注册信息安全专业人员（CISP）

知识体系大纲

版本：2.0

中国信息安全测评中心

目录

前言

信息安全作为我国信息化建设健康发展的重要因素，关系到贯彻落实科学发展观、全面建设小康社会、构建社会主义和谐社会和建设创新型社会等国家战略举措的实施，是国家安全的重要组成部分。在信息系统安全保障工作中，人是最核心、也是最活跃的因素，人员的信息安全意识、知识与技能已经成为保障信息系统安全稳定运行的重要基本要素之一。

注册信息安全专业人员（CISP）是对我国网络基础设施和重要信息系统的信息安全专业人员进行资质评定的重要形式。多年来为落实我国有关政策“加快信息安全人才培养，增强全民信息安全意识”的指导精神，构建信息安全人才体系发挥了巨大作用。

本大纲从我国国情出发，结合我国网络基础设施和重要信息系统安全保障的实际需求，以知识体系的全面性和实用性为原则，明确规定了注册信息安全专业人员应当掌握的知识要点，是 CISP 教材编制，讲师授课，学员学习，以及考试命题的重要依据。

本大纲包含以下章节：

- 第 1 章 注册信息安全专业人员（CISP）知识体系概述
- 第 2 章 知识类：信息安全保障概述
- 第 3 章 知识类：信息安全技术
- 第 4 章 知识类：信息安全管理
- 第 5 章 知识类：信息安全工程
- 第 6 章 知识类：信息安全标准法规

第 1 章 注册信息安全专业人员（CISP）知识体系概述

1.1 CISP 资质认定类别

“注册信息安全专业人员”，英文为 Certified Information Security Professional，简称 **CISP**，系经中国信息安全测评中心认定的国家信息安全专业人员，具备保障信息系统安全的专业资质。根据岗位工作需要，CISP 分为两个基础类别：

- **“注册信息安全工程师”**，英文为 Certified Information Security Engineer，简称 **CISE**。证书持有人员主要从事信息安全技术领域的工作，具有从事信息系统安全集成、安全技术测试、安全加固和安全运维的基本知识和能力；
- **“注册信息安全管理人员”**， 英文为 Certified Information Security Officer，简称 **CISO**。证书持有人员主要从事信息安全管理领域的工作，具有组织信息安全风险评估、信息安全总体规划编制、信息安全策略制度制定和监督落实的基本知识和能力。

“注册信息安全专业人员”在两个基础类别之上还有两个扩展类别：

- **“注册信息安全专业人员-审计师”**，简称 **CISP-AUIT**（原 CISA）。证书持有人主要从事信息安全审计工作，在全面掌握信息安全基本知识技能的基础上，具有较强的信息安全风险评估、安全检查实践能力。
- **“注册信息安全专业人员-灾难恢复工程师”**，简称 **CISP-DRP**。证书持有人主要从事信息系统灾难恢复工作，在全面掌握信息安全基本知识技能的基础上，具有较强的信息系统灾难恢复建设和管理的实践能力。

1.2 大纲范围

本大纲涵盖了 CISE 和 CISO 两种 CISP 基础类别注册人员需要掌握的知识要点。

CISP-AUIT 注册人员需要在本文规定的知识要点基础上，更加深入地掌握有关信息系统审计和风险评估的知识，有关内容将在 CISP-AUIT 专门的知识大纲中进行介绍，而不在本大纲范围内。

CISP-DRP 注册人员需要在本文规定的知识要点基础上，更加深入地掌握有关信息系统灾难恢复工作的知识，有关内容将在 CISP-DRP 专门的知识大纲中进行介绍，而不在本大纲范围内。

1.3 CISP 知识体系框架结构

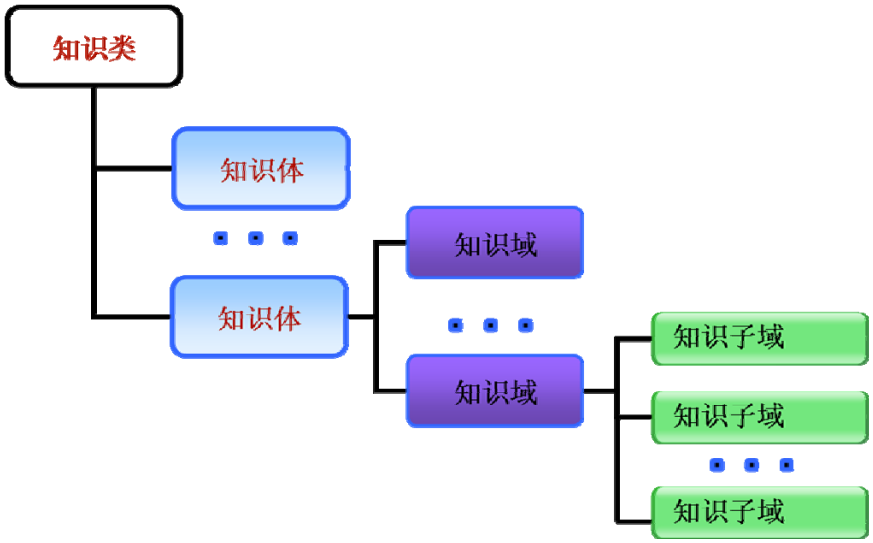
CISP 知识体系使用组件模块化的结构，包括知识类、知识体、知识域和知识子域四个层次。

- **知识类：**是对信息安全保障知识领域的总体划分，包含信息安全专业人员需要掌握的五大知识类别；
- **知识体：**是知识类中由属于同一技术领域的知识内容构成的相对独立、成体系的知识集合；
- **知识域：**是对知识体进一步分解细化形成的完整的知识组件；
- **知识子域：**是构成知识域的基本模块，由一至多个具体知识要点构成。

本大纲规定了知识子域中每一个知识要点的内容和深度要求，分为“了解”、“理解”、和“掌握”三类。

- **了解：**是最低深度要求，学员只需要正确认识该知识要点的基本概念和原理；
- **理解：**是中等深度要求，学员需要在正确认识该知识要点的基本概念和原理的基础上，深入理解其内容，并可以进行进一步的判断和推理；
- **掌握：**是最高深度要求，学员需要正确认识该知识要点的概念、原理，并在深入理解的基础上灵活运用。

图表 1-1描述了CISP知识体系的结构：



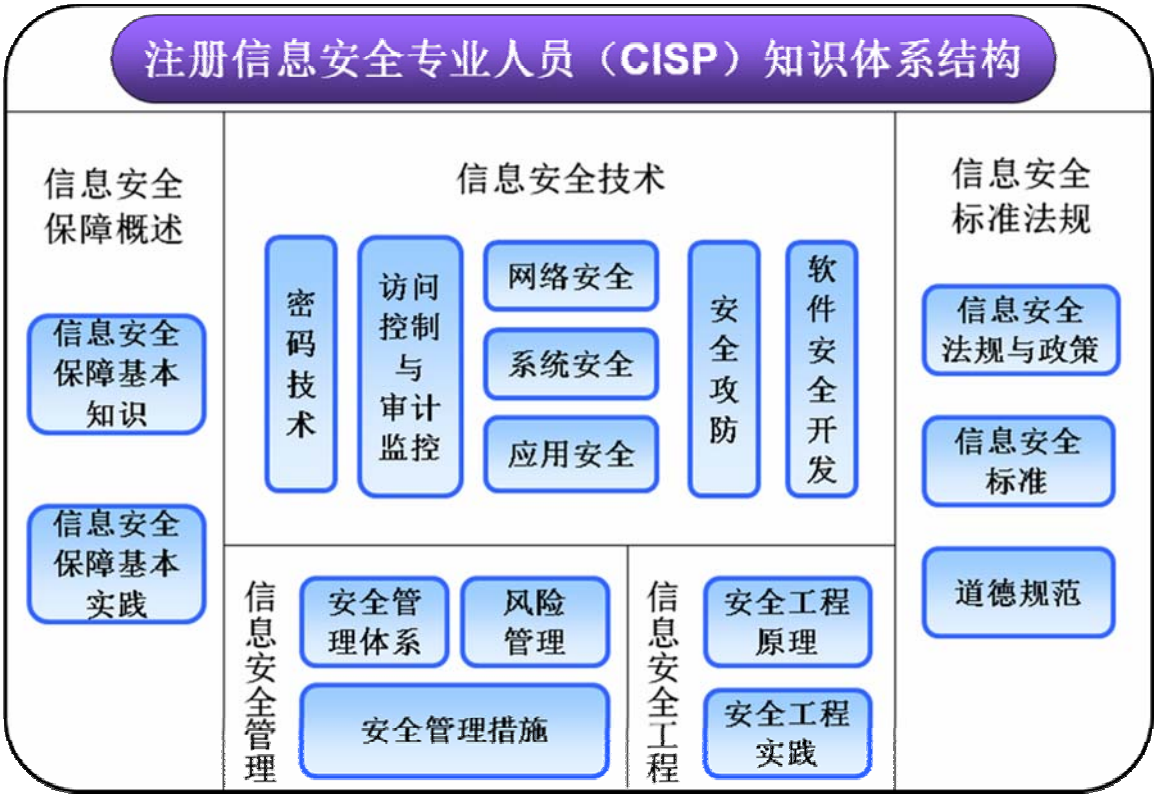
图表 1-1：CISP知识体系的组件模块结构

在整个注册信息安全专业人员（CISP）的知识体系结构中，共包括信息安全保障概述、信息安全技术、信息安全管理、信息安全工程和信息安全标准法规这五个知识类，每个知识类根据其逻辑划分为多个知识体，每个知识体包含多个知识域，每个知识域由一个或多个知识子域组成。

