第10章 信息安全管理

罗文坚

主要内容

- **10.1 概述**
- **10.2 信息安全风险管理**
- **10.3 信息安全标准**
- **10.4 信息安全法律法规及道德规范**

概述

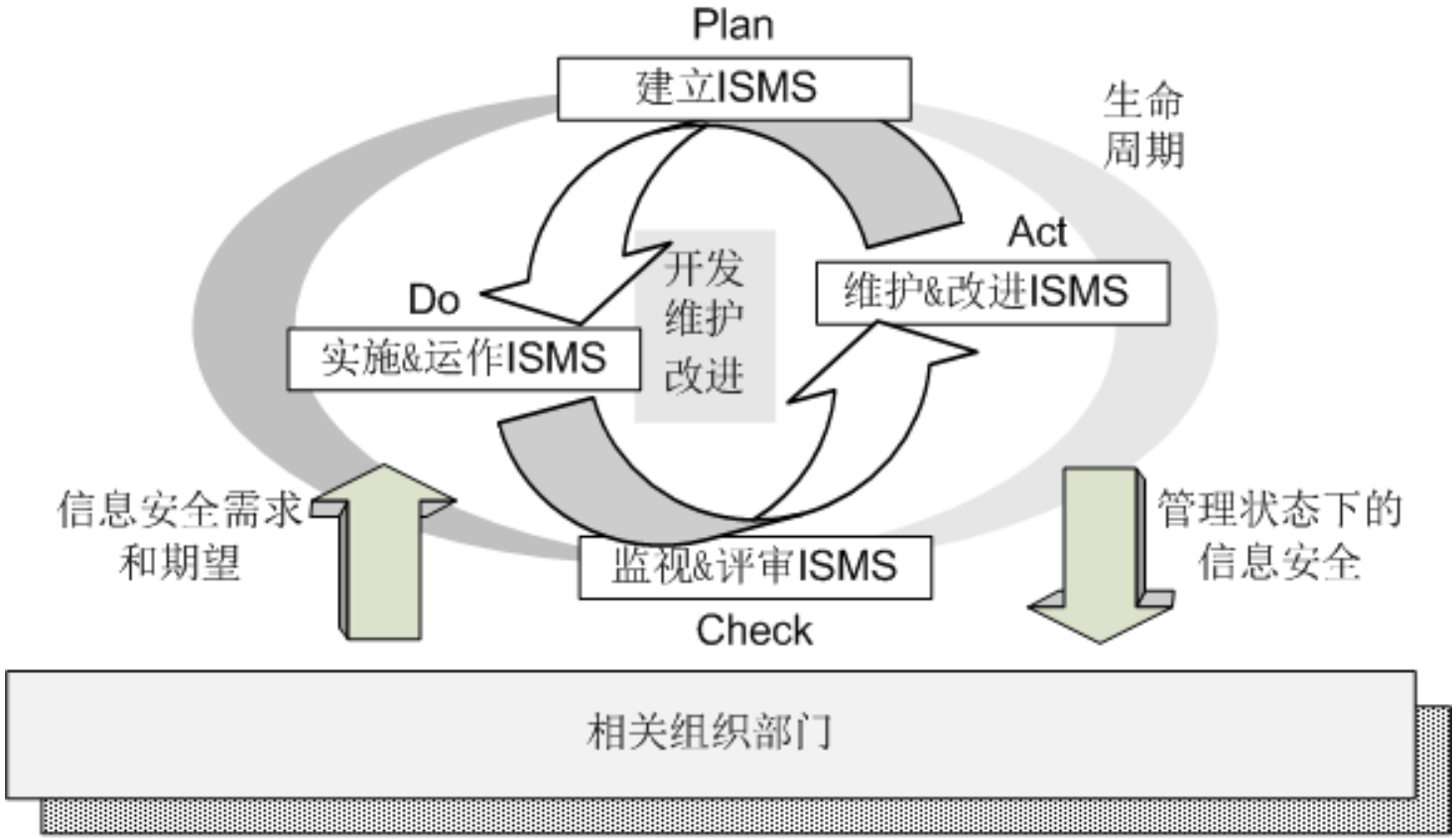
- 当今社会已经进入到信息化社会，其信息安全是建立在信息社会的基础设施及信息服务系统之间的互联、互通、互操作意义上的安全需求上。

- 安全需求可以分为安全技术需求和安全管理需求两个方面。

- 管理在信息安全中的重要性高于安全技术层面，“三分技术，七分管理”的理念在业界中已经得到共识。

信息安全管理体系ISMS

- 信息安全管理体系ISMS（Information Security Management System）是从管理学惯用的过程模型PDCA（Plan、Do、Check、Act）发展演化而来。



信息安全管理的PDCA模型

ISMS

- 信息安全管理体系（ISMS）是一个系统化、过程化的管理体系，体系的建立不可能一蹴而就，需要全面、系统、科学的风险评估、制度保证和有效监督机制。
- ISMS应该体现预防控制为主的思想，强调遵守国家有关信息安全的法律法规，强调全过程的动态调整，从而确保整个安全体系在有效管理控制下，不断改进完善以适应新的安全需求。
- 在建立信息安全管理体系的各环节中，安全需求的提出是ISMS的前提，运作实施、监视评审和维护改进是重要步骤，而可管理的信息安全是最终的目标。
- 在各环节中，风险评估管理、标准规范管理以及制度法规管理这三项工作直接影到响整个信息安全管理体系是否能够有效实行，因此也具有非常重要的地位。

风险评估

- 风险评估（Risk Assessment）是指对信息资产所面临的威胁、存在的弱点、可能导致的安全事件以及三者综合作用所带来的风险进行评估。

- 作为风险管理的基础，风险评估是组织确定信息安全需求的一个重要手段。

- 风险评估管理就是指在信息安全管理体系的各环节中，合理地利用风险评估技术对信息系统及资产进行安全性分析及风险管理，为规划设计完善信息安全解决方案提供基础资料，属于信息安全管理体系的规划环节。

标准规范管理

- 标准规范管理可理解为在规划实施信息安全解决方案时，各项工作遵循国际或国家相关标准规范，有完善的检查机制。
- 国际标准可以分为互操作标准、技术与工程标准、信息安全管理与控制标准三类。
  - 互操作标准主要是非标准组织研发的算法和协议经过自发的选择过程，成为了所谓的“事实标准”，如AES、RSA、SSL以及通用脆弱性描述标准CVE等。
  - 技术与工程标准主要指由标准化组织制定的用于规范信息安全产品、技术和工程的标准，如信息产品通用评测准则（ISO 15408）、安全系统工程能力成熟度模型（SSE-CMM）、美国信息安全白皮书（TCSEC）等。
  - 信息安全管理与控制标准是指由标准化组织制定的用于指导和管理信息安全解决方案实施过程的标准规范，如信息安全管理体系标准（BS-7799）、信息安全管理标准（ISO 13335）以及信息和相关技术控制目标（COBIT）等。

制度法规管理

- 制度法规管理是指宣传国家及各部门制定的相关制度法规，并监督有关人员是否遵守这些制度法规。

- 每个组织部门（如企事业单位、公司以及各种团体等）都有信息安全规章制度。有关人员严格遵守这些规章制度，对于一个组织部门的信息安全来说十分重要，而完善的规章制度和建全的监管机制更是必不可少。

- 除了有关的组织部门自己制定的相关规章制度之外，国家的有关信息安全法律法规更是有关人员需要遵守的。
  - 目前在计算机系统、互联网以及其它信息领域中，国家均制定了相关法律法规进行约束管理，如果触犯，势必受到相应的惩罚。

