- 信息安全：信息在产生、处理、传输、存储、使用、销毁过程中的安全
- 信息安全包含：系统安全、数据安全、内容安全、行为安全四个层次
- 信息系统的脆弱性主要包括：电磁泄漏、芯片的脆弱性、操作系统的安全漏洞、数据库的安全漏洞、通信协议的安全漏洞、移动存储介质的安全漏洞
- 安全威胁的来源：自然因素、人为因素
- 人为安全威胁的来源：物理攻击、网络攻击、恶意代码、安全管理
- 信息系统安全问题的根源：信息系统的开放性、信息系统的脆弱性、黑客的恶意入侵
- 信息系统安全分为：物理安全、系统软件安全、网络安全、应用软件安全、安全管理
- 信息系统基本安全属性：保密性、完整性、可用性

- 在 ISO7498-2 标准中，安全体系结构框架包含：管理体系、技术体系、组织体系
- 安全体系结构的类型分为：抽象体系、逻辑体系、通用体系、特殊体系。
- 密码算法的安全性依赖于：密钥数量的空间大小、破译密文所花费的计算量
- 安全体系结构框架包含：安全需求、安全策略、安全机制、安全模型
- 数据保密性可以分为：连接保密性、无连接保密性、选择字段保密性、通信业务流保密性
- IPSec 的两种工作模式分别为：传输模式、隧道模式
- 基于实体的安全体系结构中，安全属性包括：标识属性、认证属性、访问控制属性、保密及完整性属性
- 安全模型用于准确描述系统在功能和结构上的安全特性，它反映了一定的安全策略。

- 物理安全主要包括：设备物理安全、环境物理安全、系统物理安全
- 设备安全威胁主要是：设备的被盗与被毁、电磁干扰、电磁泄漏、声光泄露
- 系统安全涉及的技术要求包括：灾难备份与恢复、设备的资源性能状态和设备鉴别、访问控制、边界测量

- 公钥密码体制：明文、密文、公钥、私钥、加密算法、解密算法
- 对付重放攻击的方法有：序列号、时间戳、挑战/应答
- 基于生理特征的身份认证技术中，生理特征必须具有如下特性：普遍性、唯一性、可测量性、稳定性、安全性

- 访问控制是对主体访问客体的能力或权力的限制，它包括：主体、客体、引用监控器、访问控制策略
- 访问控制的二元组描述方法通常包含：访问控制矩阵、访问控制表、访问能力表、授权关系表
- 基于所有权的访问控制分为：自主访问控制、强制访问控制
- 访问控制实现的类别包括：接入访问控制、资源访问控制、网络端口和节点访问控制

- 强制访问控制两种常见模型为：BLP 模型、Biba 模型
- 基于角色的访问控制模型族中包括：RBAC0、RBAC1、RBAC2、RBAC3
- 基于属性的访问控制模型以属性为最小的授权单位，替代基于角色的访问控制模型中以身份标识为依据的授权方式
- 基于属性的模型中主要涉及四类实体属性：主体属性、客体属性、环境属性、权限属性

- 操作系统面临的安全威胁包括：病毒、蠕虫、木马、逻辑炸弹、隐蔽通道、天窗
- 操作系统的安全目标是：对系统的用户身份认证，依据安全策略对用户操作进行访问控制， 阻止用户对系统资源的非法访问， 监督系统运行的安全， 保证系统自身的安全性和完整性
- 操作系统的存储保护中，数据存储单元可以分为：字、字块、页面、段
- 操作系统的硬件安全机制包括：存储保护、运行保护、I/O 保护
- 病毒的特点是：隐蔽性、潜伏性、破坏性、寄生性、传染性
- 安全访问令牌描述的是用户访问的安全信息，安全描述符描述的是系统资源的安全信息
- 安全访问令牌分为：主令牌、模拟令牌
- 在 Windows 系统中，访问控制列表可以分为：自主访问控制列表、系统访问控制列表
- 隐蔽通道分为：隐蔽存储通道、隐蔽定时通道

