注册信息安全员（CISM）
授权培训讲义

注册信息安全员（CISM）介绍

文件编号：CNITSEC-TBWT-CISM01

版本：1.0

中国信息安全产品测评认证中心

人员培训事业部

发布日期：2006 年 3 月 1 日

©版权 2006—中国信息安全产品测评认证中心

注册信息安全员（CISM）介绍

1 中国信息安全产品测评认证中心（CNITSEC）介绍 1
2 注册信息安全员（CISM）介绍 2
2.1 全面建设信息安全人才体系 3
2.2 注册信息安全员（CISM）介绍 9
2.3 CISM 知识体系大纲介绍 22

1 中国信息安全产品测评认证中心（CNITSEC）介绍

网址：www.itsec.gov.cn

中国信息安全产品测评认证中心是经中央批准成立，国家质检总局授权、代表国家开展信息安全测评认证工作的职能机构，依据国家有关产品质量认证和信息安全管理的法律法规，管理和运行国家信息安全测评认证体系。 中国信息安全产品测评认证中心筹建于 1997 年初，1998 年 7 月以“中国互联网络安全产品测评认证中心”的名称试运行。1998 年 10 月经国家质量技术监督局授权，成立了“中国国家信息安全测评认证中心”。1999 年 2 月,中心及其安全测试实验室分别通过“中国产品质量认证机构国家认可委员会”和“中国实验室国家认可委员会”的认可。同年，国家质量技术监督局正式批准并向社会公告了《中国国家信息安全测评认证管理委员会章程》、《中国国家信息安全测评认证管理办法》、《中国国家信息安全测评认证标志和第一批实施测评认证的信息安全产品目录》等文件。2001 年 5 月，中央编制委员会正式批准认证中心的职能任务、机构和编制，将认证中心正式更名为“中国信息安全产品测评认证中心”，英文为 China Information Technology Security Certification Center，简称 CNITSEC。 中国信息安全产品测评认证中心的主要职能是：

- 对国内外信息安全产品和信息技术进行测评和认证；
- 对国内信息系统和工程进行安全性评估和认证；
- 对提供信息系统安全服务的组织和单位进行评估和认证；
- 对注册信息安全专业人员的资质进行评估和认证。

“中华人民共和国国家信息安全认证”是国家对信息安全技术、产品、信息系统安全质量以及信息安全服务资质、人员资质的最高认可。国家信息安全测评认证活动的技术依据是由中国国家信息安全测评认证管理委员会确认的有关产品质量认证和信息安全管理的国际标准、国家标准、行业标准和其他补充技术要求与技术规范。

2 注册信息安全员（CISM）介绍

随着我国社会信息化进程发展，计算机网络及信息系统在政府机构、企事业单位及社会团体的运作中发挥着越来越重要的作用，信息化水平的提高在带来巨大发展机遇的同时也带来了严峻的挑战。信息安全不仅关系着个人的隐私，也关系着国计民生，乃至整个国家的安全与利益。随着网络攻击、病毒入侵事件日益严重，信息失窃及泄密事件屡有发生，国家把信息安全保障工作迅速提到了一个非常重要的位置。中办发[2003]27 号文件《国家信息化领导小组关于加强信息安全保障工作的意见》中提出了“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，重点强调了信息安全人才培养的重要性。

在这样的大环境下，社会对信息安全人员的需求逐年增加。从国际国内形势分析，当前信息安全领域最突出的问题是：我国信息安全产业发展滞后，信息安全科研和教育滞后，而关键是信息安全人才的极度匮乏。国家间在信息安全领域的竞争，与其说是技术的竞争，不如说是人才的竞争，包括人才素质和规模的竞争。

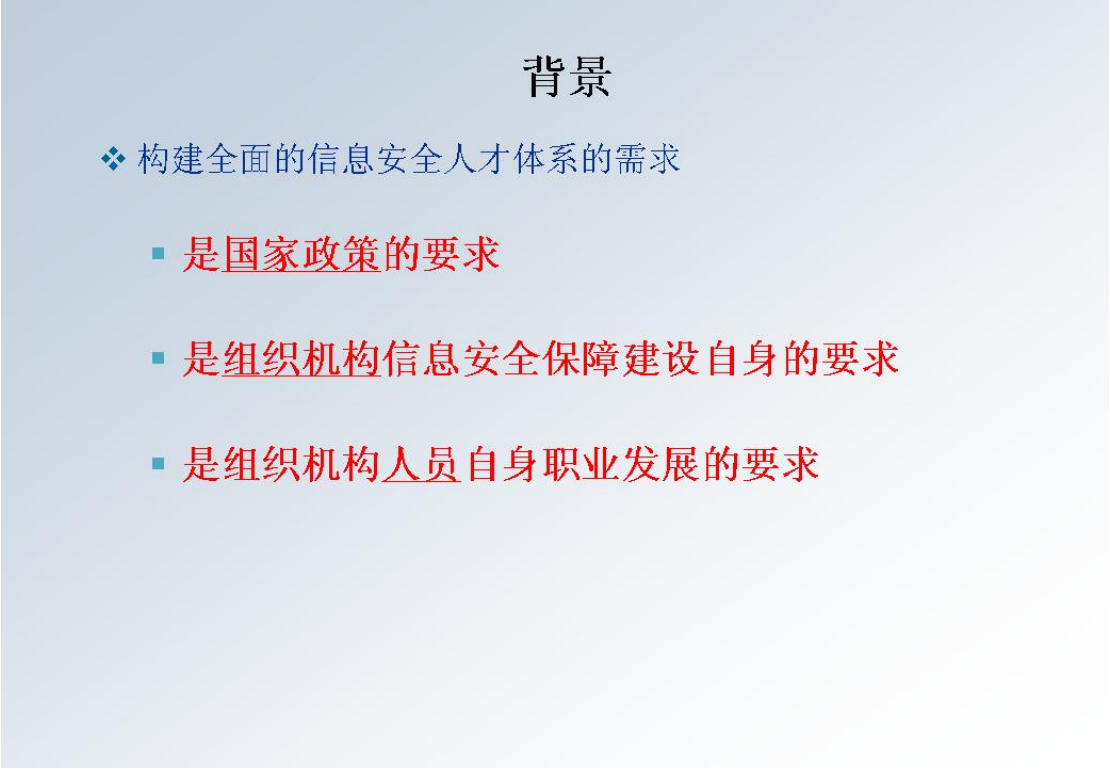
中国信息安全产品测评认证中心从 2002 年启动了“注册信息安全专业人员”（CISP）资质注册。截至目前，已为国家培养了一支近千人的信息安全专业人才队伍，对提高信息安全专业人员的职业道德和技术水平、提升信息安全产业的竞争能力和强化国家信息安全管理发挥了重要作用。中国信息安全产品测评认证中心现推出“注册信息安全员”（Certified Information Security Member，CISM）资质注册，旨在适应我国信息化迅速发展对不同层次、不同水平和不同岗位的信息安全人才的广泛需求，加大对信息安全人才的培养范围和信息安全知识的普及教育力度。

2.1 全面建设信息安全人才体系

在全面建设信息安全人才体系中，介绍了中国信息安全产品测评认证中心的信息安全人才体系战略结构。

背景

构建全面的信息安全人才体系是国家政策、组织机构自身和人员职业发展所共同的需求。



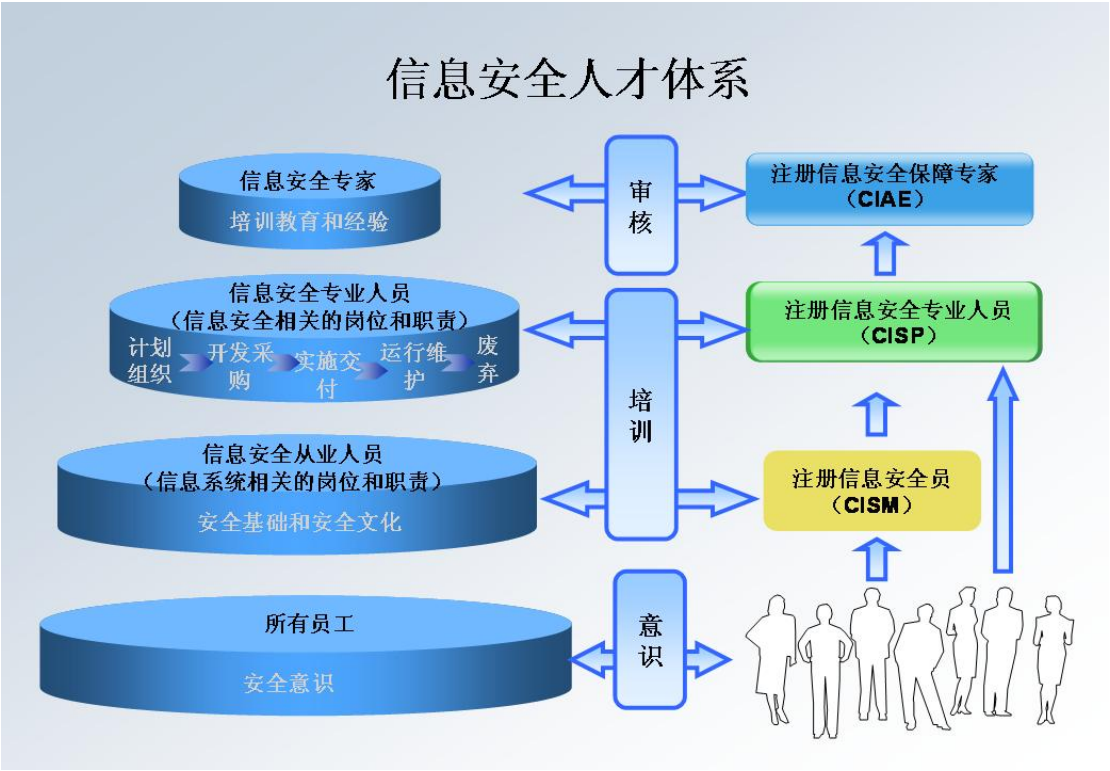
构建全面的信息安全人才体系的需求

- **是国家政策的要求**
  - 中办发[2003]27 号文件《国家信息化领导小组关于加强信息安全保障工作的意见》中提出了“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，重点强调了信息安全人才培养的重要性。
- **是组织机构信息安全保障建设自身的要求**
  - 企事业单位、政府机构等组织机构在信息安全保障建设、信息化建设中，需要有一个完整层次化的信息安全人才队伍以保障其信息安全、保障其信息化建设，从而保障其业务和使命
- **是组织机构人员自身职业发展的要求**