CISP 知识体系结构共包含五个知识类，分别为：

- **信息安全保障概述**：介绍了信息安全保障的框架、基本原理和实践，它是注册信息安全专业人员首先需要掌握的基础知识。
- **信息安全技术**：主要包括密码技术、访问控制、审计监控等安全技术机制，网络、系统软件和应用等层次的基本安全原理和实践，以及信息安全攻防和软件安全开发相关的技术知识和实践。
- **信息安全管理**：主要包括信息安全管理体系建设、信息安全风险管理、具体信息安全管理措施等同信息安全相关的管理知识和实践。
- **信息安全工程**：主要包括同信息安全相关的工程知识和实践。
- **信息安全标准法规**：主要包括信息安全相关的标准、法律法规和道德规范，是注册信息安全专业人员需要掌握的通用基础知识。

图表 1-2描述了CISP知识体系结构框架：



图表 1-2：CISP知识体系结构框架

1.4 CISP（CISE/CISO）考试试题结构

CISP 考试题型均为单项选择题，共 100 题，每题 1 分，得到 70 分以上（含 70 分）为通过。

CISP 两种基础类别“注册信息安全工程师”（CISE）和“注册信息安全管理人员”（CISO）的注册人员都需要学习和掌握 CISP 知识体系结构框架中的所有内容。由于两种注册证书持有人的工作岗位和工作领域的不同，考试的侧重点有所区别，因此，所对应的试题比例不同。

表格 1-1中描述了CISE/CISO考试的各知识类的比例。

表格 1-1：CISP（CISE/CISO）试题结构

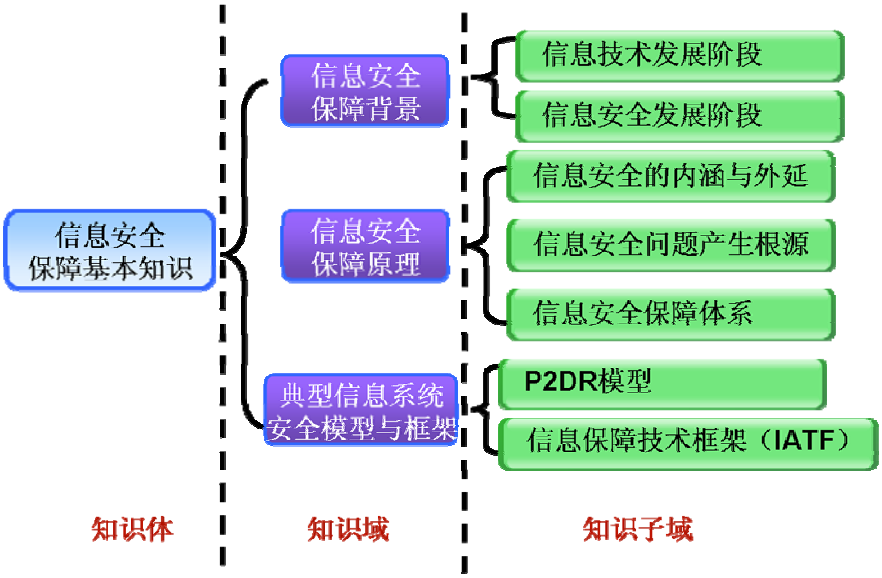
CISP 资质类型 / 知识类别	CISE	CISO
信息安全保障概述	**10%**	**10%**
信息安全技术	**50%**	**30%**
信息安全管理	**20%**	**40%**
信息安全工程	**10%**	**10%**
信息安全标准和法律法规	**10%**	**10%**

第 2 章 知识类：信息安全保障概述

信息安全保障体系概述介绍了信息安全保障的框架、基本原理和实践，它是注册信息安全专业人员首先需要掌握的基础知识。通过本部分的学习，学员应当：

- 理解信息安全保障的意义和内涵；
- 掌握信息安全保障工作的总体思路和基本实践方法。

2.1 知识体：信息安全保障基本知识



图表 2-1：知识体：信息安全保障基本知识

2.1.1 知识域：信息安全保障背景

- 知识子域：信息技术发展阶段
  - 了解电报/电话、计算机、网络等阶段信息技术发展概况
  - 了解信息化和网络对个人、企事业单位和社会团体、经济发展、社会稳定、国家安全等方面的影响；
- 知识子域：信息安全发展阶段
  - 了解通信保密、计算机安全和信息安全保障
  - 了解各个阶段信息安全面临的主要威胁和防护措施

2.1.2 知识域：信息安全保障原理

- 知识子域：信息安全的内涵和外延
  - 理解信息安全的特征与范畴

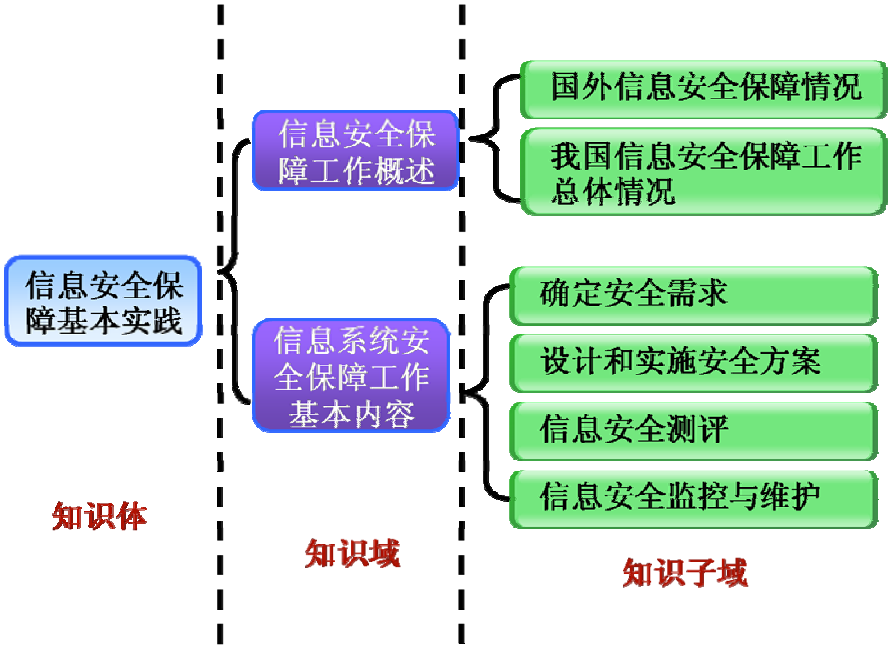
- ◆ 理解信息安全的地位和作用
- ◆ 理解信息安全、信息系统和系统业务使命之间的关系

- 知识子域：信息安全问题产生的根源
  - ◆ 理解信息安全的内因：信息系统的复杂性
  - ◆ 理解信息安全的外因：人为和环境的威胁
- 知识子域：信息安全保障体系
  - ◆ 理解安全保障需要贯穿系统生命周期
  - ◆ 理解保密性、可用性和完整性三个信息安全特征
  - ◆ 理解策略和风险是安全保障的核心问题
  - ◆ 理解技术、管理、工程过程和人员是基本保障要素
  - ◆ 理解业务使命实现是信息安全保障的根本目的

2.1.3 知识域：典型信息系统安全模型与框架

- 知识子域：P2DR 模型
  - ◆ 理解 P2DR 模型的基本原理：策略、防护、检测、响应
  - ◆ 理解 P2DR 数学公式所表达的安全目标
- 知识子域：信息保障技术框架
  - ◆ 理解 IATF 深度防御思想
  - ◆ 理解 IATF 对信息技术系统四个方面的安全需求划分及基本实现方法：本地计算环境、区域边界、网络及基础设施、支撑性基础设施

2.2 知识体：信息安全保障基本实践



图表 2-2：知识体：信息安全保障基本实践

2.2.1 知识域：信息安全保障工作概况

- 知识子域：国外信息安全保障情况
  - 了解发达国家信息安全状况和信息安全保障的主要举措
- 知识子域：我国信息安全保障工作总体情况
  - 了解我国信息安全保障工作发展阶段
  - 理解国家信息安全保障基本原则
  - 了解国家信息安全保障建设主要内容

2.2.2 知识域：信息系统安全保障工作基本内容

- 知识子域：确定安全需求
  - 理解确定信息系统安全保障需求的作用
  - 理解确定信息系统安全保障需求的方法和原则
- 知识子域：设计和实施信息安全方案
  - 理解信息安全方案的作用和主要内容
  - 理解制定信息安全方案的主要原则
  - 理解信息安全方案实施的主要原则
- 知识子域：信息安全测评
  - 了解信息安全测评的重要性

- 了解国内外信息安全测评概况
- 理解信息安全产品测评方法和流程
- 理解信息系统安全测评方法和流程
- 了解服务商资质测评方法和流程
- 了解信息安全人员资质测评方法和流程

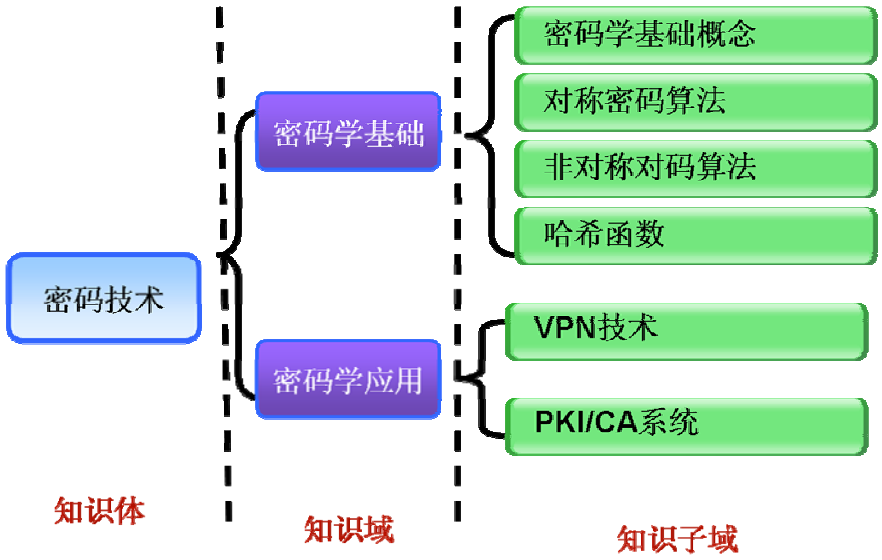
- 知识子域：信息安全监控与维护
  - 理解在系统生命周期中持续提高信息系统安全保障能力的意义
  - 理解信息系统安全监控与维护的主要原则

