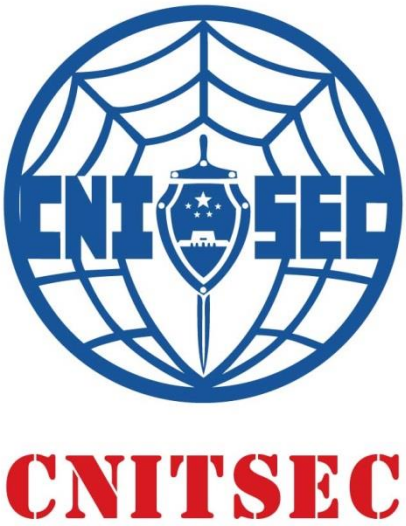
注册信息安全员（CISM）
知识体系大纲



版本：3.0

中国信息安全测评中心

发布日期：2015 年 1 月 30 日

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、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。

注册信息安全员（CISM）是由中国信息安全测评中心向政府机构、社会团体、企事业单位中的信息安全工作人员颁发的专业资质证书，是对我国信息安全人员进行资质评定的重要形式之一。持证人员掌握保障信息系统安全的基本知识和技能，具备从事信息安全相关工作的基本能力。

CISM 知识体系大纲面向注册信息安全培训人员，以及信息系统维护人员的工作需求，注重基本知识和实践操作。大纲内容从我国国情出发，根据地方/行业信息安全管理的实际工作需要，以实用性和操作性为原则，明确规定了 CISM 应当掌握的知识要点，是 CISM 教材编制、讲师授课、学员学习，以及考试命题的重要依据。

1 注册信息安全员（CISM）知识体系概述

1.1 CISM 资质介绍

“注册信息安全员”，英文为 Certified Information Security Member，简称 CISM。CISM 面向政府机构、社会团体、企事业单位中从事信息安全相关工作的人员。CISM 证书由中国信息安全测评中心颁发，持证人员掌握保障信息系统安全的基本知识和技能，具备从事信息安全相关工作的基本能力。

1.2 CISM 知识体系介绍

1.2.1 大纲范围

本大纲涵盖了 CISM 注册人员需要掌握的知识要点，主要包括信息安全保障概述、信息安全技术、信息安全管理、信息安全工程以及地方/行业信息安全五部分，其中信息安全工程和地方/行业信息安全保障的内容由地方或行业自行定制。

1.2.2 知识体系结构

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）和知识域（缩写为 KA）的结构。其中，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）。图 1-1 描述了 CISM 知识体系的层次结构：

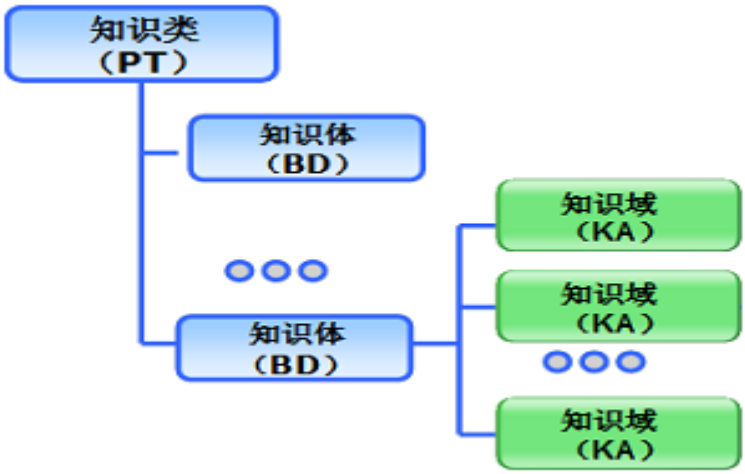


图 1-1：CISM 知识体系的层次结构

在整个注册信息安全员（CISM）的知识体系结构中，共包括三个必修知识类和两个可选知识类，其中必修知识类为信息安全保障基础、信息安全技术和信息安全管理，可选知识类为信息安全工程、地方/行业信息安全，分别为：