- 作为人员本身，在其工作和职业发展中，需要充实其信息安全保障相关的知识和经验，以更好地开展其工作并为自己的职业发展提供帮助。

信息安全人才体系

对组织机构来说，应建立一个完整的信息安全人才体系。

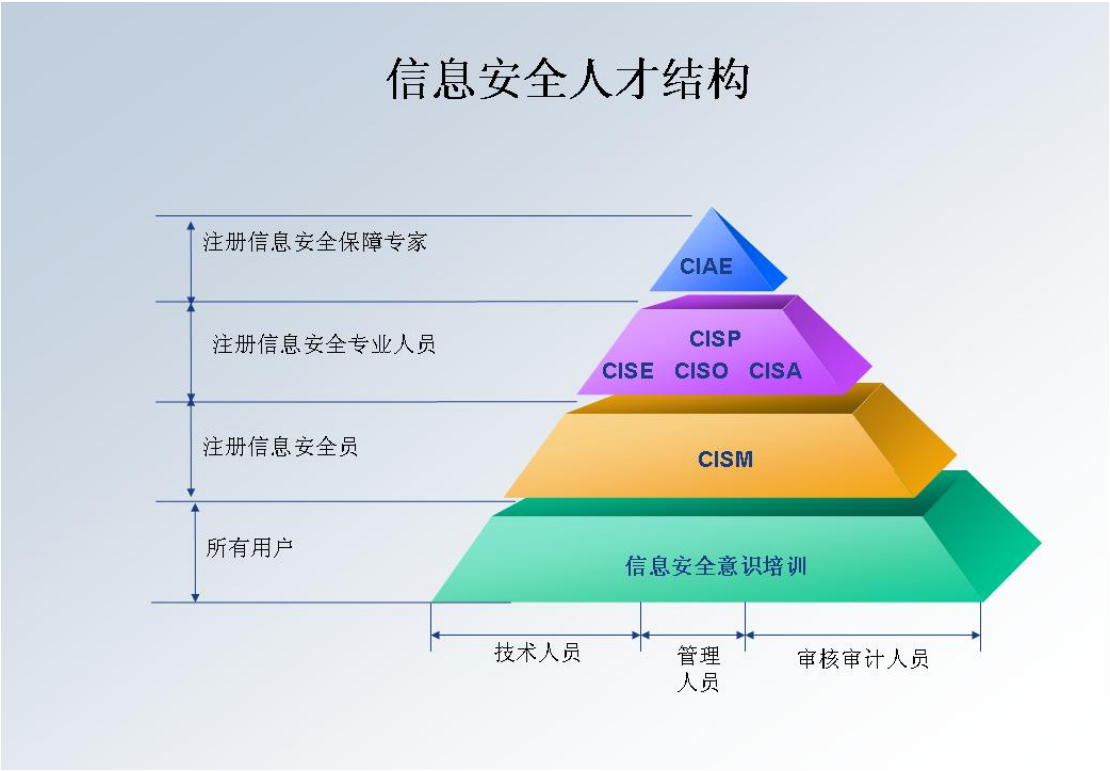


对组织机构来说，应建立一个完整的信息安全人才体系，信息安全人才体系应包括：

- 所有员工：需要进行信息安全保障意识教育，具体可以使用各种海报、组织机构网站上发布相关信息等以增强所有员工的安全意识；
- 对于涉及信息系统的岗位和职责的员工而言，需要进行相应的信息安全保障培训；注册信息安全员（CISM）为这些员工提供了全面的信息安全保障基础知识；
- 对于信息安全专业人员而言，应建立更全面专业的信息安全保障知识和经验；注册信息安全专业人员（CISP）为这些人员提供了信息安全专业知识能力的证明；
- 注册信息安全保障专家（CIAE）是在获得 CISP 基础上得到中国信息安全产品测评认证中心审核认可的信息安全保障领域的专家。

信息安全人才结构

整个信息安全人才结构是一个金字塔型的人才梯队。

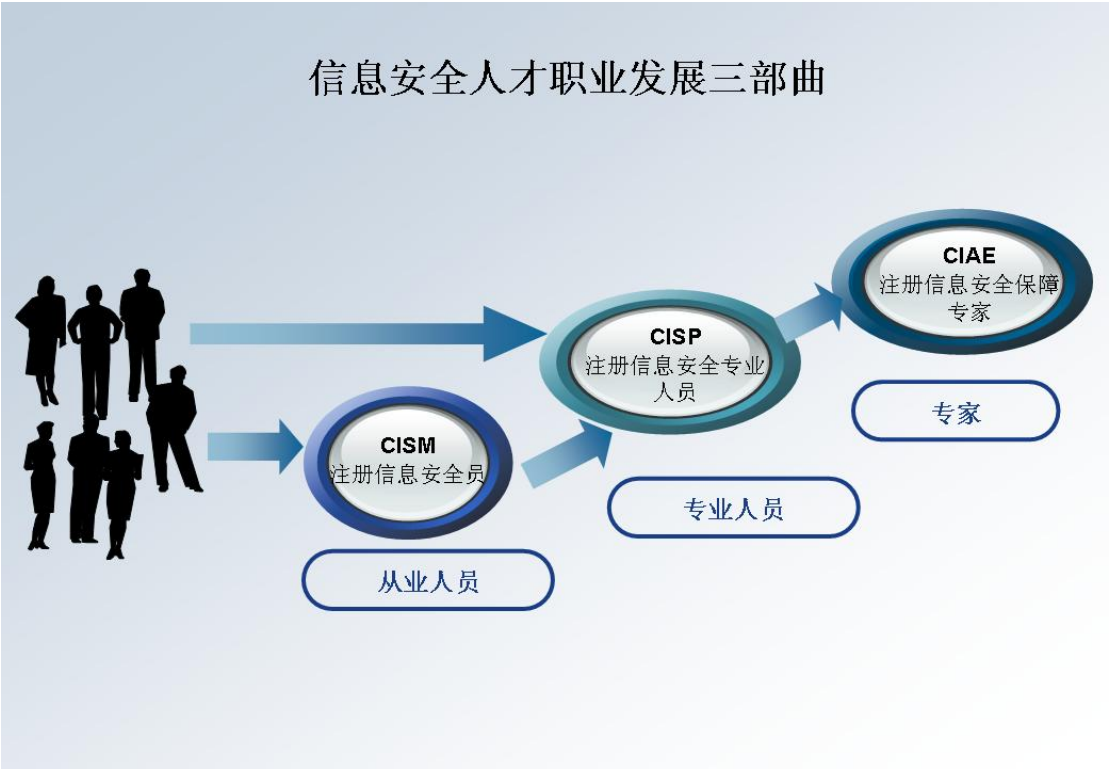


整个信息安全人才结构是一个金字塔型的人才梯队：

- 从纵向来看，人才梯队分为注册信息安全员（CISM）、注册信息安全专业人员（CISP）和注册信息安全保障专家（CIAE）；
- 从横向来看，信息安全人才根据其工作的领域和重点分别有技术、管理、审核审计三个领域和方向。

