注册信息安全专业人员（CISP）

知识体系大纲

CNITSEC

版本：3.0

发布日期：2014 年 12 月 1 日

生效日期：2015 年 1 月 1 日

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及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开展在职培训的重要形式，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
- 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：信息安全法规标准

第 1 章 注册信息安全专业人员（CISP）知识体系概述

1.1 CISP 类别

“注册信息安全专业人员”，英文为 Certified Information Security Professional ，简称 **CISP**，根据岗位工作需要，分为四个类别：

- “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。
- “注册信息系统审计师”，英文为 Certified Information System Auditor，简称 **CISP-A**。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。
- “注册信息安全开发人员”，英文为 Certified Information Security Developer，简称 CISD。证书持有人主要从事软件开发相关工作，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安全开发能力、熟练掌握应用安全。

1.2 大纲范围

本大纲涵盖了 CISE 和 CISO 两类注册人员需要掌握的知识要点。

CISP-A 需要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-A 知识体系大纲中进行介绍。

CISD 需要更加深入地掌握有关信息系统安全开发的知识，有关内容将在 CISD 知识体系大纲中进行介绍。

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 1-1 描述了 CISP 知识体系的结构：

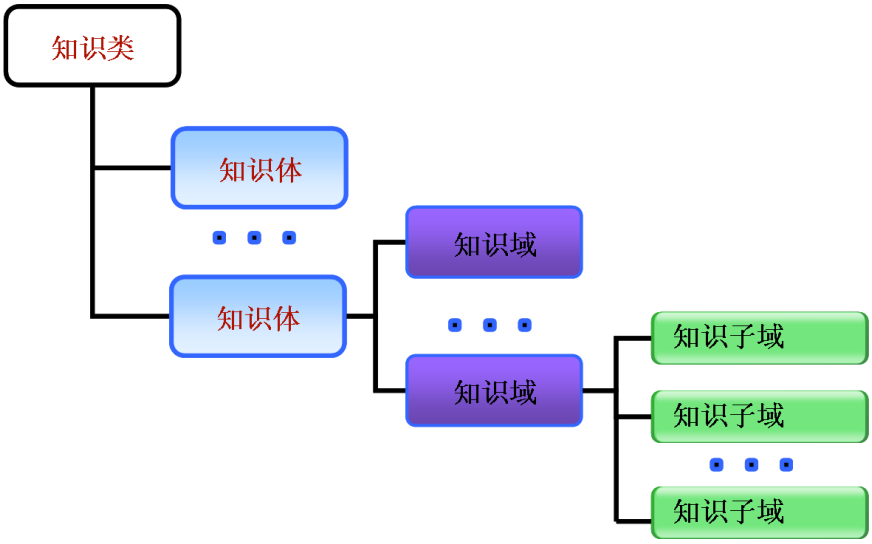

图 1-1：CISP 知识体系的组件模块结构

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、信息安全技术、信息安全管理、信息安全工程和信息安全法规标准这五个知识类，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：**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、访问控制等安全技术与机制，网络、操作系统、数据库和应用软件等方面的基本安全原理和实践，以及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、安全管理措施等相关的管理知识和实践。
- **信息安全工程**：主要包括信息安全相关的工程的基本理论和实践方法。
- **信息安全法规标准**：主要包括信息安全相关的法律法规、政策、标准和道德规范，是注册信息安全专业人员需要掌握的通用基础知识。

图 1-2 描述了 CISP 知识体系结构框架：

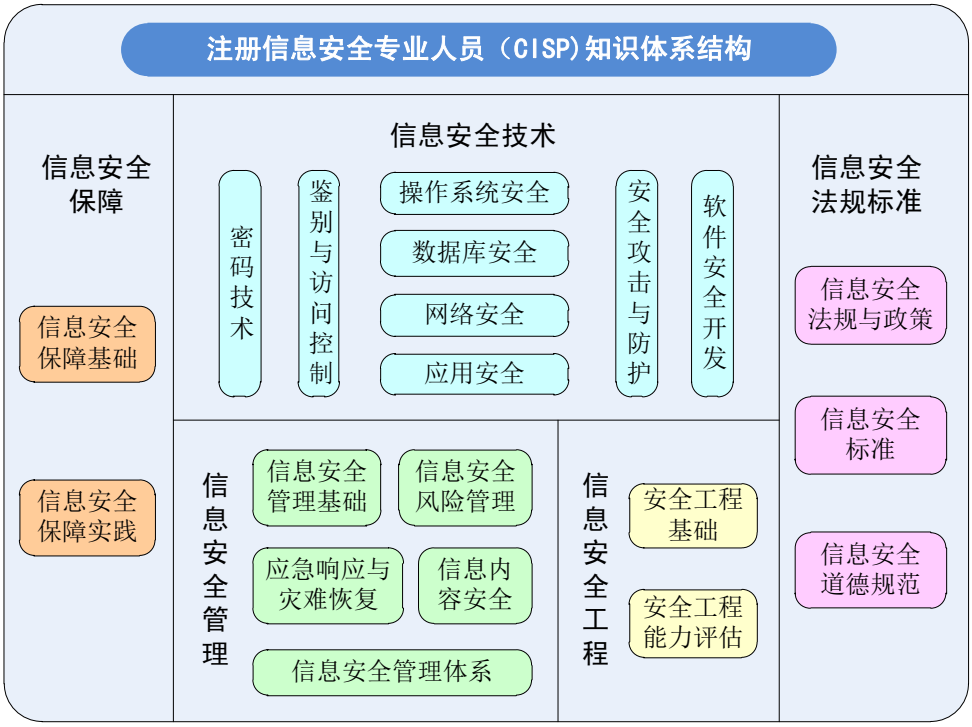

图 1-2：CISP 知识体系结构框架

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。

“注册信息安全工程师”（CISE）和“注册信息安全管理人员”（CISO）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 1-1 中描述了 CISE/CISO 考试各知识类试题的所占比例。

表 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	**10%**	**10%**
信息安全技术	**50%**	**20%**
信息安全管理	**20%**	**50%**
信息安全工程	**10%**	**10%**
信息安全法规标准	**10%**	**10%**

第 2 章 知识类：信息安全保障

信息安全保障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：信息安全保障基础

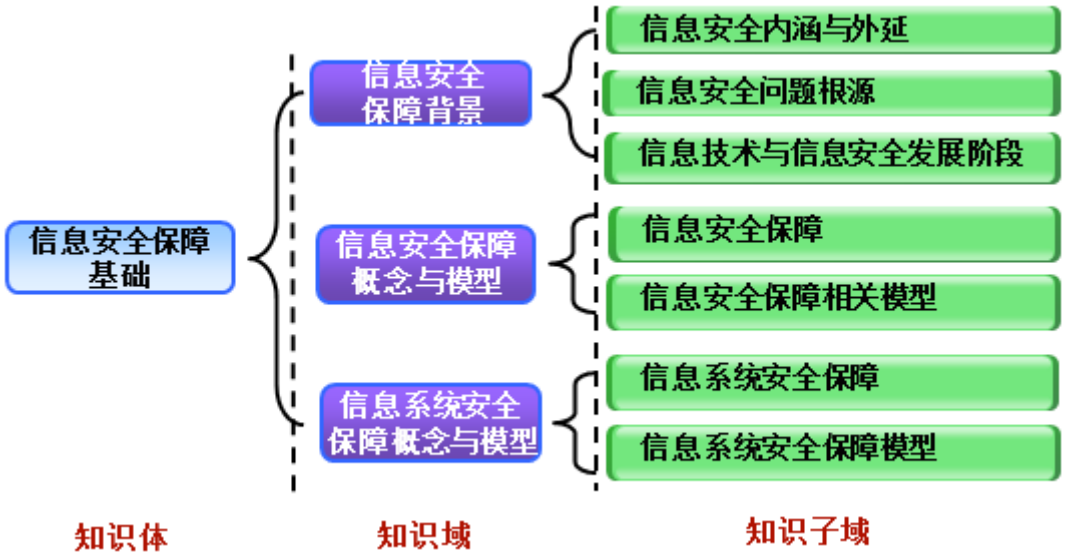

图 2-1：知识体：信息安全保障基础

2.1.1 知识域：信息安全保障背景

- 知识子域：信息安全内涵与外延
  - 理解信息安全基本概念，理解信息安全基本属性：保密性、完整性和可用性
  - 理解信息安全的特征与范畴
- 知识子域：信息安全问题根源
  - 理解信息安全问题产生的内因是信息系统自身存在脆弱性
  - 理解信息安全问题产生的外因是信息系统面临着众多威胁
- 知识子域：信息技术与信息安全发展阶段
  - 了解通信、计算机、网络和网络化社会等阶段信息技术的发展概况
  - 了解信息技术和网络对经济发展、社会稳定及国家安全等方面的影响

- ◆ 了解通信安全、计算机安全、信息系统安全和信息安全保障等阶段信息安全的发展概况，
- ◆ 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：信息安全保障概念与模型

- 知识子域：信息安全保障
  - ◆ 理解信息安全保障的概念
  - ◆ 理解信息安全保障与信息安全、信息系统安全的区别
- 知识子域：信息安全保障相关模型
  - ◆ 理解 P2DR 模型的基本原理：策略、防护、检测及响应，以及 P2DR 公式所表达的安全目标
  - ◆ 理解 IATF 的深度防御思想，及其将信息系统在技术层面的防御划分为本地计算环境、区域边界、网络基础设施和支撑性基础设施四个方面，理解每一方面的安全需求及基本实现方法

2.1.3 知识域：信息系统安全保障概念与模型

- 知识子域：信息系统安全保障
  - ◆ 了解信息系统的概念及其包含的基本资源
  - ◆ 理解信息系统安全保障的概念，以及风险、业务使命等信息系统安全保障相关概念及其之间的关系
- 知识子域：信息系统安全保障模型
  - ◆ 理解信息系统安全保障模型中生命周期、保障要素和安全特征的含义和内容
  - ◆ 理解风险和策略是信息系统安全保障的核心问题
  - ◆ 理解业务使命实现是信息安全保障的根本目的