立法现状

- 1973年， 瑞典率先在世界上制定第一部含有计算机犯罪处罚内容的《瑞典国家数据保护法》。

- 根据英国学者巴雷特的归纳，各国对计算机犯罪的立法，主要采取了两种方案：
  - 一种是制定计算机犯罪的专项立法，如美国、英国等；
  - 一种是通过修订法典，增加规定有关计算机犯罪的内容，如法国、俄罗斯等。

- 目前我国现行法律法规中，与信息安全有关的已有近百部。
  - 涉及网络与信息系统安全、信息内容安全、信息安全系统与产品、保密及密码管理、计算机病毒与危害性程序防治、金融等特定领域的信息安全、信息安全犯罪制裁等多个领域，初步形成了我国信息安全的法律体系。

道德规范

- 道德规范也是信息领域从业人员及广大用户应该遵守的。
  - 包括计算机从业人员道德规范、网络用户道德规范以及服务商道德规范等。

- 信息安全道德规范的基本出发点：
  - 一切个人信息行为必须服从于信息社会的整体利益，即个体利益服从整体利益；
  - 对于运营商来说，信息网络的规划和运行应以服务于社会成员整体为目的。

- 信息安全管理是一个十分复杂的综合管理体系，规章制度、法律法规和道德规范是管理的基础，标准规范是信息系统实施和安全运行的保证，风险管理是建设信息安全管理体系的重要手段。

主要内容

- 10.1 概述
- 10.2 信息安全风险管理
  - 10.2.1 风险评估
  - 10.2.2 风险控制
- 10.3 信息安全标准
- 10.4 信息安全法律法规及道德规范

信息安全风险管理

- 信息安全风险管理是信息安全管理的重要部分。
  - 是规划、建设、实施及完善信息安全管理体系的基础和主要目标。
  - 其核心内容包括风险评估和风险控制两个部分。

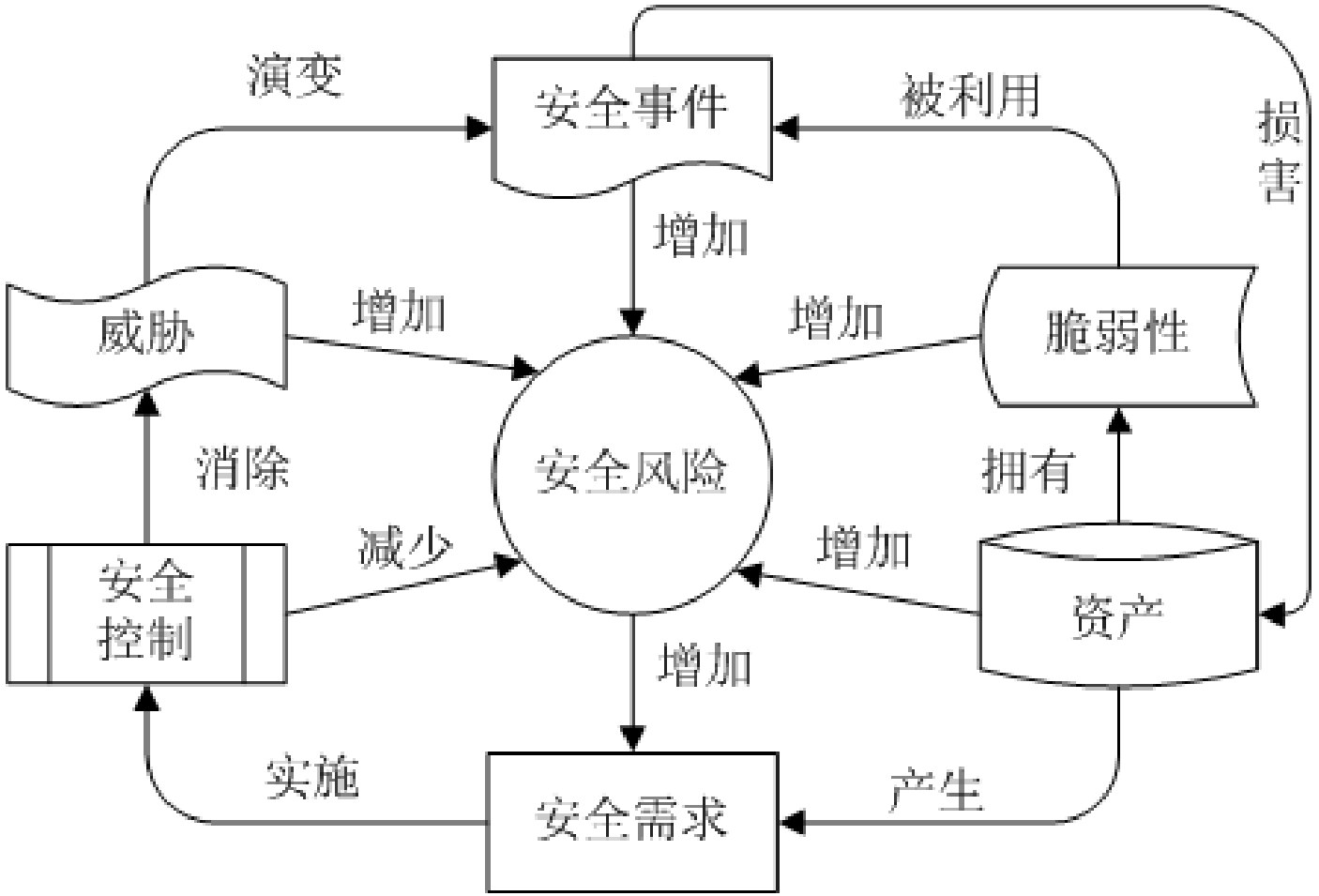
- 风险管理的概念来源于商业领域，主要指对商业行为或目的投资的风险进行分析、评估与管理，力求以最小的风险获得最大的收益。

风险评估

- 风险评估主要包括风险分析和风险评价。
  - 风险分析是指全面地识别风险来源及类型；
  - 风险评价是指依据风险标准估算风险水平，确定风险的严重性。
- 一般认为，与信息安全风险有关的因素主要包括威胁、脆弱性、资产、安全控制等。
  - 威胁（Threat），主要指可能导致资产或组织受到损害的安全事件的潜在因素。
  - 脆弱性（Vulnerability），一般指资产中存在的可能被潜在威胁所利用的缺陷或薄弱点，如操作系统漏洞等。
  - 资产（Assets），是指对组织具有价值的信息资源，是安全策略保护的对象。
  - 安全控制（Security Control），是指用于消除或减低安全风险所采取的某种安全行为，包括措施、程序及机制等。

信息安全风险因素及相互关系

- 风险因素之间相互作用、相互影响；安全风险随各因素的变化呈现动态调整演变趋势。



风险描述

- 风险可以描述成关于威胁发生概率和发生时的破坏程度的函数，用数学符号描述如下：

$$R_i(A_i, T_i, V_i) = P(T_i) \times F(T_i)$$

  - A_i表示资产，V_i表示A_i存在的脆弱性，T_i表示针对资产A_i的脆弱性V_i的威胁；
  - $R_i(A_i, T_i, V_i)$表示因为存在威胁T_i而使资产A_i具有的风险；
  - $P(T_i)$表示威胁T_i发生的概率，$F(T_i)$表示威胁T_i发生时的破坏程度。

