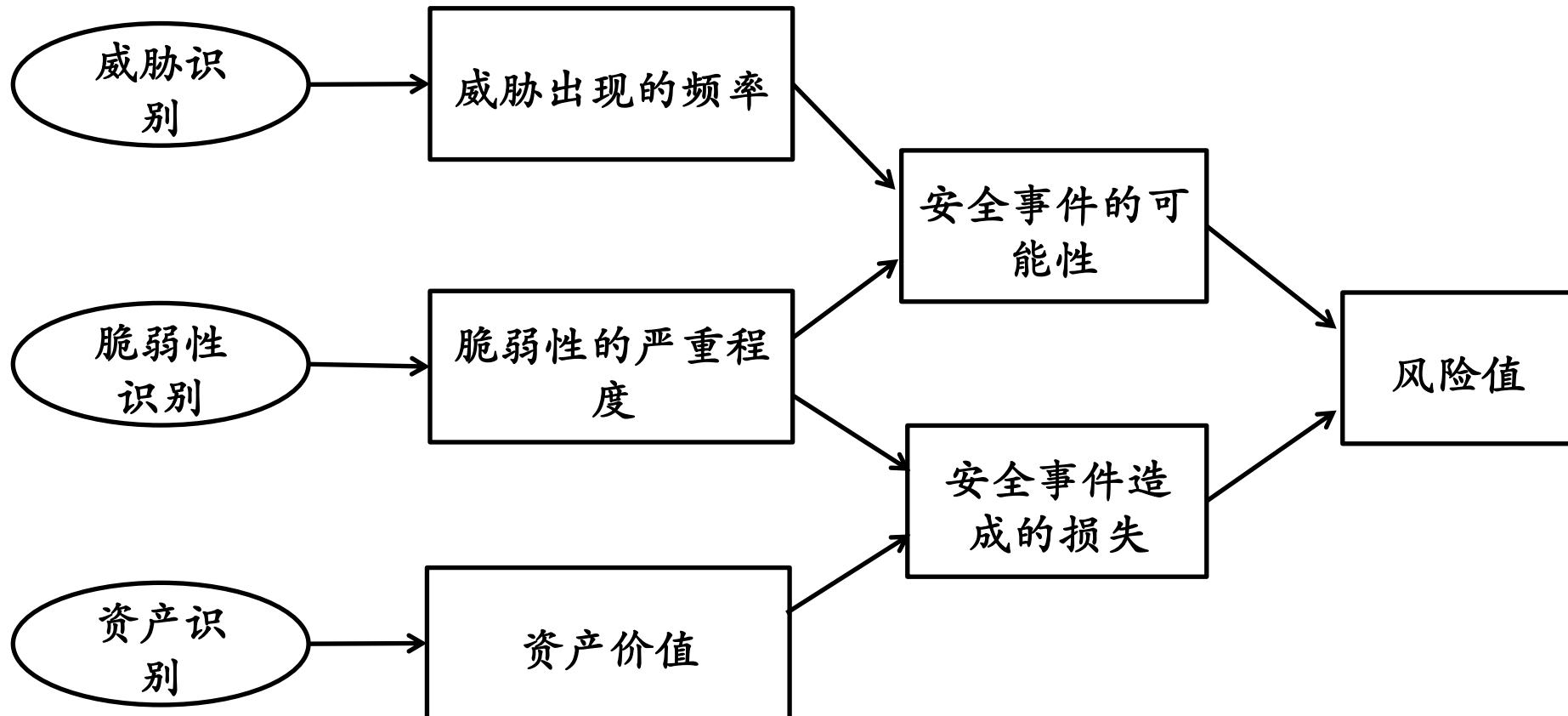


概述

- 信息安全风险评估就是从风险管理角度，运用科学的方法和手段，系统地分析信息系统所面临的威胁及其存在的脆弱性，评估安全事件一旦发生可能造成的危害程度，提出有针对性的抵御威胁的防护对策和整改措施，为防范和化解信息安全风险，将风险控制在可接受的水平，从而最大限度地保障信息安全提供科学依据



风险分析原理



第二章介绍过：通用弱点评价体系（CVSS）



本章内容概要

- 信息安全管理概述
- 信息安全管理体系
- 信息安全风险评估
- 我国信息安全的法律体系
- 我国信息安全标准化体系



我国信息安全相关法律法规总览

刑法修正案(七)在刑法第285条中增加两款(第二款、第三款):

