注册信息安全专业人员

知识体系大纲

（CISE/CISO）

版本：4.2

生效日期：2019 年 3 月 1 日

中国信息安全测评中心

中国信息产业商会信息安全产业分会

目　录

概述

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。

为了加快信息安全人才的培养，中国信息安全测评中心依据中编办批准开展“信息安全人员培训与资质认证”的职能，推出了代表国家对信息安全专业人员能力认可的 CISP 和对信息化工作人员信息安全基本能力认可的 CISM。CISP 与 CISM 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。

适用范围

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，涵盖了 CISP 中的 CISE、CISO 两类注册人员和 CISM 需要掌握的知识要点，是 CISM 和 CISE/CISO 教材编制、讲师授课、学员学习以及考试命题的重要依据。

框架结构

知识体系使用组件模块化的结构，包括知识域、知识子域、知识点三个层次。每个知识点根据内容和深度要求，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。

知识体系结构包括信息安全保障、网络安全监管、信息安全管理、业务连续性、安全工程与运营、安全评估、信息安全支撑技术、物理与网络通信安全、计算环境安全、软件安全开发共十个知识域。每个知识域包括多个知识子域，每个知识子域包括一个或多个知识点要求。

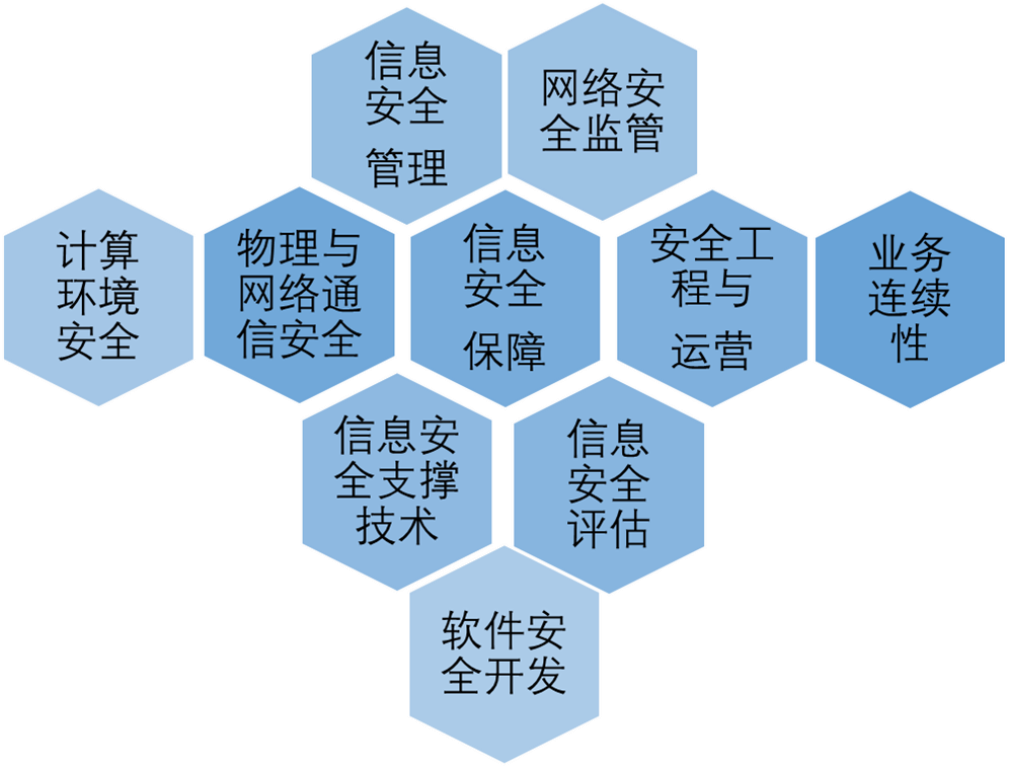

图 1：知识体系结构框架

CISE/CISO 培训课程与知识域一一对应，每一门课程对应一个知识域。CISM 培训信息安全保障、网络安全监管、信息安全管理、信息安全支撑技术四个知识域的内容。课程如下表所示：

序号	CISE/CISO	CISM
1	信息安全保障	信息安全保障
2	网络安全监管	网络安全监管
3	信息安全管理	信息安全管理
4	业务连续性	
5	安全工程与运营	
6	安全评估	
7	信息安全支撑技术	信息安全支撑技术
8	物理与网络通信安全	
9	计算环境安全	
10	软件安全开发	