信息安全人才职业发展三部曲

信息安全专业人员应为其自身的职业发展建立其职业发展的路线。



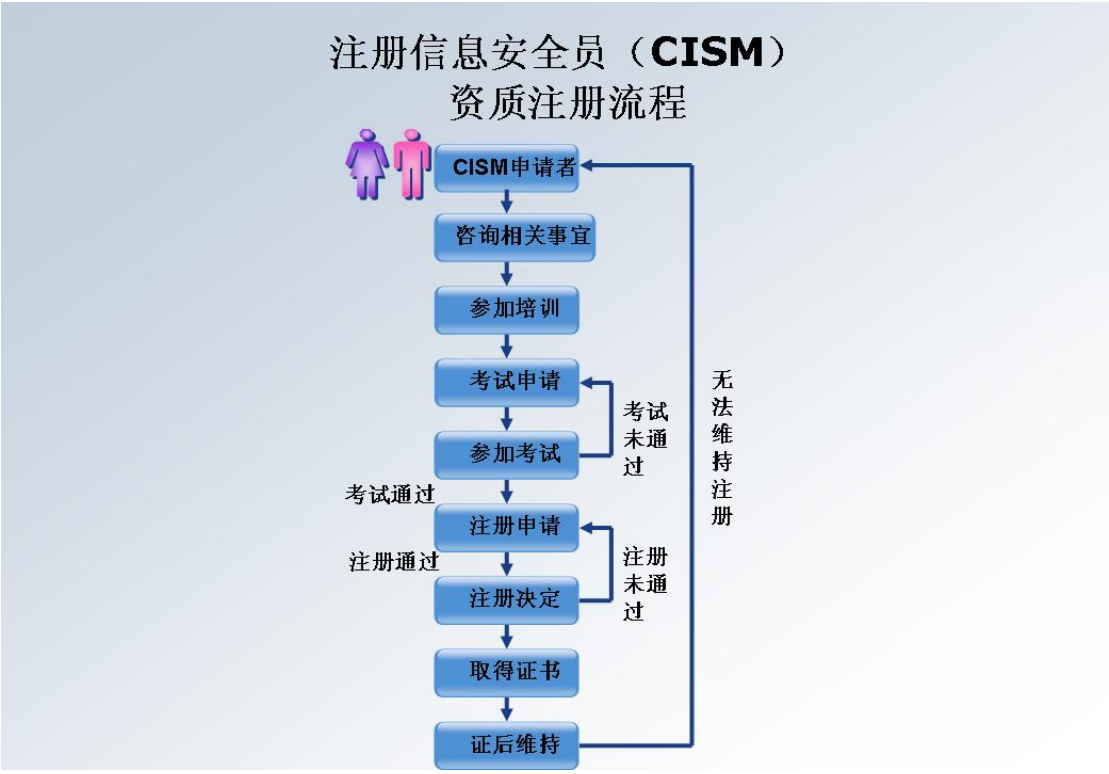
信息安全专业人员应为其自身的职业发展建立其职业发展的路线，信息安全专业人员职业发展三部曲包括 CISM 信息安全从业人员、CISP 信息安全专业人员和 CIAE 信息安全专家。

2.2 注册信息安全员（CISM）介绍

注册信息安全员（CISM）介绍中，介绍了 CISM 的资质注册流程、CISM 知识体系结构、CISM 课程设计、知识体系大纲的特点以及 CISM 的服务等。

CISM 资质注册流程

整个 CISM 资质注册流程包括申请、培训、考试、注册和证后维持等阶段。



CISM 知识体系结构

下图描述了 CISM 知识体系结构的整体。

整个 CISM 知识体系中，共包括 5 个信息安全领域：信息安全保障基础、信息安全标准法规、信息安全技术、信息安全管理和信息安全工程；并进一步分成为 12 知识域。

CISM 的课程设计

下面描述了 CISM 的课程设计和时间安排。

CISM的课程设计

	类别	课程	推荐时间
CISM01	安全保障基础	信息系统安全保障框架	0.5天
CISM02		信息系统安全保障测评	
CISM03	标准法规	信息安全标准	0.5天
CISM04		信息安全法规	
CISM05	安全技术	密码技术和应用	0.5天
CISM06		常见网络安全技术	0.5天
CISM07		恶意代码防护技术	
CISM08		系统和常见应用安全	0.5天
CISM09	安全管理	信息安全管理基础	0.5天
CISM10		信息安全管理技术	0.5天
CISM11	安全工程	安全工程过程和实践	0.5天
CISM12		安全工程监理咨询和实践	
-	复习	复习迎考	0.5天
-	考试	考试	0.5天

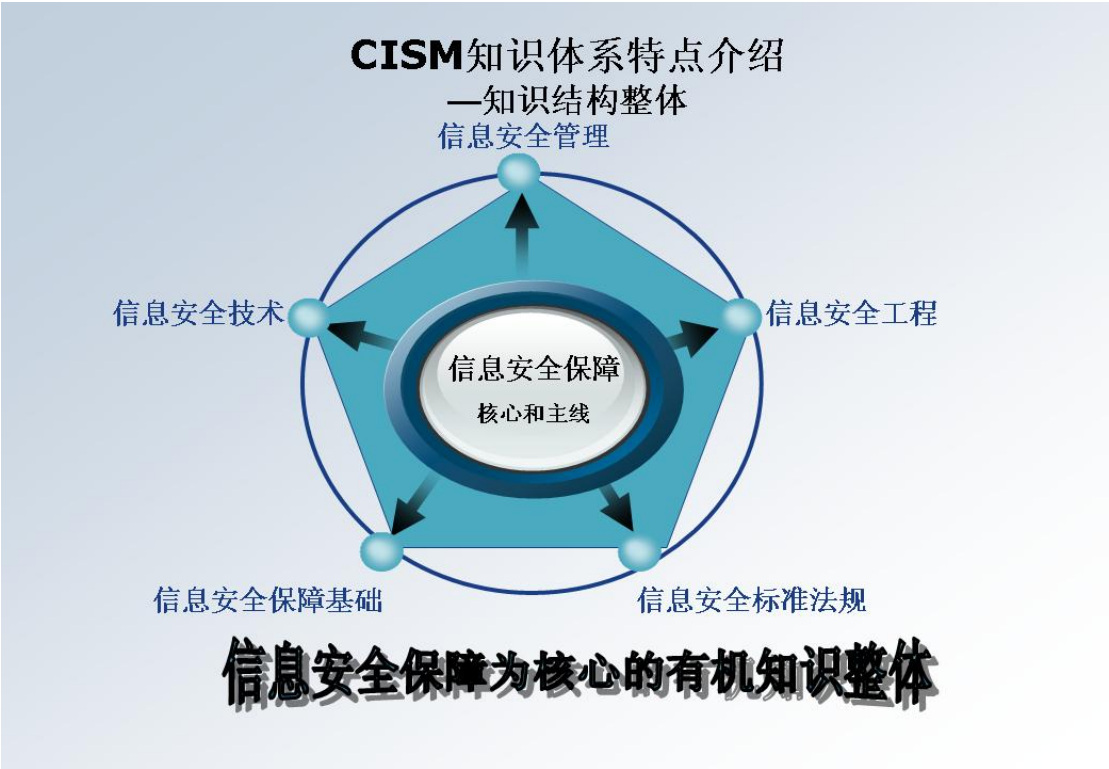
CISM 课程设计覆盖了 CISM 知识体系大纲的内容，整个培训课程设计为 5 天，其中最后一天为复习和考试。

- **CISM01 信息系统安全保障框架**：介绍信息安全保障框架的概念和内容。
- **CISM02 信息系统全保障测评**：介绍信息安全产品、系统、人员和服务测评的概念和内容。
- **CISM03 信息安全标准**：介绍国际/国内信息安全管理、技术、工程等领域主要标准的关系和内容。
- **CISM04 信息安全法规**：介绍信息安全相关的国内法律法规。
- **CISM05 密码技术和应用**：介绍密码技术的基本知识，以及公钥基础设施（PKI）和数字签名等的应用。
- **CISM06 常见网络安全技术**：介绍网络安全基本概念，并包括对防火墙、入侵检测、VPN 等常见网络安全技术。

- **CISM07：恶意代码防护技术：**介绍各种恶意代码的基本概念和防护技术。
- **CISM08：系统及常见应用安全：**介绍 Windows 操作系统等主流操作系统，以及 Web、邮件、DNS 等常见应用安全。
- **CISM09：信息安全管理基础：**介绍信息安全管理的基础知识。
- **CISM10：信息安全管理技术：**介绍风险管理、灾难恢复管理的基础知识和实践考虑。
- **CISM11：安全工程过程和实践：**介绍信息安全工程过程的基础知识和实践考虑。
- **CM12：安全工程监理资源和实践：** 介绍信息安全工程监理咨询的基础知识和实践考虑。
- 答疑和复习，准备考试
- 正式考试

CISM 知识体系特点介绍（一）

CISM 知识体系的特点之一是以保障为核心的有机知识整体。

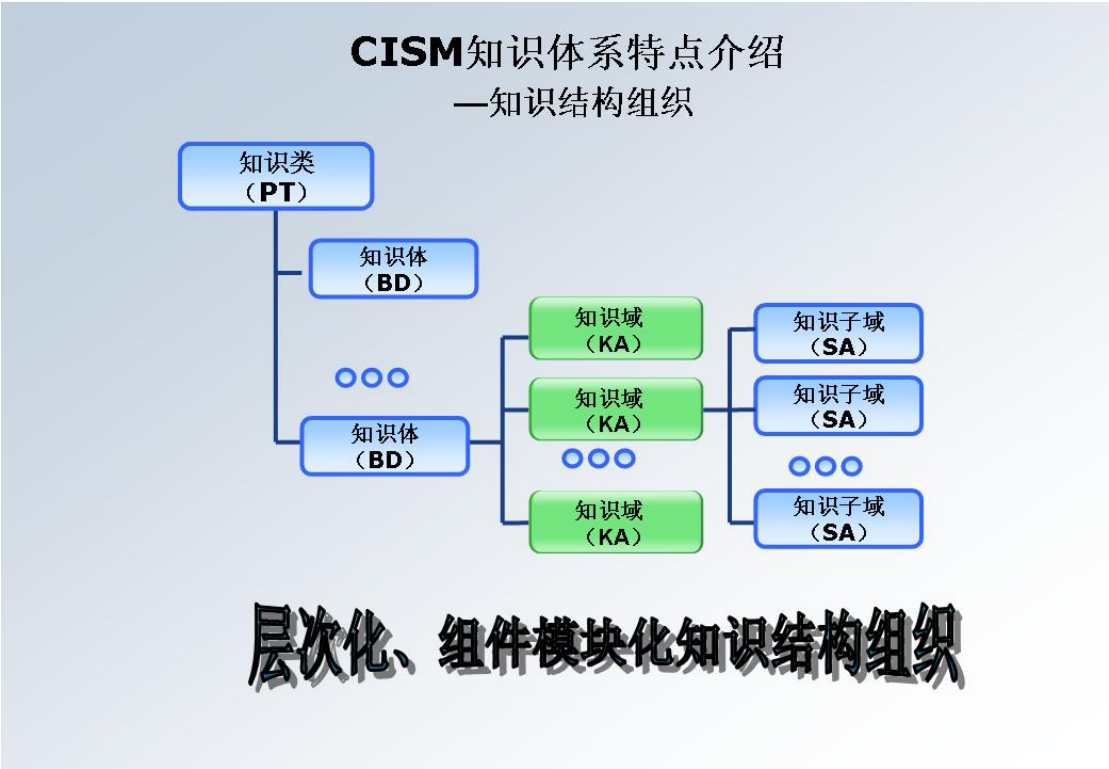


CISM 为信息安全从业人员建立了完整的、厂商中立的信息安全保障基础知识。

从 CISM 知识体系结构的设计来看，CISM 知识体系是以信息安全保障（IA）为核心和主线，覆盖信息安全管理、信息安全技术、信息安全工程、信息安全保障基础和信息安全标准法规五部分的有机知识整体。

