注册信息安全员（CISM）

知识体系大纲

文件编号：CNITSEC-TBCP-306

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 15 日

信息安全保障参考文件

类别

本文件为中国信息安全产品测评认证中心（CNITSEC）人员培训事业部指南类文件。

咨询及索取

关于中国信息安全产品测评认证中心信息安全人员培训相关的文件，请与中国信息安全产品测评认证中心人员培训事业部处接洽。在中国信息安全产品测评认证中心网址：www.itsec.gov.cn 上可获取本文件，也可从中国信息安全产品测评认证中心人员培训事业部处获得本文的电子文本。

版权

联系信息

关于中国信息安全产品测评认证中心（CNITSEC）信息安全人员培训相关的更多信息，请与中国信息安全产品测评认证中心（CNITSEC）人员培训事业部处联系：

联系方式：中国信息安全产品测评认证中心人员培训事业部

地址：北京市海淀区西三环北路 27 号北科大厦 9 层

邮编：100089

传真：010-68462942

电子邮件：training@itsec.gov.cn

目录

目录.....II
注册信息安全员知识体系介绍.....1
1 注册信息安全员（CISM）知识体系概述.....2
1.1 CISM 资质证书介绍.....2
1.2 CISM 知识体系介绍.....2
1.2.1 概述.....2
1.2.2 CISM 知识体系框架结构介绍.....4
1.2.3 CISM 的课程设计.....6
2 知识类：信息安全保障基础.....8
2.1 概述.....8
2.2 原理说明.....9
2.2.1 概述.....9
2.2.2 知识体：信息安全保障框架.....9
2.2.3 知识体：信息安全保障测评.....10
2.3 知识体系大纲.....10
2.3.1 BD（知识体）：信息安全保障框架.....10
2.3.2 BD（知识体）：信息安全保障测评.....11
3 知识类：信息安全技术.....12
3.1 概述.....12
3.2 原理说明.....12
3.2.1 概述.....12
3.2.2 知识体：密码技术和应用.....13
3.2.3 知识体：常见网络安全技术.....13
3.2.4 知识体：恶意代码防护技术.....13
3.2.5 知识体：系统和常见应用安全.....13
3.3 知识体系大纲.....13
3.3.1 BD（知识体）：密码技术和应用.....13
3.3.2 BD（知识体）：常见网络安全技术.....14
3.3.3 BD（知识体）：恶意代码防护技术.....15
3.3.4 BD（知识体）：系统和常见应用安全.....15
4 知识类：信息安全管理.....16
4.1 概述.....16
4.2 原理说明.....16
4.2.1 概述.....16

4.2.2 知识体：安全管理基础 17
4.2.3 知识体：安全管理技术 17
4.3 知识体系大纲 17
4.3.1 BD（知识体）：安全管理基础 17
4.3.2 BD（知识体）：安全管理技术 18
5 知识类：信息安全工程 20
5.1 概述 20
5.2 原理说明 20
5.2.1 概述 20
5.2.2 知识体：安全工程过程和实践 21
5.2.3 知识体：安全工程监理咨询和实践 21
5.3 知识体系大纲 21
5.3.1 BD（知识体）：安全工程过程和实践 21
5.3.2 BD（知识体）：安全工程监理咨询和实践 21
6 知识类：信息安全标准和法律法规 22
6.1 概述 22
6.2 原理说明 22
6.3 知识体系大纲 23
6.3.1 BD（知识体）：信息安全标准 23
6.3.2 BD（知识体）：信息安全法律法规 23

注册信息安全员知识体系介绍

注册信息安全员知识体系介绍中将介绍本次注册信息安全员（CISM）考试大纲的结构和内容。

本部分包含以下章节：

- 第 1 章 注册信息安全员（CISM）知识体系概述
- 第 2 章 知识类：信息安全保障基础
- 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

1 注册信息安全员（CISM）知识体系概述

1.1 CISM 资质证书介绍

“注册信息安全员”，英文为 Certified Information Security Member，简称 CISM。注册信息安全员是有关信息安全企业、信息安全咨询服务机构、信息安全测评认证机构（包含授权测评机构）、社会各组织、团体、大专院校、企事业单位有关信息系统（网络）建设、运行和应用管理的技术部门（含标准化部门）的信息安全员，具备信息安全员的资质和能力，系经中国信息安全产品测评认证中心实施国家认证。

有关“注册信息安全员”（简称 CISM）的更详细的相关资料，请查阅网址 www.itsec.gov.cn。

1.2 CISM 知识体系介绍

1.2.1 概述

本文所提供的 CISM 知识体系大纲是我们这几年在信息安全保障领域学习、研究和实践的成果。注册信息安全员知识体系大纲主要是基于我们以下信息安全保障建设和评估的理论和实践工作的总结：