- 由于某组织部门可能存在很多资产和相应的脆弱性，故该组织的资产总风险可以描述如下：

$$R_{总} = \sum_{i=1}^{n} R_i(A,T,V) = \sum_{i=1}^{n} P(T_i) \times F(T_i)$$

- 上述关于风险的数学表达式，只是给出了风险评估的概念性描述。

风险评估的任务

- 风险评估的任务：
  ① 识别组织面临的各种风险，了解总体的安全状况；
  ② 分析计算风险概率，预估可能带来的负面影响；
  ③ 评价组织承受风险的能力，确定各项安全建设的优先等级；
  ④ 推荐风险控制策略，为安全需求提供依据。

- 风险评估的操作范围可以是整个组织，也可以是组织中的某一部门，或者独立的信息系统、特定系统组件和服务等。

- 针对不同的情况，选择适当的风险评估方法对有效地完成评估工作来说十分重要。常见的风险评估方法有基线评估方法、详细评估方法和组合评估方法等。

基线评估（Baseline Assessment）

- 基线评估是有关组织根据其实际情况（所在行业、业务环境与性质等），对信息系统进行安全基线检查（将现有的安全措施与安全基线规定的措施进行比较，计算之间的差距），得出基本的安全需求，给出风险控制方案。
- 所谓的基线就是在诸多标准规范中确定的一组安全控制措施或者惯例，这些措施和惯例可以满足特定环境下的信息系统的基本安全需求，使信息系统达到一定的安全防护水平。
- 组织可以采用国际标准和国家标准（如BS 7799-1、ISO 13335-4）、行业标准或推荐（例如德国联邦安全局IT基线保护手册）以及来自其他具有相似商务目标和规模的组织的惯例作为安全基线。
- 基线评估的优点是需要的资源少、周期短、操作简单，是经济有效的风险评估途径。也有缺点，比如基线水准的高低难以设定。如果过高，可能导致资源浪费和限制过度；如果过低，可能难以达到所需的安全要求。

详细评估Detailed Assessment

- 详细评估是指组织对信息资产进行详细识别和评价，对可能引起风险的威胁和脆弱性进行充分地评估，根据全面系统的风险评估结果来确定安全需求及控制方案。
- 这种评估途径集中体现了风险管理的思想，全面系统地评估资产风险，在充分了解信息安全具体情况下，力争将风险降低到可接受的水平。
- 详细评估的优点在于组织可以通过详细的风险评估对信息安全风险有较全面的认识，能够准确确定目前的安全水平和安全需求。
- 详细的风险评估可能是一个非常耗费资源的过程，包括时间、精力和技术。因此，组织应该仔细设定待评估的信息资产范围，以减少工作量。

组合评估

- 组合评估要求首先对所有的系统进行一次初步的风险评估，依据各信息资产的实际价值和可能面临的风险，划分出不同的评估范围，对于具有较高重要性的资产部分采取详细风险评估，而其它部分采用基线风险评估。

- 组合评估将基线和详细风险评估的优势结合起来，既节省了评估所耗费的资源，又能确保获得一个全面系统的评估结果，而且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优先关注。

- 组合评估的缺点是，如果初步的高级风险评估不够准确，可能导致某些本需要详细评估的系统被忽略。

主要内容

- 10.1 概述
- 10.2 信息安全风险管理
  - 10.2.1 风险评估
  - 10.2.2 风险控制
- 10.3 信息安全标准
- 10.4 信息安全法律法规及道德规范

风险控制

- 风险控制是信息安全风险管理在风险评估完成之后的另一项重要工作。

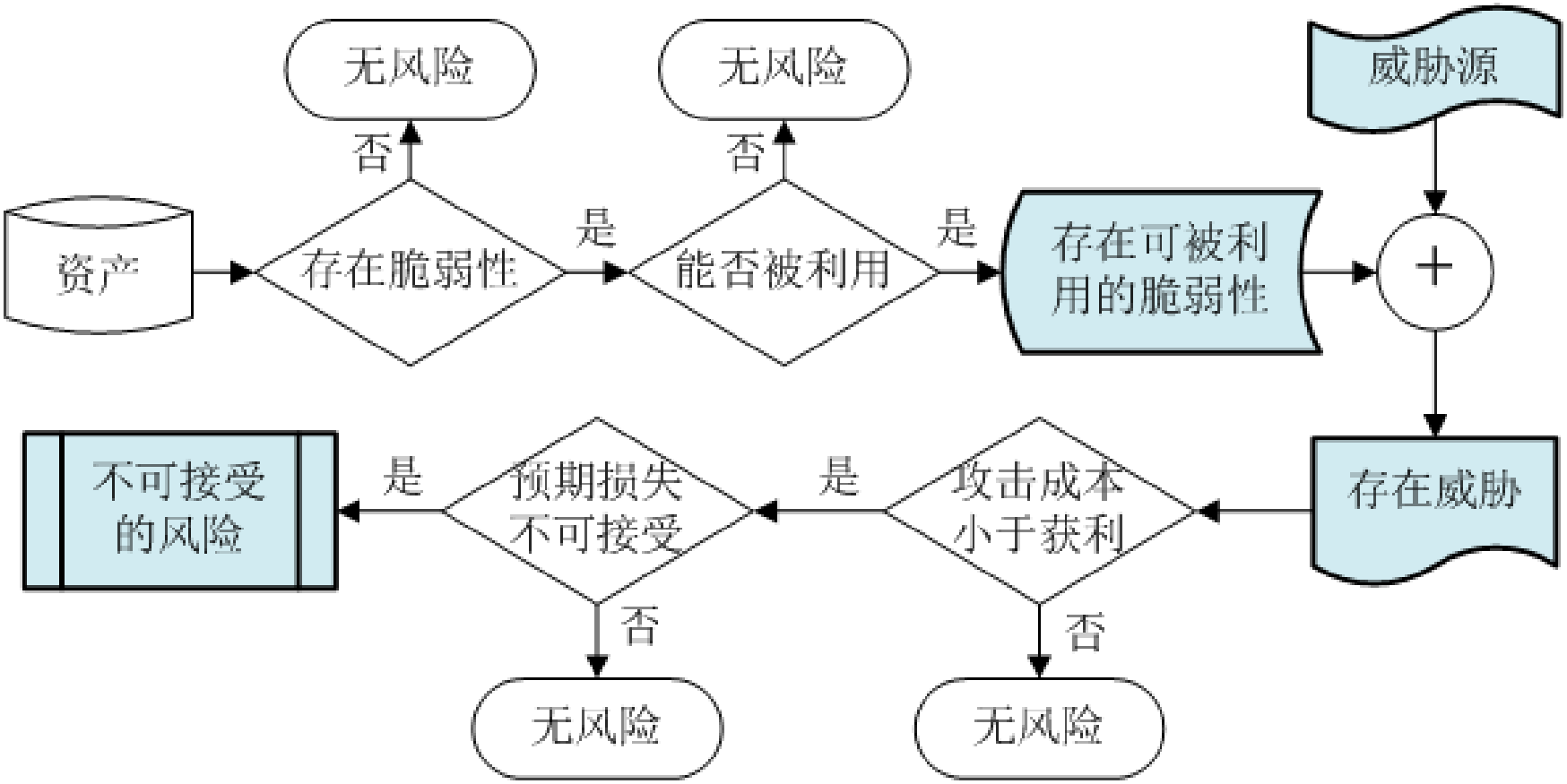
- 风险控制的任务是对风险评估结论及建议中的各项安全措施进行分析评估，确定优先级以及具体实施的步骤。

- 风险控制的目标是将安全风险降低到一个可接受的范围内。
  - 消除所有风险往往是不切实际的，甚至也是近乎不可能的。
  - 安全管理人员有责任运用最小成本来实现最合适的控制，使潜在安全风险对该组织造成的负面影响最小化。