CISM 知识体系特点介绍（二）

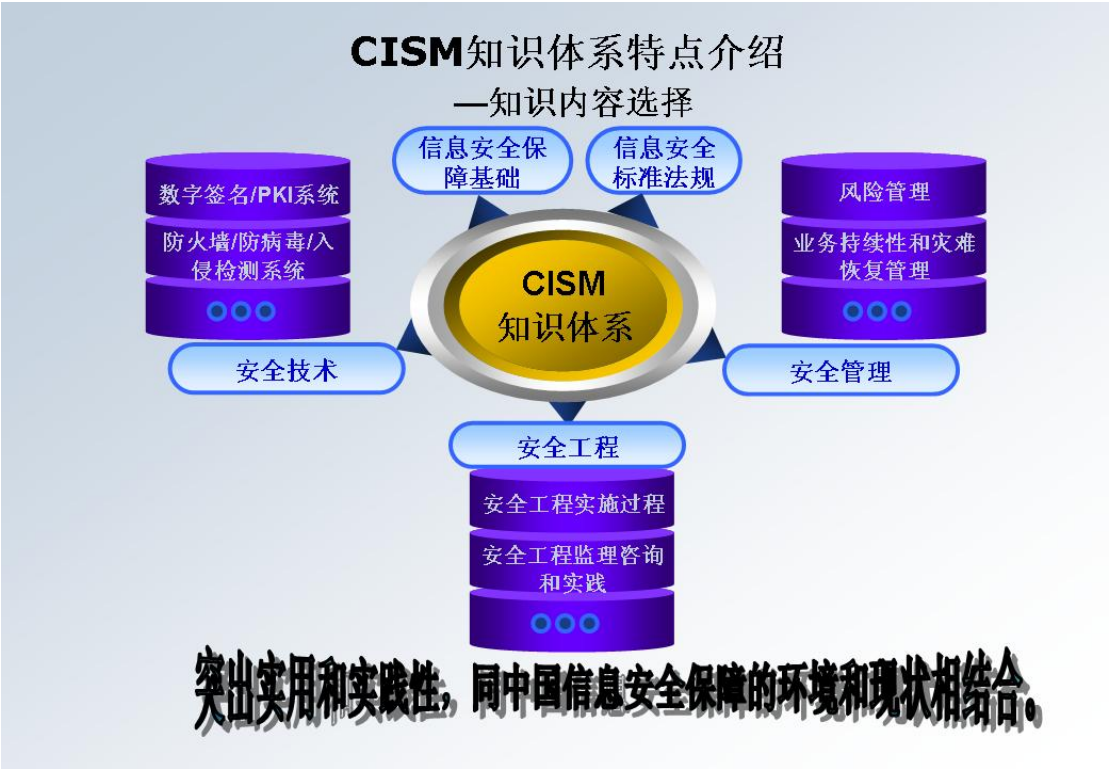
CISM 知识体系结构采用层次化的结构。



从 CISM 的知识结构组织来看，采用层次化、组件模块化的知识结构组织，更加严谨、科学地将知识结构化，方便了 CISM 培训学习人员根据知识域来掌握 CISM 的知识要点。

CISM 知识体系特点介绍（三）

在知识内容选择上，CISM 更强调实用和实践性。



从 CISM 的知识内容选择来看，CISM 知识体系结构更突出了实用和实践性，并充分同我国信息安全保障的环境和现状相结合。例如：在安全技术领域中，包含了对数字签名、PKI 系统、防病强、防病毒和入侵检测系统等信息安全保障领域里最常见和最重要的信息安全技术和产品的讨论；在安全管理领域里，包含了同国家政策相关的风险管理、灾难备份（即业务持续性和灾难恢复管理）的讨论以及在我国国情下的具体实践考虑等的介绍和讨论。

CISM 培训服务和管理——授权培训机构

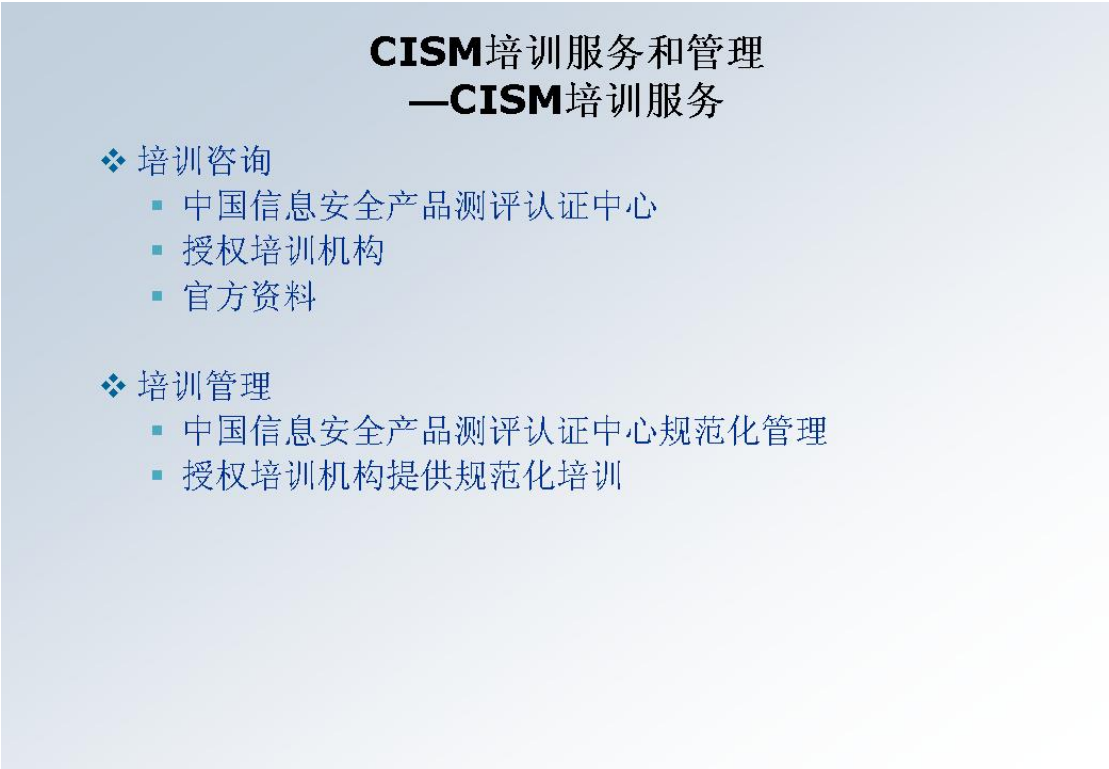
CISM培训服务和管理
—授权培训机构

- 请查阅中心网站 www.itsec.gov.cn 以获得授权培训机构最新名单及联系方式。

- 北京天融信网络安全技术有限公司
- 联想计算机系统技术服务有限公司
- 北京冠群金辰软件有限公司
- 北京清华万博网络技术股份有限公司
- 广东省颐东通信公司
- 北京江南科友科技有限公司
- 深圳市安络科技有限公司
- 上海金诺网络安全技术发展股份有限公司
- 吉首大学张家界学院
- 北京世纪互联信息系统有限公司
- 北京启明星辰信息技术有限公司
- 北京银长城信息技术有限公司
- 北京中贸技术培训中心有限公司
- 中国信息安全产品测评认证中心云南测评中心
- 上海颐东通信公司
- 北京思源新创信息安全资讯有限公司

CISM 培训服务和管理——培训服务

中心依据 ISO 9000 建立了完善的质量管理体系。



- 培训咨询：可向中国信息安全产品测评认证中心和授权培训机构基辛咨询，具体咨询方式包括：
  - 中心网站和电话咨询
  - 授权机构网站和电话咨询
  - 官方资料：CISM 宣传彩页、CISM 申请资料
- 培训管理
  - 中国信息安全产品测评认证中心规范化管理
    - 统一规范的授权培训机构和培训教师管理
    - 统一规范的知识体系大纲
    - 统一规范的培训教材和培训讲义
  - 授权培训机构提供规范化培训

CISM 培训服务和管理——CISM 培训服务

CISM培训服务和管理
—CISM培训服务

- 考试和注册
  - 中心负责考试的管理
    - 严格的考试管理规章制度和管理
    - 考试安排
      - 根据授权培训机构需要和申请，提供CISM考试
      - 中心网站发布定期的考试日期和地点
    - 考试依据：知识体系大纲、培训讲义和培训教材为主
  - 中心负责注册的管理
    - 注册依据：中心发布的注册管理文件
    - 提供注册发布等服务