2.2 知识体：信息安全保障实践

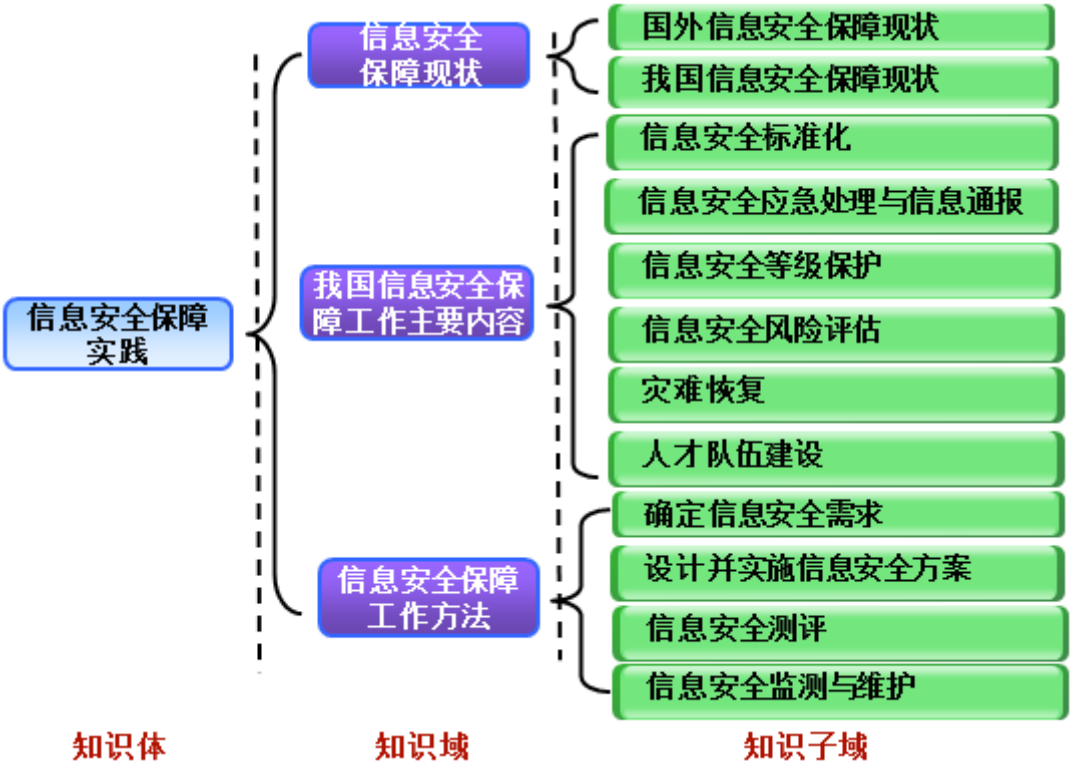

图 2-2：知识体：信息安全保障实践

2.2.1 知识域：信息安全保障现状

- 知识子域：国外信息安全保障现状
  - ◆ 了解发达国家信息安全状况和信息安全保障的主要举措
  - ◆ 了解发达国家信息安全保障建设动态
- 知识子域：我国信息安全保障现状
  - ◆ 了解我国信息化与信息安全形势
  - ◆ 了解我国信息安全保障发展阶段
  - ◆ 理解我国信息安全保障基本思路
  - ◆ 了解我国信息安全保障目标
  - ◆ 了解我国信息安全保障的整体规划
  - ◆ 了解我国信息安全保障体系的框架

2.2.2 知识域：我国信息安全保障工作主要内容

- 知识子域：信息安全标准化
  - ◆ 了解信息安全标准化的意义
  - ◆ 了解我国信息安全标准化工作的实践情况

- 知识子域：信息安全应急处理与信息通报
  - ◆ 了解信息安全应急处理与信息通报的意义
  - ◆ 了解我国信息安全应急处理与信息通报工作的实践情况
- 知识子域：信息安全等级保护
  - ◆ 了解我国信息安全等级保护的意义
  - ◆ 了解我国信息安全等级保护工作的实践情况
- 知识子域：信息安全风险评估
  - ◆ 了解信息安全风险评估的意义
  - ◆ 了解我国信息安全风险评估工作的实践情况
- 知识子域：灾难恢复
  - ◆ 了解灾难恢复的意义
  - ◆ 了解我国灾难恢复工作的实践情况
- 知识子域：人才队伍建设
  - ◆ 了解人才队伍建设的意义
  - ◆ 了解我国信息安全人才队伍建设工作的实践情况

2.2.3 知识域：信息安全保障工作方法

- 知识子域：确定信息安全需求
  - ◆ 了解确定信息安全保障需求的作用
  - ◆ 了解确定信息安全保障需求的方法和原则
- 知识子域：设计并实施信息安全方案
  - ◆ 了解信息安全方案的作用和主要内容
  - ◆ 了解制定信息安全方案的主要原则
  - ◆ 了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
  - ◆ 了解信息产品安全测评方法
  - ◆ 了解信息系统安全测评方法
  - ◆ 了解服务商资质测评方法
  - ◆ 了解信息安全人员资质测评方法
- 知识子域：信息安全监测与维护
  - ◆ 了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
  - ◆ 了解信息系统安全监测与维护的主要原则

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：

- 理解密码、访问控制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、操作系统软件、数据库、应用软件信息安全防护的基本知识和技术；
- 理解信息安全攻击与防护的基本知识和技术；
- 理解软件安全开发的基本方法。

3.1 知识体：密码技术

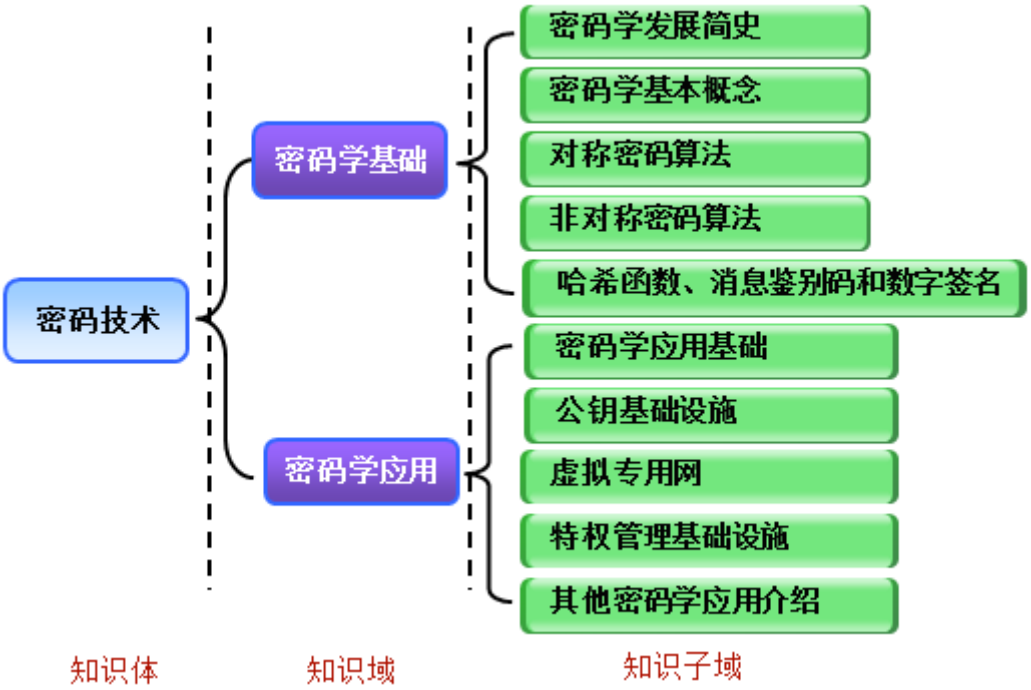

图 3-1：知识体：密码技术

3.1.1 知识域：密码学基础

- 知识子域：密码学发展简史
  - 了解密码学的发展阶段及各阶段特点
  - 了解每一阶段密码应用状况
- 知识子域：密码学基本概念

- ◆ 理解密码通信模型，理解密码学加密、解密、算法、密钥等概念
- ◆ 理解科克霍夫原则，理解算法复杂程度和密钥长度是影响密码系统安全性的基本因素
- ◆ 理解古典密码的特点及算法类型
- ◆ 掌握密码体制的分类和特点
- ◆ 理解密钥管理的重要性，理解密钥生命周期概念，了解密钥产生、分配、使用、更换和注销等过程的管理特点
- ◆ 了解密码协议的概念及类型，了解 Diffie-Hellman 密钥协商协议的实现原理

- 知识子域：对称密码算法
  - ◆ 理解对称密码算法的优缺点和应用场合
  - ◆ 理解 DES、3DES、AES、IDEA 算法的特点
- 知识子域：非对称密码算法
  - ◆ 理解非对称密码算法的优缺点和应用场合
  - ◆ 理解 RSA 算法的特点
  - ◆ 了解 EIGamal、ECC 等算法的特点
- 知识子域：哈希函数、消息鉴别码和数字签名
  - ◆ 理解哈希函数的特点和作用，了解 MD5 算法、SHA-1 算法的原理和应用
  - ◆ 理解消息鉴别码的特点和作用，了解 MAC、HMAC 的原理和应用
  - ◆ 理解数字签名的原理和应用，了解 DSA 和 RSA 签名方案及区别

3.1.2 知识域：密码学应用

- 知识子域：密码学应用基础
  - ◆ 理解使用密码学手段解决机密性、完整性、鉴别、不可否认性以及授权等信息安全要素的实现方法
  - ◆ 了解常见密码应用场景和分类产品
- 知识子域：公钥基础设施
  - ◆ 了解 PKI/CA 中 CA、RA、数字证书、LDAP、OCSP、CRL 等概念
  - ◆ 理解 PKI/CA 体系结构和作用
  - ◆ 掌握 PKI/CA 中数字证书的申请、发布及注销等流程
  - ◆ 了解 PKI/CA 的典型应用
- 知识子域：虚拟专用网络
  - ◆ 理解 VPN 的概念、分类和功能

- ◆ 理解 IPSec 协议的工作原理和特点
- ◆ 理解 SSL 协议的工作原理和特点

- 知识子域：特权管理基础设施
  - ◆ 了解 PMI/AA 的概念和作用
  - ◆ 掌握 PMI 和 PKI 的区别
  - ◆ 了解 PMI/AA 的体系结构，以及属性证书的特点和应用
- 知识子域：其他密码学应用介绍
  - ◆ 理解动态口令认证特点、实现原理及应用
  - ◆ 理解动态口令和静态口令的优缺点对比