第 3 章 知识类：信息安全技术

信息安全技术是注册信息安全专业人员需要掌握的主体知识内容之一。通过本部分的学习，学员应当：

- 掌握密码技术、访问控制技术、审计技术等信息安全保障技术的原理和基本实现方法
- 掌握计算机网络、系统软件、应用软件信息安全防护的基本知识和实践技能
- 掌握信息安全攻防的基本知识和实践技能
- 理解软件安全开发的基本方法

3.1 知识体：密码技术



图表 3-1：知识体：密码技术

3.1.1 知识域：密码学基础

- 知识子域：密码学基础概念
  - 理解密码编码学和密码分析学的概念
  - 了解科克霍夫原则和影响密码系统的安全性的基本因素：复杂程度、密钥机密性、密钥长度、初始化向量
  - 了解密码的基本类型：换位（置换）密码、替代（代换）密码、流密码、分组密码的概念

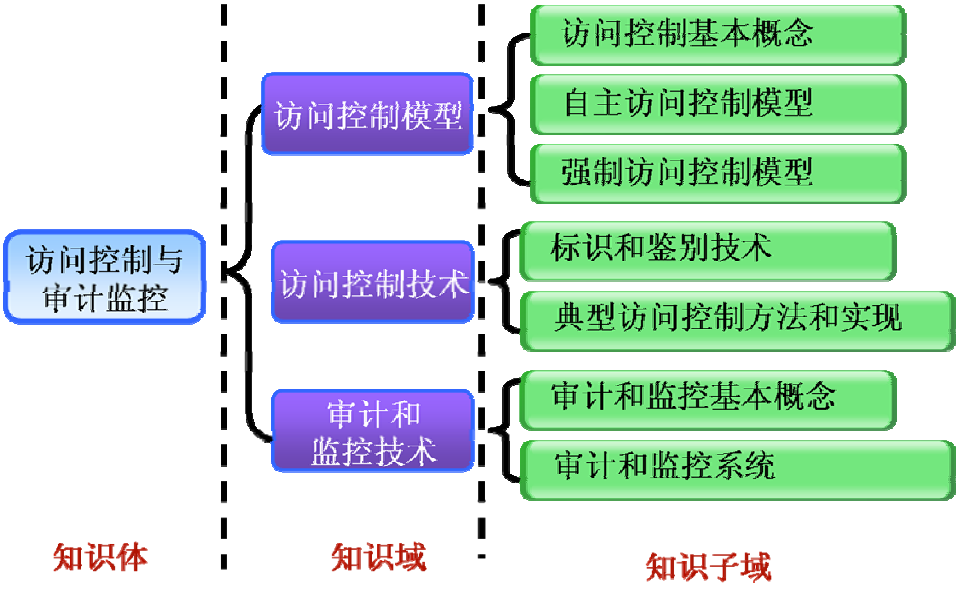
- ◆ 了解密码破解的典型方式：唯密文攻击、已知明文攻击、选择明文攻击、选择密文攻击、旁路攻击、重放攻击、统计式攻击等
- ◆ 掌握密码体制的分类
- ◆ 了解密钥管理的概念，包括密钥管理体制、密钥交换协议和密钥的产生、分配、更换和注销等。

- 知识子域：对称密码算法
  - ◆ 理解对称加密算法的优缺点
  - ◆ 了解 DES、AES、IDEA 三种典型对称加密算法的工作原理
- 知识子域：非对称密码算法
  - ◆ 理解非对称密码算法的功能和优缺点
  - ◆ 理解掌握 RSA 公钥密码体制：RSA 的算法描述、RSA 的实现、RSA 的安全性、RSA 在应用中的问题
  - ◆ 了解其他非对称密码算法的特点：Diffie – Hellman、ELGamal、DSA、ECC 等
- 知识子域：哈希函数
  - ◆ 理解哈希（Hash）函数的作用
  - ◆ 了解 MD5 算法、SHA-1 算法的工作原理
  - ◆ 理解消息鉴别码、数字签名的原理和应用

3.1.2 知识域：密码学应用

- 知识子域：VPN 技术
  - ◆ 理解 VPN 以及隧道技术、加解密技术、密钥管理技术及身份鉴别技术的作用
  - ◆ 掌握 IPSec 的组成和工作原理
  - ◆ 掌握 SSL 的组成和工作原理
- 知识子域：PKI/CA 系统
  - ◆ 理解 PKI/CA 的原理和作用
  - ◆ 掌握 PKI/CA 的体系结构和各部分的作用
  - ◆ 了解 PKI/CA 的典型应用
  - ◆ 掌握 PKI/CA 的工作流程

3.2 知识体：访问控制与审计监控



图表 3-2：知识体：访问控制与审计监控

3.2.1 知识域：访问控制模型

- 知识子域：访问控制基本概念
  - 理解标识、鉴别和授权等访问控制的基本概念
  - 理解各种安全模型的分类
- 知识子域：自主访问控制模型
  - 理解自主访问控制的含义
  - 了解访问矩阵模型，理解和分析应用访问矩阵模型的实现（访问控制列表、权能列表）
  - 理解基于角色的访问控制模型（RBAC）的特点和优势
- 知识子域：强制访问控制模型
  - 理解强制访问控制的分类和含义
  - 掌握典型强制访问控制模型：Bell-Lapudula 模型、Biba 模型、Chinese Wall 模型和 Clark-Wilson 模型
- 知识子域：基于角色访问控制模型
  - 理解基于角色的访问控制模型（RBAC）的特点和优势

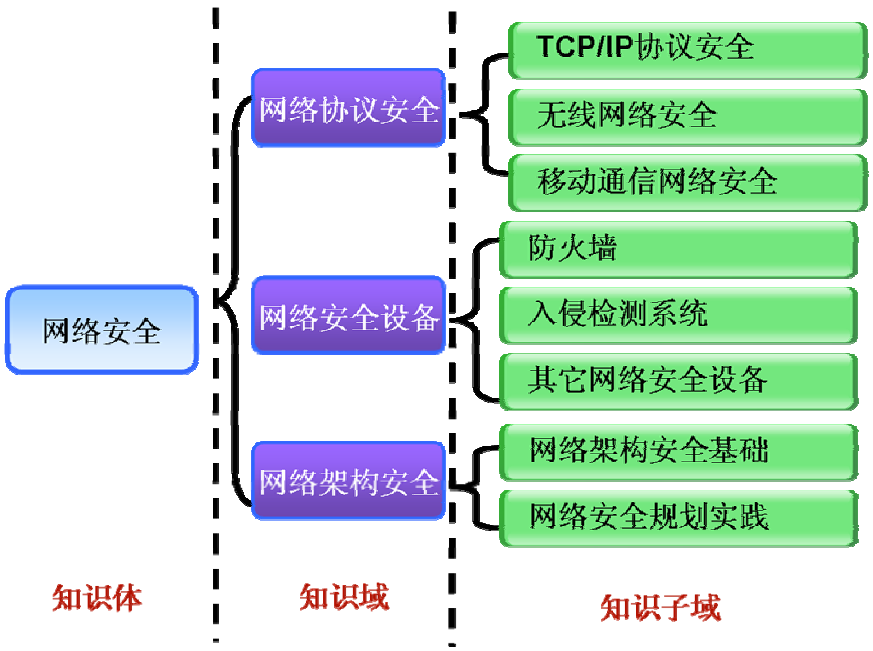
3.2.2 知识域：访问控制技术

- 知识子域：标识和鉴别技术
  - 理解账号和口令管理的基本原则
  - 了解生物识别技术及其实现（虹膜、指纹、掌纹等）
  - 了解其他鉴别技术（令牌、票据等）
  - 了解单点登录技术（SSO）及其实现（Kerberos 等）
- 知识子域：典型访问控制方法和实现
  - 理解集中访问控制的基本概念及其实现（RADIUS、TACACS、TACACS+和 Diameter 等）
  - 理解非集中访问控制的基本概念及其实现（域等）

3.2.3 知识域：审计和监控技术

- 知识子域：信息安全审计
  - 了解安全审计的基本概念
  - 理解安全审计的作用和目标
  - 了解审计系统的组成结构
- 知识子域：安全监控
  - 了解常用安全监控技术
  - 掌握内容审计系统模型以及网络不良信息内容监控方法

3.3 知识体：网络安全



图表 3-3：知识体：网络安全

3.3.1 知识域：网络协议安全

- 知识子域：TCP/IP 协议安全
  - 理解开放互联系统模型 ISO/OSI 七层协议模型
  - 理解 TCP/IP 协议体系结构和工作原理及其安全特性，了解 IPV6 的安全优势
- 知识子域：无线网络安全
  - 理解 802.11 和 WAPI 无线网络协议原理及其安全特性
- 知识子域：移动通信网络安全
  - 了解 3G 网络基本概念及安全特性