CISM 培训服务和管理——CISM 注册发布

中心为通过 CISM 注册的人员提供向社会公众发布的服务。

CISM 注册信息信息安全员的服务

本幻灯片描述了中心所提供的其他注册人员后续服务。

CISM培训服务和管理
—CISM注册信息安全员的服务

- 中心为注册信息安全员提供以下服务
  - CISM注册发布和进入中心人才库，供企业、政府机构等公开查询
  - 中心优先向中国信息产业商会信息安全产业分会的成员单位和相关企事业单位、政府机构提供推荐
  - 提供《国家信息安全测评认证》杂志
  - 优先参与中心所举办的各类信息安全专业会议和论坛
  - 。。。

2.3 CISM 知识体系大纲介绍

信息安全保障基础

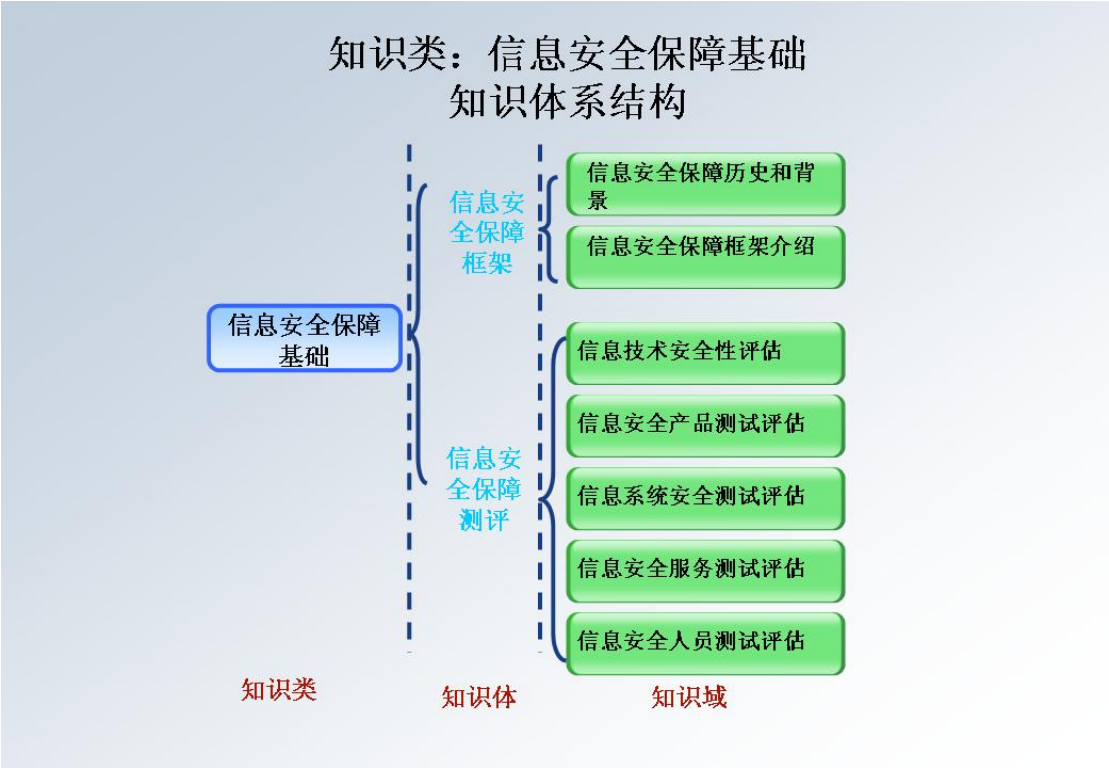
在注册信息安全员（CISM）知识体系的五个知识类中，信息安全保障基础以及信息安全标准和法律法规是注册信息安全员知识体系结构的基础，其中信息安全保障基础知识类为注册信息安全员（CISM）的所有人员提供了信息安全保障整体知识的背景知识和基础知识。

信息安全保障基础知识类中，主要描述了信息安全保障框架、信息安全保障测评的基础知识。通过对信息安全保障基础知识类的学习和研究，信息安全专业人员就可以理解和掌握信息安全保障建设和评估的整体概念和知识，并将帮助信息安全员建立信息安全整个知识体系的基础。

整个信息安全保障基础知识类（PT）包括信息安全保障框架和信息安全保障测评两个知识体（BD），并进一步细分为七个知识域：

- 信息安全保障框架：包括信息安全保障历史和背景、信息安全保障框架两个知识域；
- 信息安全保障测评：包括信息技术安全性评估、信息安全产品测试评估、信息系统安全测试评估、信息安全服务测试评估和信息安全人员测试评估五个知识域。

PT：信息安全保障基础知识类



BD（知识体）：信息安全保障框架

信息安全体系知识类共包括两个知识域：

- KA（知识域）：信息安全保障历史和背景
  理解信息安全保障的背景和历史；
  理解信息安全保障的定义、模型和含义。
- KA（知识域）：信息安全保障框架
  理解和掌握信息安全保障框架的内容、结构和含义；
  理解和掌握信息安全保障框架同组织机构的实际信息安全保障建设工作的结合。

BD（知识体）：信息安全保障测评

- KA（知识域）：信息技术安全性评估
  - SA（知识子域）：信息技术安全评估的历史和发展
    理解和掌握信息技术安全性评估准则发展的背景、历史和关系；
  - SA（知识子域）：可信计算机系统评估准则

理解和掌握可信计算机系统评估准则（TCSEC）以及彩虹系列的内容和含义；

- SA（知识子域）：IT 安全性评估通用准则（CC）

  理解和掌握信息技术安全性评估主则（CC）的内容和含义。

- KA（知识域）：信息安全产品测试评估

  理解信息安全产品测试评估的标准、内容、流程和方法。

- KA（知识域）：信息系统安全测试评估

  理解信息系统安全测试评估的标准、内容、流程和方法。

- KA（知识域）：信息安全服务测试评估

  理解信息安全服务测试评估的标准、内容、流程和方法。

- KA（知识域）：信息安全人员测试评估

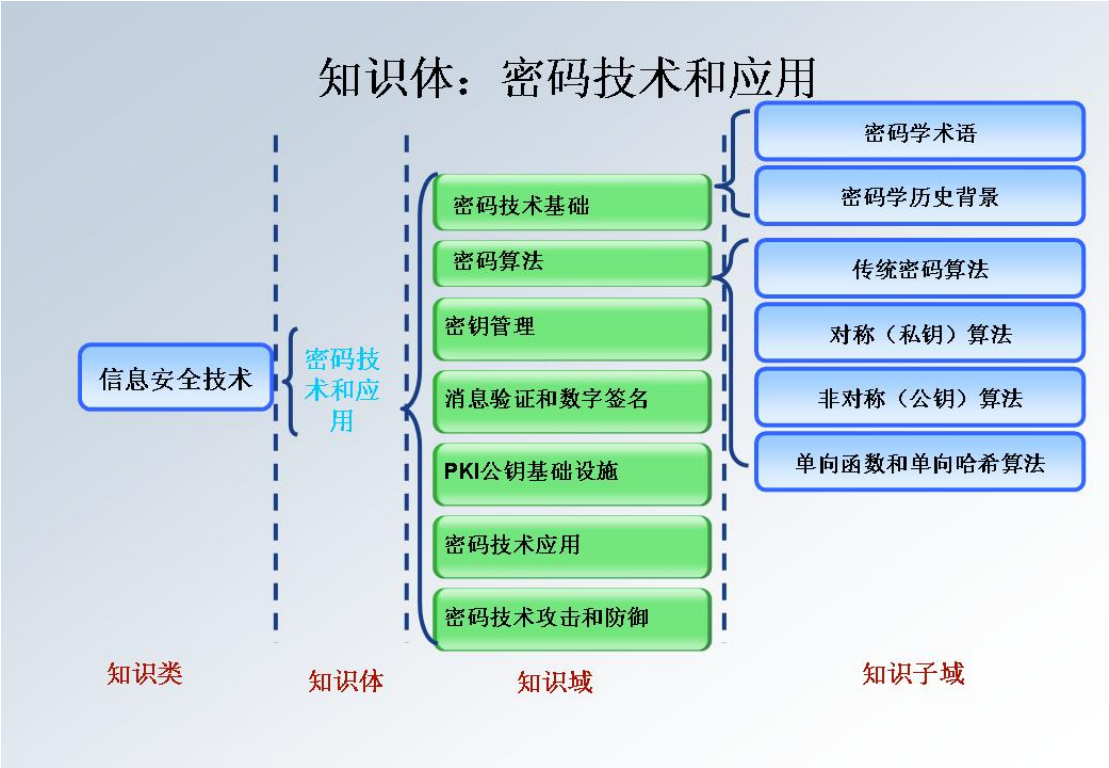
  理解信息安全人员测试评估的标准、内容、流程和方法。

信息安全技术

在注册信息安全员（CISM）的五个知识类中，信息安全技术、信息安全管理和信息安全工程是信息安全保障的具体保障实现领域。学习和掌握信息安全技术知识类，将帮助我们学习掌握和实践信息安全技术相关的知识和技能，并将其运用在信息安全技术保障的工作和学习之中。

信息安全技术知识类分为密码技术和应用、常见网络安全技术、恶意代码防护技术以及系统和常见应用安全四个知识体。

BD：密码技术和应用知识体



BD（知识体）：密码技术和应用

- KA（知识域）：密码技术基础
  - SA：密码学术语
    理解密码学的基本定义和术语；
  - SA：密码学历史背景
    理解密码学的发展阶段和历史。
- KA（知识域）：密码算法
  - SA：传统密码算法
    理解置换和替换传统密码算法。
  - SA：对称（私钥）算法
    理解对称算法的基本概念；
    理解常见的对称算法（DES、3DES、Blowfish、IDEA、RC 系列和 AES 等）。
  - SA：非对称（公钥）算法
    理解非对称算法的基本概念；