表 1：培训课程设置

考试试题结构

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）都需要学习和掌握本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。

CISM 考试四个知识域出题比例相同。

序号	知识域	CISE	CISO	CISM
1	信息安全保障	10%	10%	25%
2	网络安全监管	8%	10%	25%
3	信息安全管理	10%	16%	25%
4	业务连续性	8%	10%	0%
5	安全工程与运营	10%	12%	0%
6	安全评估	8%	12%	0%
7	信息安全支撑技术	10%	8%	25%
8	物理与网络通信安全	12%	8%	0%
9	计算环境安全	12%	8%	0%
10	软件安全开发	12%	6%	0%

表 2：考试试题比例

一、知识域：信息安全保障

1.1 知识子域：信息安全保障基础

1.1.1 信息安全概念

了解信息安全的定义及信息安全问题侠义、广义两层概念与区别；

理解信息安全问题的根源（内因和外因）；

理解信息安全的系统性、动态性、无边界、非传统等特征；

了解威胁情报、态势感知的基本概念及对信息安全的作用。

1.1.2 信息安全属性

理解信息安全属性的概念及 CIA 三元组（保密性、完整性、可用性）；

了解真实性、不可否认性、可问责性、可靠性等其他不可缺少的信息安全属性。

1.1.3 信息安全视角

了解国家视角对信息安全的关注点（网络战、关键基础设施保护、法律建设与标准化）及相关概念；

了解企业视角对信息安全的关注点（业务连续性管理、资产保护、合规性）及相关概念；

了解个人视角对信息安全的关注点（隐私保护、个人资产保护、社会工程学）及相关概念。

1.1.4 信息安全发展阶段

了解通信安全阶段的核心安全需求、主要技术措施；

了解计算机安全阶段信息安全需求、主要技术措施及阶段的标志；

了解信息系统安全阶段的安全需求、主要技术措施及阶段的标志；

了解信息安全保障阶段与系统安全阶段的区别，信息安全保障的概念及我国信息安全保障工作的总体要求、主要原则；

了解网络空间的概念，理解网络空间安全对国家安全的重要性。

1.1.5 信息安全保障新领域

了解工业控制系统中 SCADA、DCS、PLC 等基本概念，理解工业控制系统的重要性，面临的安全威胁及安全防护的基本思路；

了解云计算所面临的安全风险及云计算安全框架，了解虚拟化安全的基本概念；

了解物联网基本概念、技术架构及相应的安全问题；

了解大数据的概念，大数据应用及大数据平台安全的基本概念；

了解移动互联网面临的安全问题及安全策略；

了解智慧的世界的概念。

1.2 知识子域：安全保障框架模型

1.2.1 基于时间的 PDR 与 PPDR 模型

理解基于时间的 PDR、PPDR 模型的核心思想及出发点；

理解 PPDR 模型与 PDR 模型的本质区别；

了解基于时间判断系统安全性的方式。

1.2.2 信息安全保障技术框架

理解信息安全保障技术框架（IATF）的“深度防御”核心思想、三个核心要素及四个焦点领域；

了解保护区域边界的原则和技术实现方式；

了解保护计算环境的原则和技术实现方式；

了解保护网络基础设施的原则和技术实现方式；

了解支撑性基础设施建设的概念及技术实现。

1.2.3 信息系统安全保障评估框架

理解信息系统保障相关概念及信息安全保障的核心目标；

了解信息系统保障评估的相关概念和关系；

理解信息系统安全保障评估模型主要特点，生命周期、保障要素等概念。

1.2.4 企业安全架构

了解企业安全架构的概念；

了解舍伍德商业应用安全架构模型构成及生命周期。

二、知识域：网络安全监管

2.1 知识子域：网络安全法律体系建设

2.1.1 计算机犯罪

了解计算机犯罪的概念、特征及计算机犯罪的发展趋势。