- **信息安全保障测评工作实践的总结**。中国信息安全产品测评认证中心（www.itsec.gov.cn）是经中央批准成立、国家质量监督检验检疫总局授权、代表国家开展信息安全测评认证工作的职能机构，依据国家授权对外开展信息安全产品、信息系统安全、信息安全服务资质和注册信息安全专业人员的测评认证业务。在中心多年的信息安全保障测评工作实践中，我们从信息安全保障的评价评估角度进行了大量的实践，在实践中我们不断了解和总结我国信息安全保障建设工作中信息安全人才建设的经验和教训，并将信息安全人才建设中所普遍存在的人才知识体系结构、信息安全保障工作中所关注的热点、不足之处以及实践的要求进行归纳总结，综合至我们这次所编制的注册信息安全员知识体系大纲中。
- **信息安全保障建设咨询工作实践的总结。**在中心所开展的四项测评业务的基础之上，为了履行我们在国家信息安全保障建设中的职责和义务，中心也开展了大量的国家部委等国家重要信息基础设施的安全保障建设和咨询工作。在国家信息安全保障建设的咨询工作中，例如在金财、金税等国家重要信息基础设施的安全保障建设工作中，我们从信息安全保障建设的第一线积累了大量的经验，并将这些经验进行总

结和归纳，综合至注册信息安全员的知识体系大纲中，以帮助信息安全保障相关的人员能够更有效、高效地学习、理解和开展其信息安全保障建设工作。

- **信息安全保障理论研究工作的总结。**中国信息安全产品测评认证中心从成立起，就致力于信息安全保障的前沿理论研究以及理论和实践的结合工作，将国际国外最新的一些理论研究工作引入中国并进一步同我国国情结合。从将国际通用的信息技术评估的通用准则（即 ISO/IEC 15408 国际标准）引入并成为国家标准 GB/T 188336 开始，中心始终致力于包括信息技术、风险评估和信息系统安全保障等的最前沿的研究和实践。注册信息安全员知识体系大纲的结构和内容，也是我们对这些理论研究工作的反应，以形成信息安全员知识体系大纲更科学、严谨的结构和内容。

基于我们在信息安全保障领域的这些学习、研究和实践的成果，注册信息安全员知识体系大纲从整体上主要有以下的特点和特色：

- **从知识结构整体上：以信息安全保障基础（IA）作为贯穿整个 CISM 知识体系大纲的主线，形成以安全保障以及标准法规为基础、覆盖信息安全技术、管理和工程保障领域的信息安全保障基础有机知识整体。**

  近几年，我们对国内和国际信息安全认证、培训和教育领域做了大量的研究，为了更好地学习和实践，我们自己也亲自参与并获得了信息安全领域的几乎所有国内外知名的认证和考试的证书。在这些信息安全培训的学习、研究和实践中，我们发现信息安全相关的一些考试提供了非常优秀的知识域的描述，但是在整个知识体系的构建上，缺乏一条贯穿整个知识体系的主线。因此，在本次的知识体系大纲中，从整体上我们使用信息安全保障基础作为整个 CISM 知识体系大纲的主线和灵魂，更完整的诠释了信息安全保障基础的有机知识整体，以更好地帮助相关人员从整体上理解和实践信息安全保障的建设工作。

- **从知识结构组织上：使用知识类（PT）-知识体（BD）-知识域（KA）-知识子域（SA）来组织的组件模块化的知识体系结构，使整个知识体系大纲的结构更清晰、重点更突出、更易于结构化和模块化的学习和扩展**

  信息安全是架构在信息技术等知识基础之上的一门综合的学科，因此信息安全的学习是一件非常庞大复杂的任务。在信息安全的学习过程中，我们需要一种更加结构化和科学化的方法来将信息安全的相关知识进行梳理分析，并进一步根据需要进行更深入的学习、研究和实践。

在本次知识体系大纲的编制过程中，我们根据信息安全领域的知识的内在联系和关系通过知识类、知识体、知识域和知识子域的结构进行分析和分解，形成了新的覆盖内容更广泛、重点更突出、更强调实践性和实用性的组件模块化的知识体系结构。这样，一方面读者可以更清晰、深入地了解信息安全的各知识组成、知识重点以及各知识内容的内在联系，方便了读者的学习、理解和复习；另一方面，读者可以根据这些组件模块，结合自己的工作需求和知识结构，有区别、有重点地有的放矢地学习和应用，提供了更好的灵活性和实用性。