3.3.2 知识域：网络安全设备

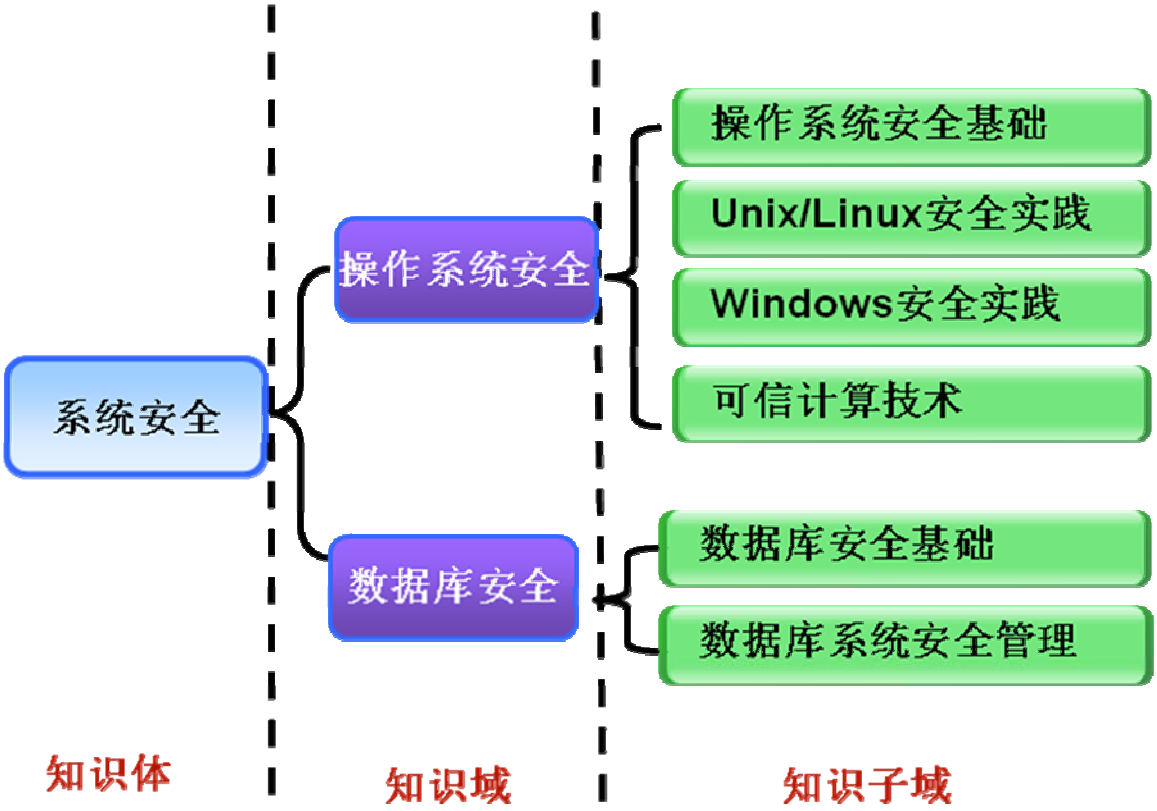
- 知识子域：防火墙技术
  - 理解防火墙的作用
  - 理解包过滤技术、状态检测技术和应用代理技术的原理和优缺点
  - 掌握防火墙选择和使用中的基本注意事项
- 知识子域：入侵检测技术
  - 理解审计和监控的基本概念
  - 理解入侵检测基本概念和工作原理
  - 理解入侵检测的分类
  - 掌握入侵检测系统选择和使用中的基本注意事项
- 知识子域：其它网络安全技术
  - 了解安全隔离与信息交换系统（网闸）、入侵防御系统（IPS）、安全管理平台（SOC）、统一威胁管理系统（UTM）、网络准入控制（NAC）等常见网络安全技术产品的概念和作用

3.3.3 知识域：网络架构安全

- 知识子域：网络架构安全基础
  - 理解网络安全域的含义
  - 理解网络边界防护的含义
  - 理解网络线路冗余的作用
- 知识子域：网络安全规划实践
  - 掌握 IP 地址规划、VLAN 划分的基本安全原则

- 掌握网络设备安全配置（交换机、路由器、无线局域网）的基本原则
- 掌握网络安全设备部署和配置的基本原则

3.4 知识体：系统安全



图表 3-4：知识体：系统安全

3.4.1 知识域：操作系统安全

- 知识子域：操作系统基础
  - 了解操作系统体系架构和基本概念（进程、文件、对象、用户接口、系统调用）；
  - 了解操作系统基本实现机制（CPU 模式与保护环、进程隔离、进程调度）
- 知识子域：Unix/Linux 安全实践
  - 了解 unix/linux 系统架构和关键系统组件；
  - 理解系统服务和系统进程；
  - 理解 unix/linux 系统启动过程

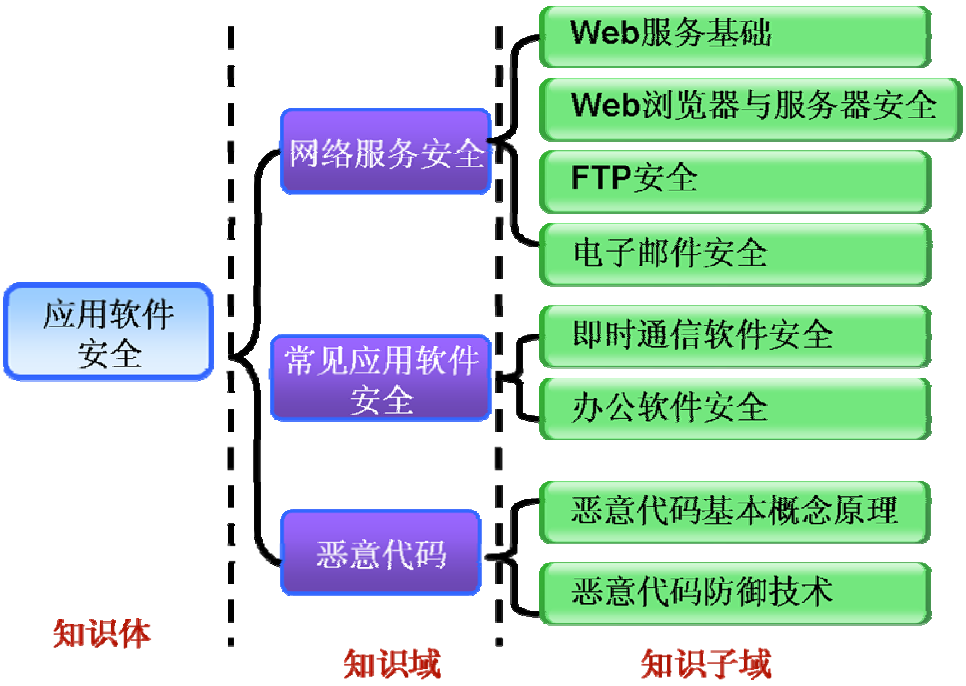
- 理解 unix/Linux 系统安全实现，包括文件系统安全、身份认证与验证授权、账号安全、日志与审计等

- 知识子域：Windows 安全实践
  - 了解 Windows 系统架构和关键系统组件；
  - 理解系统服务和系统进程；
  - 理解 Windows 系统启动过程
  - 理解 Windows 系统安全实现，包括文件系统安全、身份认证与验证授权、账号安全、日志与审计等
- 知识子域：可信计算技术
  - 了解可信计算技术的产生及发展
  - 了解我国可信计算技术，及其与 TCG 可信计算技术的区别

3.4.2 知识域：数据库安全

- 知识子域：数据库安全基础
  - 了解数据库概念
  - 掌握结构化查询语言 SQL
  - 理解数据库安全概念
  - 理解数据库安全功能
  - 理解数据库“视图” 对于数据保密性的作用
  - 理解“规则与默认”和“事务管理”对于数据完整性的作用
- 知识子域：数据库管理系统安全管理
  - 理解数据库威胁与防护
  - 掌握数据库安全特性检查
  - 掌握数据库运行安全监控
  - 了解数据库管理系统产品安全
  - 理解数据库管理系统安全要求

3.5 知识体：应用安全



图表 3-5：知识体：应用软件安全

3.5.1 知识域：网络服务安全

- 知识子域：Web 服务基础
  - 了解 Web 工作机制
  - 了解 Web 站点体系结构，J2EE、SOA 等
- 知识子域： Web 浏览器与服务器安全
  - 了解 HTTP 协议的安全缺陷
  - 理解 Web 服务器常见安全漏洞和防范方法
  - 掌握 IE 浏览器与 Windows IIS 安全设置
- 知识子域：电子邮件安全
  - 了解 SMTP、POP 等典型电子邮件协议的安全问题
  - 理解电子邮件客户端和服务器的常见漏洞和防范方法
- 知识子域：FTP 安全
  - 了解 FTP 协议的安全问题
  - 理解 FTP 的常见安全漏洞和防范方法

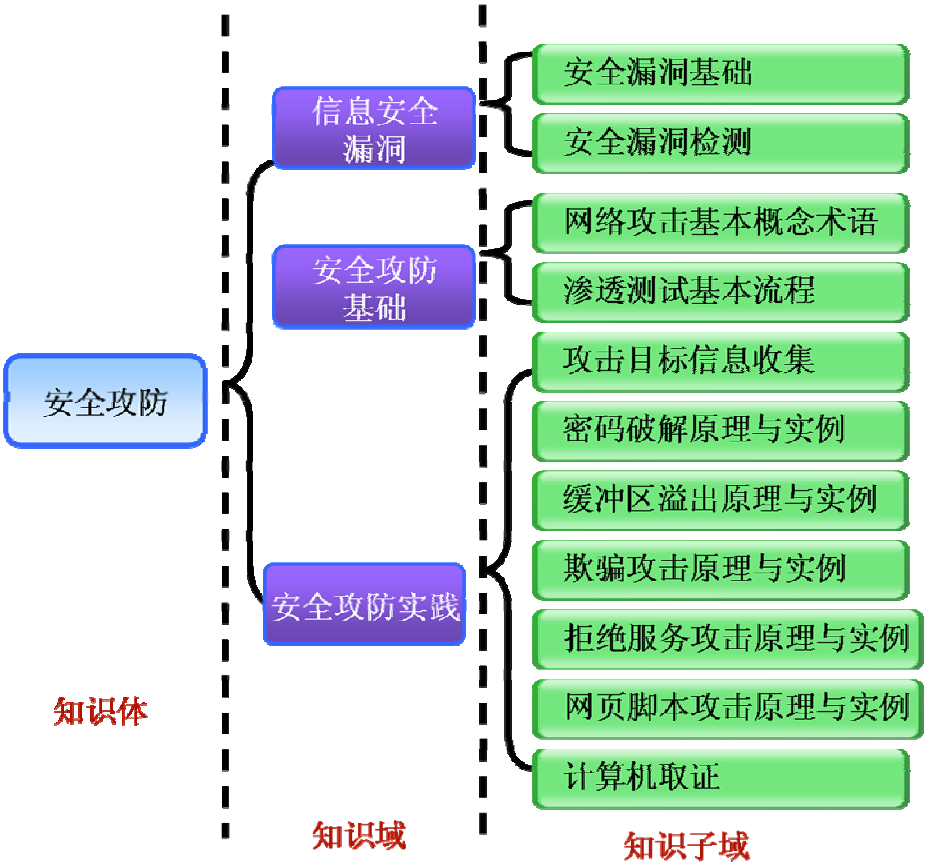
3.5.2 知识域：常见应用软件安全

- 知识子域：即时通信软件安全
  - 了解常用即时通信软件常见安全漏洞和防范方法
- 知识子域：办公软件安全
  - 了解常用办公软件（如 Micosoft Word）安全功能的使用方法