2.1.2 我国立法体系

了解我国多级立法机制及相关机构职能；

了解立法分类（法律、行政法规及地方性法规）等概念。

2.1.3 网络安全法

理解网络安全法出台背景；

理解网络安全法中定义的网络、网络安全等基本概念及网络空间主权原则；

了解网络运行安全制度、关键基础设施保护制度、等级保护制度、网络安全审查制度的相关要求。

2.1.4 网络安全相关法规建设

了解行政违法相关概念及相关行政处罚；

了解刑事责任、常见网络安全犯罪及量刑等概念；

了解民事违法相关概念及违法民事处罚；

了解国家安全法、保密法、电子签名法、反恐怖主义法、密码法中网络安全相关条款。

2.2 知识子域：网络安全国家政策

2.2.1 国家网络空间安全战略

了解国家 《网络空间安全战略》中总结的七种新机遇、六大严峻挑战及建设网络强国的战略目标；

了解《国家网络空间战略》提出的四项基本原则和九大任务；

2.2.2 国家网络安全等保政策

了解我国网络安全等级保护相关政策。

2.3 知识子域：网络安全道德准则

2.3.1 道德约束

了解道德的概念，道德与法律的差异；

理解道德约束相关概念。

2.3.2 职业道德准则

理解信息安全从业人员遵守职业道德的重要性；

了解目前国际团体和组织制作的职业道德规范文件；

理解《CISP 职业道德准则》的要求；

2.4 知识子域：信息安全标准

2.4.1 信息安全标准基础

了解标准的基本概念及标准的作用、标准化的特点及原则等；

了解国际信息安全标准化组织和我国信息安全标准化组织；

了解我国标准分类。

2.4.2 我国信息安全标准

了解我国信息安全标准体系的构成。

2.4.3 等级保护标准族

了解网络安全等级保护标准体系；

掌握等级保护实施流程中定级、备案的工作要求并了解整改、测评相关要求；

了解等级保护 2.0 的相关变化。

三、知识域：信息安全管理

3.1 知识子域：信息安全管理基础

3.1.1 基本概念

了解信息、信息安全管理、信息安全管理体系等基本概念。

3.1.2 信息安全管理的作用

理解信息安全管理的作用，对组织内部和组织外部的价值。

3.2 知识子域：信息安全风险管理

3.2.1 风险管理基本概念

了解信息安全风险、风险管理的概念；

理解信息安全风险管理的作用和价值；

3.2.2 常见风险管理模型

了解 COSO 报告、ISO31000、COBIT 等风险管理模型。

3.2.3 安全风险管理基本过程

理解风险管理的背景建立、风险评估、风险处理、批准监督、监控审查和沟通咨询六个方面的工作目标及内容；

3.3 知识子域：信息安全管理体系建设

3.3.1 信息安全管理体系成功因素

理解 GB/T 29246-2017 中描述的信息安全管理体系成功的主要因素。

3.3.2 PDCA 过程

理解 PDCA 过程模型的构成及作用；

了解 ISO/IEC 27001:2013 中定义的 PDCA 过程方法四个阶段工作。

3.3.3 信息安全管理体系建设过程

掌握规划与建立阶段组织背景、领导力、计划、支持等主要工作的内容；

理解实施与运行、监视和评审、维护和改进阶段工作内容。

3.3.4 文档化

理解文档化的重要性并了解文件体系及文件控制的方式。

3.4 知识子域：信息安全管理体系最佳实践

3.4.1 信息安全管理体系控制类型

了解预防性、检测性、纠正性控制措施的差别及应用。

3.4.2 信息安全管理体系控制措施结构

了解 ISO 27002 中控制措施的分类及控制措施描述结构。

3.4.3 信息安全管理体系控制措施

了解安全方针、信息安全组织、人力资源安全、资产管理、访问控制、密码学、物理和环境安全、操作安全、通信安全、安全采购开发和维护、供应商关系、安全事件管理、业务连续性管理及合规性 14 个控制类别的控制目标、控制措施并理解实施指南的相关要素。