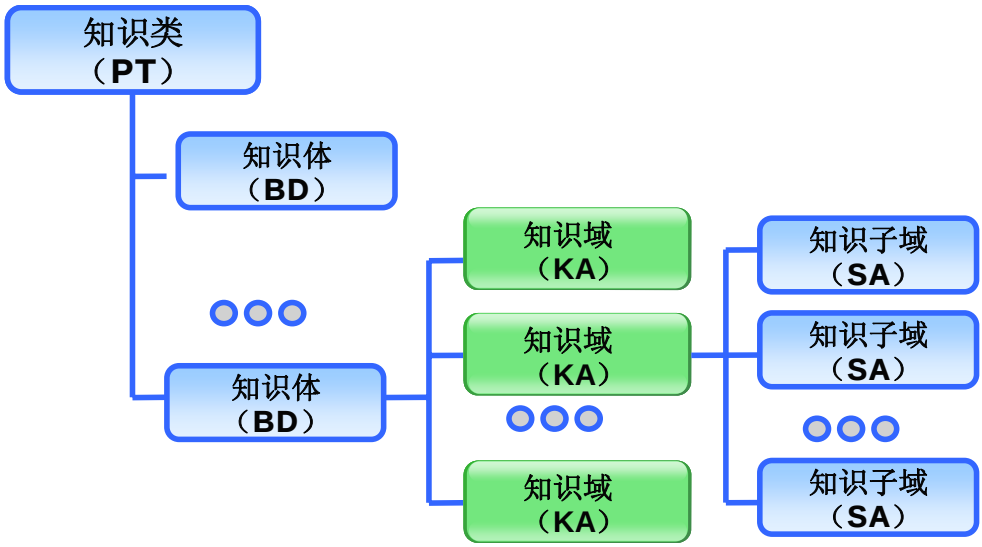
- **从知识内容的选择上：更加突出实用和实践性，突出同中国信息安全保障的环境和现状相结合。**

  CISM 的知识内容和课程设计上，将理论技术同实际工作相结合，对防火墙、防病毒、入侵检测等常见安全技术和产品进行深入介绍，更突出实用和实践性。在信息安全管理技术中，更加强调当前我国信息安全管理中风险管理和灾难备份的管理，更突出同我国信息安全保障的环境和现状相结合。

在介绍了 CISM 知识体系大纲的主要特点后，本章后面的内容将简单描述一下本次知识体系大纲的结构和内容。

1.2.2 CISM 知识体系框架结构介绍

CISM 知识体系使用层次化、组件化和模块化的结构，即 CISM 知识体系使用知识类（缩写为 PT）、知识体（缩写为 BD）、知识域（缩写为 KA）和知识子域（缩写为 SA）的结构，图表 1-1 描述了 CISM 知识体系的组件模块结构：



图表 1-1：CISM 知识体系的组件模块结构

在整个注册信息安全员（CISM）的知识体系结构中，共包括信息安全体系和模型、信息安全标准和法律法规、信息安全技术、信息安全管理和信息安全工程这五个知识类（PT），每个知识类根据其逻辑划分为一个或多个知识体（BD），每个知识体包含一个或多个知识域（KA），每个知识域由一个或多个知识子域组成。

知识类、知识体、知识域和知识子域的划分和内容并不是随意选择的，它们模块结构的含义如下：

- **知识类（PT）**是根据整个信息安全保障基础领域的分类来划分，共包括信息安全保障基础、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五个知识类；
- **知识体（BD）**是在知识类的分类范围内对知识域的逻辑组织划分；
- **知识域（KA）**是知识体系结构的主要知识点组成结构，它描述了注册信息安全员知识体系结构的实际主要内容；
- **知识子域（SA）**是进一步划分、细化描述知识域的组成部分。

知识类、知识体、知识域和知识子域的描述如下：

- **知识类（PT）：**在 CISM 知识体系结构中，共包括五个知识类，它们分别为：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。
- **知识体（BD）：**每个知识类都由一个或多个知识体组成，例如：在信息安全保障基础知识类（PT）包含两个知识体-安全体系知识体和安全模型知识体。
- **知识域（KA）：**每个知识体由一个或多个知识域组成，知识域是 CISM 知识体系结构的主要知识点的分类，在 CISM 知识体系中，主要的考试内容是根据知识域来划分展开的。
- **知识子域（SA）：**每个知识域可以包括也可以不包括知识子域，知识子域是对知识域的进一步划分。

在完成对 CISM 知识体系的模块结构的介绍后，我们就可以来学习 CISM 知识体系的具体结构内容介绍了。

CISM 知识体系结构共包含五个知识类，分别为：

- **信息安全保障基础：**信息安全保障为 CISM 学员提供了建设和评估信息安全保障工作的基础知识。学习和掌握信息安全保障基础是整个注册信息安全员知识体系的基础之一。
- **信息安全标准法规：**信息安全标准和法律法规主要讨论了信息安全相关的标准和法律法规。学习和掌握信息安全标准和法律法规是注册信息安全员知识体系的另一个基础知识领域。

- **信息安全技术**：信息安全技术主要讨论了同信息安全相关的技术知识和实践。
- **信息安全管理**：信息安全管理主要讨论了同信息安全相关的管理知识和实践。
- **信息安全工程**：信息安全工程主要讨论了同信息安全相关的工程知识和实践。