风险控制手段

- 风险控制通常采用如下三种手段来降低安全风险：
  - 风险承受是指运行的信息系统具有良好的健壮性，可以接受潜在的风险并稳定运行，或采取简单的安全措施，就可以把风险降低到一个可接受的级别。
  - 风险规避是指通过消除风险出现的必要条件（如识别出风险后，放弃系统某项功能或关闭系统）来规避风险。
  - 风险转移是指通过使用其它措施来补偿损失，从而转移风险，如购买保险等。
- 一般来说，风险控制措施是以消除安全风险产生条件、切断风险形成的路线为基本手段，最终阻止风险的发生或将风险降低到可接受水平。

安全风险系统判断过程


无风险
无风险
威胁源
否
否
资产
存在脆弱性
是
能否被利用
是
存在可被利用的脆弱性
+
不可接受的风险
是
预期损失不可接受
是
攻击成本小于获利
存在威胁
否
否
无风险
无风险

风险控制具体做法

- 风险控制具体做法：
  1. 当存在系统脆弱性时，减少或修补系统脆弱性，降低脆弱性被攻击利用的可能性；
  2. 当系统脆弱性可利用时，运用层次化保护、结构化设计以及管理控制等手段，防止脆弱性被利用或降低被利用后的危害程度；
  3. 当攻击成本小于攻击可能的获利时，运用保护措施，通过提高攻击者成本来降低攻击者的攻击动机，如加强访问控制，限制系统用户的访问对象和行为，降低攻击获利；
  4. 当风险预期损失较大时，优化系统设计、加强容错容灾以及运用非技术类保护措施来限制攻击的范围，从而将风险降低到可接受范围。

具体的风险控制措施

类别	措施	属性
技术类	身份认证技术 加密技术 防火墙技术 入侵检测技术 系统审计 蜜罐、蜜网技术	预防性 预防性 预防性 检查性 检查性 纠正性
运营类	物理访问控制，如重要设备使用授权等； 容灾、容侵，如系统备份、数据备份等； 物理安全检测技术，防盗技术、防火技术等；	预防性 预防性 检查性
管理类	责任分配 权限管理 安全培训 人员控制 定期安全审计	预防性 预防性 预防性 预防性 检查性

NIST SP800系列标准

- 实施风险控制措施是一个系统化工程，美国NIST制定的NIST SP800系列标准中给出了较详细的具体实施流程，包括七个步骤。

- 第一步 对实施控制措施的优先级进行排序，分配资源时，对标有不可接受的高等级的风险项应该给予较高的优先级；
- 第二步 评估所建议的安全选项，风险评估结论中建议的控制措施对于具体的单位及其信息系统可能不是最适合或最可行的，因此要对所建议的控制措施的可行性和有效性进行分析，选择出最适当的控制措施；
- 第三步 进行成本效益分析，为决策管理层提供风险控制措施的成本效益分析报告；

NIST SP800系列标准

- 第四步 在成本效益分析的基础上，确定即将实施的成本有效性最好的安全措施；
- 第五步 遴选出那些拥有合适的专长和技能，可实现所选控制措施的人员（内部人员或外部合同商），并赋以相应责任；
- 第六步 制定控制措施的实现计划，计划内容主要包括风险评估报告给出的风险、风险级别以及所建议的安全措施，实施控制的优先级队列、预期安全控制列表、实现预期安全控制时所需的资源、负责人员清单、开始日期、完成日期以及维护要求等；
- 第七步 分析计算出残余风险，风险控制可以降低风险级别，但不会根除风险，因此安全措施实施后仍然存在的残余风险。

主要内容

- 10.1 概述
- 10.2 信息安全风险管理
- 10.3 信息安全标准
  - 10.3.1 信息安全标准概述
  - 10.3.2 信息技术安全性评估通用准则（CC）
  - 10.3.3 信息安全管理体系标准
  - 10.3.4 中国的有关信息安全标准
- 10.4 信息安全法律法规及道德规范

信息安全标准

- 技术与工程、互操作、信息安全管理与控制三类标准。
- 技术与工程标准最多也最详细，它们有效地推动了信息安全产品的开发及国际化，如CC、SSE-CMM等标准。
- 互操作标准多数为所谓的“事实标准”，这些标准对信息安全领域的发展同样做出了巨大的贡献，如RSA、DES、CVE等标准。
- 信息安全管理与控制标准的意义在于可以更具体有效地指导信息安全具体实践，其中BS 7799就是这类标准的代表，其卓越成绩也已得到业界共识。

重要标准

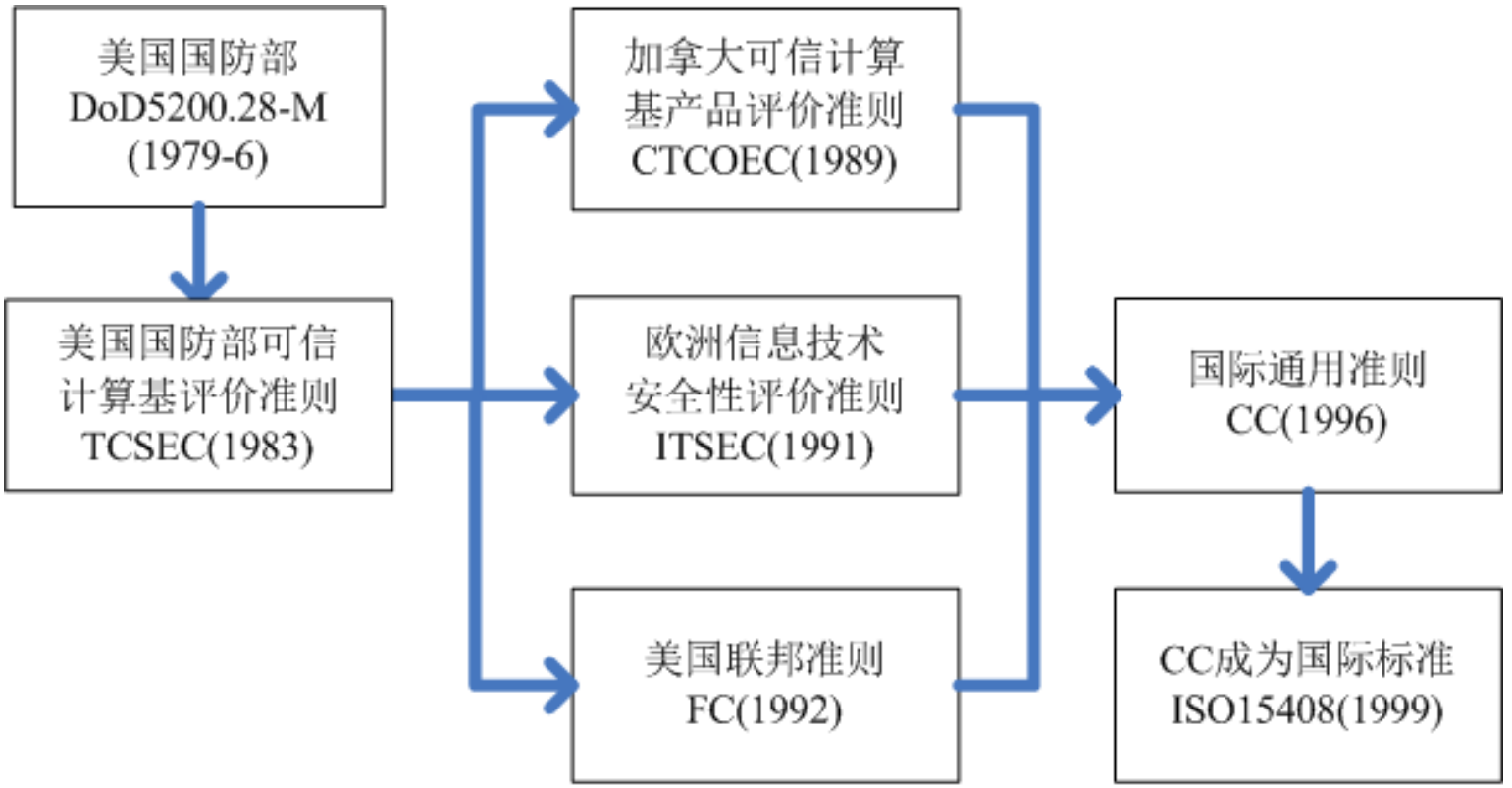
- 1996年，通用标准CC（Common Criteria）是在TESEC、ITSEC、CTCPEC、FC等信息安全标准的基础上演变形成的。
- 1996年，ISO/IEC TR 13335，早前GMITS（Guidelines for the Management of IT Security），新版称作MICTS（Management of Information and Communications Technology Security）。
- SSE-CMM （System Security Engineering Capability Maturity Model）模型是由美国国家安全局NSA领导开发的专门用于系统安全工程的能力成熟度模型。
- CVE（Common Vulnerabilities & Exposures），即通用漏洞及披露，是IDnA（Intrusion Detection and Assessment）的行业标准。
- 1995年，BS 7799是英国标准协会BSI（British Standards Institute）针对信息安全管理而制定的标准，2000年被采纳为ISO/IEC 17799。
- 1996年，COBIT（Control Objectives for Information and related Technology），目前国际上通用的信息系统审计标准。