- 数据库安全是保证数据库信息的机密性、完整性、可用性、可控性、隐私性，防止系统软件及其数据遭到破坏、更改、泄漏
- 数据库的结构分为：外部层、概念层、内部层
- 数据库系统一般分为：数据库、数据库管理系统
- 数据库加密分为：库内加密、库外加密
- 安全审计的分析方法包括：潜在违规分析、基于异常检测的描述、简单攻击试探法、复杂攻击试探法
- 数据库的恢复技术包含：事务故障恢复、系统故障恢复、介质故障恢复

- 入侵是指任何试图破坏或危及信息系统资源的完整性、机密性和可用性的行为
- 入侵检测系统能够检测的入侵行为包括：试图闯入、成功闯入、冒充其他用户、违反安全策略、合法用户的泄露、独占及恶意使用资源
- 审计数据的预处理方法包括：数据集成、数据清理、数据变换、数据简化、数据融合
- 入侵信号的主要分析方法：模式匹配、统计分析、完整性分析

- 一个可信平台必须包括三个可信根：RTM、RTS、RTR
- 平台证明引入了 AIK 对 PCR 值和随机数 N 在 TPM 的控制下的签名，保证了平台配置信息的完整性和新鲜性，从而大大提高了通信的安全性

- TPM 只允许两种操作来修改 PCR 的值：重置操作、扩展操作
- RTM 是平台启动时首先执行的一段程序，它是由 CRTM 控制的计算引擎
- 可信计算的基本功能是：完整性度量存储和报告、平台证明、受保护能力
- TPM 至少应该具备的功能是：对称/非对称加密、安全存储、完整性度量、签名认证
- TCG 可信计算的概念定义了：可鉴别性、完整性、机密性

- 信息系统安全管理的核心是：风险管理
- 信息系统安全管理的五要素分别为：管理的主体、管理的客体、管理目标、管理手段、管理环境
- 信息系统安全管理分为：宏观管理、微观管理
- 信息系统安全的宏观管理属于政府管理范畴，包括：战略方针、各项政策、法律和法规、标准
- 信息系统安全的微观管理属于机构管理范畴，包括：策略、规章、制度、实践
- 信息系统安全管理中的 PDCA 模型分为：计划(p)、实施(D)、检查(C)、处置(A)
- 安全控制措施主要分三种类型：管理控制、技术控制、物理控制
- 信息系统安全管理体系建设过程：信息系统安全管理体系、等级保护、风险评估
- 人员安全管理的原则是：职责分离原则、岗位轮换原则、最小特权原则、强制休假原则、限幅级别
- 信息系统安全管理措施包括：物理安全管理、系统安全管理、运行安全管理、数据安全管理、人员管理、技术文档安全管理
- 信息系统安全等级保护是从与信息系统安全相关的：物理层面、网络层面、系统层面、应用层面、管理层面对信息和信息系统实施分等级保护
- 信息系统安全管理措施中的运行安全管理包括：故障管理、性能管理、变更管理
- 信息系统安全管理措施主要类型有：管理控制、技术控制、物理控制
- 启动 PDCA 循环的启动器是指：提供必需的资源、选择风险管理方法、确定评审方法、文件化实践

- 信息系统安全风险分析涉及：资产、威胁、脆弱性三个基本要素
- 评价资产的三个安全属性是：保密性、完整性、可用性
- 信息系统安全等级保护实施应遵循：自主保护原则、重点保护原则、同步建设原则、动态调整原则
- 信息系统建设的起点和源头是：信息系统安全风险评估
- 威胁的基本属性包括：威胁的主体、影响的对象、动机、途径
- 信息系统基本安全需求包含：基本安全技术需求、基本管理需求
- 基本安全技术需求包含：物理安全、网络安全、系统安全、应用安全、数据安全
- 基本管理要求包括：安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理