在图表 1-2 中，从整体上描述了 CISM 的知识体系结构框架。

图表 1-2：CISM 知识体系结构框架

1.2.3 CISM 的课程设计

“注册信息安全员”（CISM），是从事信息安全领域工作的人员的专业资质和能力的证明，图表 1-3 描述 CISM 的课程安排和介绍。

课程编号	类别	课程	课程介绍	推荐时间
01	安全保障基础	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	0.5 天
02		信息系统安全保障测评	介绍信息安全产品、系统、人员和服务测评的概念和内容	
03	标准法规	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	0.5 天

课程编号	类别	课程	课程介绍	推荐时间
			系和内容	
04		信息安全法规	介绍信息安全相关的国内法律法规	
05	安全技术	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	0.5 天
06		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	0.5 天
07		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	
08		系统和常见应用安全	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	0.5 天
09	安全管理	信息安全管理基础	介绍信息安全管理的基础知识	0.5 天
10		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	0.5 天
11	安全工程	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	0.5 天
12		安全工程监理咨询和实践	介绍信息安全工程监理咨询的基础知识和实践考虑	
-	复习	复习迎考	答疑和复习，准备考试	0.5 天
-	考试	考试	正式考试	0.5 天
备注：CISM 共包括信息安全保障基础、信息安全标准法规、信息安全管理、信息安全技术和信息安全工程五个领域的 12 门课程，共计 5 天（其中包括半天的复习迎考和半天的考试）的培训课程要求。				

图表 1-3：CISM 课程安排

2 知识类：信息安全保障基础

2.1 概述

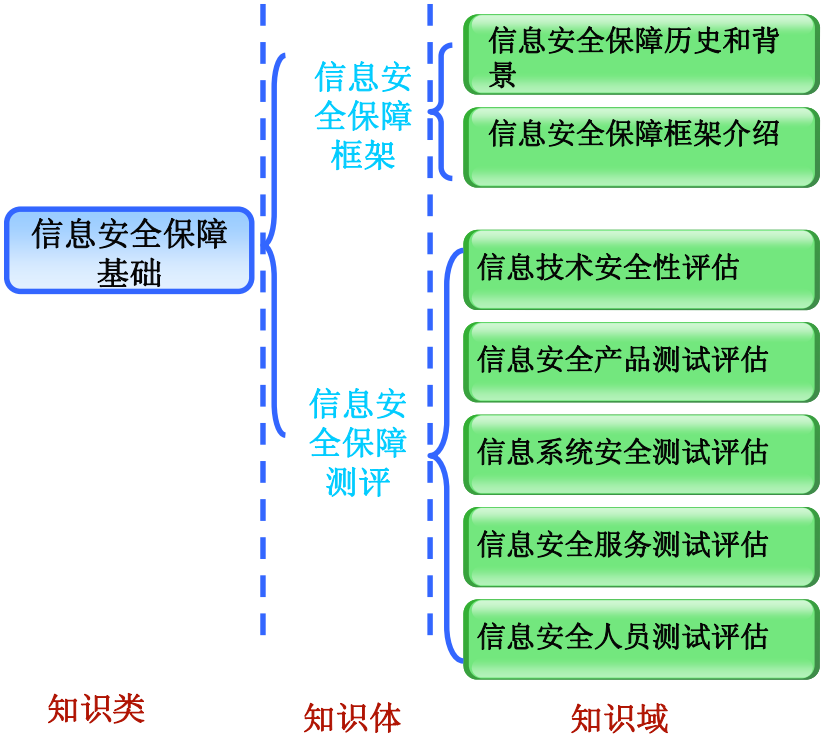
在注册信息安全员（CISM）知识体系的五个知识类中，信息安全保障基础以及信息安全标准和法律法规是注册信息安全员知识体系结构的基础，其中信息安全保障基础知识类为注册信息安全员（CISM）的所有人员提供了信息安全保障整体知识的背景知识和基础知识。