主要内容

- 10.1 概述
- 10.2 信息安全风险管理
- 10.3 信息安全标准
  - 10.3.1 信息安全标准概述
  - 10.3.2 信息技术安全性评估通用准则（CC）
  - 10.3.3 信息安全管理体系标准
  - 10.3.4 中国的有关信息安全标准
- 10.4 信息安全法律法规及道德规范

信息安全产品标准CC

- CC标准是“The Common Criteria for Information Technology security Evaluation”的缩写，《信息技术安全性通用评估标准》，在美国和欧洲等推出的测评准则上发展起来的。



CC标准的演进历程

CC文档结构

- CC标准提倡安全工程的思想，通过信息安全产品的开发、评价、使用全过程的各个环节的综合考虑来确保产品的安全性。

- 第1部分“简介和一般模型”，介绍CC中的有关术语、基本概念和一般模型以及与评估有关的一些框架，附录部分主要介绍“保护轮廓”和“安全目标”的基本内容；

- 第2部分“安全功能要求”，这部分以“类、子类、组件”的方式提出安全功能要求，对每一个“类”的具体描述除正文之外，在提示性附录中还有进一步的解释；

- 第3部分“安全保证要求”，定义了评估保证级别，介绍了“保护轮廓”和“安全目标”的评估，并同样以“类、子类、组件”的方式提出安全保证要求。

CC标准的内容

- CC标准的内容主要包括：
  - 安全需求的定义；
  - 需求定义的用法；
  - 安全可信度级别；
  - 安全产品的开发和产品安全性评价等几个方面。

- 安全需求的定义
  - CC标准对安全需求的表示形式给出了一套定义方法，并将安全需求分成产品安全功能方面的需求和安全保证措施方面的需求两个独立的范畴来定义。
  - 安全功能需求主要用于描述产品应该提供的安全功能。
  - 安全保证需求，即安全保证措施方面的需求，主要用于描述产品的安全可信度以及为获取一定的可信度应该采取的措施。

安全需求的定义

- 在CC标准中，安全需求以类、族、组件的形式进行定义，给出了对安全需求进行分组归类的方法。对全部安全需求进行分析，根据不同的侧重点，划分成若干大组，每个大组就称为一个类。

安全功能需求类（共11项）	安全保证需求类（共7项）
安全审计类	构造管理类
通信类	发行与使用类
加密支持类	开发类
用户数据保护类	指南文档类
身份识别与认证类	生命周期支持类
安全管理类	测试类
隐私类	脆弱性评估类
安全功能件保护类	
资源使用类	
安全产品访问类	
可信路径/通道类。	

需求定义的用法

- 安全需求定义中的“类、族、组件”体现的是分类方法，安全需求由组件体现，选择需求组件等同选择安全需求。

- CC标准定义了三种类型的组织结构用于描述产品安全需求，分别是安全组件包、保护轮廓定义和安全对象定义。
  - 安全组件包是把多个安全需求组件组合在一起所得到的组件集合。
  - 保护轮廓定义是一份安全需求说明书，是针对某一类安全环境确立相应的安全目标，进而定义为实现这些安全目标所需要的安全需求，保护轮廓定义的主要内容包括定义简述、产品说明、安全环境、安全目标、安全需求、应用注释和理论依据等。
  - 安全对象定义是一份安全需求与概要设计说明书，不同的是安全对象定义的安全需求是为某一特定的安全产品而定义的，具体的安全需求可通过引用一个或多个保护轮廓定义来定义，也可从头定义。安全对象定义的组成部分主要包括定义简述、产品说明、安全环境、安全目标、安全需求、产品概要说明、保护轮廓定义的引用声明和理论依据等。

安全可信度级别

级别	定义	可信度级别描述
EALl	职能式测试级	表示信息保护问题得到了适当的处理；
EAL2	结构式测试级	表示评价时需要得到开发人员的配合，该级提供低中级的独立安全保证；
EAL3	基于方法学的测试与检查级	要求在设计阶段实施积极的安全工程思想，提供中级的独立安全保证。
EAL4	基于方法学的设计、测试与审查级	要求按照商业化开发惯例实施安全工程思想，提供中高级的独立安全保证。
EAL5	半形式化的设计与测试级	要求按照严格的商业化开发惯例，应用专业安全工程技术及思想，提供高等级的独立安全保证。
EAL6	半形式化验证的设计与测试级	通过在严格的开发环境中应用安全工程技术来获取高的安全保证，使产品能在高度危险的环境中使用。
EAL7	形式化验证的设计与测试级	目标是使产品能在极端危险的环境中使用。目前只限于可进行形式化分析的安全产品。

安全产品的开发

- CC标准体现了软件工程与安全工程相结合思想。
- 信息安全产品必须按照软件工程和安全工程的方法进行开发才能较好地获得预期的安全可信度。
- 安全产品从需求分析到产品的最终实现，整个开发过程可依次分为应用环境分析、明确产品安全环境、确立安全目标、形成产品安全需求、安全产品概要设计、安全产品实现等几个阶段。
- 各个阶段顺序进行，前一个阶段的工作结果是后一个阶段的工作基础。有时前面阶段的工作也需要根据后面阶段工作的反馈内容进行完善拓展，形成循环往复的过程。
- 开发出来的产品经过安全性评价和可用性鉴定后，再投入实际使用。

产品安全性评价

- CC标准在评价安全产品时，把待评价的安全产品及其相关指南文档资料作为评价对象。

- CC定义了三种评价类型，分别为安全功能需求评价、安全保证需求评价和安全产品评价。
  - 第一项评价的目的是证明安全功能需求是完全的、一致的和技术良好的，能用作可评价的安全产品的需求表示；
  - 第二项评价的目的是证明安全保证需求是完全的、一致的和技术良好的，可作为相应安全产品评价的基础。如果安全保证需求中含有安全功能需求一致性的声明，还要证明安全保证需求能完全满足安全功能需求。
  - 最后一项安全产品评价的目的是要证明被评价的安全产品能够满足安全保证的安全需求。