3.5 知识子域：信息安全管理体系度量

3.5.1 基本概念

了解 ISMS 测量的基本概念、方法选择和作用；

了解 27004 定义的测量模型。

3.5.2 测量要求与实现

了解测量实现的工作内容。

四、知识域：业务连续性

4.1 知识子域：业务连续性管理

4.1.1 业务连续性管理基础

了解业务连续性、业务连续性管理的概念；

理解业务连续性管理对组织机构的重要性；

了解业务连续性管理生命周期六个阶段的工作内容。

4.1.2 业务连续性计划

了解业务连续性计划的概念及制定业务连续性计划的四个步骤；

理解组织管理在业务连续性计划过程中的重要性及四个要素；

理解业务影响分析在业务连续性计划过程中的作用及各项工作内容；

了解业务连续性计划制定和批准实施工作的内容并理解风险降低、风险转移、风险规避和风险接受四种风险处置方式；

了解业务连续性计划文档化的作用、文档应包括的内容及批准、实施、评估及维护等相关概念。

4.2 知识子域：信息安全应急响应

4.2.1 信息安全事件与应急响应

了解信息安全事件的概念及应急响应在信息安全保障工作中的重要性；

了解我国信息安全事件的分类分级标准；

了解国际及我国信息安全应急响应组织；

了解应急响应组织架构。

4.2.2 网络安全应急响应预案

了解网络安全应急响应预案的概念及作用；

理解应急响应演练的作用、分类、方式及流程。

4.2.3 计算机取证及保全

了解计算机取证的概念及取证的过程；

理解计算机取证过程中准备、保护、提取、分析和提交五个步骤的工作内容。

4.2.4 信息安全应急响应管理过程

了解应急响应管理中准备、检测、遏制、根除、恢复和跟踪总结六个阶段的工作内容和目标。

4.3 知识子域：灾难备份与恢复

4.3.1 灾难备份与恢复基础

了解灾难备份、灾难恢复计划的概念及作用；

理解 RTO、RPO 等灾备的关键指标；

了解国家灾备相关政策与标准；

了解灾难恢复组织结构。

4.3.2 灾难恢复相关技术

了解 DAS、SAN、NAS 等存储技术的概念及应用区别；

了解全备份、增量备份、差分备份等备份方式的区别；

了解常用的备份介质；

理解磁盘冗余阵列 RAID-0、RAID-1、RAID-5 等配置的差别；

了解冷站、温站、热站等概念。

4.3.3 灾难恢复策略

了解国际标准 SHARE78 对灾难备份的能力划分的 0~6 级的区别；

理解我国《重要信息系统灾难恢复指南》中划分的 6 个灾难恢复等级要求；

了解企业常用的容灾策略中数据容灾、系统容灾、应用容灾的概念；

了解确定灾难恢复能力级别的方法。

4.3.4 灾难恢复管理过程

了解灾难恢复管理规划的作用及工作过程；

理解灾难恢复需求分析风险分析、业务影响分析和确定灾难恢复目标三个子步骤的工作内容和目标；

理解灾难恢复策略制定的原则和工作方法；

了解灾难恢复策略实现的工作步骤和要求；

了解灾难恢复预案的制定与管理工作内容及要求。

五、知识域：安全工程与运营

5.1 知识子域：系统安全工程

5.1.1 系统安全工程基础

理解系统安全工程的概念及系统安全工程的必要性。

5.1.2 系统安全工程理论基础

了解系统工程思想、项目管理方法、质量管理体系、能力成熟度模型等基础理论；

理解能力成熟度模型的基本思想及相关概念。

5.1.3 系统安全工程能力成熟度模型

了解系统安全工程能力成熟度模型基本概念；

了解系统安全工程能力成熟度模型的体系结构及域维、能力维相关概念；

5.1.4 SSE-CMM 安全工程过程

理解风险过程包括的评估威胁、评估脆弱性、评估影响及评估安全风险这四个过程区域及其基本实施；

理解工程过程包括的确定安全需求、提供安全输入、管理安全控制、监控安全态势及协调安全五个过程区域及其基本实施；

理解保证过程中验证和证实安全及建立保证论据两个过程区域及其基本实施。

5.1.5 SSE-CMM 安全工程能力

理解能力成熟度级别的概念；

掌握 1~5 级不同成熟度级别应具有的公共特征。

5.2 知识子域：安全运营

5.2.1 安全运营概念

了解安全运营的概念；

5.2.2 安全运营管理