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。

信息安全保障基础知识类的组件模块结构如下：



图表 2-1：信息安全保障基础知识类（PT）的知识体系结构概述

2.2 原理说明

2.2.1 概述

在信息安全保障基础知识类中，共包括 2 个知识体，7 个知识域。

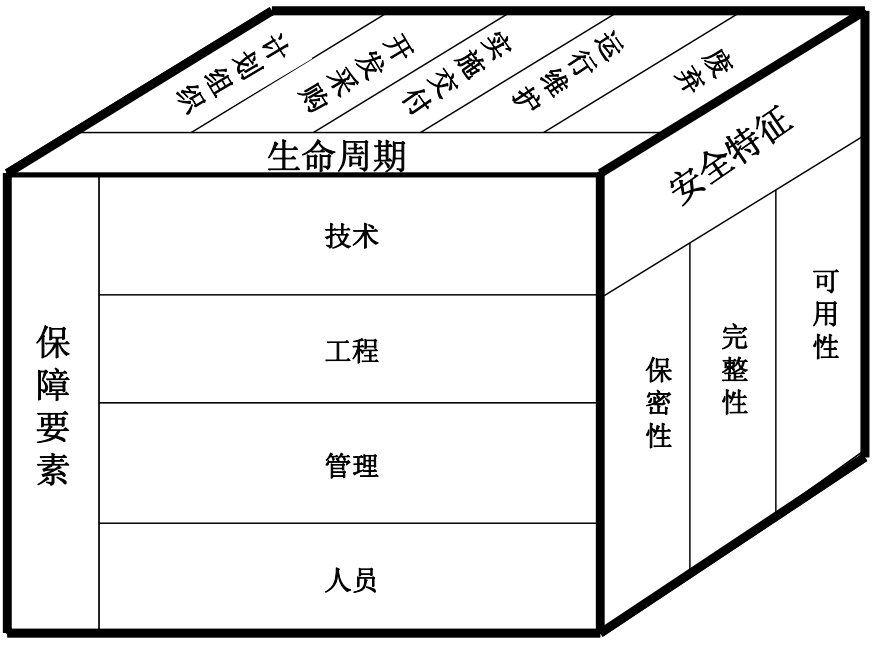
信息安全保障基础知识类分为信息安全保障框架和信息安全保障测评，它们从信息安全的背景、信息安全保障的建设和评估等不同视角描述了信息安全保障的整体概念。

2.2.2 知识体：信息安全保障框架

在信息安全保障框架知识体的学习中，其主要的原理在于理解信息安全保障的概念以及信息安全保障的模型。

信息安全保障是以风险和策略为出发点和核心，即从信息系统所面临的风险和信息系统所处的环境出发制定组织机构信息系统安全保障策略，通过在信息系统的整个生命周期中从技术、工程、管理和人员等方面提出安全保障要求，确保信息的保密性、完整性和可用性特征，实现和贯彻组织机构策略并将风险降低到可接受的程度，达到保护组织机构信息和信息系统资产，从而保障组织机构实现其使命的最终目的。在信息系统安全保障评估框架中，评估对象的含义更加广泛，它不仅涉及具体产品和产品系统，而且还包含信息系统运行环境的管理、工程等范畴，即用于采集、处理、存储、传输、分发和部署信息的整个基础设施、组织结构、人员和组件等总和的信息系统。

信息安全保障的模型如下：



图表 2-2：知识体-安全体系原理：信息安全保障模型

整个信息系统安全保障模型是一个以风险和策略为基础，包含保障要素、生命周期和信息特征三方面的模型。模型的主要特点是：

- 以安全概念和关系为基础，将风险和策略作为信息系统安全保障的基础和核心
- 强调信息系统安全保障的持续发展的动态安全模型，即强调信息系统安全保障应渗入整个信息系统生命周期的全过程。
- 强调信息系统安全保障的概念，信息系统的安全保障是通过综合技术、管理、工程和人员的要求等措施实施和实现信息系统的安全保障目标，通过对信息系统的技术、管理、工程和人员要求的认证认可、评估结果提供了对信息系统安全保障的信心。
- 通过风险和策略基础，生命周期和保证层面，从而使信息系统安全保障实现信息技术安全根本原则：信息的可用性、完整性和可用性特征，从而达到保障组织机构执行其使命的根本目的。

在建立了对信息安全保障概念和信息安全模型理解的基础上，我们就可以进一步展开对信息安全技术、安全管理和安全工程保障的理解，并进一步理解和掌握相关信息安全测试评估的内容。

2.2.3 知识体：信息安全保障测评

信息安全保障测评是从测评的角度来了解信息安全保障。在我们的具体工作实践中，提供了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这四类测评服务，它们分别从产品、系统、服务企业和人员角度给出了信息安全保障建设和评估的要求和内容。