主要内容

- 10.1 概述
- 10.2 信息安全风险管理
- 10.3 信息安全标准
  - 10.3.1 信息安全标准概述
  - 10.3.2 信息技术安全性评估通用准则（CC）
  - 10.3.3 信息安全管理体系标准
  - 10.3.4 中国的有关信息安全标准
- 10.4 信息安全法律法规及道德规范

信息安全管理体系标准BS7799

- BS7799是英国标准协会（British Standards Institute，BSI）针对信息安全管理而制定的一个标准，共分为两个部分。
  - 第一部分BS7799-1是《信息安全管理实施细则》，也就是国际标准化组织的ISO/IEC 17799标准的部分，主要提供给负责信息安全系统开发的人员参考使用，其中分11个标题，定义了133项安全控制（最佳惯例）。
  - 第二部分BS7799-2是《信息安全管理体系规范》（即ISO/IEC 27001），其中详细说明了建立、实施和维护信息安全管理体系的要求，可用来指导相关人员去应用ISO/IEC 17799，其最终目的是建立适合企业所需的信息安全管理体系。

信息安全管理实施细则-11个方面定义

- 在BS 7799-1《信息安全管理实施细则》中，从11个方面定义了133项控制措施。

- 这11个方面分别是：

1. 安全策略
2. 组织信息安全
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

建立信息安全管理体系六个基本步骤

- 步骤一、定义信息安全策略 信息安全策略是组织信息安全的最高方针，需要根据组织内各个部门的实际情况，分别制订不同的信息安全策略。
- 步骤二、定义ISMS的范围 ISMS的范围描述了需要进行信息安全管理的领域轮廓，组织根据自己的实际情况，在整个范围或个别部门构架ISMS。
- 步骤三、进行信息安全风险评估 信息安全风险评估的复杂程度将取决于风险的复杂程度和受保护资产的敏感程度，所采用的评估措施应该与组织对信息资产风险的保护需求相一致。
- 步骤四、信息安全风险管理 根据风险评估的结果进行相应的风险管理。
- 步骤五、确定控制目标和选择控制措施 控制目标的确定和控制措施的选择原则是费用不超过风险所造成的损失。
- 步骤六、准备信息安全适用性声明 信息安全适用性声明纪录了组织内相关的风险控制目标和针对每种风险所采取的各种控制措施。

主要内容

- 10.1 概述
- 10.2 信息安全风险管理
- 10.3 信息安全标准
  - 10.3.1 信息安全标准概述
  - 10.3.2 信息技术安全性评估通用准则（CC）
  - 10.3.3 信息安全管理体系标准
  - 10.3.4 中国的有关信息安全标准
- 10.4 信息安全法律法规及道德规范

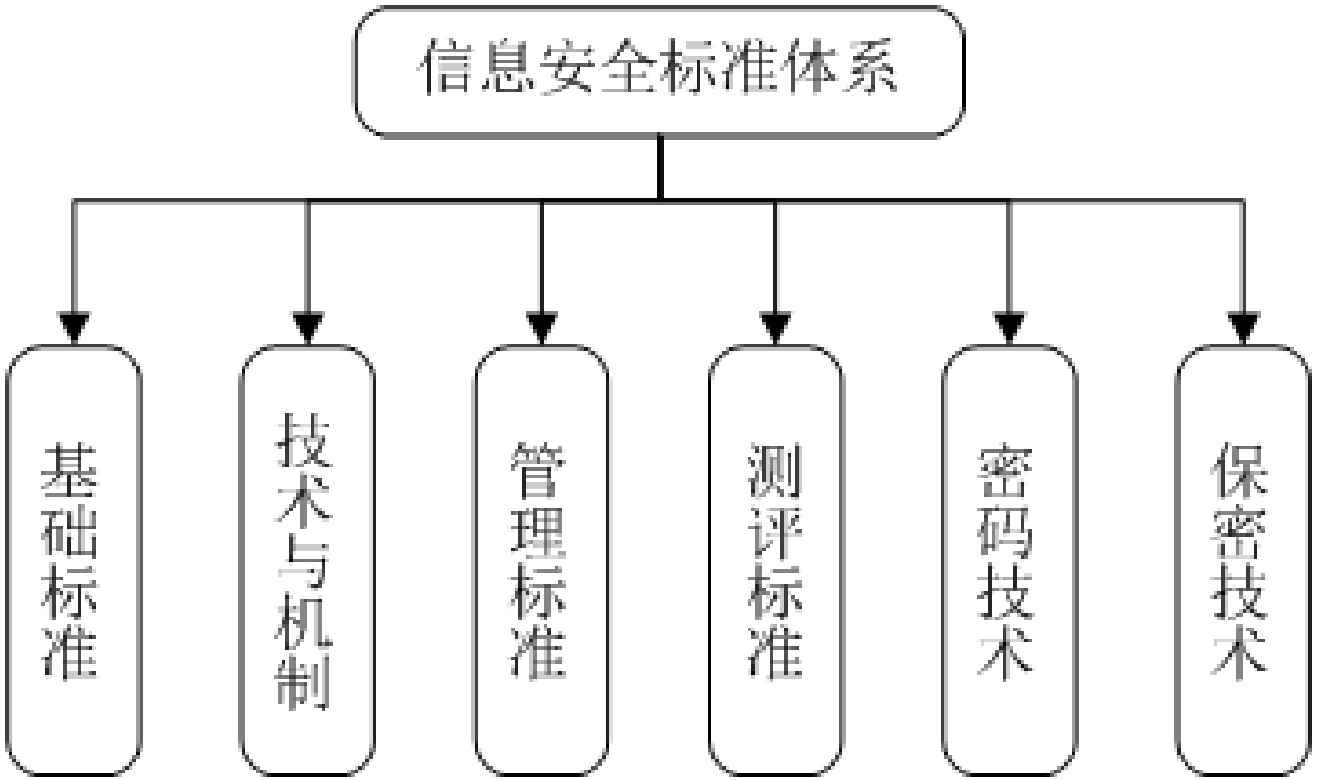
中国的有关信息安全标准

- 1985年，发布了第一个标准GB4943“信息技术设备的安全”，并于1994年发布了第一批信息安全技术标准。

- 截止2008年11月，国家共发布有关信息安全技术、产品、测评和管理的国家标准69项（不包括密码与保密标准）。

- 同时，公安部、国家保密局、国家密码管理委员会等相继制定、颁布了一批信息安全的行业标准，为推动信息安全技术在各行业的应用和普及发挥了积极的作用。

国家信息安全标准体系



国家信息安全标准体系

- 基础标准主要定义或描述信息安全领域的安全术语、体系结构、模型、框架等内容。
- 技术与机制标准主要包括标识与鉴别、授权与访问控制、实体管理、物理安全等内容。
- 管理标准主要包括管理基础、管理要素、管理支撑技术、工程与服务等内容。
- 测评标准主要分为基础标准、产品标准、系统标准三部分，每一部分均针对其对象提出了安全级别标准及相应的测试方法。

国家信息安全标准体系

- 密码技术标准主要包括基础标准、技术标准和管理标准三部分。
  - 基础标准描述了密码术语、密码算法配用和秘钥配用；
  - 技术标准涉及密码协议、密码管理、密码检测评估、密码算法、密码芯片、密码产品、密码管理应用接口以及密码应用服务系统等内容；
  - 管理标准涉及密码产品的开发、生产及使用等内容。

- 保密技术标准主要分为技术标准和管理标准两部分。
  - 技术标准包括电磁泄露发射防护与检测、涉密信息系统技术要求和测评、保密产品技术要求和测评、涉密信息消除和介质销毁以及其他技术标准等内容；
  - 管理标准包括电子文件管理、涉密信息管理和实验室要求三部分内容。