3.2 知识体：鉴别与访问控制

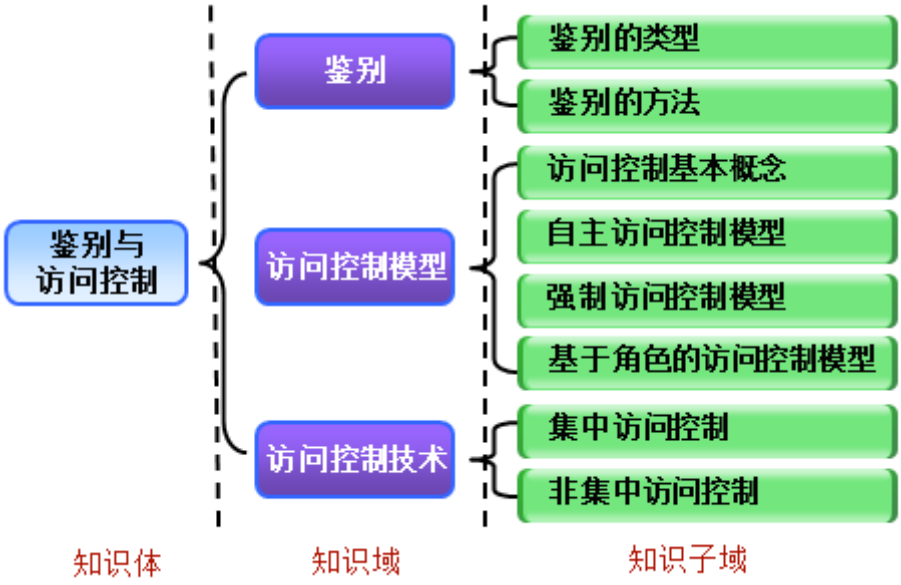

图 3-2：知识体：鉴别与访问控制

3.2.1 知识域：鉴别

- 知识子域：鉴别的类型
  - ◆ 理解标识、鉴别的概念和作用
  - ◆ 理解单向鉴别、双向鉴别和第三方鉴别的区别
- 知识子域：鉴别的方法
  - ◆ 理解基于所知、所有和生物特征的三种基本鉴别方法及其特点
  - ◆ 理解每种鉴别方法及组合鉴别方法的强度

3.2.2 知识域：访问控制模型

- 知识子域：访问控制基本概念
  - ◆ 理解访问控制的作用
  - ◆ 理解主体、客体、访问权限等基本概念
  - ◆ 理解访问控制模型的一般构成
- 知识子域：自主访问控制
  - ◆ 理解自主访问控制（DAC）的含义
  - ◆ 理解 DAC 的常用描述方式访问控制矩阵模型，及其两种常见实现方法：访问控制表、能力表，了解其他实现方法如前缀表、保护位
  - ◆ 理解 DAC 的特点
- 知识子域：强制访问控制
  - ◆ 理解强制访问控制（MAC）的分类和含义
  - ◆ 理解典型 MAC 模型：Bell-Lapudula 模型、Biba 模型
  - ◆ 了解 Chinese Wall 模型和 Clark-Wilson 模型
  - ◆ 理解 MAC 的特点
- 知识子域：基于角色的访问控制
  - ◆ 理解基于角色的访问控制（RBAC）模型的基本组成
  - ◆ 理解 RBAC 的特点

3.2.3 知识域：访问控制技术

- 知识子域：集中访问控制
  - ◆ 理解集中访问控制的基本概念
  - ◆ 理解实现集中访问控制的常用协议：Kerberos 协议、AAA 协议
  - ◆ 了解三个常见的 AAA 协议：RADIUS、TACACS+和 Diameter，以及每个协议的优缺点
- 知识子域：非集中访问控制
  - ◆ 理解非集中访问控制的基本概念
  - ◆ 理解域等非集中访问控制的实现方式

3.3 知识体：网络安全

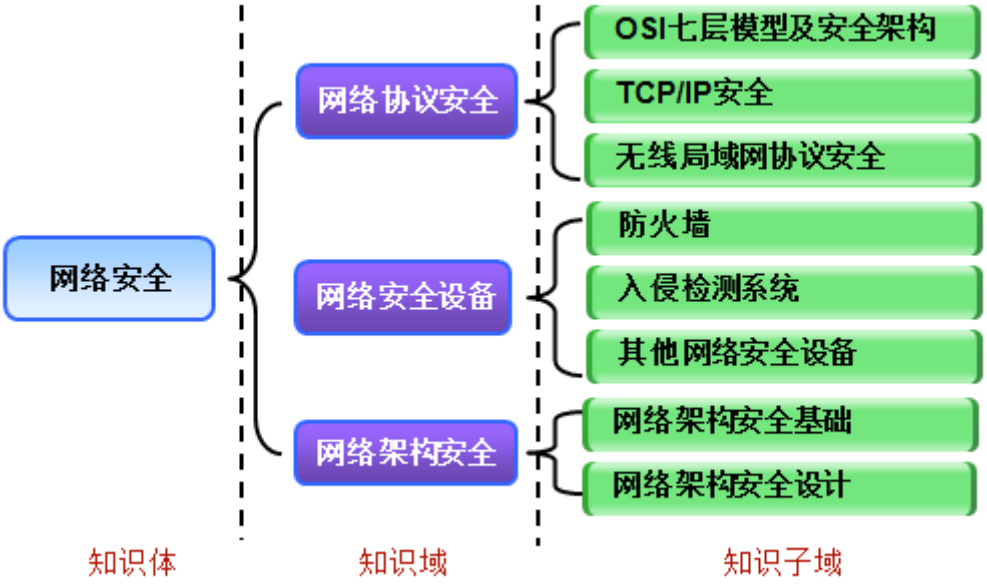

图 3-3：知识体：网络安全

3.3.1 知识域：网络协议安全

- 知识子域：OSI 七层模型及安全架构
  - 了解开放系统互联（OSI）模型的七层网络通信结构及通信过程，了解每一层的功能
  - 了解 OSI 安全架构的核心内容：基于 8 类安全机制提供 5 类安全服务
- 知识子域：TCP/IP 安全
  - 了解 TCP/IP 协议模型及各层典型协议的功能
  - 理解基于 TCP/IP 的典型安全协议
  - 了解 IPv6 的安全特点
- 知识子域：无线局域网协议安全
  - 了解无线局域网的基本组成与特点
  - 了解 WEP、802.11i、WAPI 等无线局域网安全实现

3.3.2 知识域：网络安全设备

- 知识子域：防火墙
  - 理解防火墙的作用、功能及分类

- ◆ 理解包过滤技术、状态检测技术和应用代理技术等防火墙主要技术原理
- ◆ 掌握防火墙的典型部署方式
- ◆ 理解防火墙的局限性

- 知识子域：入侵检测系统
  - ◆ 理解入侵检测系统的作用、功能及分类
  - ◆ 了解入侵检测系统的主要技术原理
  - ◆ 掌握入侵检测系统的典型部署方式
  - ◆ 理解入侵检测系统的局限性
- 知识子域：其他网络安全设备
  - ◆ 了解安全隔离与信息交换系统的原理、特点及适用场景
  - ◆ 了解入侵防御系统（IPS）的原理与特点
  - ◆ 了解安全管理平台（SOC）的主要功能
  - ◆ 了解统一威胁管理系统（UTM）的功能与特点
  - ◆ 了解网络准入控制（NAC）的功能、组成及控制方式

3.3.3 知识域：网络架构安全

- 知识子域：网络架构安全基础
  - ◆ 理解网络架构安全的含义
  - ◆ 理解网络架构安全设计的主要工作
- 知识子域：网络架构安全设计
  - ◆ 理解网络安全域划分应考虑的主要因素
  - ◆ 理解 IP 地址规划方法
  - ◆ 理解 VLAN 划分的作用与策略
  - ◆ 理解路由交换设备安全配置常见的要求
  - ◆ 理解网络边界访问控制策略的类型
  - ◆ 理解网络冗余配置应考虑的因素

3.4 知识体：操作系统与数据库安全

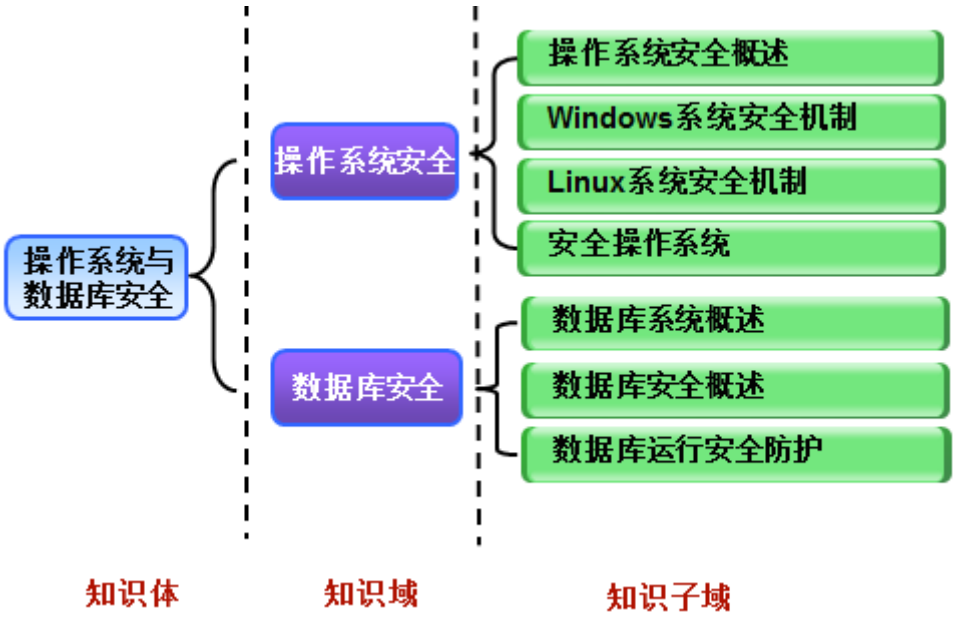

图 3-4：知识体：操作系统与数据库安全

3.4.1 知识域：操作系统安全

- 知识子域：操作系统安全概述
  - ◆ 了解操作系统的作用与功能
  - ◆ 了解操作系统的主要安全设计机制
  - ◆ 理解操作系统的安全配置要点
- 知识子域：Windows 系统安全机制
  - ◆ 理解 Windows 系统标识与鉴别、访问控制、用户账户控制、安全审计、文件系统的安全机制和安全策略
  - ◆ 掌握 Windows 系统的安全配置方法
- 知识子域： Linux 系统安全机制
  - ◆ 理解 Linux 系统标识与鉴别、访问控制、安全审计、文件系统、特权管理的安全机制
  - ◆ 掌握 Linux 系统的安全配置方法
- 知识子域：安全操作系统
  - ◆ 了解安全操作系统的发展
  - ◆ 了解安全操作系统的设计原则