理解常见的非对称算法（MH、RSA、ECC、DH、DSA、Elgema 等）。

- SA：单向函数和单向哈希算法

  理解解单向函数、单向哈希算法等基本概念；

  理解常见的单向哈西算法（MD 系列、RSA、HAVAL 和 HMAC 等）。

- KA（知识域）：密钥管理

  理解密钥管理的基本概念

- KA（知识域）：消息验证和数字签名

  理解消息验证、数字签名的原理和应用；

- KA（知识域）：PKI 公钥基础设施

  理解 PKI 公钥基础设施的基本原理和应用。

- KA（知识域）：密码技术应用

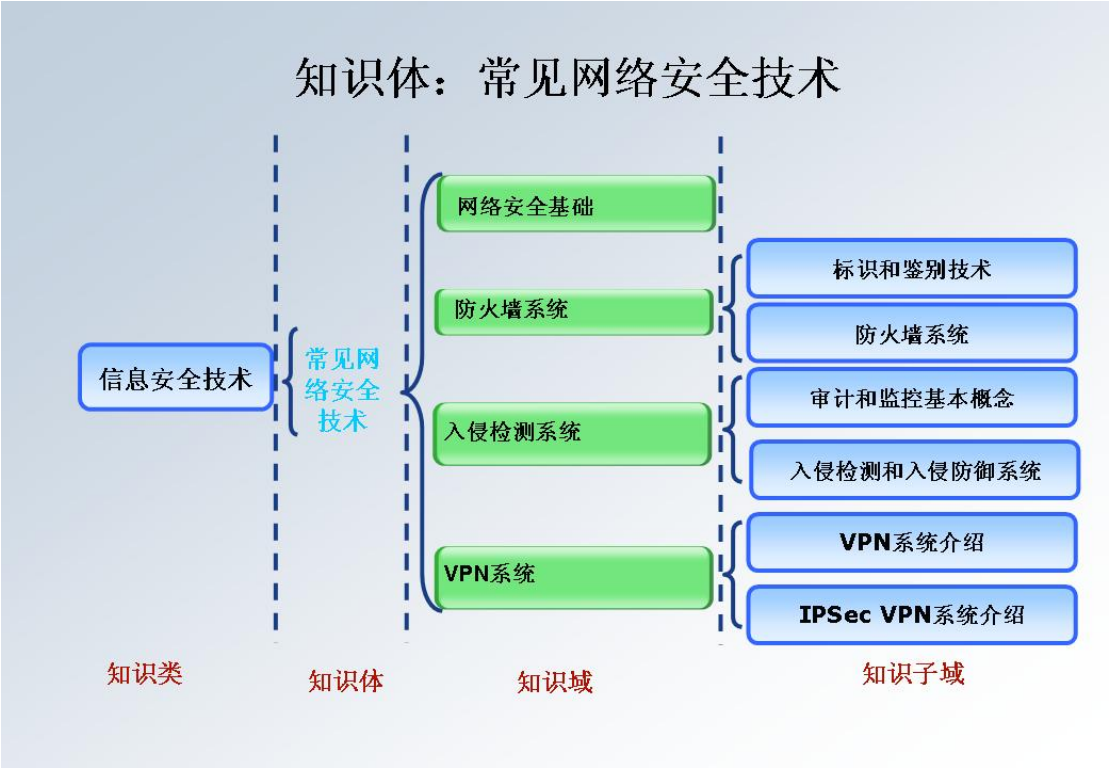
  理解密码技术在 OSI 和 TCP/IP 中的应用基础；

- KA（知识域）：密码技术攻击和防御

  理解密码技术攻击和防御的基本概念；

  理解特定的密码攻击算法（生日攻击等）。

BD：常见网络安全技术知识体



BD（知识体）：常见网络安全技术

- KA（知识域）：网络安全基础
  理解网络技术的基础知识；
  理解深度防御网络安全体系的知识和应用。
- KA（知识域）：防火墙系统
  - SA：标识和鉴别技术
    理解标识和鉴别的定义和基本概念；
  - SA：防火墙系统
    理解入侵检测和入侵防御系统的基本概念；
    理解入侵检测和入侵防御系统的分类和应用。
- KA（知识域）：入侵检测系统
  - SA：审计和监控基本概念
    理解审计和监控的基本概念。
  - SA：入侵检测和入侵防御系统
    理解入侵检测和入侵防御系统的基本概念；

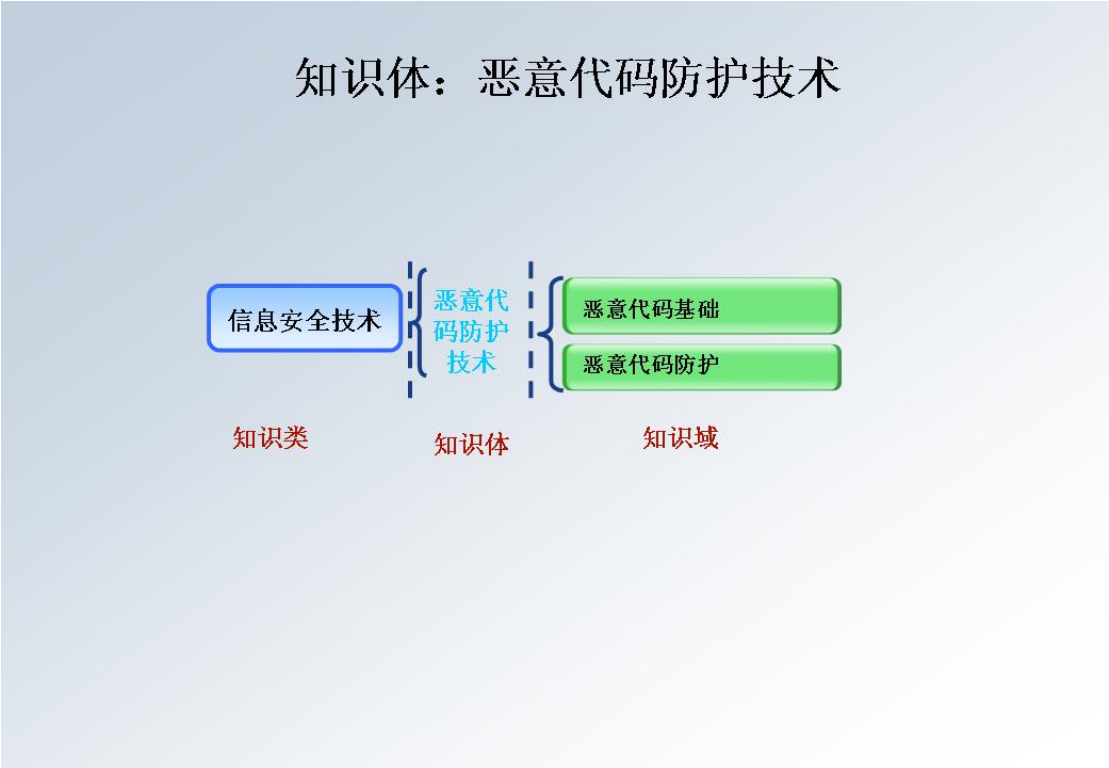
理解入侵检测和入侵防御系统的分类和应用。

- KA（知识域）：VPN 系统
  - SA：VPN 系统介绍

    理解各种 VPN 技术的分类和基本概念
  - SA：IPSec VPN 系统介绍

    理解 IPSec VPN 的标准、基本概念和应用

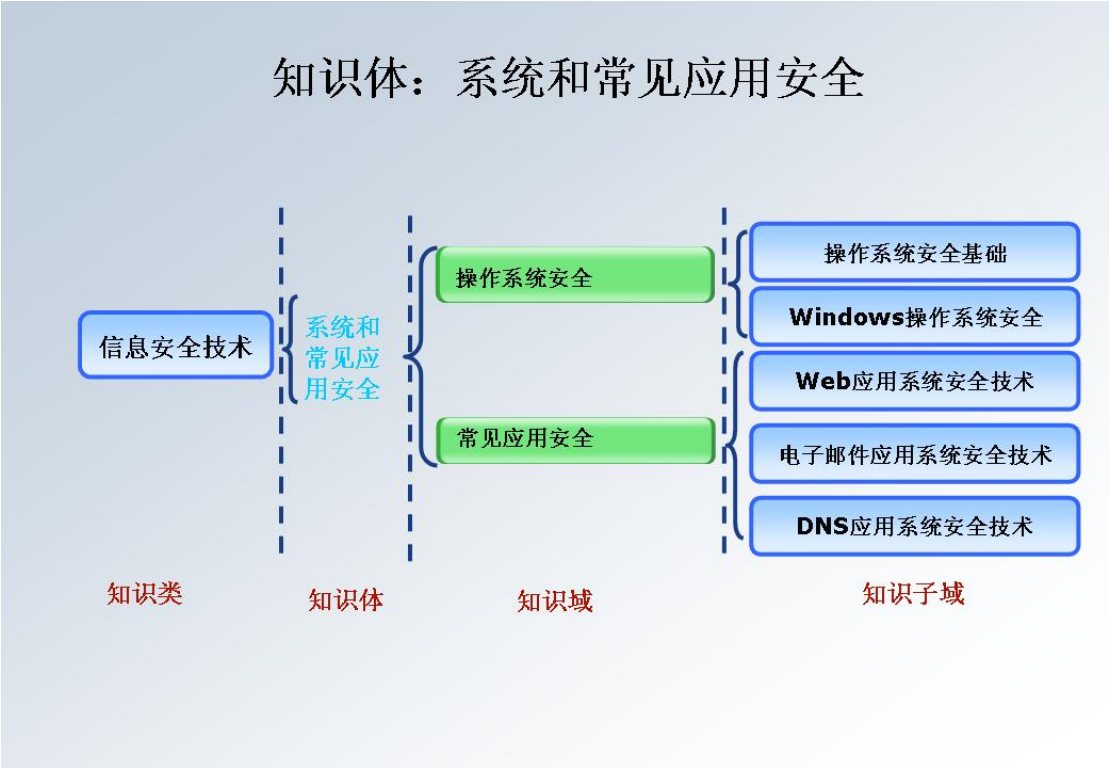
BD：恶意代码防护技术知识体



BD（知识体）：恶意代码防护技术

- KA（知识域）：恶意代码基础
  理解病毒/蠕虫/特洛伊木马等恶意代码的基本概念和原理；
- KA（知识域）：恶意代码防护
  理解恶意代码的攻击过程和防护技术。