GB17895-1999 计算机信息系统安全保护等级划分准则

- 在我国众多的信息安全标准中，公安部主持制定、国家质量技术监督局发布的中华人民共和国国家标准GB17895-1999《计算机信息系统安全保护等级划分准则》被认为我国信息安全标准的奠基石。

- 该准则将信息系统安全分为5个等级：自主保护级、系统审计保护级、安全标记保护级、结构化保护级和访问验证保护级。

五个安全等级

- 第一级，用户自主保护级：本级的计算机信息系统可信计算基通过隔离用户与数据，使用户具备自主安全保护的能力。它具有多种形式的控制能力，对用户实施访问控制，即为用户提供可行的手段，保护用户和用户组信息，避免其他用户对数据的非法读写与破坏。
- 第二级，系统审计保护级：与用户自主保护级相比，本级的计算机信息系统可信计算基实施了粒度更细的自主访问控制，它通过登录规程、审计安全性相关事件和隔离资源，使用户对自己的行为负责。
- 第三级，安全标记保护级：本级的计算机信息系统可信计算基具有系统审计保护级所有功能。此外，还提供有关安全策略模型、数据标记以及主体对客体强制访问控制的非形式化描述，具有准确地标记输出信息的能力，消除通过测试发现的任何错误。

五个安全等级

- 第四级，结构化保护级：本级的计算机信息系统可信计算基建立于一个明确定义的形式化安全策略模型之上，它要求将第三级系统中的自主和强制访问控制扩展到所有主体与客体。此外，还要考虑隐蔽通道。
- 第五级，访问验证保护级：本级的计算机信息系统可信计算基满足访问监控器需求。访问监控器仲裁主体对客体的全部访问。

主要内容

- 10.1 概述
- 10.2 信息安全风险管理
- 10.3 信息安全标准
- 10.4 信息安全法律法规及道德规范
  - 10.4.1 信息犯罪
  - 10.4.2 信息安全道德规范
  - 10.4.3 信息安全法律规范

信息犯罪

- 信息资源是当今社会的重要资产，围绕信息资源的犯罪已成为影响社会安定的重要因素。
- 信息犯罪是以信息技术为犯罪手段，故意实施的有社会危害性的，依据法律规定，应当予以刑罚处罚的行为。
- 目前多数的信息犯罪均属于计算机及网络犯罪。
- 公安部给出的定义：“所谓计算机犯罪，就是在信息活动领域中，以计算机信息系统或计算机信息知识作为手段，或者针对计算机信息系统，对国家、团体或个人造成危害，依据法律规定，应当予以刑罚处罚的行为”。
- 学界认为，“网络犯罪就是行为主体以计算机或计算机网络为犯罪工具或攻击对象，故意实施的危害计算机网络安全的，触犯有关法律规范的行为。”

信息犯罪分类

- 信息犯罪一般可以分为两类：一类是以信息资源为侵害对象，另一类是以非信息资源的主体为侵害对象。
- 以信息资源为犯罪对象的犯罪常见的有：
  - 信息破坏：犯罪主体出于某种动机，利用非法手段进入未授权的系统或对他人的信息资源进行非法控制，具体行为表现为故意利用损坏、删除、修改、增加、干扰等手段，对信息系统内部的硬件、软件以及传输的信息进行破坏，从而导致网络信息丢失、篡改、更换等，严重的可引起系统或网络的瘫痪。
  - 信息窃取：此类犯罪是指未经信息所有者同意，擅自秘密窃取或非法使用其信息的犯罪行为。
  - 信息滥用：这类犯罪是指由使用者违规操作，在信息系统中输入或者传播非法数据信息，毁灭、篡改、取代、涂改数据库中储存的信息，给他人造成损害的犯罪行为。

信息犯罪危害性

- 妨害国家安全和社会稳定的信息犯罪：犯罪主体利用网络信息造谣、诽谤或者发表、传播有害信息，煽动颠覆国家政权、推翻社会制度、分裂国家及破坏国家统一等。
- 妨害社会秩序和市场秩序的信息犯罪：犯罪主体利用信息网络从事虚假宣传、非法经营及其它非法活动，对社会秩序和正规的市场秩序造成恶劣影响。例如，一些犯罪分子利用网上购物的无纸化和实物不可见的特点，发布虚假商品出售信息，在骗取购物者钱财之后便销声匿迹，致使许多消费者上当受骗。此种行为严重破坏了市场经济秩序和社会秩序。
- 妨害他人人身、财产权利的信息犯罪：犯罪主体利用信息网络侮辱诽谤他人或者骗取他人财产（包含信息财产）。例如，通过信息网络，以窃取及公布他人隐私、编造各种丑闻以及窃取他人信用卡信息等方法为手段，以达到损害他人的隐私权、名誉权和骗取他人财产的目的。

信息犯罪的显著特点

- 智能化：以计算机及网络犯罪为例，犯罪者大多是掌握计算机和网络技术的专业人才。
- 多样性：信息技术手段的多样性，必然造就信息犯罪行为的多样性。
- 隐蔽性强：犯罪分子可能只需要向计算机输入错误指令或简单篡改软件程序，作案时间短，甚至可以设计犯罪程序在一段时间后才运行发作，致使一般人很难觉察到。
- 侦查取证困难：以计算机犯罪为例，实施犯罪一般为异地作案，而且所有证据均为电子数据，犯罪分子可能在实施犯罪后，直接毁灭电子犯罪现场，致使侦查工作和罪证采集相当困难。
- 犯罪后果严重：信息安全专家普遍认为，信息犯罪危害性的大小，取决于信息资源的社会作用。作用越大，信息犯罪的后果越严重。

主要内容

- 10.1 概述
- 10.2 信息安全风险管理
- 10.3 信息安全标准
- 10.4 信息安全法律法规及道德规范
  - 10.4.1 信息犯罪
  - 10.4.2 信息安全道德规范
  - 10.4.3 信息安全法律规范

信息安全道德规范

- 信息安全道德规范应该基于三个原则，即整体原则、兼容原则和互惠原则。
  - 整体原则是指一切信息活动必须服从于社会、国家等团体的整体利益。个体利益服从整体利益，不得以损害团体整体利益为代价谋取个人利益。
  - 兼容原则是指社会的各主体间的信息活动方式应符合某种公认的规范和标准，个人的具体行为应该被他人及整个社会所接受，最终实现信息活动的规范化和信息交流的无障碍化。
  - 互惠原则是指任何一个使用者必须认识到，每个个体均是信息资源使用者和享受者，也是信息资源的生产者和提供者，在拥有享用信息资源的权利同时，也应承担信息社会对其成员所要求的责任。信息交流是双向的，主体间的关系是交互式的，权利和义务是相辅相成的。

美国Computer Ethics Institute的十条戒律

1. 不应用计算机去伤害别人；
2. 不应干扰别人的计算机工作；
3. 不应窥探别人的文件；
4. 不应用计算机进行偷窃；
5. 不应用计算机作伪证；
6. 不应使用或拷贝你没有付钱的软件；
7. 不应未经许可而使用别人的计算机资源；
8. 不应盗用别人智力成果；
9. 应该考虑你所编的程序的社会后果；
10. 应该以深思熟虑和慎重的方式来使用计算机。

ACM提倡的伦理道德和职业规范

- 美国的计算机协会（The Association of Computing Machinery）
  1. 为社会和人类做出贡献；
  2. 避免伤害他人；
  3. 要诚实可靠；
  4. 要公正并且不采取歧视性行为；
  5. 尊重包括版权和专利在内的财产权；
  6. 尊重知识产权；
  7. 尊重他人的隐私；
  8. 保守秘密。