2.3 知识体系大纲

2.3.1 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。

2.3.2 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。

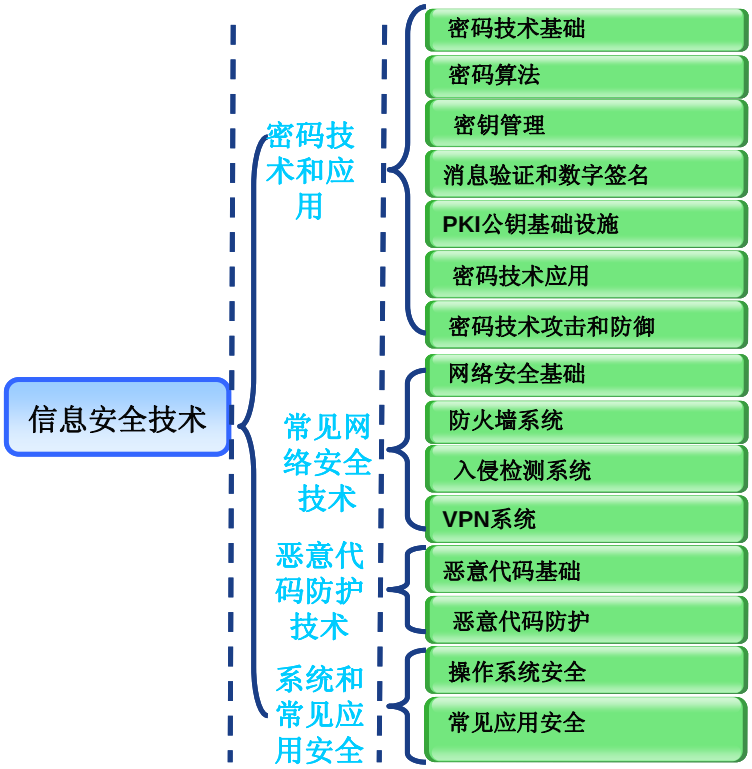
3 知识类：信息安全技术

3.1 概述

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。

信息安全技术的知识体系结构如图表 3-1 所示：



图表 3-1：信息安全技术知识类（PT）的知识体系结构概述

3.2 原理说明

3.2.1 概述

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。

3.2.2 知识体：密码技术和应用

在密码技术及应用知识体中，首先介绍传统密码技术的一些基本术语和定义，以及密码学的发展历史背景介绍；在完成对密码技术基础知识的理解后，进一步介绍三类密码算法：私钥（对称）密码算法、公钥（非对称）密码算法以及单向函数和单向哈希算法；密码系统是密码算法的进一步组合和应用，在密码系统中，主要介绍了密钥管理、数字签名和 PKI 公钥基础设施；最后简要介绍了密码系统在应用系统中的应用，以及密码攻防技术。

3.2.3 知识体：常见网络安全技术

在常见网络安全技术知识体中，首先介绍了网络安全基础的基础知识，然后结合网络安全实践，分别对防火墙系统、入侵检测系统和 VPN 系统等常见的网络安全产品系统进行了详细的介绍和说明。

3.2.4 知识体：恶意代码防护技术

恶意代码技术安全知识体讨论了恶意代码的概念、分类等的基础知识，然后结合实际讨论了恶意代码的防护技术。

3.2.5 知识体：系统和常见应用安全

系统和常见应用安全知识体讨论了操作系统安全和 Windows 操作系统安全的实践知识，然后讨论了以及 Web、邮件、DNS 等常见应用安全的实践知识。

3.3 知识体系大纲

3.3.1 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）。

3.3.2 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

3.3.3 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。

3.3.4 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。

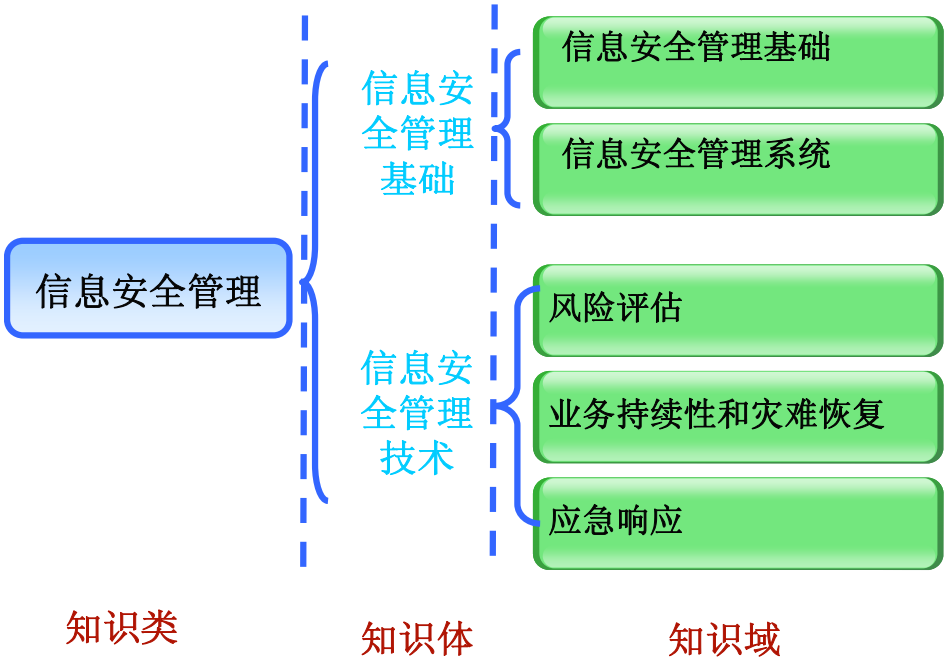
4 知识类：信息安全管理

4.1 概述

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。

信息安全管理的知识体系结构如图表 4-1 所示。



图表 4-1：信息安全管理知识类（PT）的知识体系结构概述

4.2 原理说明

4.2.1 概述

信息安全管理知识类中，分为安全管理基础和安全管理技术两个知识体。在这两个知识体中，安全管理基础描述了信息安全管理相关和信息安全管理系统的基础知识，安全管理基础的描述为学习整个信息安全管理知识奠定了基础；安全管理技术包括风险管理、业务持续性和灾难恢复管理以及事件响应管理，它们是信息安全管理中的主要安全管理措施。