违反国家规定,侵入前款规定以外的计算机信息系统或者采用其他技术手段,获取该计算机信息系统中存储、处理或者传输的数据,或者对该计算机信息系统实施非法控制,情节严重的,处三年以下有期徒刑或者拘役,并处或者单处罚金;情节特别严重的,处三年以上七年以下有期徒刑,并处罚金。

| | | |
|------------------|--------------------------------|-----|
| 六. 2004年..... | 9.3 境外组织和个人在华使用密码产品管理办法..... | 102 |
| 6.1 中华人民共和国 | 十. 2009年..... | 103 |
| 七. 2005年..... | 10.1 刑法修正案(七)关于信息安全的修订与解读..... | 111 |
| 7.1 互联网安全保护..... | 10.2 深圳经济特区企业技术秘密保护条例..... | 113 |
| | 十一. 2010年..... | 113 |

提供专门用于侵入、非法控制计算机信息系统的程序、工具,或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具,情节严重的,依照前款的规定处罚。



网络与系统安全不可儿戏

- 《最高人民法院、最高人民检察院关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》
 - 2011年6月20日最高人民法院审判委员会第1524次会议、2011年7月11日最高人民检察院第十一届检察委员会第63次会议通过
 - 自2011年9月1日起施行



知法守法

- 网络与系统安全**攻防**实验必须严格限制在局域网范围内
- 了解保密相关法律法规
 - 泄密坐牢，卖密杀头
 - 涉密不联网，联网不涉密



我国主要信息安全法律

- 《中华人民共和国宪法》（第四十条）
- 《中华人民共和国保守国家秘密法》
- 《中华人民共和国国家安全法》（第十条、十一条等）
- 《中华人民共和国人民警察法》（第六条、十六条等）
- 《中华人民共和国刑法》（第二百八十五条、二百八十六条、二百八十七条）
- 《全国人民代表大会常务委员会关于维护互联网安全的决定》
- 《中华人民共和国电子签名法》
- 《中华人民共和国治安管理处罚法》（第二十九条、四十二条等）



我国主要信息安全行政法规

- 《中华人民共和国计算机信息系统安全保护条例》
- 《中华人民共和国计算机信息网络国际联网管理暂行规定》
- 《商用密码管理条例》
- 《中华人民共和国电信条例》
- 《互联网信息服务管理办法》
- 《互联网上网服务营业场所管理条例》
- 《信息网络传播权保护条例》



我国主要信息安全部门规章

- 《计算机信息系统专用产品检测和销售许可证管理办法》（公安部令第32号）
- 《计算机信息网络国际联网安全保护管理办法》（公安部令第33号）
- 《计算机病毒防治管理办法》（公安部令第51号）
- 《非经营性互联网信息服务备案管理办法》（信息产业部令第33号）
- 《互联网IP地址备案管理办法》（信息产业部令第34号）
- 《互联网新闻信息服务管理规定》（国务院新闻办公室、信息产业部令第37号）
- 《电子出版物管理规定》（新闻出版总署令第11号）



我国地方性法规和地方政府规章

- 地方性法规
 - 《北京市信息化促进条例》
 - 《天津市信息化促进条例》
 - 《山东省信息化促进条例》
- 地方政府规章
 - 《福建省计算机信息系统安全管理办法》
 - 《安徽省计算机信息系统安全保护办法》
 - 《广东省计算机信息系统安全保护管理规定》
 - 《北京市公共服务网络与信息系统安全管理规定》



我国信息安全立法存在的问题

- 结构不合理
- 立法部门之间缺乏统筹规划
- 法规制度的制定实施针对性和操作性不够强
- 有些法规制度明显落后于技术发展
- 公民个人权益缺乏法律保护
 - 《个人信息保护法》迟迟不能制定
- 刑事程序立法亟待完善