3.4.2 知识域：数据库安全

- 知识子域：数据库系统概述
  - 了解数据库基本概念和主要功能
  - 了解构化查询语言 SQL 的功能
  - 了解数据库管理系统（DBMS）的一般架构
- 知识子域：数据库安全概述
  - 了解数据库的安全需求
  - 了解数据库的常见安全措施：用户标识和鉴别、访问控制、数据加密和安全审计
  - 理解数据库完整性要求，理解 DBMS 为了实现完整性保护必须提供：定义完整性约束条件的机制、完整性检查的方法和违约处理的机制
  - 理解数据库备份和恢复机制的重要性，了解常见的数据冗余技术和数据库恢复策略
- 知识子域：数据库运行安全防护
  - 理解数据库威胁与防护特点
  - 理解数据库事前安全防护、事中安全监控以及事后安全审计的方法

3.5 知识体：应用安全

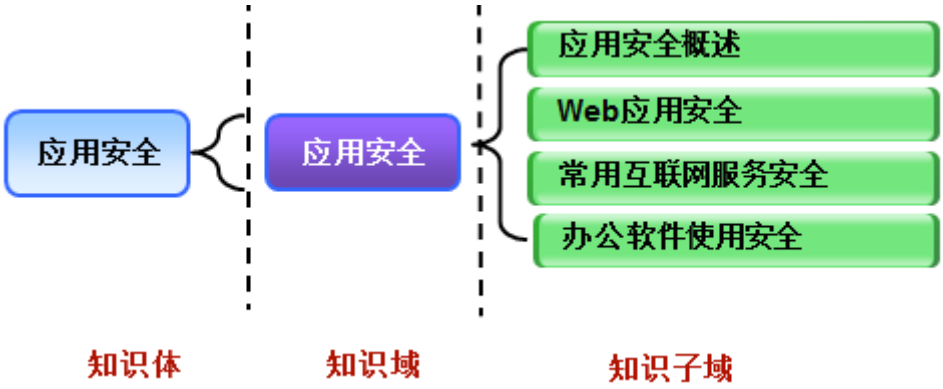

图 3-5：知识体：应用安全

3.5.1 知识域：应用安全

- 知识子域：应用安全概述
  - 理解应用安全的概念

- 了解常见应用安全威胁
- 了解等级保护规范应用安全防护要点

- 知识子域：Web 应用安全
  - 理解 Web 工作机制及 Web 应用安全问题产生的原因
  - 了解常见 Web 服务运行平台的安全配置要点
  - 了解互联网浏览面临的安全威胁及应对方法
  - 了解 Web 安全防护产品如 Web 应用防火墙和网页防篡改产品的功能和特点
- 知识子域：常用互联网服务安全
  - 了解电子邮件应用的安全缺陷和防御措施
  - 了解 FTP 应用安全缺陷和防御措施
  - 了解远程管理的安全问题及防御措施
  - 了解域名应用的安全问题及防御措施
- 知识子域：办公软件使用安全
  - 了解使用文字处理程序的安全防护要点
  - 了解使用即时通信软件的安全防护要点

3.6 知识体：安全漏洞、恶意代码与攻防

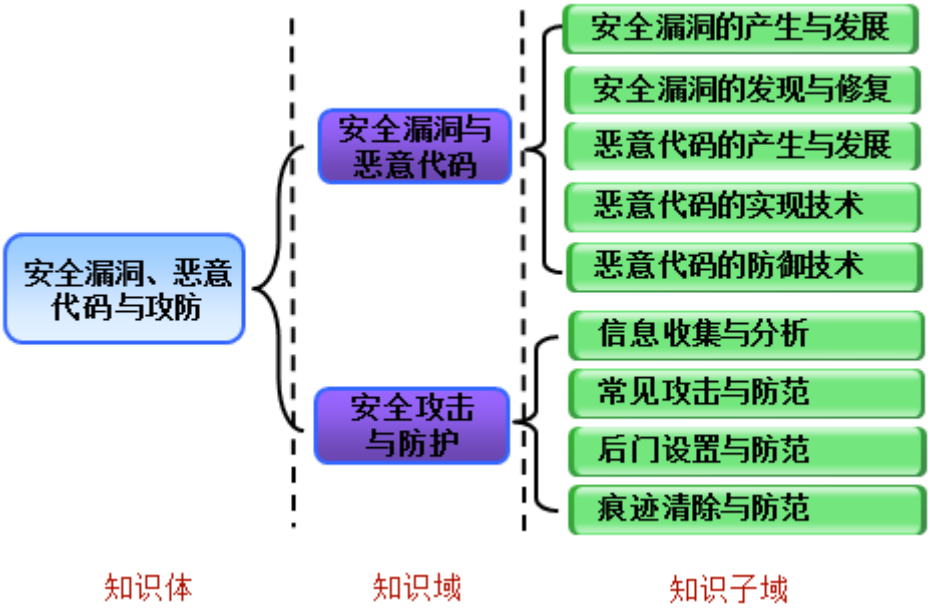

图 3-6：知识体：安全漏洞、恶意代码与攻防

3.6.1 知识域：安全漏洞与恶意代码

- 知识子域：安全漏洞的产生与发展

- ◆ 了解安全漏洞的概念和产生的原因
- ◆ 了解国内外常见的安全漏洞分类
- ◆ 了解安全漏洞的发展趋势

- 知识子域：安全漏洞的发现与修复
  - ◆ 了解安全漏洞的静态与动态挖掘方法的基本原理
  - ◆ 了解补丁分类及修复时应注意的问题
- 知识子域：恶意代码的产生与发展
  - ◆ 了解恶意代码的发展历史及趋势
  - ◆ 了解恶意代码的分类
  - ◆ 理解恶意代码的传播方式
- 知识子域：恶意代码的实现技术
  - ◆ 理解恶意代码修改配置文件、修改注册表、设置系统服务等加载方式
  - ◆ 理解恶意代码进程、网络及系统隐藏技术
  - ◆ 理解恶意代码进程保护和检测对抗自我保护技术
- 知识子域：恶意代码的防御技术
  - ◆ 理解增强安全策略与意识、减少漏洞、减轻威胁等恶意代码预防方法
  - ◆ 理解恶意代码特征码扫描、利用沙箱技术、行为检测等检测方法
  - ◆ 理解恶意代码静态与动态分析方法
  - ◆ 理解不同类型恶意代码的清除方法

3.6.2 知识域：安全攻击与防护

- 知识子域：信息收集与分析
  - ◆ 了解信息收集与分析的作用
  - ◆ 理解快速定位、定点挖掘、漏洞查询等信息收集与分析的方法
  - ◆ 理解信息收集与分析的防范措施
- 知识子域：常见攻击与防范
  - ◆ 理解默认口令攻击、字典攻击及暴力攻击等方式的口令破解原理与防范措施
  - ◆ 理解社会工程学攻击的方法与防范措施
  - ◆ 理解 IP 欺骗、ARP 欺骗和 DNS 欺骗的原理与防范措施
  - ◆ 理解 SYN Flood、UDP Flood、Teardrop 攻击等典型 DOS/DDOS 的原理与防范措施
  - ◆ 理解缓冲区溢出攻击的原理与防范措施

- ◆ 理解 SQL 注入攻击的原理与防范措施
- ◆ 理解跨站脚本攻击的原理与防范措施

- 知识子域：后门设置与防范
  - ◆ 理解攻击者设置系统后门的常用方法
  - ◆ 理解针对后门的防范措施
- 知识子域：痕迹清除与防范
  - ◆ 理解攻击者清除痕迹的常用方法
  - ◆ 理解针对痕迹清除的防范措施

3.7 知识体：软件安全开发

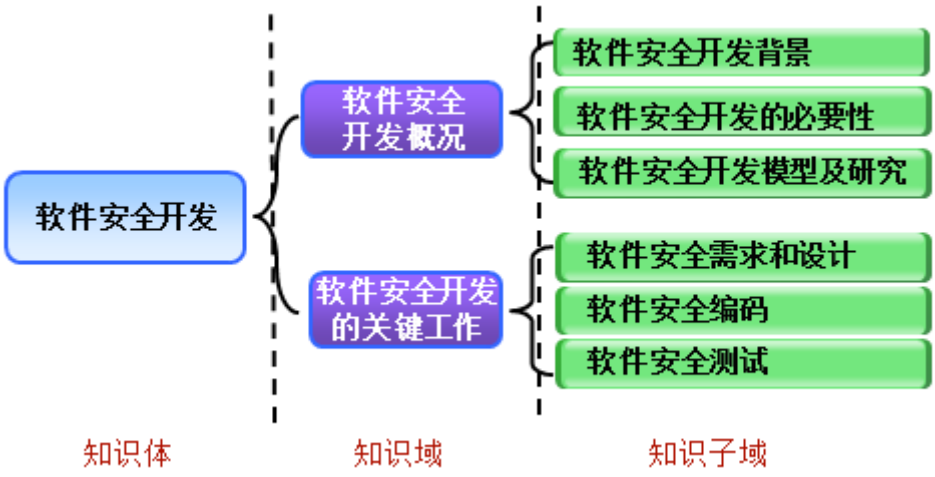

图 3-7：知识体：软件安全开发

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
  - ◆ 了解软件的发展和产生的安全问题
  - ◆ 了解软件安全问题产生的原因
- 知识子域：软件安全开发的必要性
  - ◆ 理解软件安全保障的含义、思路和目标
  - ◆ 了解传统软件开发的局限性
  - ◆ 理解软件安全开发生命周期的概念和必要性
- 知识子域：软件安全开发模型及研究
  - ◆ 了解安全开发生命周期（SDL）的发展历程，理解 SDL 的主要内容
  - ◆ 了解使安全成为软件开发必须的部分（BSI）系列模型