3.5.3 知识域：恶意代码

- 知识子域：恶意代码基本概念原理
  - 了解恶意代码的历史和发展趋势
  - 理解常见恶意代码病毒、蠕虫、木马传播方式和危害的特点
  - 了解恶意代码实现的关键技术（生存技术、隐蔽技术、攻击及植入技术等）
- 知识子域：恶意代码防御技术
  - 掌握恶意代码预防的策略、意识、技术和工具
  - 了解恶意代码发现和分析技术
  - 了解恶意代码清除技术

3.6 知识体：安全攻防



图表 3-6：知识体：安全攻防

3.6.1 知识域：信息安全漏洞

- 知识子域：安全漏洞基础
  - 理解漏洞的概念，分类分级
  - 了解漏洞的危害、产生的原因
  - 了解常用的漏洞库：CNNVD、CVE 等
- 知识子域：安全漏洞检测
  - 了解基于源代码的漏洞检测方法与技术
  - 了解基于二进制代码的漏洞检测方法与技术

3.6.2 知识域：安全攻防基础

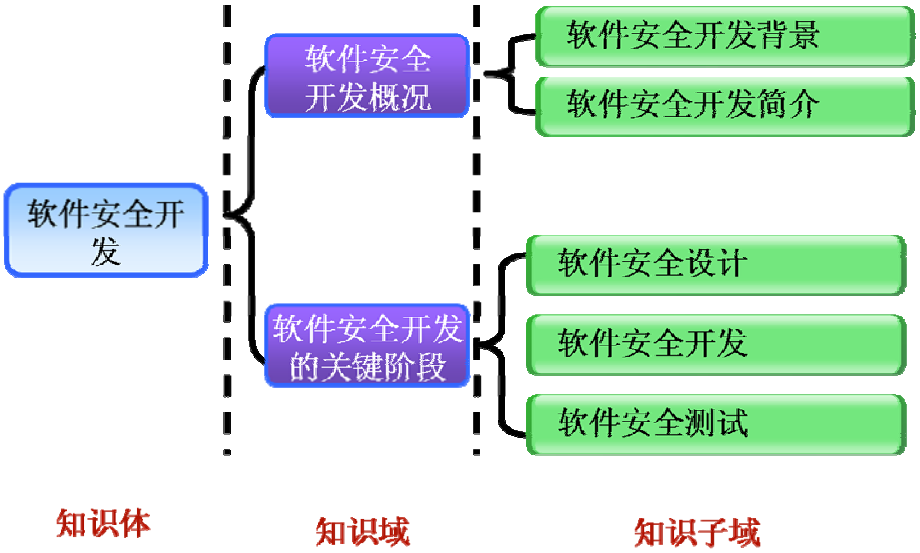
- 知识子域：网络攻击基本概念术语
  - 了解黑客攻击的分类：主动攻击、被动攻击
  - 理解黑客攻击的常用术语：如后门、0-day、提权、社会工程等
- 知识子域：网络攻击基本流程

- ◆ 了解侦查踩点、定位绘制目标、实施攻击、扩大战果、打扫战场等网络攻击的基本步骤
- ◆ 了解以上各个阶段常用的攻击手段和工具

3.6.3 知识域：安全攻防实践

- 知识子域：攻击目标信息收集
  - ◆ 了解目标系统网络地址、软件版本等信息获取方式
  - ◆ 了解网络网络设备、系统软件、应用软件扫描攻击的常用工具
- 知识子域：密码破解原理与实例
  - ◆ 了解暴力破解和字典攻击的常用技术和工具
- 知识子域：缓冲区溢出原理与实例
  - ◆ 理解缓冲区溢出的原理和危害
  - ◆ 了解防范缓冲区溢出的基本方法
- 知识子域：欺骗攻击原理与实例
  - ◆ 理解 IP 欺骗、ARP 欺骗、DNS 欺骗的原理和危害
  - ◆ 了解防范欺骗攻击的基本方法
- 知识子域：拒绝服务攻击原理与实例
  - ◆ 理解 SYN Flood、UDP Flood、Land 攻击、Teardrop 攻击等典型 DOS 攻击的原理和危害
  - ◆ 理解 DDOS 攻击的原理
  - ◆ 了解防范 DOS/DDOS 攻击的基本方法
- 知识子域：网页脚本原理与实例
  - ◆ 理解 SQL 注入攻击的原理和危害
  - ◆ 了解防范 SQL 注入攻击的基本方法
  - ◆ 理解跨站脚本攻击的原理和危害
  - ◆ 了解防范跨站脚本攻击的基本方法
- 知识子域：计算机取证
  - ◆ 了解计算机取证的概念和作用
  - ◆ 了解计算机取证的原则、基本步骤、常用方法和工具

3.7 知识体：软件安全开发



3.7.1 知识域：软件安全开发概况

- 知识子域：软件安全开发背景
  - 了解人们对安全的软件需求
  - 了解当前软件开发方法不足以生成安全的软件
  - 了解软件安全开发的发展历史
- 知识子域：软件安全开发简介
  - 理解软件安全开发七个阶段的主要目的和措施
  - 理解软件安全开发在安全设计和威胁建模中的基本术语

3.7.2 知识域：软件安全开发的关键阶段

- 知识子域：软件安全设计
  - 理解减少攻击面的基本步骤和主要对象
  - 了解常用软件中减少攻击面的保护措施
  - 了解威胁建模的目的
  - 掌握威胁建模的过程
  - 理解威胁建模的关键因素及作用
- 知识子域：软件安全开发
  - 掌握缓冲区溢出、整数错误、跨站脚本、SQL 注入等六种常见软件代码安全漏洞的成因及防范措施
  - 了解常见源代码分析工具的用途
  - 掌握编码时禁止使用的函数

- 了解如何减少潜在可被利用的编码结构和设计
- 理解代码审查的主要内容和过程

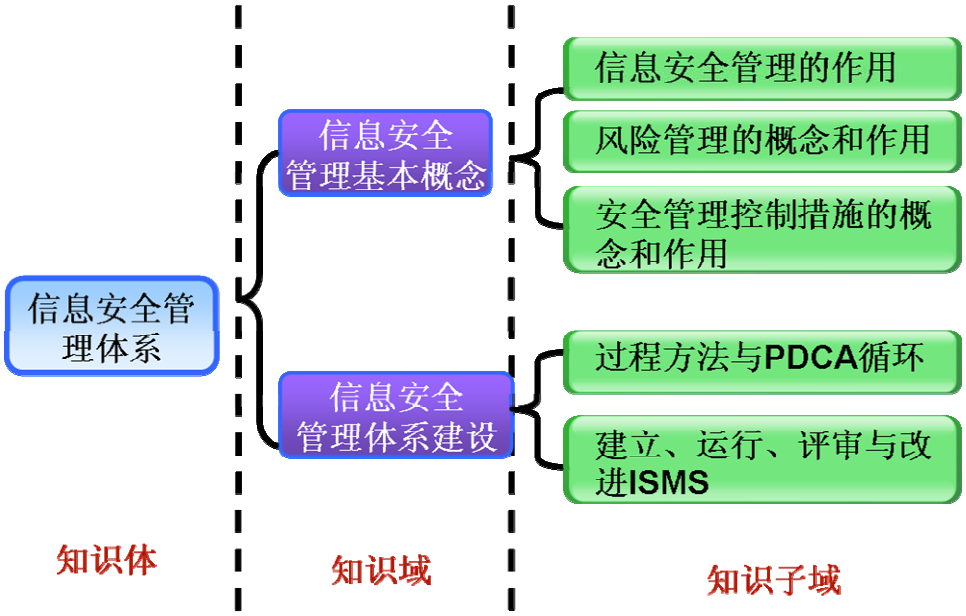
- 知识子域：软件安全测试
  - 了解常用模糊测试的类型
  - 了解常用模糊测试的过程和方法
  - 了解审核并更新威胁模型，以及重新评估软件的受攻击面

第 4 章 知识类：信息安全管理

信息安全管理是注册信息安全专业人员需要掌握的主体知识内容之一。通过本部分的学习，学员应当：

- 理解信息安全管理对于保障信息系统安全的作用
- 理解信息安全管理体系、风险管理和信息安全管理控制措施的含义
- 掌握建立和完善信息安全管理体系的一般方法
- 掌握信息安全风险管理工作的方法和一般原则
- 掌握各个信息安全管理控制措施的作用及最佳实践

4.1 知识体：信息安全管理体系



图表 4-1：知识体：信息安全管理体系

4.1.1 知识域：信息安全管理基本概念

- 知识子域： 信息安全管理的作用
  - 理解信息安全“技管并重”原则的意义
  - 理解成功实施信息安全管理工作的关键因素
- 知识子域： 风险管理的概念和作用
  - 理解信息安全风险的概念：资产价值、威胁、脆弱性、防护措施、影响、可能性
  - 理解风险评估是信息安全管理工作的基础