- **信息安全保障基础：**本知识类介绍信息安全有关的基本概念和模型，并介绍了我国有关的信息安全保障实践工作和信息安全政策法规标准，该知识类是 CISM 知识体系的基础知识。
- **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，包括密码及网络安全、终端及数据安全、信息安全攻防技术等知识体。
- **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，包括信息安全管理基础及信息安全管理体系措施两个知识体。
- **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，本部分为可选内容，可以按照信息安全工程基础和安全工程能力成熟度模型两个知识体来组织具体内容。
- **地方/行业定制课程：**本知识类为可选内容，各地或各行业可根据自身信息安全管理需求定制课程内容，可以按照地方/行业信息安全保障简介、地方/行业信息安全政策法规、地方/行业安全技术要求等知识体组织，具体内容不在本大纲中介绍。

在图 1-2 中，从整体上描述了 CISM 的知识体系结构框架。

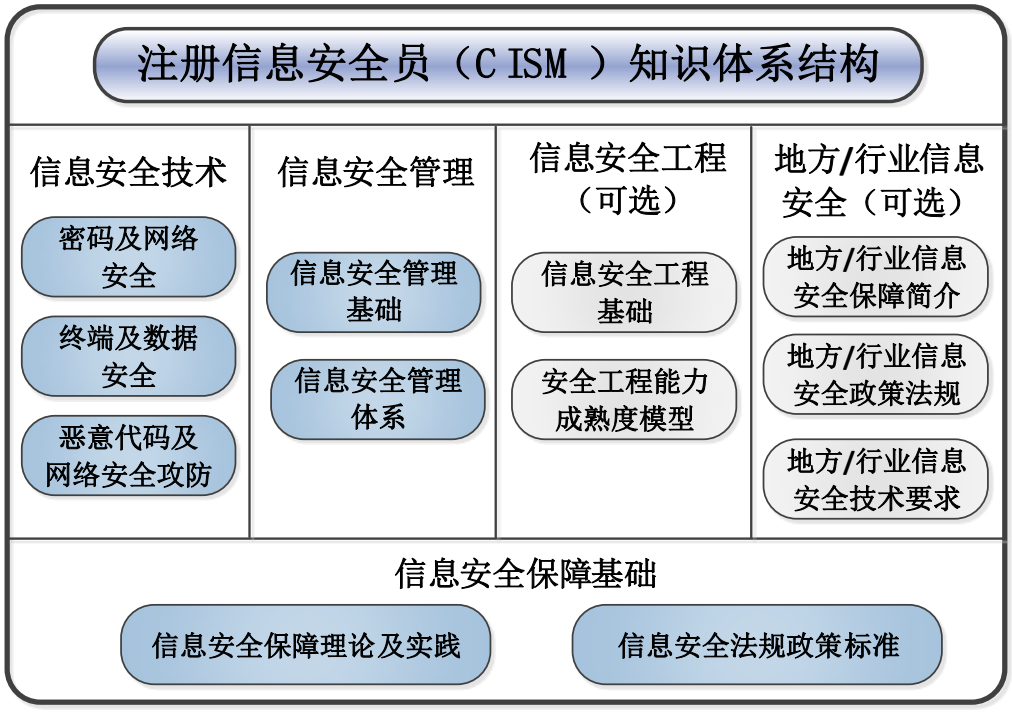


图 1-2：CISM 知识体系结构

1.2.3 考试题目

CISM 考试时间为 2 个小时，所有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。表 1-1 CISM 考试试题结构

中描述了 CISM 考试的各知识类的比例。

表 1-1 CISM 考试试题结构

知识类别	题目比例
信息安全保障基础	**20%**
信息安全技术	**50%**
信息安全管理	**30%**

1.2.4 课程时间安排

根据 CISM 知识体系大纲和教材内容，本大纲给出按三天培训时间设计的培训内容和课时安排，如表 1-2 所示。各地方各行业在培训时，也可以根据自己的实际情况参考执行。