- ◆ 了解综合的轻量级应用安全过程（CLASP）的主要内容
- ◆ 了解软件保障成熟度模型（SAMM）的框架
- ◆ 了解各个模型的特点及适用性

3.7.2 知识域：软件安全开发的关键工作

- 知识子域：软件安全需求和设计
  - ◆ 了解软件安全需求分析和安全设计的重要性
  - ◆ 理解软件安全设计基本原则
  - ◆ 理解影响系统安全性的 6 类威胁，以及威胁建模过程
- 知识子域：软件安全编码
  - ◆ 理解通用安全编码准则：验证输入、避免缓冲区溢出、程序内部安全、安全调用组件、禁止使用不安全函数等
  - ◆ 理解使用安全编译技术对提高编码安全水平的作用，了解常用安全编译技术
  - ◆ 理解源代码审核的目的及方式，了解常见源代码静态审核工具
- 知识子域：软件安全测试
  - ◆ 了解软件安全测试的重要性和基本概念
  - ◆ 理解模糊测试的目的、方法和步骤，以及影响模糊测试效果的关键因素
  - ◆ 理解渗透测试的目的、方法和步骤，以及渗透测试应注意的问题

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：信息安全管理基础

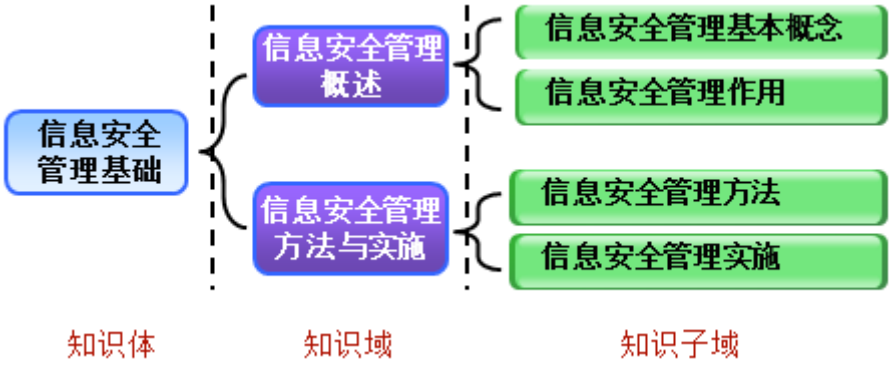

图 4-1：知识体：信息安全管理基础

4.1.1 知识域：信息安全管理概述

- 知识子域：信息安全管理基本概念
  - ◆ 理解管理、信息安全管理的概念，理解信息安全管理的对象
  - ◆ 理解以建立体系的方式实施信息安全管理的必要性
  - ◆ 理解体系、管理体系、信息安全管理体系的概念
- 知识子域：信息安全管理作用
  - ◆ 理解信息安全管理的重要作用
  - ◆ 理解信息安全管理体系的作用
  - ◆ 理解实施信息安全管理的关键成功因素

4.1.2 知识域：信息安全管理方法与实施

- 知识子域：信息安全管理方法

- ◆ 理解风险管理是信息安全管理的基本方法，理解风险评估是信息安全管理的基础，风险处理是信息安全管理的核心，理解控制措施是管理风险的具体手段
- ◆ 理解过程方法是信息安全管理的基本方法，理解过程和过程方法的含义，理解 PDCA 模型

- 知识子域：信息安全管理实施
  - ◆ 理解建设信息安全管理体系是系统地实施信息安全管理的一种方法
  - ◆ 理解建设信息安全等级保护是系统地实施信息安全管理的一种方法
  - ◆ 了解基于 NIST SP 800 进行信息安全建设是实施信息安全管理的一种方法

4.2 知识体：信息安全风险管理

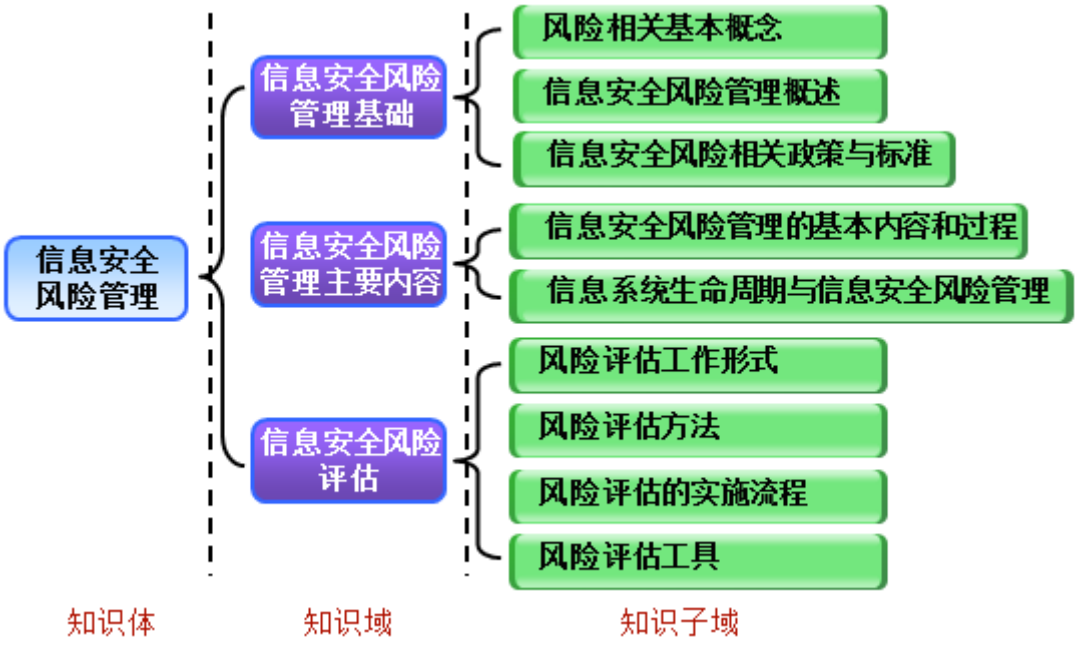

图 4-2：知识体：信息安全风险管理

4.2.1 知识域：信息安全风险管理基础

- 知识子域：风险相关基本概念
  - ◆ 理解风险的概念，理解资产、威胁、脆弱性、业务战略、安全事件、安全需求、安全措施等风险相关概念

- ◆ 理解风险准则、风险评估、风险处理、风险管理、残余风险的概念，掌握信息安全风险评估的概念
- ◆ 理解风险相关要素之间的关系

- 知识子域：信息安全风险管理概述
  - ◆ 理解实施风险管理的主要原则
  - ◆ 理解风险管理的范围和对象
- 知识子域：信息安全风险相关政策与标准
  - ◆ 了解我国有关信息安全风险管理的政策要求
  - ◆ 了解信息安全风险管理相关的国内外标准

4.2.2 知识域：信息安全风险管理主要内容

- 知识子域：信息安全风险管理的基本内容和过程
  - ◆ 理解背景建立的主要工作内容
  - ◆ 理解风险评估的主要工作内容
  - ◆ 理解风险处理的主要工作内容
  - ◆ 理解批准监督的主要工作内容
  - ◆ 理解监控审查的主要工作内容
  - ◆ 理解沟通咨询的主要工作内容
- 知识子域：信息系统生命周期与信息安全风险管理
  - ◆ 理解信息系统生命周期与信息安全风险管理的关系
  - ◆ 理解系统规划阶段的风险管理工作内容
  - ◆ 理解系统设计阶段的风险管理工作内容
  - ◆ 理解系统实施阶段的风险管理工作内容
  - ◆ 理解系统运行维护阶段的风险管理工作内容
  - ◆ 理解系统废弃阶段的风险管理工作内容

4.2.3 知识域：信息安全风险评估

- 知识子域：风险评估工作形式
  - ◆ 理解自评估和检查评估的风险评估工作形式
  - ◆ 理解自评估和检查评估的区别及优缺点
  - ◆ 理解风险评估、检查评估和等级保护测评之间的关系
- 知识子域：风险评估方法
  - ◆ 理解定性风险分析方法
  - ◆ 理解定量风险分析方法，掌握年度预期损失（ALE）的计算方法
  - ◆ 理解半定量风险分析方法

- ◆ 理解定性和定量风险分析方法的优缺点
- 知识子域：风险评估的实施流程
  - ◆ 掌握风险评估准备阶段的工作内容
  - ◆ 掌握风险要素识别阶段的工作内容
  - ◆ 掌握风险分析阶段的工作内容和工作步骤
  - ◆ 掌握风险结果判定阶段的工作内容
- 知识子域：风险评估工具
  - ◆ 了解风险评估工具的分类
  - ◆ 了解常用风险评估工具