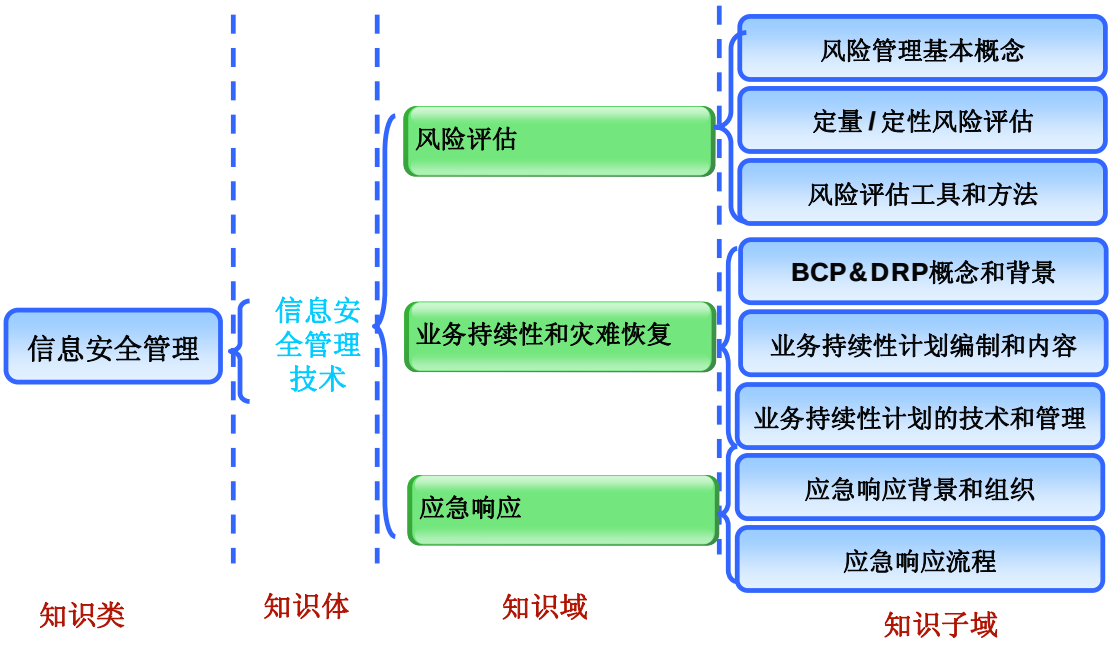
4.2.2 知识体：安全管理基础

知识体安全管理基础包括信息安全管理基础以及信息安全管理系统两个知识域。在信息安全管理基础知识域中描述了保密性、完整性和可靠性（CIA）以及抗抵赖性和可追究性信息安全基本服务，描述了安全策略的含义的分类，信息/数据分类和含义，安全控制的各种分类方法等，这些构成了信息安全管理的基本概念。在信息安全管理系统中，描述了建设信息安全管理系统的基本概念和最佳实践。