表 1-2 CISM 课程时间安排

课程编号	课程名	课程介绍	课时
CISM0101	信息安全保障基础	介绍信息安全保障基本知识，信息安全保障框架模型、信息安全保障实践，以及国家信息安全法规、政策和标准方面知识。	3
CISM0201	密码及网络安全	介绍密码基本知识、网络安全防护策略及常见的网络安全产品。	3
CISM0202	终端及数据安全	介绍 Windows 7 操作系统和 IE 浏览器、电子邮件即时通讯软件等常见桌面应用的安全配置，介绍个人文件加密、文件粉碎、数据备份和数据防泄漏等数据保护技术。	3
CISM0203	恶意代码及网络安全攻防	介绍恶意代码的概念和防御查杀技术，介绍网络安全攻击与防护的各阶段中相关技术及工具。	3

课程编号	课程名	课程介绍	课时
CISM0301	信息安全管理基础	介绍信息安全管理基本概念、风险管理、等级保护等基础知识，介绍应急响应与灾难恢复管理相关概念、策略和主要内容。	3
CISM0302	信息安全管理体系	介绍信息安全管理体系、信息安全管理控制措施方面知识。	3
总计培训 18 学时（3 天），考试 2 小时			

2 知识类：信息安全保障基础

2.1 知识体：信息安全保障理论及实践

- 知识域：信息安全保障基础知识
  - ◆ 理解信息安全的典型安全威胁
  - ◆ 理解信息安全问题产生的根源
  - ◆ 掌握信息安全三个基本要素（保密性、完整性和可用性）的概念和含义
  - ◆ 了解信息安全发展的阶段及各阶段主要特点
  - ◆ 理解信息安全保障的概念和内涵
- 知识域：信息安全保障模型
  - ◆ 了解信息系统、风险、保障和使命之间的关系
  - ◆ 掌握信息系统安全保障模型，理解其保障要素、生命周期和安全特征的内容和含义
  - ◆ 理解 PDCA 模型内容和特点
  - ◆ 了解信息保障技术框架（IATF）的核心要素和焦点区域
- 知识域：我国信息安全保障工作实践
  - ◆ 理解我国信息安全工作的发展阶段划分情况
  - ◆ 了解我国信息安全保障工作的目标和主要内容
  - ◆ 了解我国信息安全保障工作实践成果

2.2 知识体：信息安全法规政策标准

- 知识域：重点信息安全法律法规解读
  - ◆ 了解我国信息安全法律体系情况
  - ◆ 理解《中华人民共和国保守国家秘密法》中主要条款
  - ◆ 了解《刑法》、《中华人民共和国电子签名法》关于信息安全的重要条款
  - ◆ 了解《中华人民共和国计算机信息系统安全保护条例》的有关内容
- 知识域：重点信息安全政策解读
  - ◆ 理解《国家信息化领导小组关于加强信息安全保障工作的意见》的重要性和有关内容
  - ◆ 了解《国务院关于大力推进信息化发展和切实保障信息安全的若干意见》的有关内容

- 知识域：信息安全标准知识
  - ◆ 理解我国国家标准、行业标准、地方标准和企业标准以及强制性、推荐性和标准化指导性技术文件等分类情况
  - ◆ 了解我国信息安全标准体系
  - ◆ 了解国外主要的信息安全标准化组织情况
  - ◆ 了解《可信计算机系统评估准则》、《信息技术安全性评估通用准则》等标准发展历史

3 知识类：信息安全技术

3.1 知识体：密码及网络安全

- 知识域：密码学基础知识
  - ◆ 了解密码学的基本概念和术语
  - ◆ 理解对称算法特点
  - ◆ 理解非对称算法特点
  - ◆ 了解散列算法、消息鉴别码和签名算法的作用
- 知识域：网络安全规划及策略
  - ◆ 了解网络安全面临的威胁及网络安全基本目标
  - ◆ 了解常见网络结构的安全配置
- 知识域：常见网络安全设备
  - ◆ 理解网络边界安全产品功能和主要产品，理解防火墙、入侵检测系统的功能特点
  - ◆ 理解网络连接安全产品功能和主要产品，了解 IPSec VPN 和 SSL VPN 特点和区别
  - ◆ 了解网络应用安全产品功能和相关产品
  - ◆ 了解安全管理平台、统一威胁管理以及网络安全审计等产品功能