4.3 知识体：信息安全管理体系

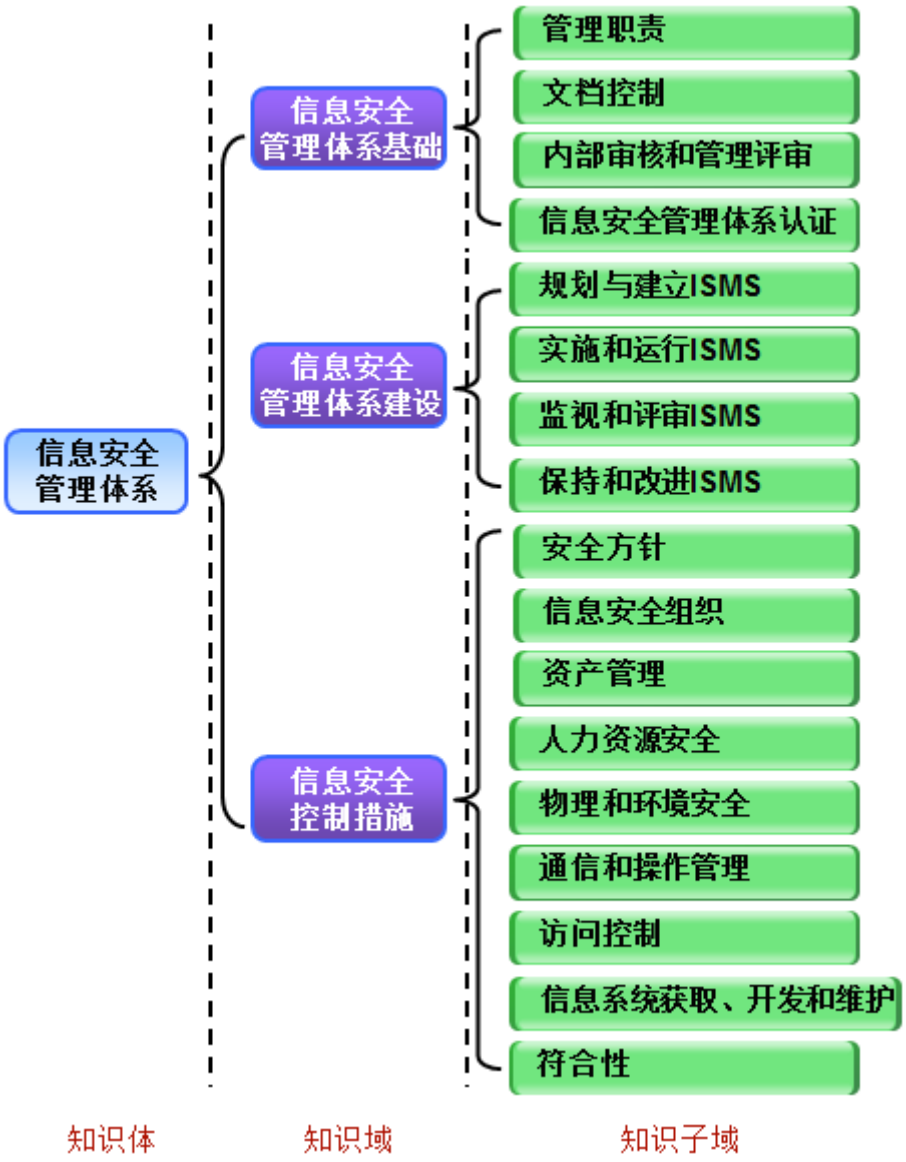

图 4-3：知识体：信息安全管理体系

4.3.1 知识域：信息安全管理体系基础

- 知识子域：管理职责
  - ◆ 理解管理者履行管理职责对成功实施信息安全管理体系（ISMS）的重要推动作用
  - ◆ 掌握实施 ISMS 过程中管理者应承担的管理职责的主要内容
- 知识子域：文档控制
  - ◆ 理解文档化对实施 ISMS 的重要性
  - ◆ 理解风险评估结果是编制 ISMS 文件的依据
  - ◆ 了解对 ISMS 文件和记录进行保护和控制的常规措施
- 知识子域：内部审核和管理评审
  - ◆ 了解内部审核的概念，以及内部审核的目的、实施主体、实施方式、审核准则
  - ◆ 了解管理评审的概念，以及管理评审的目的、实施主体、实施对象、实施方式
- 知识子域：信息安全管理体系认证
  - ◆ 了解 ISMS 认证的概念
  - ◆ 理解 ISMS 认证是促进信息安全管理体系改进的一种外部驱动力

4.3.2 知识域：信息安全管理体系建设

- 知识子域：规划与建立 ISMS
  - ◆ 理解定义 ISMS 范围和边界、实施风险评估、获得管理者对残余风险的批准等规划与建立 ISMS 的主要工作内容
- 知识子域：实施和运行 ISMS
  - ◆ 理解实施风险处理计划、开发有效性测量程序、管理 ISMS 的运行等实施和运行 ISMS 的主要工作内容
- 知识子域：监视和评审 ISMS
  - ◆ 理解进行有效性测量、实施内部审核、实施管理评审等监视和评审 ISMS 的主要工作内容
- 知识子域：保持和改进 ISMS
  - ◆ 理解实施纠正和预防措施、沟通措施和改进情况等保持和改进 ISMS 的主要工作内容

4.3.3 知识域：信息安全控制措施

- 知识子域：安全方针
  - ◆ 理解信息安全方针控制目标的含义
  - ◆ 掌握信息安全方针文件和信息安全方针评审两项措施的常规控制方法
- 知识子域：信息安全组织
  - ◆ 理解内部组织控制目标的含义，掌握信息安全协调等实现这一目标的控制措施的常规实施方法
  - ◆ 理解外部各方控制目标的含义，掌握与外部各方相关风险的识别等控制措施的实施方法
- 知识子域：资产管理
  - ◆ 理解对资产负责控制目标的含义，掌握资产清单、资产责任人等控制措施的实施方法
  - ◆ 理解信息分类控制目标的含义，掌握分类指南、信息的标记和处理等控制措施的实施方法
- 知识子域：人力资源安全
  - ◆ 理解任用前控制目标的含义，掌握角色和职责、审查等控制措施的实施方法
  - ◆ 理解任用中控制目标的含义，掌握管理职责、信息安全意识教育和培训等控制措施的实施方法
  - ◆ 理解任用的终止或变化控制目标的含义，掌握终止职责、撤销访问权等控制措施的实施方法
- 知识子域：物理和环境安全
  - ◆ 理解人身安全的重要性
  - ◆ 理解安全区域控制目标的含义，掌握物理安全边界、物理入口控制等控制措施的实施方法
  - ◆ 理解设备安全控制目标的含义，掌握设备安置和保护、支持性设施等控制措施的实施方法
- 知识子域：通信和操作管理
  - ◆ 理解操作程序和职责、第三方服务交付管理、系统规划和验收、防范恶意代码、备份、网络安全管理、介质处置、信息的交换、电子商务服务、监视和访问控制这些控制目标的含义
  - ◆ 掌握实现这些控制目标的控制措施的实施方法
- 知识子域：访问控制

- ◆ 理解访问控制的业务要求、用户访问管理、用户职责、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这些控制目标的含义
- ◆ 掌握实现这些控制目标的控制措施的实施方法

- 知识子域：信息系统获取、开发与维护
  - ◆ 理解信息系统的安全需求、应用中的正确处理、密码控制、系统文件的安全、开发和支持过程中的安全、技术脆弱性管理这些控制目标的含义
  - ◆ 掌握实现这些控制目标的控制措施的实施方法
- 知识子域：符合性
  - ◆ 理解符合法律要求、符合安全策略和标准以及技术符合性、信息系统审核考虑这些控制目标的含义
  - ◆ 掌握实现这些控制目标的控制措施的实施方法

4.4 知识体：应急响应与灾难恢复

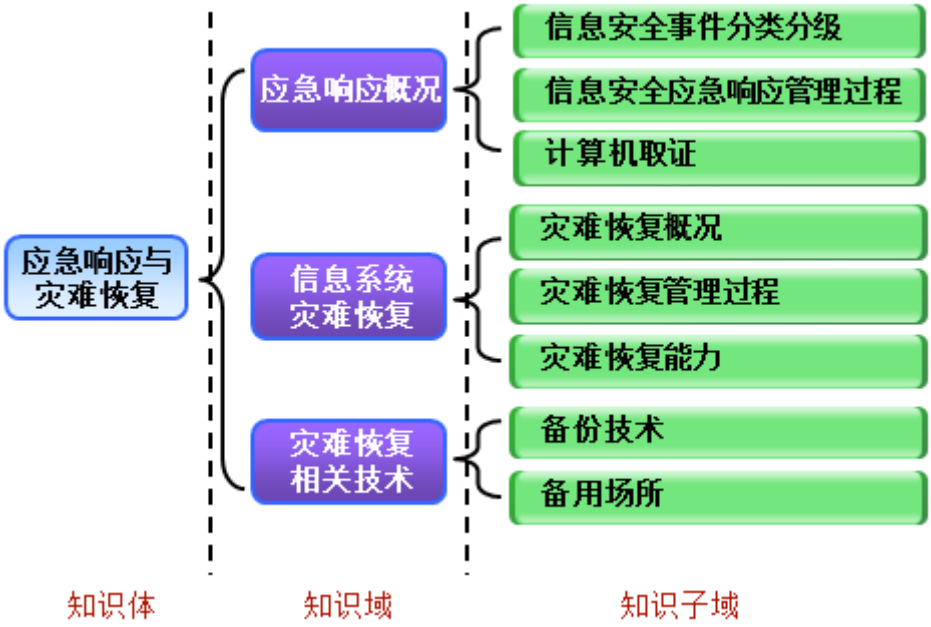

图 4-4：知识体：应急响应与灾难恢复

4.4.1 知识域：应急响应概况

- 知识子域：信息安全事件分类分级
  - ◆ 理解信息安全事件和应急响应的基本概念
  - ◆ 了解国际和我国的信息安全应急响应组织

- ◆ 了解我国信息安全事件应急响应工作的进展情况、政策要求和相关标准
- ◆ 理解我国信息安全事件分类、分级方法

- 知识子域：信息安全应急响应管理过程
  - ◆ 掌握信息安全应急响应阶段方法论
  - ◆ 掌握准备、检测、遏制、根除等应急响应阶段的主要工作内容
  - ◆ 掌握信息安全应急响应计划编制方法
- 知识子域：计算机取证
  - ◆ 了解计算机取证的概念和目的
  - ◆ 了解计算机取证的基本步骤

4.4.2 知识域：信息系统灾难恢复

- 知识子域：灾难恢复概况
  - ◆ 了解灾难恢复的历史和背景、进展情况、政策要求和相关标准
  - ◆ 理解业务连续性管理与灾难恢复相关的基本概念
  - ◆ 了解灾难恢复组织的一般结构和职责
  - ◆ 理解组织应依据自身业务特点制定适宜的灾难恢复战略
  - ◆ 理解编制详细准确的备份策略和恢复步骤文档是成功恢复的基础，理解恢复性测试的重要性
- 知识子域：灾难恢复管理过程
  - ◆ 掌握灾难恢复管理工作的主要内容
  - ◆ 掌握灾难恢复规划过程：灾难恢复需求分析、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
  - ◆ 理解同城和异地灾难备份中心的优缺点
- 知识子域：灾难恢复能力
  - ◆ 掌握国家有关标准对信息系统灾难恢复能力级别的划分
  - ◆ 理解各恢复能力级别对各类灾难恢复资源要素的指标要求
  - ◆ 掌握确定组织自身所需灾难恢复能力级别的方法