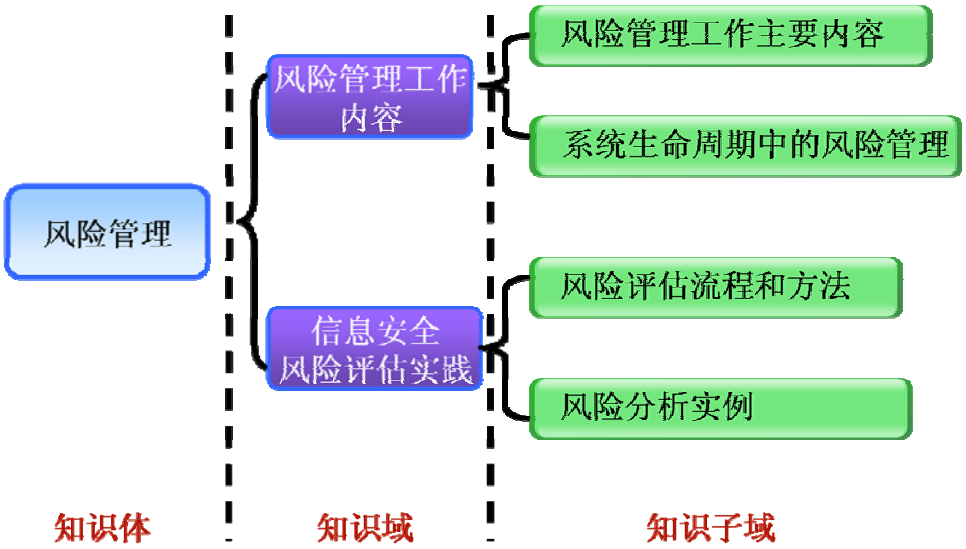
- 理解风险处置是信息安全管理工作的核心

- 知识子域： 信息安全管理控制措施的概念和作用
  - 理解安全管理控制措施是管理风险的具体手段
  - 了解 11 个基本安全管理控制措施的基本内容

4.1.2 知识域：信息安全管理体系建设

- 知识子域：过程方法与 PDCA 循环
  - 理解 ISMS 过程和过程方法的含义
  - 理解 PDCA 循环的特征和作用
- 知识子域：建立、运行、评审与改进 ISMS
  - 了解建立 ISMS 的主要工作内容
  - 了解实施和运行 ISMS 的主要工作内容
  - 了解监视和评审 ISMS 的主要工作内容
  - 了解保持和改进 ISMS 的主要工作内容

4.2 知识体：信息安全风险管理



图表 4-2：知识体：信息安全风险管理

4.2.1 知识域：风险管理工作内容

- 知识子域： 风险管理工作主要内容
  - 掌握建立背景的主要工作内容

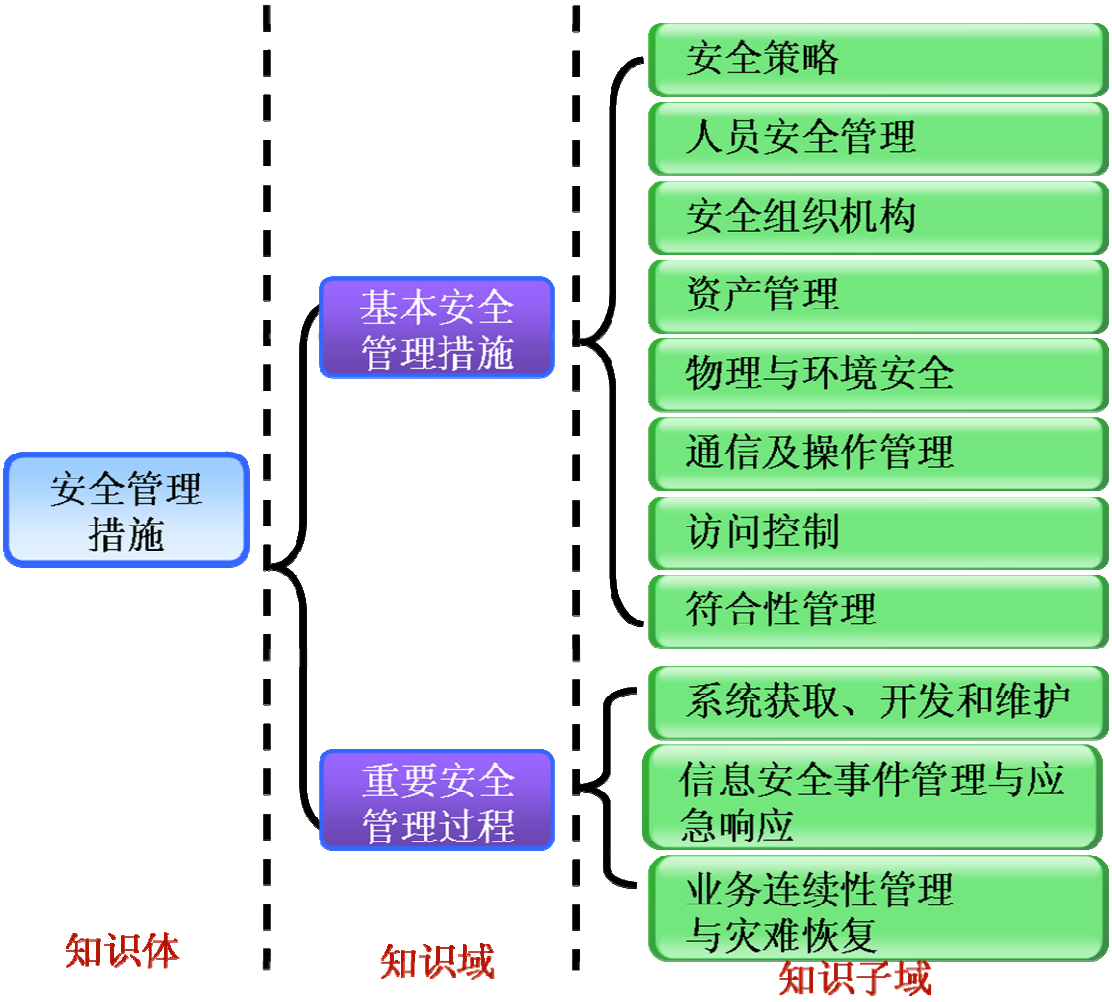
- ◆ 掌握风险评估的主要工作内容
- ◆ 掌握风险处置的主要工作内容
- ◆ 掌握批准监督的主要工作内容
- ◆ 掌握监控审查的主要工作内容
- ◆ 掌握沟通咨询的主要工作内容

- 知识子域： 系统生命周期中的风险管理
  - ◆ 掌握系统规划阶段的风险管理工作
  - ◆ 掌握系统设计阶段的风险管理工作
  - ◆ 掌握系统实施阶段的风险管理工作
  - ◆ 掌握系统运行维护阶段的风险管理工作
  - ◆ 掌握系统废弃阶段的风险管理工作

4.2.2 知识域：信息安全风险评估实践

- 知识子域：风险评估流程和方法
  - ◆ 掌握国家对开展风险评估工作的政策要求
  - ◆ 理解风险评估、检查评估和等级保护测评之间的关系
  - ◆ 掌握风险评估的实施流程：风险评估准备、资产识别、威胁评估、脆弱性评估、已有安全措施确认、风险分析、风险评估文档记录
  - ◆ 理解定量风险分析和定性风险分析的区别及优缺点
  - ◆ 理解自评估和检查评估的区别及优缺点
  - ◆ 掌握典型风险计算方法：年度损失值（ALE）、矩阵法、相乘法
  - ◆ 掌握风险评估工具：风险评估与管理工具、系统基础平台风险评估工具、风险评估辅助工具
- 知识子域：风险分析实例
  - ◆ 了解典型信息系统风险评估实践过程

4.3 知识体：安全管理措施



图表 4-3：知识体：安全管理措施

4.3.1 知识域：基本安全管理措施

- 知识子域：安全策略
  - 理解信息安全策略的定义和作用
  - 掌握编制信息安全策略方法和原则
- 知识子域：人员安全管理
  - 掌握上岗前人员安全控制：审查和角色职责定义
  - 掌握在岗期间人员安全控制：培训和惩戒措施
  - 掌握离职时人员安全控制：终止职责、资产与访问权限归还
- 知识子域：安全组织机构

- ◆ 掌握内部组织建立的原则：高层承诺和支持、职责划分、有效沟通
- ◆ 掌握外部组织建立的原则：控制外来风险、利用外部资源

- 知识子域：资产管理
  - ◆ 掌握资产责任管理的基本方法：资产清单、资产所有权和资产有效使用
  - ◆ 掌握资产分类：系统资产的分类、标识和处置
- 知识子域：物理与环境安全
  - ◆ 了解各种物理安全威胁和物理安全相关的措施的分类（预防性/检测性/恢复性等）
  - ◆ 了解物理设施安全防护措施的部署原则，例如：工作区的划分、围墙/门的选择、机房位置选择、设备废弃与重用、资产转移等；
  - ◆ 了解各种物理访问控制措施的作用，例如：智能卡、生物访问控制等物理访问控制措施等
  - ◆ 了解各种物理监控措施的作用，例如：闭路电视、传感器、报警设备等
  - ◆ 了解物理环境支持性设施的作用，例如：电力、防火、防水、温湿度控制，电缆安全与 TEMPEST 等
  - ◆ 理解人身安全的重要性
- 知识子域：通信及操作安全
  - ◆ 掌握操作程序和职责管理原则：制定操作程序规范，系统变更管理，责任分离，开发、测试与运行设施的分离
  - ◆ 了解操作及通信技术保护措施管理原则：恶意代码防护、数据备份、网络安全管理、介质处理、信息交换、审计日志
- 知识子域：访问控制
  - ◆ 理解访问控制策略制定的方法和原则
  - ◆ 理解系统用户的访问控制职责
  - ◆ 理解网络、操作系统和应用系统访问控制管理的原则
- 知识子域：符合性管理
  - ◆ 理解符合性的含义和作用
  - ◆ 了解审计措施的作用和使用注意事项