了解漏洞的概念及漏洞检测、漏洞评估等漏洞管理工作；

了解补丁管理的重要性及补丁管理工作步骤；

了解变更管理的作用及工作步骤；

了解配置管理的基本概念；

了解事件管理的基本概念。

5.3 知识子域：内容安全

5.3.1 内容安全基础

了解内容安全的概念、重要性及内容安全管理的需求。

5.3.2 数字版权

了解著作权、版权的概念；

了解数字版权管理相关概念及技术；

了解使用数据版权保护信息的措施。

5.3.3 信息保护

理解信息的价值；

了解信息泄露的途径；

了解隐私保护的概念和隐私保护措施。

5.3.4 网络舆情

了解网络舆情的概念；

了解网络舆情管理措施及网络舆情监控技术。

5.4 知识子域：社会工程学与培训教育

5.4.1 社会工程学

理解社会工程学攻击的概念及在信息安全中的重要性；

了解社会工程学利用的 6 种“人类天性基本倾向”；

理解社会工程学攻击方式及防御措施。

5.4.2 培训教育

了解“人”在信息安全体系中的作用；

理解以建立持续化体系的方式实施信息安全培训的必要性；

六、知识域：安全评估

6.1 知识子域： 安全评估基础

6.1.1 安全评估概念

了解安全评估的定义、价值、风险评估工作内容及安全评估工具类型；

了解安全评估标准的发展。

6.1.2 安全评估标准

了解 TCSEC 标准的基本目标和要求、分级等概念；

了解 ITSEC 标准的适用范围，功能准则和评估准则的级别；

了解 ISO 15408 标准的适用范围、作用和使用中的局限性；

了解 GB/T 18336 的结构、作用及评估过程；

理解评估对象（TOE）、保护轮廓（PP）、安全目标（ST）、评估保证级（EAL）等关键概念；

了解信息安全等级测评的作用和过程。

6.2 知识子域：安全评估实施

6.2.1 风险评估相关要素

理解资产、威胁、脆弱性、安全风险、安全措施、残余风险等风险评估相关要素及相互关系。

6.2.2 风险评估途径与方法

了解基线评估等风险评估途径及自评估、检查评估等风险评估方法；

了解基于知识的评估，理解定性评估、定量评估的概念及区别并掌握定量分析中量化风险的方法。

6.2.3 风险评估的基本过程

了解风险评估基本过程；

理解风险评估准备工作内容；

掌握风险识别中资产的赋值方法；

理解风险分析的方法；

了解风险结果判定、风险处理计划、残余风险评估等阶段工作内容。

6.3.4 风险评估文档

了解风险评估文档化工作的重要性及对文档的相关要求；

6.3 知识子域：信息系统审计

6.3.1 审计原则与方法

了解信息系统审计职能、流程、内部控制及审计标准；

6.3.2 审计技术控制

了解脆弱性措施、渗透测试等审计技术控制措施；

6.3.3 审计管理控制

了解账户管理、备份验证等审计管理控制措施；

6.2.4 审计报告

了解信息系统审计报告标准 SAS70 和 SOC；

七、知识域：信息安全支撑技术

7.1 知识子域：密码学

7.1.1 基本概念

了解古典密码、近代密码、现代密码等各密码学发展阶段的特点；
了解基本保密通信模型；
理解密码系统安全性相关概念（科克霍夫准则、密码系统安全性评估）
了解密码算法分类的概念。

7.1.2 对称密码算法

理解对称密码算法的概念及算法特点；
了解 DES、3DES、AES 等典型对称密码算法。

7.1.3 公钥密码算法

理解非对称密码算法（公钥算法）的概念及算法特点；
了解 RSA、SM2 等典型非对称密码算法。

7.1.4 其他密码服务

理解哈希函数、消息认证码、数字签名等密码服务的作用。

7.1.5 公钥基础设施

了解 PKI 的基本概念及 PKI 体系构成；
理解 CA 及其他组件在 PKI 体系中的作用；
了解掌握 PKI 的应用场景。

7.2 知识子域：身份鉴别

7.2.1 身份鉴别的概念

理解标识与鉴别、鉴别类型、鉴别方式等基本概念。

7.2.2 基于实体所知的鉴别

理解基于实体所知的鉴别方式及特点；
了解口令破解、嗅探、重放攻击等针对实体所知鉴别方式的攻击方式；
掌握对抗口令破解的防御措施；
理解对抗嗅探攻击、重放攻击的防御措施。