南加利福尼亚大学网络伦理声明

- 南加利福尼亚大学网络伦理声明指出了六种不道德网络行为：
  1. 有意地造成网络交通混乱或擅自闯入网络及其相联的系统；
  2. 商业性地或欺骗性地利用大学计算机资源；
  3. 偷窃资料、设备或智力成果；
  4. 未经许可接近他人的文件；
  5. 在公共用户场合做出引起混乱或造成破坏的行动；
  6. 伪造电子函件信息。

中国互联网协会行业自律规范

- 《中国互联网行业自律公约》2002年
- 《互联网新闻信息服务自律公约》2003年
- 《互联网站禁止传播淫秽、色情等不良信息自律规范》2004年
- 《中国互联网协会互联网公共电子邮件服务规范》2004年
- 《搜索引擎服务商抵制违法和不良信息自律规范》2004年
- 《中国互联网网络版权自律公约》2005年
- 《文明上网自律公约》2006年
- 《抵制恶意软件自律公约》2006年
- 《博客服务自律公约》2007年
- 《中国互联网协会反垃圾短信息自律公约》2008发布
- 《中国互联网协会短信息服务规范（试行）》2008年

《文明上网自律公约》

- **2006年4月19日发布的《文明上网自律公约》：**
  - 自觉遵纪守法，倡导社会公德，促进绿色网络建设；
  - 提倡先进文化，摒弃消极颓废，促进网络文明健康；
  - 提倡自主创新，摒弃盗版剽窃，促进网络应用繁荣；
  - 提倡互相尊重，摒弃造谣诽谤，促进网络和谐共处；
  - 提倡诚实守信，摒弃弄虚作假，促进网络安全可信；
  - 提倡社会关爱，摒弃低俗沉迷，促进少年健康成长；
  - 提倡公平竞争，摒弃尔虞我诈，促进网络百花齐放；
  - 提倡人人受益，消除数字鸿沟，促进信息资源共享。

主要内容

- 10.1 概述
- 10.2 信息安全风险管理
- 10.3 信息安全标准
- 10.4 信息安全法律法规及道德规范
  - 10.4.1 信息犯罪
  - 10.4.2 信息安全道德规范
  - 10.4.3 信息安全法律规范

信息安全法律法规

- 建立完善信息安全法律体系是当今重要课题。
  - 一方面法律法规是震慑和惩罚信息犯罪的重要工具，
  - 另一方面法律法规也是合法实施各项信息安全技术的理论依据。
- 1973 年，瑞典《瑞典国家数据保护法》。
- 美国的《信息自由法》、《计算机欺诈和滥用法》、《计算机安全法》、《国家信息基础设施保护法》、《通信净化法》、《个人隐私法》、《儿童网上保护法》、《爱国者法案》、《联邦信息安全管理法案》、《关键基础设施标识、优先级和保护》以及《涉密国家安全信息》等法律法规。
- 德国的《信息和通讯服务规范法》、法国的《互联网络宪章》、英国的《三R互联网络安全规则》、俄罗斯的《联邦信息、信息化和信息保护法》、日本的《电讯事业法》等，
- 欧洲理事会也出台了《网络犯罪公约》。

我国信息安全法律

- 1994年2月，颁布的《中华人民共和国计算机信息系统安全保护条例》，赋予公安机关行使对计算机信息系统的安全保护工作的监督管理职权。
- 1995年2月，颁布的《中华人民共和国人民警察法》，明确了公安机关具有监督管理计算机信息系统安全的职责。
- 我国有关信息安全的立法原则是重点保护、预防为主、责任明确、严格管理和促进社会发展。
- 我国的信息安全法律法规可分为四类：
  - 通用性法律法规
  - 惩戒信息犯罪的法律
  - 针对信息网络安全的特别规定
  - 规范信息安全技术及管理方面的规定

通用性法律法规

- 如宪法、国家安全法、国家秘密法等，这些法律没有针对信息安全的规定，但约束的对象包括危害信息安全行为。
- 例如：
  - 中华人民共和国宪法的第四十条规定“中华人民共和国公民的通信自由和通信秘密受法律的保护。除因国家安全或者追查刑事犯罪的需要，由公安机关或者检察机关依照法律规定的程序对通信进行检查外，任何组织或者个人不得以任何理由侵犯公民的通信自由和通信秘密。”
  - 中华人民共和国国家安全法的第十条规定“国家安全机关因侦察危害国家安全行为的需要，根据国家有关规定，经过严格的批准手续，可以采取技术侦察措施”。第十一条规定“国家安全机关为维护国家安全的需要，可以查验组织和个人的电子通信工具、器材等设备、设施”；第二十一条规定“任何个人和组织都不得非法持有、使用窃听、窃照等专用间谍器材”。
  - 中华人民共和国保守国家秘密法的第三条规定“一切国家机关、武装力量、政党、社会团体、企业事业单位和公民都有保守国家秘密的义务”。

惩戒信息犯罪的法律

- 这类法律包括《中华人民共和国刑法》、《全国人大常委会关于维护互联网安全的决定》等。这类法律中的有关法律条文可以作为规范和惩罚网络犯罪的法律规定。

- 中华人民共和国刑法的第二百一十九条规定“有下列侵犯商业秘密行为之一，给商业秘密的权利人造成重大损失的，处三年以下有期徒刑或者拘役，并处或者单处罚金；造成特别严重后果的，处三年以上七年以下有期徒刑，并处罚金”。侵犯商业秘密行为包括：
  - 以盗窃、利诱、胁迫或者其他不正当手段获取权利人的商业秘密的；
  - 披露、使用或者允许他人使用以前项手段获取的权利人的商业秘密的；
  - 违反约定或者违反权利人有关保守商业秘密的要求，披露、使用或者允许他人使用其所掌握的商业秘密的。

针对信息网络安全的特别规定

- 这类法律规定主要有《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》、《中华人民共和国计算机软件保护条例》等。

- 这些法律规定的立法目的是保护信息系统、网络以及软件等信息资源，从法律上明确哪些行为构成违反法律法规，并可能被追究相关民事或刑事责任。

规范信息安全技术及管理方面的规定

- 这类法律主要有《商用密码管理条例》、《计算机信息系统安全专用产品检测和销售许可证管理办法》、《计算机病毒防治管理办法》等。

- 商用密码管理条例的第三条规定“商用密码技术属于国家秘密。国家对商用密码产品的科研、生产、销售和使用实行专控管理。”

- 商用密码管理条例的第七条规定“商用密码产品由国家密码管理机构指定的单位生产。未经指定，任何单位或者个人不得生产商用密码产品。”

信息安全法律法规体系组成

- 我国信息安全法律法规体系主要由六个部分组成：
  1. 法律，例如：《中华人民共和国宪法》。
  2. 行政法规，例如：《中华人民共和国计算机信息系统安全保护条例》。
  3. 部门规章和规范性文件，例如，公安部的《计算机信息系统安全专用产品检测和销售许可证管理办法》。
  4. 地方性法规，例如，《湖南省信息化条例》。
  5. 地方政府规章，例如，《四川省计算机信息系统安全保护管理办法》。
  6. 司法解释，例如，《关于审理扰乱电信市场管理秩序案件具体应用法律若干问题的解释》。

习题

1. 习题2（1）：如何理解信息安全管理的内涵？
2. 习题2（2）：各信息安全风险因素之间的关系是怎样的？
3. 习题2（3）：风险评估的主要任务有哪些？
4. 习题2（4）：实施风险控制主要包括那些步骤？
5. 习题2（5）： CC标准与BS 7799标准有什么区别？