BD：系统和常见应用安全知识体



BD（知识体）：系统和常见应用安全

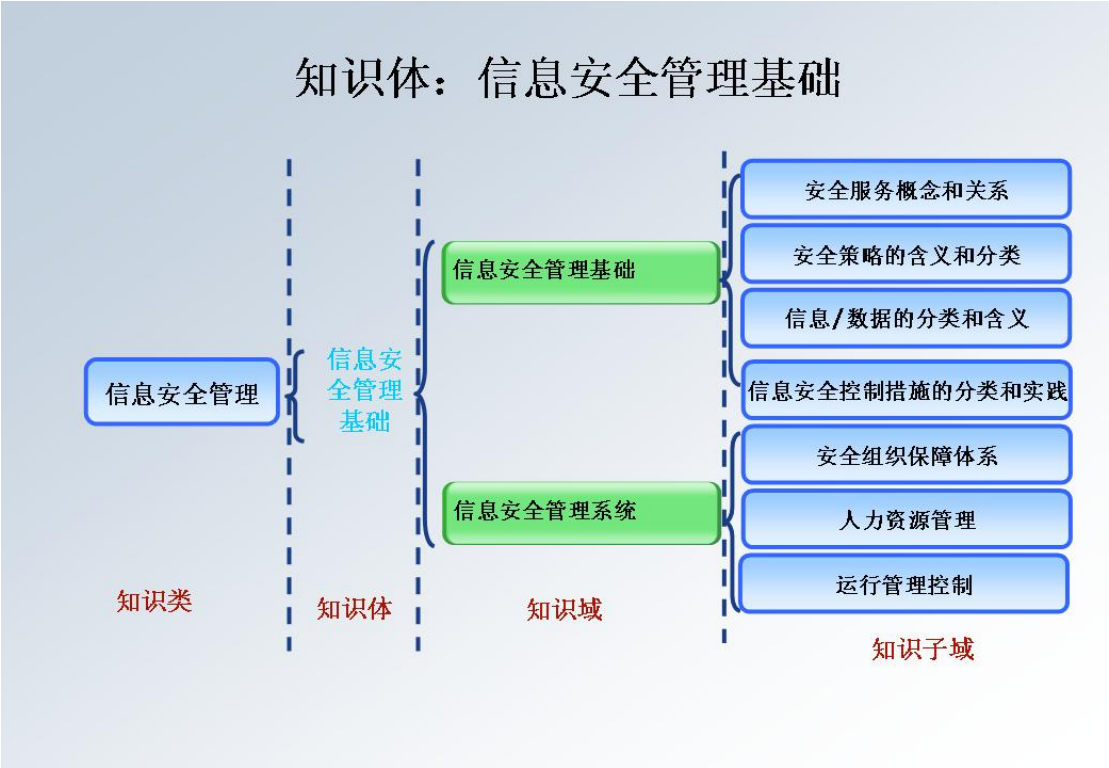
- KA（知识域）：操作系统安全
  - SA：操作系统安全基础
    理解操作系统的基本原理和基本安全技术。
  - SA：Windows 操作系统安全技术
    理解 Windows 操作系统的基本原理、安全技术和实践。
- KA（知识域）：常见应用安全
  - SA：Web 应用系统安全技术
    理解 Web 应用系统的基本原理、结构和相关安全技术。
  - SA：电子邮件应用系统安全技术
    理解电子邮件的基本原理、结构和相关安全技术。
  - SA：DNS 应用系统安全技术
    理解 DNS 的基本原理、结构和相关安全技术。

信息安全管理

在注册信息安全员（CISM）的五个知识类中，信息安全技术、信息安全管理和信息安全工程是信息安全保障的具体保障实现领域。学习和掌握信息安全管理知识类，将帮助我们学习掌握和实践信息安全管理的相关知识和技能并运用在信息安全管理保障的工作和学习之中。

信息安全管理知识类分为信息安全管理基础、安全管理技术两个知识体和五个知识域。

BD：信息安全管理基础知识体



BD（知识体）：安全管理基础

- 知识域（KA）：信息安全管理基础
  - SA：安全服务概念和关系
    理解 CIA（保密性、完整性和可用性）和可追究性、抗抵赖性的概念和关系。
  - SA：安全策略的含义和分类
    理解安全策略概念、含义；
    理解策略制定的方法；
    理解策略文件的分类。
  - SA：信息/数据的分类和含义
    理解信息/数据的分类方法、内容和含义。
  - SA：信息安全控制措施的分类和实践
    理解信息安全控制措施的不同分类方法和具体实践。
- 知识域（KA）：信息安全管理系统
  - SA：安全组织保障体系

理解安全组织体系结构，以及相关岗位和职责。

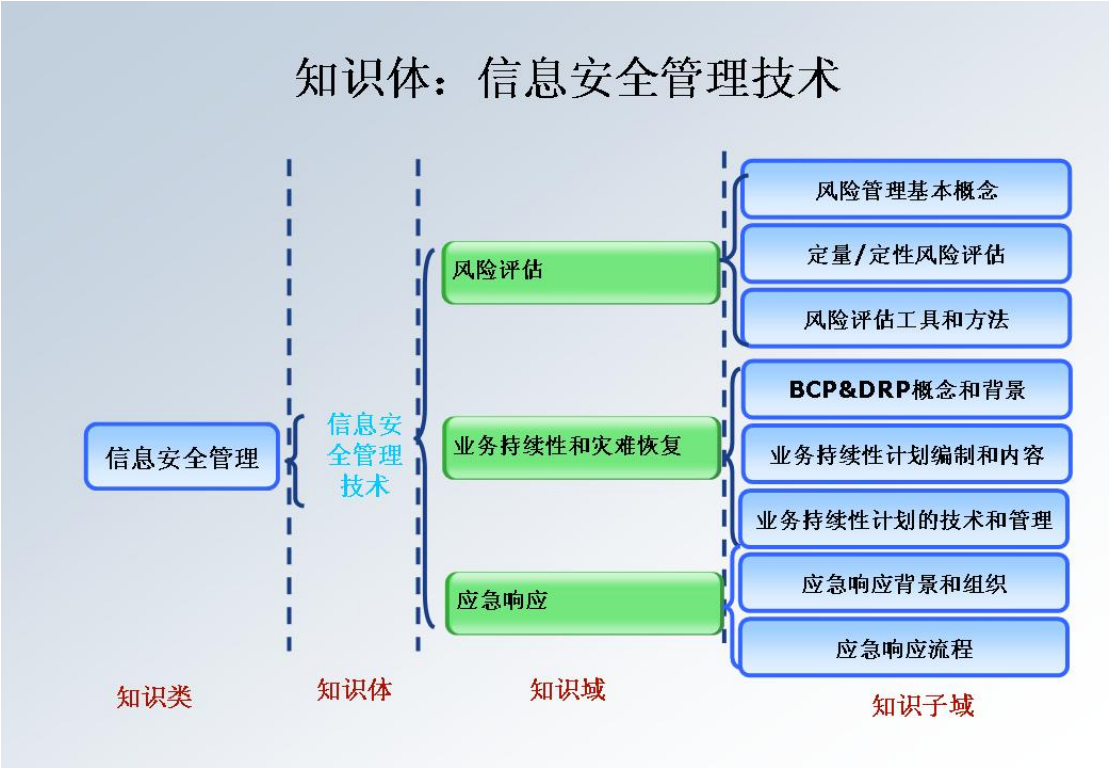
- SA：人力资源管理

  理解员工入职、培训、修假、解聘等相关的安全管理。

- SA：运行管理控制

  理解职责分离、岗位轮换和安全意识等安全运行管理的原则和实践。

BD：信息安全管理技术知识体



BD（知识体）：安全管理技术

- 知识域（KA）：风险评估
  - SA：风险管理基本概念
    理解风险管理的概念、内容和步骤；
    理解风险管理的要素（威胁/脆弱性/资产/影响）。
  - SA：定量和定性风险评估
    理解定量和定性风险评估的区别；
    理解定量风险评估的流程、方法和内容；
    理解定性风险评估的流程、方法和内容。
  - SA：风险评估工具和方法
    理解风险评估相关的各种工具和方法。
- 知识域（KA）：业务持续性计划和灾难恢复计划
  - SA：BCP&DRP 概念和背景
    理解灾难恢复计划/业务持续性计划的概念、区别和含义。
  - SA：业务持续性计划的编制和内容