4.3.2 知识域：重要安全管理过程

- 知识子域：系统采购、开发与维护
  - ◆ 理解安全要求是信息系统需求的重要组成部分

- 理解信息技术产品的采购的安全原则：符合标准法规，风险与经济性的平衡，安全性测试等
- 理解信息系统开发和实施的安全原则：规范的开发方法，严格的源代码测试，对安装包、测试数据和程序源代码的保护
- 理解系统运行阶段安全管理的基本原则，包括漏洞和补丁管理、系统更新、废弃等

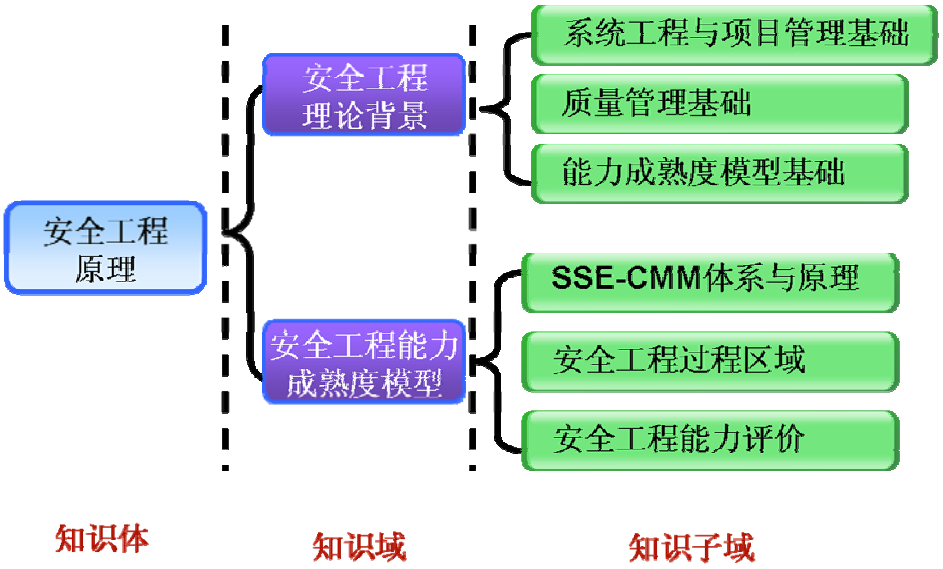
- 知识子域： 信息安全事件管理与应急响应
  - 理解信息安全事件管理和应急响应的本概念
  - 了解我国信息安全事件应急响应工作的进展情况和政策要求
  - 掌握信息安全应急响应阶段方法论
  - 掌握信息安全应急响应计划编制方法
  - 掌握应急响应小组的作用和建立方法
  - 理解我国信息安全事件分级分类方法
  - 了解国际和我国信息安全应急响应组织
- 知识子域：业务连续性管理与灾难恢复
  - 理解业务连续性管理与灾难恢复的基本概念
  - 了解我国灾难恢复工作的进展情况和政策要求
  - 了解数据储存和数据备份与恢复的基本技术
  - 掌握灾难恢复管理过程：需求分析、灾难恢复策略制定、灾难恢复策略实现、灾难恢复预案制定和管理
  - 掌握国家有关标准对灾难恢复系统级别和各级别的指标要求

第 5 章 知识类：信息安全工程

信息安全工程是注册信息安全专业人员需要掌握的主体知识内容之一。通过本部分的学习，学员应当：

- 理解信息安全建设必须同信息化建设“同步规划、同步实施”的原则
- 理解如何运用信息安全能力成熟度模型理论评价和改进信息安全工程能力
- 掌握在信息系统生命周期中的各阶段运用“信息系统安全工程”来保障安全性
- 了解信息安全工程监理的作用和基本工作内容

5.1 知识体：信息安全工程原理



图表 5-1：知识体：信息安全工程理论

5.1.1 知识域：安全工程理论背景

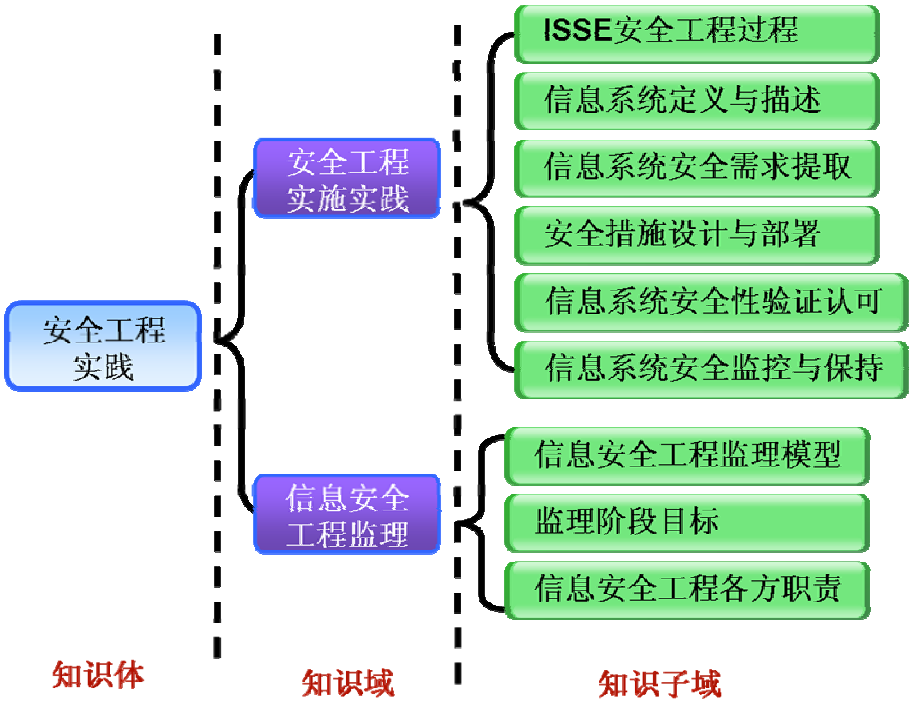
- 知识子域： 系统工程与项目管理基础
  - 了解系统工程基本思想
  - 了解项目管理基本概念和要素
- 知识子域：质量管理基础
  - 了解质量管理基本概念
- 知识子域：能力成熟度模型
  - 理解“工程能力成熟度”基本思想

- 了解能力成熟度模型的应用范围
- 了解“过程能力方案”和“组织机构成熟度方案”的区别

5.1.2 知识域： 安全工程能力成熟度模型

- 知识子域： SSE-CMM 体系与原理
  - 了解 SSE-CMM 的适用范围
  - 了解过程、过程区和过程能力的概念
  - 了解域维/安全过程区与能力维/公共特征的关系
- 知识子域： 安全工程过程区域
  - 了解过程类、过程区和基本实施的关系
  - 理解风险过程、工程过程和保证过程的含义
  - 了解各个安全工程过程区的含义
- 知识子域： 安全工程能力评价
  - 理解能力级别、公共特征和通用实施的关系
  - 理解各个信息安全工程能力级别的含义

5.2 知识体：信息安全工程实践



图表 5-2：知识体：信息安全工程实践

5.2.1 知识域： 安全工程实施实践

- 知识子域： ISSE 安全工程过程
  - 了解系统生命周期的概念和组成阶段：概念与需求定义、系统功能设计、系统开发与获取、系统实现与测试、系统维护与废弃
  - 理解 ISSE 的含义：将系统工程思想应用于信息安全领域，在系统生命周期的各阶段充分考虑和实施安全措施
  - 理解 ISSE 阶段划分及各阶段的主要工作内容
- 知识子域： 信息系统定义与描述
  - 理解信息安全必须与信息系统同步规划
  - 理解信息系统用途、架构等特征对安全风险特征的影响
- 知识子域： 信息系统安全需求提取
  - 理解风险评估结果是安全需求的重要决定因素
  - 理解国家政策法规和合同协议等符合性要求是安全需求的重要决定因素
- 知识子域： 安全措施设计与部署
  - 理解信息安全必须与信息系统同步实施
  - 理解根据安全需求有针对性地设计和部署安全措施的必要性
- 知识子域： 信息系统安全性验证与认可
  - 理解信息安全措施必须与信息系统同步运行
  - 理解风险评估是重要系统验收和投入运行前的必要工作
- 知识子域： 信息系统安全监控与保持
  - 理解信息安全工作需要覆盖系统全生命周期
  - 理解持续的风险评估和风险消控是保障系统安全的必要工作

5.2.2 知识域： 信息安全工程监理

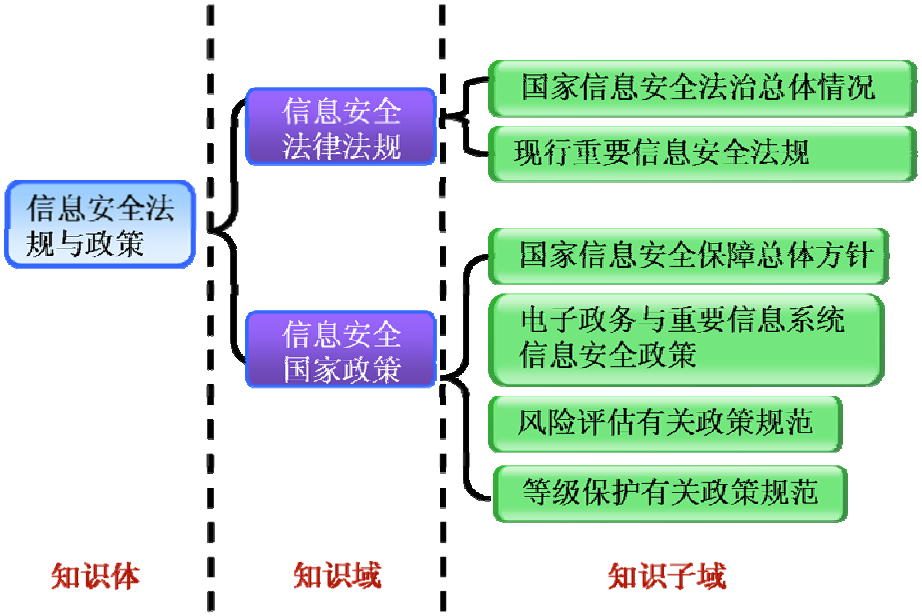
- 知识子域： 信息安全工程监理模型
  - 了解信息安全工程监理工作的意义
  - 了解信息安全工程监理阶段、监理管理和控制手段和监理支撑要素
- 知识子域： 监理阶段目标
  - 了解信息安全工程招标、设计、实施和验收阶段监理方的工作目标
- 知识子域： 信息安全工程各方职责
  - 了解信息安全工程招标、设计、实施和验收阶段业务单位、承建单位和监理单位的职责和工作流程