7.2.3 基于实体所有的鉴别

理解基于实体所有的鉴别方式及特点；
了解集成电路卡、内存卡、安全卡、CPU 卡等常用鉴别物品。

7.2.4 基于实体特征的鉴别

理解基于实体特征的鉴别方式及特点；

了解指纹、虹膜、声纹等常用的生物识别技术；
理解基于实体特征鉴别有效性判定的方法。

7.2.5 kerberos 体系

理解单点登录概念及其特点；
了解 Kerberos 体系架构及基本认证过程。

7.2.6 认证、授权和计费

了解 AAA 的概念及 RADIUS、TACACS+协议特点；

7.3 知识子域：访问控制

7.3.1 访问控制模型的基本概念

理解访问控制的概念、作用及访问控制模型的概念。

7.3.2 自主访问控制模型

理解自主访问控制模型相关概念及模型特点；
理解访问控制列表与访问能力表实现访问控制功能的区别。

7.3.3 强制访问控制模型

理解强制访问控制模型的概念及特点；
了解 Bell-LaPadula 模型的作用及特点；
了解 Biba 模型的作用及特点；
了解 Clark-Wilson 的作用及特点；
了解 Chinese Wall 模型的作用及特点。

7.3.4 基于角色的访问控制模型

了解基于角色的访问控制模型基本概念及特点；
了解基于角色的访问控制模型的构成及访问控制规则。

7.3.5 特权管理基础设施

了解 PMI 的主要功能、体系架构及应用。

八、知识域：物理与网络通信安全

8.1 知识子域：物理与环境安全

8.1.1 环境安全

了解物理安全的重要性；

了解场地和环境安全应关注的因素：包括场地选择、抗震及承重、防火、防水、供电、空气调节、电磁防护、雷击及静电等防护技术。

8.1.2 设施安全

了解安全区域的概念及设立安全区域的作用；

了解边界防护的概念及相关防护要求；

了解审计与监控的概念及相关防护技术。

8.1.3 传输安全

理解同轴电缆、双绞线、光纤等有线传输技术及安全特点；

理解无线安全传输技术及安全特点。

8.2 知识子域：OSI 通信模型

8.2.1 OSI 模型

理解 OSI 七层模型构成及每一层的作用；

理解协议分层的作用。

8.2.2 OSI 模型通信过程

理解 OSI 模型通信过程及数据封装、分用等概念。

8.2.3 OSI 模型安全体系构成

了解 OSI 模型安全体系的构成；

了解 OSI 模型的五类安全服务、八种安全机制的概念。

8.3 知识子域：TCP/IP 协议安全

8.3.1 协议结构及安全问题

了解 TCP/IP 协议的体系及每一层的作用；

了解网络接口层的安全问题；

了解 IP 协议的工作机制及面临的安全问题；

了解传输层协议 TCP 和 UDP 的工作机制及面临的安全问题；

了解应用层协议面临安全问题。

8.3.2 安全解决方案

了解基于 TCP/IP 协议簇的安全架构；

了解 IPv6 对网络安全的价值。

8.4 知识子域：无线通信安全

8.4.1 无线局域网安全

了解无线局域网安全协议 WEP、WPA2、WAPI 等工作机制及优缺点；
理解无线局域网安全防护策略。

8.4.2 蓝牙通信安全

了解蓝牙技术面临的保密性、完整性、非授权连接、拒绝服务等安全威胁；
理解使用蓝牙的安全措施。

8.4.3 RFID 通信安全

了解 RFID 的概念及针对标签、针对读写器和针对信道的攻击方式；
理解 RFID 安全防护措施。

8.5 知识子域：典型网络攻击及防范

8.5.1 欺骗攻击

理解 IP 欺骗、ARP 欺骗、DNS 欺骗等电子欺骗攻击的实现方式及防护措施。

8.5.2 拒绝服务攻击

理解 SYN Flood、UDP Flood、Teardrop 等拒绝服务攻击实现方式；
了解分布式拒绝服务攻击实现方式及拒绝服务攻击应对策略。

8.6 知识子域：网络安全防护技术

8.6.1 边界安全防护

了解防火墙产品的实现技术、部署方式、作用及局限性；
了解安全隔离与信息交换系统的实现技术、部署方式和作用；
了解 IPS、UTM、防病毒网关等边界安全防护技术的概念。