理解业务持续性计划编制的过程和步骤。

理解业务持续性计划本身的内容。

- SA：业务持续性计划的技术和管理

  理解业务持续性计划相关的技术，包括备份（全备份/增量备份/差分备份等）和外站存储（热战/冷战/温站/移动站）、磁盘技术（RAID技术）等技术；

  理解业务持续性计划相关的管理，包括软件托管、互惠协议等；

  理解业务持续性和灾难恢复的分类和指标（包括 SHARE 七级分级、RPO/RTO 概念）等。

- 知识域（KA）：应急响应
  - SA：应急响应背景和组织

    理解应急响应的背景知识和相关组织机构。
  - SA：应急响应流程

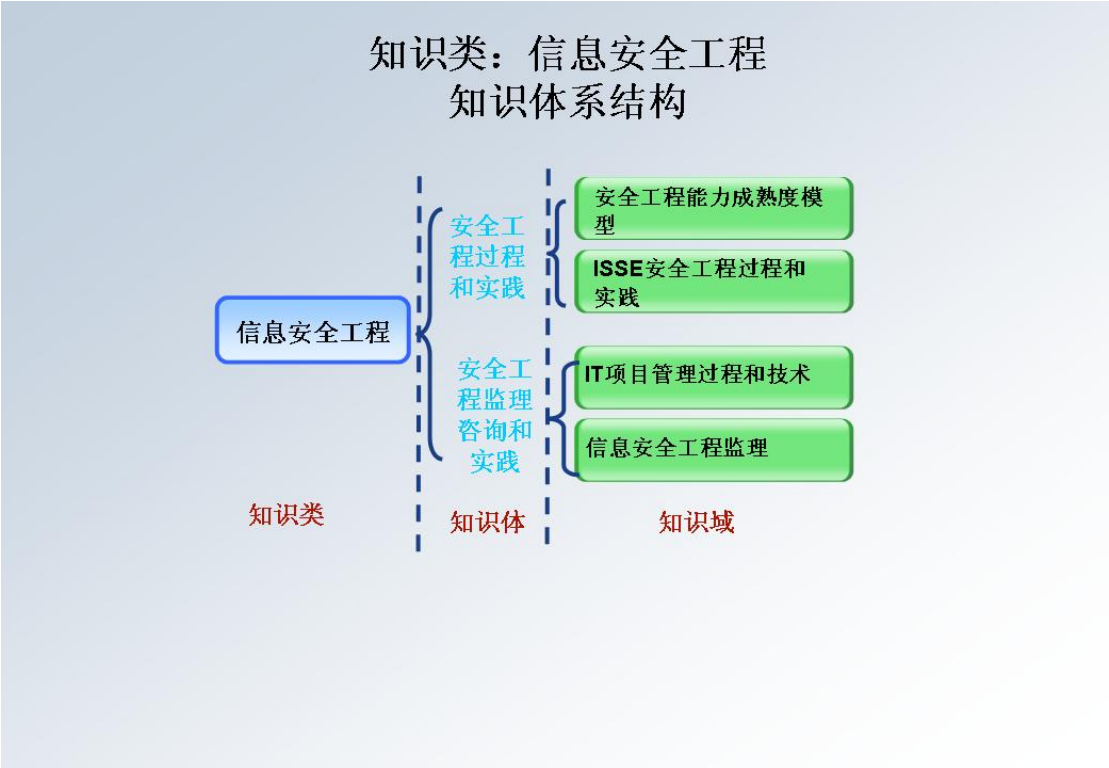
    理解应急响应的流程和方法。

信息安全工程

在注册信息安全员（CISM）的五个知识类中，信息安全技术、信息安全管理和信息安全工程是信息安全保障的具体保障实现领域。学习和掌握信息安全工程知识类，将帮助我们学习掌握和实践信息安全工程的相关知识和技能并运用在信息安全工程保障的工作和学习之中。

信息安全工程知识类分为安全工程过程和实践以及安全工程监理咨询和实践两个知识体和四个知识域。

PT：信息安全工程知识类



BD（知识体）：安全工程过程和实践

- 知识域（KA）：安全工程能力成熟度模型
  理解信息系统安全工程能力成熟度模型（SSE-CMM，即 ISO/IEC 21827）的基本概念。
- 知识域（KA）：ISSE 安全工程过程和实践
  理解信息系统安全工程 ISSE 的基本概念以及需求分析过程等的实践。

BD（知识体）：安全工程监理咨询和实践

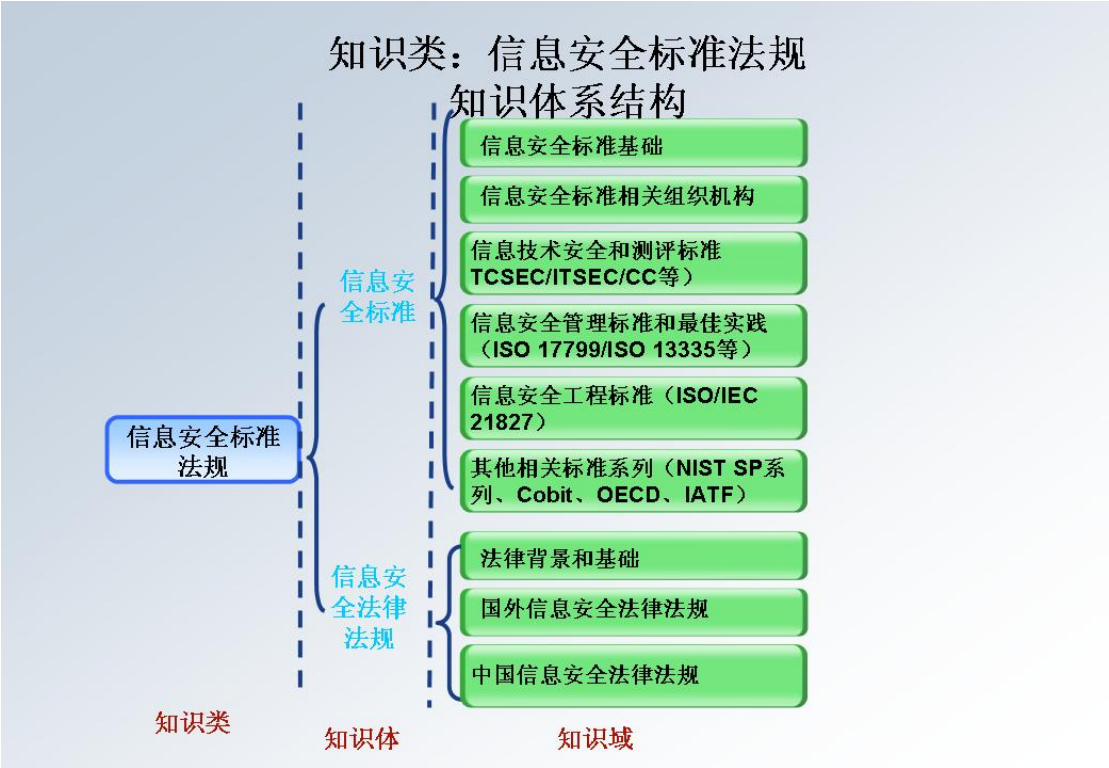
- 知识域（KA）：IT 项目管理过程和技术
  理解 IT 项目管理过程以及项目管理相关的技术，例如：PERT 技术等。
- 知识域（KA）：信息安全工程监理
  理解信息安全工程监理的过程和具体内容。

信息安全标准法规

在注册信息安全员（CISM）知识体系的五个知识类中，信息安全体系和模型以及信息安全标准和法律法规是注册信息安全员知识体系结构的基础，其中信息安全标准和法律法规是信息安全专业所必须了解的通用基础知识和法律法规基础。注册信息安全员（CISM）的所有人员都必须学习和掌握信息安全标准和法律法规知识类的相关知识。

信息安全标准和法律法规知识类（PT）包括信息安全标准和信息安全法律法规两个知识体（BD）。

PT：信息安全标准法规知识类



BD（知识体）：信息安全标准

- KA（知识域）：信息安全标准基础
  理解标准化的基本原则。
- KA（知识域）：信息安全相关标准组织机构
  理解同信息安全标准相关的组织机构和相关标准，包括国际 ISO/IEC JTC1 SC27 工作组、欧洲、美国、德国等国际、区域、国家等相关制定信息安全标准的组织机构及其相关标准。
- KA（知识域）：信息技术安全和测评标准
  理解信息技术测评标准的历史和发展（TCSEC/ITSEC/CPCSEC/CC 等）；
  理解桔皮书（TCSEC）标准的内容；
  理解通用准则（ISO/IEC 15408 idt GB/T 18336）的结构和内容；
  理解 IATF 深度防御技术框架。
- KA（知识域）：信息安全管理标准和最佳实践
  理解 ISO/IEC 17799，ISO/IEC 13335 等主要信息安全管理标准。

- KA（知识域）：信息安全工程标准和最佳实践
  理解 ISO/IEC 21827（SSE-CMM）等主要信息安全工程标准。
- KA（知识域）：其他相关标准
  理解 NIST SP 系列、Cobit、OECD、IATF 等相关标准、最佳实践和指南。

BD（知识体）：信息安全法律法规

- KA（知识域）：法律背景和基础
  理解学习法律的背景意义以及国际法律体系分类等背景知识。
- KA（知识域）：国外信息安全法律法规
  理解国外（主要是美国）相关的信息安全法律法规。
- KA（知识域）：中国信息安全法律法规

理解国内相关的信息安全法律法规和政策。