4.4.3 知识域：灾难恢复相关技术

- 知识子域：备份技术
  - ◆ 理解全备份、增量备份和差分备份三种备份方式
  - ◆ 理解三种备份方式的特点
- 知识子域：备用场所
  - ◆ 了解冷站、温站、热站、移动站和镜像站等类别的备用场所的概念，了解各类备用场所具有的功能、备战性程度

- 了解由组织拥有或运行维护的专用站点、同内部或外部实体通过签署互惠协议而确定的备用站点、向专业商业组织租用的备用站点在建设和管理方式方面的不同

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；
- 理解如何运用信息安全能力成熟度模型评价和改进信息安全工程能力。

5.1 知识体：信息安全工程基础

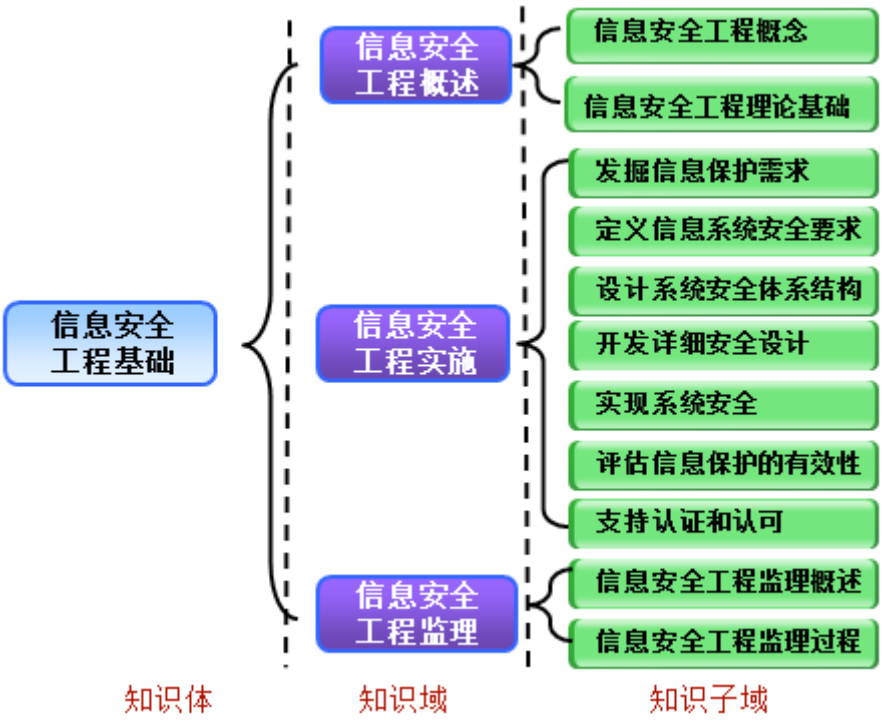

图 5-1：知识体：信息安全工程基础

5.1.1 知识域：信息安全工程概述

- 知识子域：信息安全工程概念
  - ◆ 了解信息安全工程的重要性和意义
  - ◆ 了解信息安全工程的基本原则
- 知识子域：信息安全工程理论基础

- ◆ 了解系统工程基本思想
- ◆ 了解项目管理基本概念和要素
- ◆ 了解质量管理基本概念
- ◆ 理解“能力成熟度模型”基本思想

5.1.2 知识域：信息安全工程实施

- 知识子域： 发掘信息保护需求
  - ◆ 理解 ISSE 的本质和一般过程
  - ◆ 理解确定信息保护需求的重要决定因素及主要工作内容
- 知识子域：定义信息系统安全要求
  - ◆ 了解定义系统安全背景环境、定义安全操作概念等定义信息系统安全要求阶段的主要信息安全工作内容
- 知识子域：设计系统安全体系结构
  - ◆ 理解设计并分析系统安全体系结构、向体系结构分配安全服务等设计系统安全体系结构阶段的主要信息安全工作内容
- 知识子域：开发详细安全设计
  - ◆ 了解进行均衡取舍研究、定义系统安全设计元素等开发详细安全设计阶段的主要信息安全工作内容
- 知识子域：实现系统安全
  - ◆ 理解支持安全实现和集成、支持测试和评估等实现系统安全阶段的主要信息安全工作内容
  - ◆ 了解安全防护措施的部署需要符合总体安全需求和设计方案
- 知识子域：评估信息保护的有效性
  - ◆ 理解前述每一阶段应实施的评估信息保护有效性的工作内容
- 知识子域：支持认证和认可
  - ◆ 了解认证和认可是确保工程质量和安全性的一种保障机制
  - ◆ 了解前述每一阶段应进行的支持认证和认可的活动

5.1.3 知识域：信息安全工程监理

- 知识子域：信息安全工程监理概述
  - ◆ 理解信息安全工程监理工作的意义
  - ◆ 理解信息安全工程监理的一般模型
  - ◆ 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：信息安全工监理程过程

- 了解工程招标阶段监理的目标、监理工作内容和监理重点
- 了解工程设计阶段的监理目标、监理工作内容和监理重点
- 了解工程实施阶段监理的目标、监理工作内容和监理重点
- 了解工程验收阶段的监理目标、监理工作内容和监理重点

5.2 知识体：信息安全工程能力评估

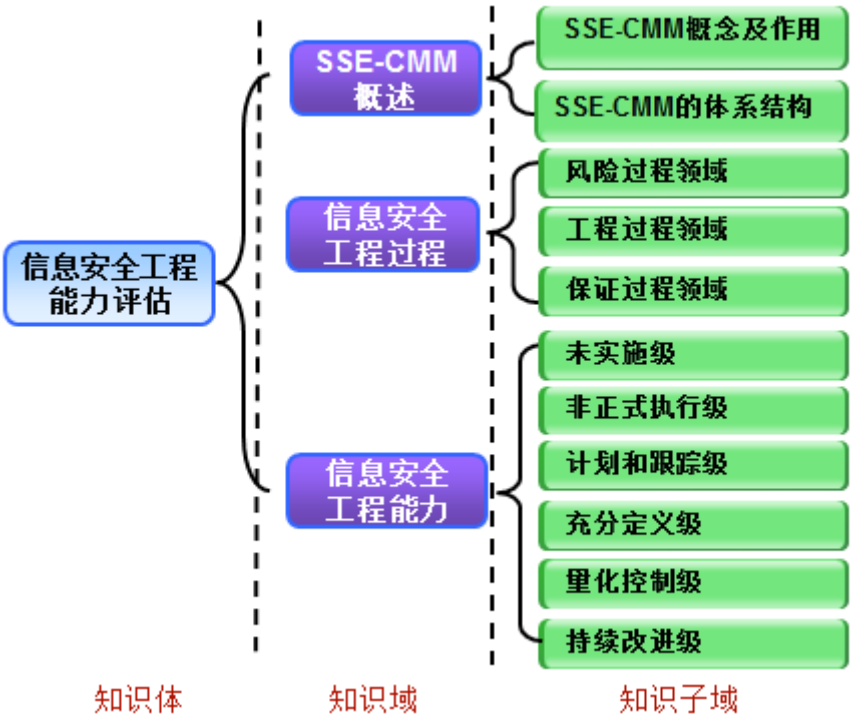

图 5-2：知识体：信息安全工程能力评估

5.2.1 知识域：SSE-CMM 概述

- 知识子域：SSE-CMM 概念及作用
  - 理解 SSE-CMM 的概念及作用
  - 了解 SSE-CMM 的适用范围
- 知识子域： SSE-CMM 的体系结构
  - 理解 SSE-CMM 的二维体系结构
  - 了解域维的组织结构，理解基本实施、过程区域、过程类的概念
  - 了解能力维的组织结构，理解通用实施、公共特征、能力级别的概念

5.2.2 知识域：信息安全工程过程

- 知识子域：风险过程领域
  - ◆ 理解风险过程领域相关活动的目的
  - ◆ 掌握风险过程领域的相关活动和工作内容
- 知识子域：工程过程领域
  - ◆ 理解工程过程领域相关活动的目的
  - ◆ 掌握工程过程领域应实施的过程区域及其基本实施
- 知识子域：保证过程领域
  - ◆ 理解保证过程领域相关活动的目的
  - ◆ 掌握保证过程领域应实施的过程区域及其基本实施

5.2.3 知识域：信息安全工程能力

- 知识子域：未实施级
  - ◆ 理解能力成熟度为未实施级（0 级）的信息安全工程组织和工程过程的含义
- 知识子域：非正式执行级
  - ◆ 理解非正式执行级（1 级）的设计思想
  - ◆ 掌握能力成熟度达到 1 级应具有的公共特征
- 知识子域：计划和跟踪级
  - ◆ 理解计划和跟踪级（2 级）的设计思想
  - ◆ 掌握能力成熟度达到 2 级应具有的公共特征
- 知识子域：充分定义级
  - ◆ 理解充分定义级（3 级）的设计思想
  - ◆ 掌握能力成熟度达到 3 级应具有的公共特征
- 知识子域：量化控制级
  - ◆ 了解量化控制级（4 级）的设计思想
  - ◆ 了解能力成熟度达到 4 级应具有的公共特征
- 知识子域：持续改进级
  - ◆ 了解持续改进级（5 级）的设计思想
  - ◆ 了解能力成熟度达到 5 级应具有的公共特征

第 6 章 知识类：信息安全法规标准

信息安全法律、法规、政策、规章、标准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。通过本部分的学习，学员应当：

- 理解遵循信息安全法律、法规、政策、规章、标准和道德规范的重要性；
- 理解我国重点信息安全法律、法规、政策、规章和标准的有关要求；
- 了解信息安全标准体系及其有关内容；
- 理解 CISP 道德规范，了解通行的有关信息安全道德规范；
- 了解与各自行业和地方相关的法规、政策和标准的要求。