3.2 知识体：终端及数据安全

- 知识域：操作系统安全及 Windows 7 安全设置
  - ◆ 了解操作系统安全的重要性
  - ◆ 了解 Windows 7 系统安全配置常见策略和措施
- 知识域：终端安全防护产品
  - ◆ 了解主机审计产品的主要功能
  - ◆ 了解主机安全监控产品的主要功能

- 知识域：终端应用安全
  - 了解 IE 浏览器的安全配置和安全使用技巧
  - 了解电子邮件、即时通讯软件的常见安全问题和安全保护手段
  - 了解公钥基础设施的概念和在 Web 访问、网络支付中的应用安全
- 知识域：数据安全
  - 理解数据加密的重要性和常见手段
  - 了解数据防泄漏的含义和有关产品功能
  - 了解数据安全删除重要性和措施
  - 了解数据备份重要性和措施

3.3 知识体：恶意代码及网络安全攻防

- 知识域：恶意代码与防范
  - 理解恶意代码的定义
  - 了解恶意代码发展过程和趋势
  - 理解典型的恶意代码的传播方式和危害
  - 了解恶意代码的防御措施
- 知识域：网络安全攻防技术
  - 了解网络攻击的基本步骤
  - 了解信息收集、目标分析实现及防御措施
  - 理解攻击者利用人性弱点、协议缺陷、软件缺陷等漏洞进行攻击的技术原理及防御措施
  - 了解攻击者设置后门的实现方式及防御措施
  - 了解渗透测试的特点、流程及实现工具

4 知识类：信息安全管理

4.1 知识体：信息安全管理基础

- 知识域：信息安全管理概念
  - 了解信息安全管理的概念和内涵
  - 理解信息安全管理和信息安全技术的关系
- 知识域：信息安全风险管理
  - 理解信息安全风险的含义，理解威胁、脆弱性、影响和风险等要素及相互关系
  - 掌握信息安全风险管理的主要内容和流程

- ◆ 理解风险评估的作用、工作形式和评估方法
- 知识域：信息安全等级保护
  - ◆ 掌握等级保护的定级要素及级别划分准则
  - ◆ 了解等级保护的工作流程
  - ◆ 理解等级保护有关的重要国家政策和标准
  - ◆ 理解等级保护的管理要求主要内容
- 知识域：信息安全应急响应
  - ◆ 了解应急响应的有关概念、发展过程和特点
  - ◆ 了解我国应急响应有关标准
  - ◆ 了解信息安全事件分类的方法
  - ◆ 理解信息安全事件分级要素和各级别含义
  - ◆ 了解应急响应组织工作的主要内容
- 知识域：信息安全灾难恢复
  - ◆ 理解灾难恢复的概念和含义
  - ◆ 理解恢复时间目标（RTO）和恢复点目标（RPO）等术语含义
  - ◆ 了解我国灾难恢复有关标准
  - ◆ 了解灾难恢复能力等级划分情况
  - ◆ 了解异地灾备、系统级灾备、完全备份等有关策略含义和特点

4.2 知识体：信息安全管理体系

- 知识域：信息安全管理体系概念
  - ◆ 理解信息安全管理体系（ISMS）的概念和核心过程
  - ◆ 了解信息安全管理体系文档要求
  - ◆ 了解 ISO/IEC 27000 标准族
- 知识域：信息安全管理控制措施
  - ◆ 了解信息安全管理控制措施的作用
  - ◆ 了解安全方针、人力资源安全等管理域的控制目标和主要控制措施