4.2.3 知识体：安全管理技术

在信息安全管理领域中，风险管理、业务持续性和灾难恢复管理以及事件响应管理是信息安全管理的关键管理过程。

关键信息安全技术知识体的原理说明参见图表 4-2。



图表 4-2：知识体：关键安全管理过程原理说明

4.3 知识体系大纲

4.3.1 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。

4.3.2 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。

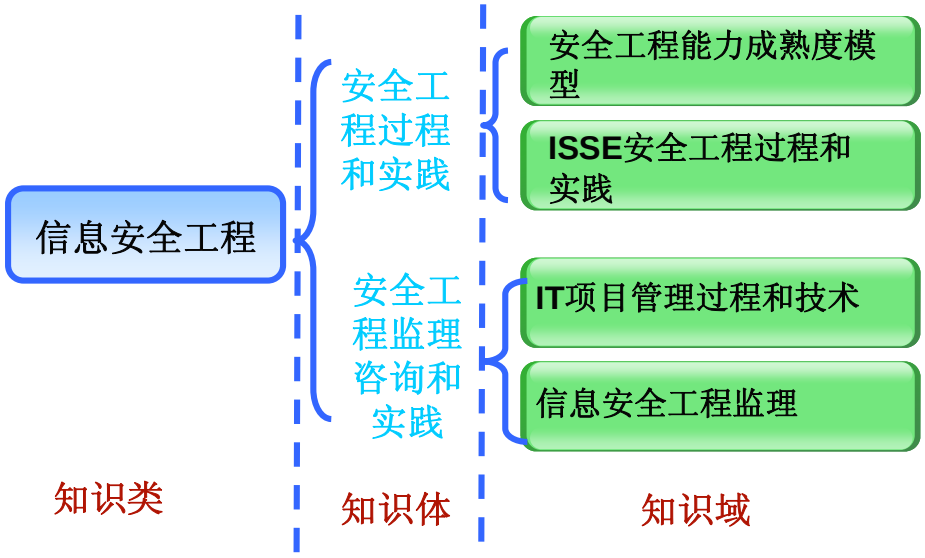
5 知识类：信息安全工程

5.1 概述

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。

信息安全工程的知识体系结构如图表 5-1 所示。



图表 5-1：信息安全工程知识类（PT）的知识体系结构概述

5.2 原理说明

5.2.1 概述

整个信息安全工程知识类分为安全工程基础、安全工程过程和实践以及项目管理过程和实践三个知识体。信安全工程过程和实践描述了 ISSE 信息系统安全工程的过程详细描述了安全工程的过程以及安全工程过程的能力成熟度模型；安全工程监理咨询和实践中，介绍了 IT 项目管理过程和技术以及信息安全工程监理。

5.2.2 知识体：安全工程过程和实践

在安全工程过程和实践知识体中，分为安全工程能力成熟度模型和 ISSE 安全工程过程和实践两个知识域。安全工程能力成熟度模型描述了安全工程过程的过程域和相应的能力成熟度模型，ISSE 安全工程过程和时间则是从实践实施角度根据工程过程生命周期的不同阶段描述了相应安全工程过程域的实施考虑。

5.2.3 知识体：安全工程监理咨询和实践

在安全工程的实施主要涉及信息系统生命周期的采购阶段，即通过系统集成方式实现信息系统安全体系架构，而信息系统安全集成同时也需要相应的项目管理技术和工具。因此在安全工程监理咨询和实践中，主要讨论了信息系统项目管理的过程和具体技术，并从监理方的角度给出了信息安全工程监理的描述。

5.3 知识体系大纲

5.3.1 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。

5.3.2 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。

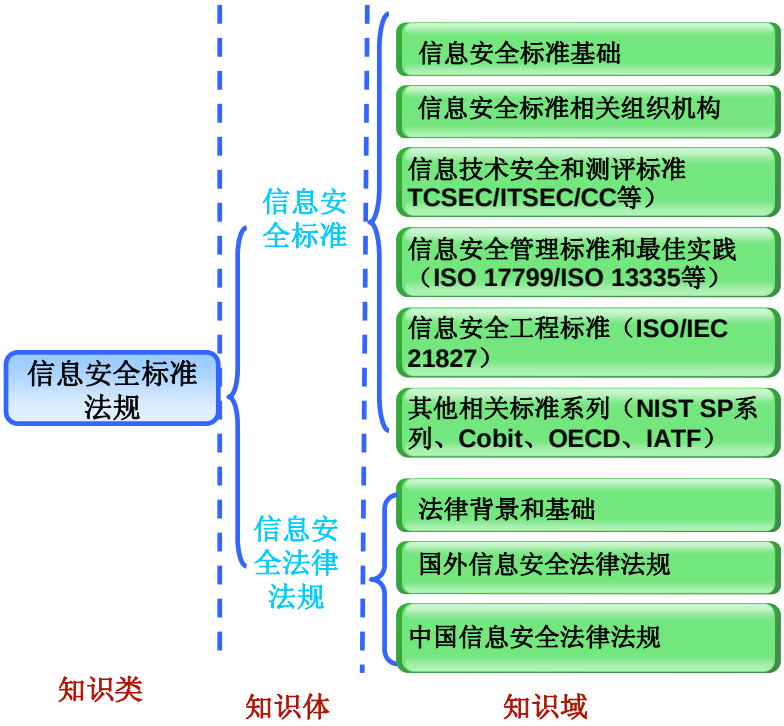
6 知识类：信息安全标准和法律法规

6.1 概述

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）。

信息安全标准和法律法规知识类的组件模块结构如下：



图表 6-1：信息安全标准和法律法规知识类（PT）的知识体系结构概述

6.2 原理说明

信息安全标准和法律法规知识类是信息安全专业人员所必须了解和掌握的。在信息安全标准和法律法规知识类中，主要讨论了信息技术安全和测评标准等信息安全标准以及国家相关的信息安全法律法规。

6.3 知识体系大纲

6.3.1 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。

6.3.2 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。