第 6 章 知识类：信息安全标准法规

信息安全标准法规是注册信息安全专业人员需要掌握的通用基础知识。通过本部分的学习，学员应当：

- 理解遵循信息安全法规、政策、标准和道德规范的重要性
- 掌握我国重点信息安全法规和政策的有关要求
- 掌握重点信息安全技术标准的有关内容
- 了解 CISP 道德规范，了解通行的有关信息安全道德规范

6.1 知识体：信息安全法规与政策



图表 6-1：知识体：信息安全法规与政策

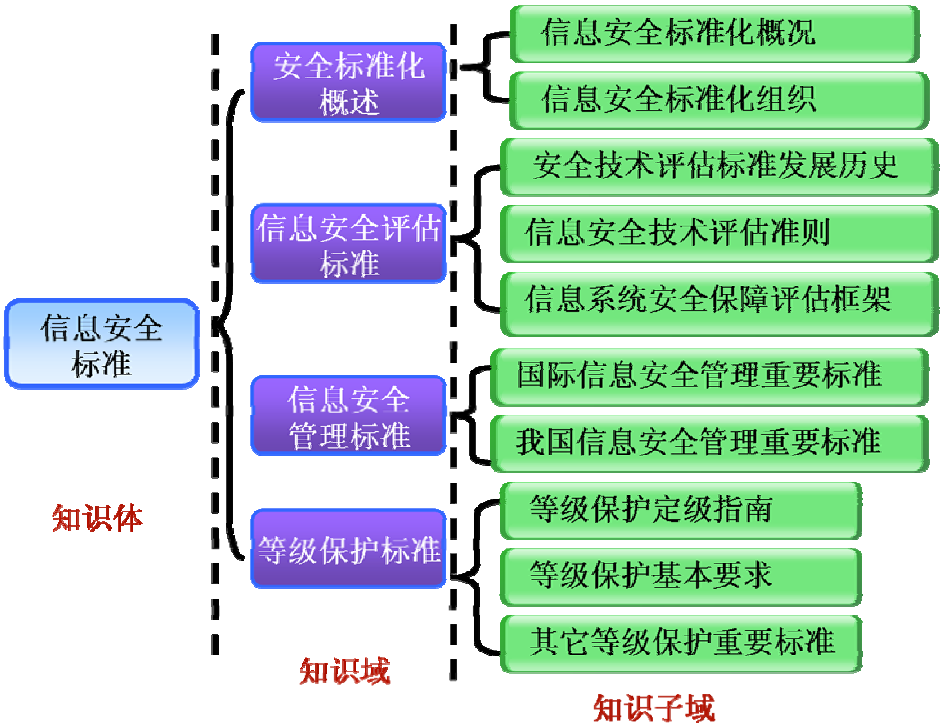
6.1.1 知识域：信息安全相关法律

- 知识子域： 国家信息安全法治总体情况
  - 了解信息安全法治建设的意义
  - 了解我国信息安全法律法规体系框架
- 知识子域： 现行重要信息安全法规
  - 掌握《保守国家秘密法》的主要内容
  - 理解《电子签名法》的意义和作用
  - 了解《刑法》有关信息安全犯罪的规定
  - 了解《全国人大常委会关于维护互联网安全的决定》

6.1.2 知识域：信息安全国家政策

- 知识子域：国家信息安全管理总体方针
  - 掌握国家有关政策对信息安全保障工作的总体要求
  - 掌握国家有关政策规定的加强信息安全保障工作主要原则
  - 掌握国家有关政策规定需要重点加强的信息安全保障工作
- 知识子域：电子政务及重要信息系统信息安全政策
  - 了解关于加强政府信息系统安全和保密管理工作的四项基本要求：明确职责、强化人员培训、完善安全措施和手段、加强信息安全检查
- 知识子域：风险评估有关政策规范
  - 了解国家有关政策对信息安全风险评估工作提出的要求
  - 了解国家有关政策对电子政务工程及国家重要信息系统建设项目风险评估专控队伍的规定
- 知识子域：等级保护有关政策规范
  - 了解《信息安全等级保护管理办法》的有关要求
- 知识子域：国家密码管理政策
  - 了解我国对密码的管理政策要求

6.2 知识体：信息安全标准



图表 6-2 知识体：信息安全标准

6.2.1 知识域：安全标准化概述

- 知识子域：信息安全标准化概况
  - 了解标准和标准化的基本概念和作用
  - 了解信息安全标准体系
- 知识子域：信息安全标准化组织
  - 了解国际信息安全标准化组织
  - 了解我国信息安全标准化组织

6.2.2 知识域：信息安全评估标准

- 知识子域：安全技术评估标准发展历史
  - 了解安全技术评估标准发展过程
  - 理解可信计算机评估准则（TCSEC）的局限性
  - 理解 GB/T 18336《信息技术安全性评估准则》（CC）的优点
- 知识子域：信息安全技术评估准则
  - 了解 CC 的结构
  - 理解 CC 的术语（TOE、PP、ST、EAL）和基本思想

- ◆ 了解使用 CC 进行信息技术产品安全性评估的基本过程
- ◆ 了解通用评估方法（CEM）

- 知识子域：信息系统安全保证评估框架
  - ◆ 了解 GB/T 20274《信息系统安全保障评估框架》的目的和意义
  - ◆ 了解《信息系统安全保障评估框架》的结构和主要内容

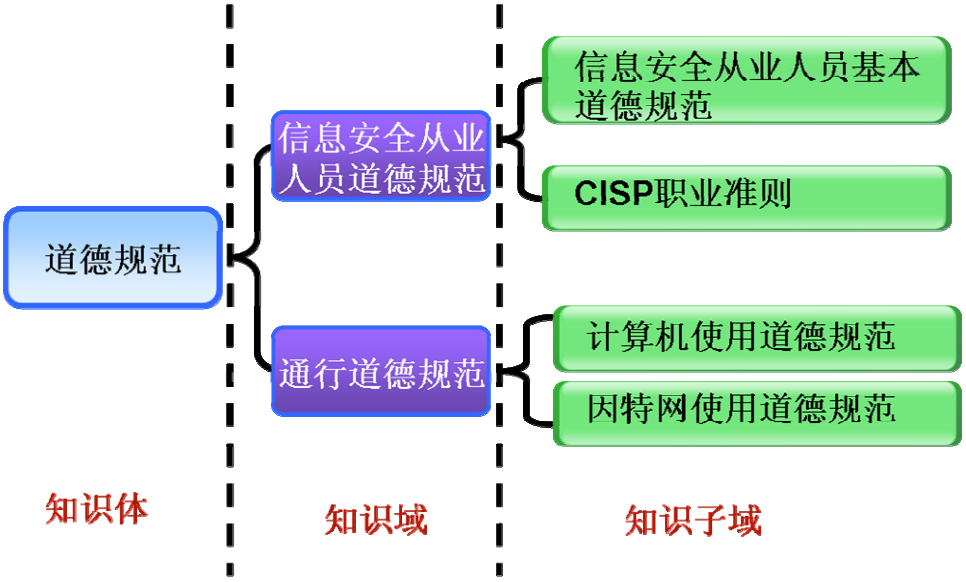
6.2.3 知识域：信息安全管理标准

- 知识子域：国际信息安全管理重要标准
  - ◆ 了解国外信息安全管理标准发展概况
  - ◆ 掌握 ISO 27001 和 ISO 27002 的主要内容
  - ◆ 了解英国和美国等发达国家的信息安全管理标准
  - ◆ 了解 CoBIT 和 ITIL 的用途
- 知识子域：我国信息安全管理重要标准
  - ◆ 掌握 GB/T 20984《信息安全风险评估规范》的主要内容
  - ◆ 掌握 GB/Z 24364《信息安全风险管理规范》的主要内容
  - ◆ 了解 GB/Z 20985《信息安全事件管理指南》的主要内容
  - ◆ 掌握 GB/Z 20986《信息安全事件分类分级指南》的主要内容
  - ◆ 掌握 GB/T 20988《信息系统灾难恢复规范》的主要内容

6.2.4 知识域：等级保护标准

- 知识子域：等级保护定级指南
  - ◆ 了解 GB/T 22240《信息系统安全保护等级定级指南》的主要内容
  - ◆ 掌握五个信息系统安全保护等级的定义
  - ◆ 掌握系统定级的要素、基本方法和流程
- 知识子域：等级保护基本要求
  - ◆ 了解 GB/T 22239《信息系统安全等级保护基本要求》的主要内容
  - ◆ 掌握五个信息系统安全保护等级对应的安全保护能力级别
  - ◆ 掌握管理基本要求包含的五个方面以及安全技术要求包含的五个方面
- 知识子域：等级保护其它重要标准
  - ◆ 了解《信息系统安全等级保护实施指南》的主要内容
  - ◆ 了解《信息系统安全等级保护测评准则》的主要内容

6.3 知识体：道德规范



图表 6-3 知识体：道德规范

6.3.1 知识域：信息安全从业人员道德规范

- 知识子域：信息安全从业人员基本道德规范
  - 理解信息安全从业人员应遵守的道德规范
- 知识子域：CISP 职业准则
  - 理解《CISP 职业道德准则》

6.3.2 知识域：通行道德规范

- 知识子域：计算机使用道德规范
  - 了解作为计算机普通用户应当遵守的基本道德规范
- 知识子域：因特网使用道德规范
  - 了解中国互联网协会《文明上网自律公约》的主要内容