8.6.2 检测与审计

了解入侵系统的作用、分类、实现技术、部署方式及应用上的局限性；
了解安全审计系统的作用。

8.6.3 接入管理

了解 VPN 的作用、关键技术及应用领域；
了解网络准入控制的作用。

九、知识域：计算环境安全

9.1 知识子域：操作系统安全

9.1.1 操作系统安全机制

了解操作系统标识与鉴别、访问控制、权限管理、信道保护、安全审计、内存存取、文件保护等安全机制。

9.1.2 操作系统安全配置

了解安全补丁、最小化部署、远程访问控制、账户及口令策略、安全审计及其他操作系统配置要点。

9.2 知识子域：信息收集与系统攻击

9.2.1 信息收集

理解信息收集的概念及公开渠道、网络、应用等信息收集的方式及防御措施。

9.2.2 缓冲区溢出攻击

理解缓冲区溢出的基本概念及危害；

理解缓冲区溢出攻击的技术原理及防御措施。

9.3 知识子域：恶意代码防护

9.3.1 恶意代码的预防

了解恶意代码的概念、传播方式及安全策略，理解减少漏洞和减轻威胁等针对恶意代码的预防措施；

9.3.2 恶意代码的检测分析

理解特征扫描、行为检测的区别及优缺点；

了解静态分析、动态分析的概念及区别。

9.3.3 恶意代码的清除

了解感染引导区、感染文件、独立型和嵌入型恶意代码清除的方式。

9.3.4 基于互联网的恶意代码防护

了解基于互联网的恶意代码防护概念。

9.4 知识子域：应用安全

9.4.1 Web 应用安全

了解 WEB 体系架构；

理解 HTTP 协议工作机制及明文传输数据、弱验证、无状态等安全问题；

理解 SQL 注入攻击的原理及危害；

了解跨站脚本安全问题的原理及危害及其他针对 WEB 的攻击方式；

了解 WEB 防火墙、网页防篡改等常见 Web 安全防护技术作用。

9.4.2 电子邮件安全

理解电子邮件工作机制及 SMTP、POP3 协议；

了解电子邮件安全问题及解决方案。

9.4.3 其他互联网应用

了解远程接入、域名系统、即时通讯等其他互联网应用安全问题及解决措施。

9.5 知识子域：数据安全

9.5.1 数据库安全

了解数据库安全要求；

掌握数据库安全防护的策略和要求。

9.5.2 数据泄露防护

了解数据泄露防护的概念。

十、知识域：软件安全开发

10.1 知识子域：软件安全开发生命周期

10.1.1 软件生命周期模型

了解软件生命周期的概念及瀑布模型、迭代模型、增量模型、快速原型模型、螺旋模型、净室模型等典型软件开发生命周期模型。

10.1.2 软件危机与安全问题

了解三次软件危机产生的原因、特点和解决方案；

了解软件安全和软件安全保障的基本概念。

10.1.3 软件安全生命周期模型

了解 SDL、CLASP、CMMI、SAMM、BSIMM 等典型的软件安全开发生命周期模型。

10.2 知识子域：软件安全需求及设计

10.2.1 威胁建模

理解威胁建模的作用及每个阶段的工作内容；

掌握 STRIDE 模型用于进行威胁建模实践。

10.2.2 软件安全需求分析

理解软件安全需求在软件安全开发过程中的重要性；

理解安全需求分析的方法和过程。

10.2.3 软件安全设计

理解软件安全设计的重要性及内容和主要活动；

理解最小特权、权限分离等安全设计的重要原则；

理解攻击面的概念并掌握降低攻击面的方法。

10.3 知识子域：软件安全实现

10.3.1 安全编码原则

了解通用安全编程准则：验证输入、避免缓冲区溢出、程序内部安全、安全调用组件、程序编写编译等；

了解编码时禁止使用的风险函数；

了解相关的安全编码标准及建议；

理解常见的代码安全问题及处置办法。

10.3.2 代码安全编译

了解代码编译需要关注的安全因素。

10.3.3 代码安全审核

理解代码审查的目的；

了解常见源代码静态分析工具及方法。

10.4 知识子域：软件安全测试

10.4.1 软件测试

了解测试用例等软件测试的基本概念；

了解常见的软件测试方法及不同测试方法之间的区别和优缺点。

10.4.2 软件安全测试

了解软件安全测试的基本概念；

理解模糊测试、渗透测试等软件安全测试方法的的原理、相互的区别以及各自的优势；

掌握安全测试的思路和方法。

10.5 知识子域：软件安全交付

10.5.1 软件供应链安全

了解软件供应链安全的概念并理解软件供应链安全措施。

10.5.2 软件安全验收

了解软件安全验收的重要性及需要考虑的内容。

10.5.3 软件安全部署

了解软件安全部署的重要性及软件安全加固、软件安全配置的概念。