6.1 知识体：信息安全法规与政策

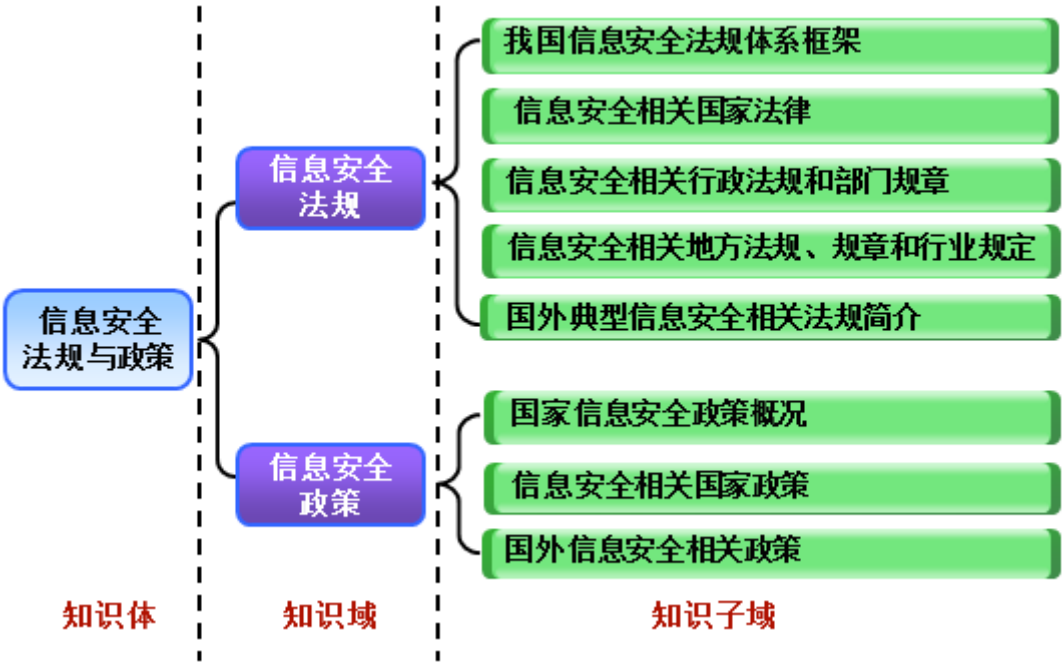

图 6-1：知识体：信息安全法规与政策

6.1.1 知识域：信息安全法规

- 知识子域：我国信息安全法规体系框架
  - 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：信息安全相关国家法律

- ◆ 了解信息保护相关法律
- ◆ 理解国家秘密的概念、基本范围和密级划分，以及保护国家秘密相关法律的要求
- ◆ 理解商业秘密的概念、基本范围，以及保护商业秘密相关法律的要求
- ◆ 理解个人信息的概念、基本范围，以及保护个人信息相关法律的要求
- ◆ 理解网络违法犯罪的概念，了解打击网络违法犯罪相关法律
- ◆ 了解在保护国家秘密、维护公共安全、规范电子签名行为等方面，我国从法律层面明确的信息安全相关工作的主管/监管机构及其具体职权

- 知识子域：信息安全相关行政法规和部门规章
  - ◆ 了解信息安全相关行政法规，掌握涉及信息安全的相关内容
  - ◆ 了解信息安全相关部门规章，掌握涉及信息安全的相关内容
- 知识子域：信息安全相关地方法规、地方规章和行业规定
  - ◆ 了解信息安全相关地方法规，掌握自身所在地方或密切相关地方涉及信息安全的相关内容
  - ◆ 了解信息安全相关地方规章，掌握自身所在地方或密切相关地方涉及信息安全的相关内容
  - ◆ 了解信息安全相关行业规定，掌握自身所在行业或密切相关行业涉及信息安全的相关内容
- 知识子域：国外典型信息安全相关法规简介
  - ◆ 了解美国信息安全相关法规概况

6.1.2 知识域：信息安全政策

- 知识子域：国家信息安全政策概况
  - ◆ 了解国家有关政策提出的加强信息安全保障工作的方针和总体要求
  - ◆ 理解国家有关政策规定的加强信息安全保障工作的主要原则
  - ◆ 理解国家有关政策规定的需要重点加强的信息安全保障工作
- 知识子域：信息安全相关国家政策
  - ◆ 了解信息安全相关国家政策
  - ◆ 理解风险评估、保密管理、应急处理、安全检查和工控安全等涉及信息安全的相关内容

- ◆ 理解信息安全等级保护政策体系，了解信息安全等级保护相关政策
- 知识子域：国外信息安全相关政策
  - ◆ 了解美国信息安全相关政策概况

6.2 知识体：信息安全标准

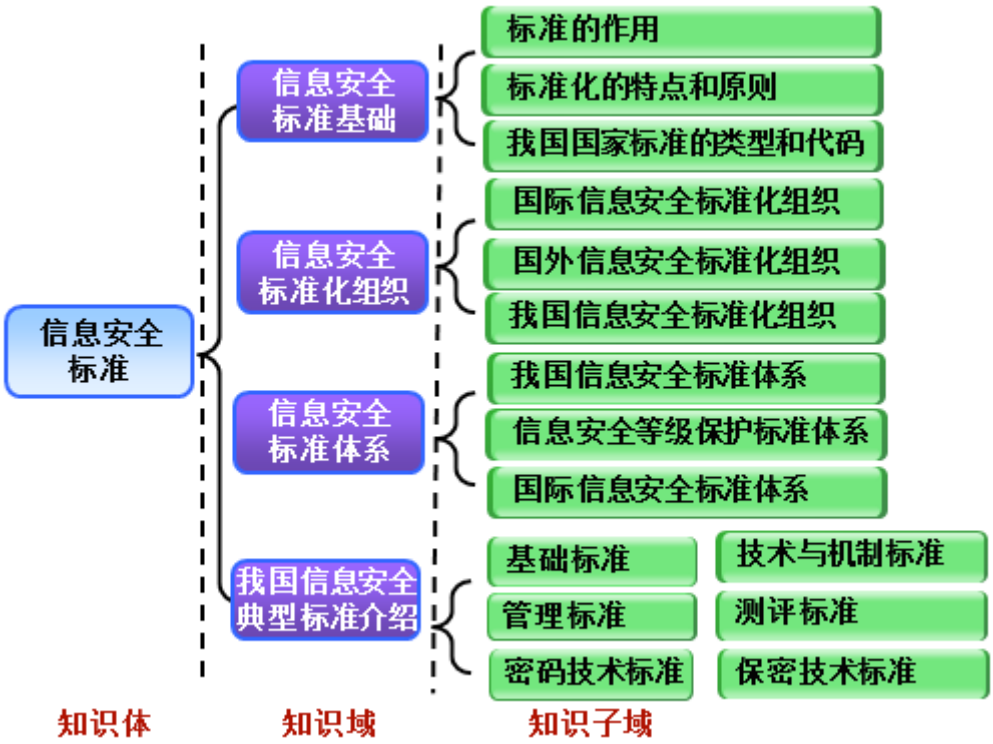

图 6-2 知识体：信息安全标准

6.2.1 知识域：信息安全标准基础

- 知识子域：标准的作用
  - ◆ 理解标准和标准化相关的基本概念
  - ◆ 了解标准的作用
- 知识子域：标准化的特点和原则
  - ◆ 了解标准化的特点
  - ◆ 了解标准化工作应遵循的原则
- 知识子域：我国国家标准的类型和代码
  - ◆ 了解强制性、推荐性和标准化指导性技术文件三类国家标准及其代码

- ◆ 了解各类标准的特点

6.2.2 知识域：信息安全标准化组织

- 知识子域：国际信息安全标准化组织
  - ◆ 了解国际信息安全标准化组织及其工作
- 知识子域：国外信息安全标准化组织
  - ◆ 了解国外典型信息安全标准化组织及其工作
- 知识子域：我国信息安全标准化组织
  - ◆ 了解我国信息安全标准化组织及其工作

6.2.3 知识域：信息安全标准体系

- 知识子域：我国信息安全标准体系
  - ◆ 了解我国信息安全标准体系框架
- 知识子域：信息安全等级保护标准体系
  - ◆ 理解信息安全等级保护标准体系
  - ◆ 理解在信息安全等级保护建设的各阶段应遵循的标准
- 知识子域：国际信息安全标准体系
  - ◆ 了解国际信息安全标准体系框架

6.2.4 知识域：我国信息安全典型标准介绍

- 知识子域：基础标准
  - ◆ 了解已发布的基础标准及其适用范围
- 知识子域：技术与机制标准
  - ◆ 了解已发布的技术与机制标准及其适用范围
- 知识子域：管理标准
  - ◆ 了解已发布的管理标准及其适用范围
- 知识子域：测评标准
  - ◆ 了解已发布的测评标准及其适用范围
  - ◆ 了解《信息技术安全性评估准则》的结构
  - ◆ 理解相关概念（TOE、PP、ST、EAL）
  - ◆ 了解《信息系统安全保障评估框架》的意义和结构
- 知识子域：密码技术标准
  - ◆ 了解已发布的密码技术标准及其适用范围

6.3 知识体：信息安全道德规范

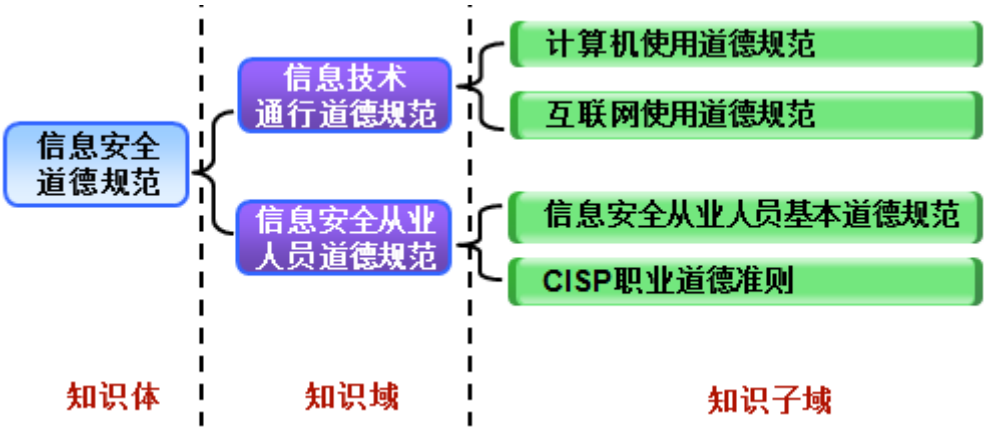

图 6-3 知识体：信息安全道德规范

6.3.1 知识域：信息技术通行道德规范

- 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：互联网使用道德规范
  - ◆ 了解中国互联网协会《文明上网自律公约》的主要内容

6.3.2 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作为社会普通一员应遵守的基本道德规范
- 知识子域：CISP 职业道德准则
  - ◆ 理解《CISP 职业道德准则》