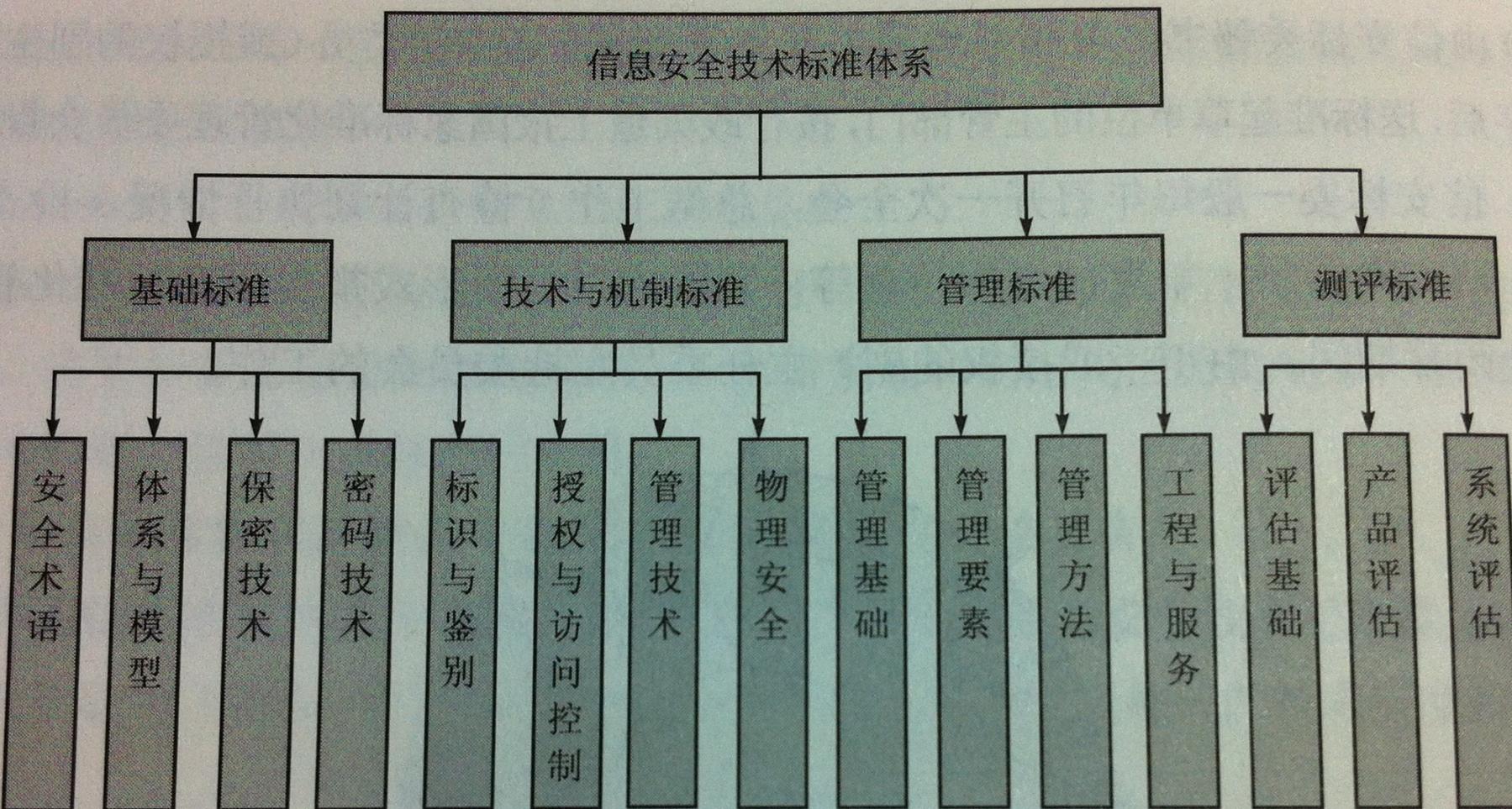


本章内容概要

- 信息安全管理概述
- 信息安全管理体系
- 信息安全风险评估
- 我国信息安全的法律体系
- 我国信息安全标准化体系



中国信息安全技术标准体系





“十一五”和“十二五”期间重点信息安全标准项目

- 2006~2010年

| 信息安全等级保护有关标准 | 涉密信息系统安全保密标准 | 密码技术和网络信任体系标准 | 电子政务信息安全标准 |
|---------------|----------------------|-----------------|---------------|
| 电子商务信息安全标准 | 信息安全政府监管有关标准 | 信息安全管理体系建设标准 | 信息安全应急与灾害有关标准 |
| 信息安全服务管理标准 | 信息安全测评标准 | 信息安全保障指标与评价体系 | 可信计算技术标准 |
| 无线通信和移动通信安全标准 | 通讯社及广播电视台等新闻发布系统安全标准 | 信息安全相关的生物特征识别标准 | 信息安全标准体系 |

- 2010~2015年

—开展安全可控信息产品和服务在电子政务、电子商务、电子医疗、金融、能源等领域，以及云计算、物联网、移动互联网和工业控制系统中的示范应用，推动组建相应的产业联盟，加快安全可控信息产品和服务产业化步伐



网络安全相关标准

- 可信计算机系统评估准则 (TCSEC)
- 可信网络解释 (TNI)
- 通用准则CC
- 《计算机信息系统安全保护等级划分准则》
- 信息安全保证技术框架
- 《信息系统安全保护等级应用指南》



参考文献

- 《信息安全产业“十二五”发展规划》解读
<http://www.cena.com.cn/a/2012-03-05/133091744165518.shtml>