

CCSC网络安全能力认证学习资料（综合版）

一、认证概述与体系结构

CCSC，即网络安全能力认证（Certification for Cyber Security Competence），是由国家计算机网络应急技术处理协调中心（CNCERT）推出的面向重点行业网络与信息安全从业人员的社会化职业技能认证。该认证体系特点为**管理与技术并重、通用与特殊兼顾、理论与实践结合**，并强调**实践能力优先**。

1. 认证方向与等级

CCSC认证主要分为**管理方向**和**技术方向**，每个方向均设置了I级和II级。

认证方向	等级	核心能力要求	适用对象
管理方向	I级	了解网络信息安全基础知识、法律法规、安全体系标准和安全管理的基本知识。	负责安全管理、合规、审计等初级人员。
	II级	掌握使用安全标准和规范，具备开展安全工作的能力。	负责安全管理、安全总监、合规经理等中级人员。
技术方向	I级	了解网络信息安全的基本知识、法律法规、标准和规范，了解网络和信息安全评估、应急响应等工作内容。	负责安全运维、安全测试、应急处置等初级技术人员。
	II级	掌握网络信息安全评估、应急响应等技术，掌握常用安全工具的使用方法，有能力发现安全风险和处理安全事件。	具备独立解决复杂安全问题的中高级技术人员。

二、CCSC管理I级与II级核心知识大纲

管理方向侧重于信息安全管理体的构建、合规性、风险评估和安全运营。

1. CCSC管理I级核心知识点（入门级）

模块	核心知识点	学习要点
信息安全基础	信息安全基本概念、CIA三要素（机密性、完整性、可用性）、风险、威胁、漏洞、资产。	理解信息安全管理的基础理论和术语。
法律法规与标准	《网络安全法》、网络安全等级保护制度（等保2.0）基本要求、关键信息基础设施保护条例、个人信息保护相关法律法规。	掌握网络安全相关的核心法律法规和国家标准体系。
安全管理基础	安全策略的制定与发布、信息安全组织架构、资产管理、人员安全管理、物理与环境安全管理。	了解信息安全管理体系统（ISMS）的基本框架和要素。
应急响应基础	应急响应流程（准备、检测、遏制、根除、恢复、总结）、常见安全事件类型。	了解安全事件的分类和基本的应急响应处理流程。

2. CCSC管理II级核心知识点（进阶级）

模块	核心知识点	学习要点
安全管理领导力	信息安全战略规划、安全文化建设、安全团队管理实践、安全预算与资源分配。	掌握作为企业安全管理主管所需的领导力和规划能力。
安全生命周期管理	同步安全规划 ：将安全融入业务规划。 同步安全建设 ：安全技术体系的选型与部署。 同步安全运营 ：日常安全监控、漏洞管理、配置管理。	掌握将安全融入企业业务和IT生命周期的能力。
风险管理	信息安全风险评估 ：风险识别、分析、评价、处置。 新技术新业务安全评估 ：云计算、大数据、移动应用等新兴技术带来的风险评估与控制。	掌握专业的风险评估方法论，能够应对复杂风险。
安全合规与审计	内部安全审计、外部合规审计（如等保测评）、安全管理体系（如ISO 27001）的建立与维护。	掌握安全合规性要求，并具备组织和实施安全审计的能力。

三、CCSC技术I级与II级核心知识大纲

技术方向侧重于网络攻防、安全防护技术、安全测评和应急响应的实战能力。

1. CCSC技术I级核心知识点（入门级）

模块	核心知识点	学习要点
信息安全基本技术	网络安全技术：防火墙、入侵检测/防御系统（IDS/IPS）、VPN、安全隔离与信息交换。密码技术：对称加密、非对称加密、哈希、数字签名、数字证书。身份认证：口令、双因素认证、PKI体系。	掌握主流安全防护产品和工具的基本原理。
IT基础设施安全	操作系统安全（Windows/Linux）配置与加固、数据库安全、网络设备安全配置。	了解IT基础设施的安全配置和加固方法。
Web应用安全	常见的Web漏洞（如SQL注入、XSS、CSRF、文件上传）、Web安全防护措施（如WAF、输入验证）。	了解Web应用面临的主要安全威胁及基础防护手段。
应急响应基础	应急响应流程（准备、检测、遏制、根除、恢复、总结）、常见安全事件类型。	了解安全事件的分类和基本的应急响应处理流程。

2. CCSC技术II级核心知识点（进阶级）

模块	核心知识点	学习要点
安全防护体系	纵深防御体系、安全运营中心（SOC）、安全信息和事件管理（SIEM）平台的使用与分析。	掌握构建和运营复杂安全防护体系的能力。
安全测评体系	渗透测试流程与方法论、漏洞扫描工具（如Nessus、AWVS）的使用、风险评估技术。	掌握网络信息安全评估的技术和方法。
应急响应体系	恶意代码分析（静态/动态）、日志分析与溯源、入侵取证技术、事件报告与总结。	掌握高级应急响应技术，能够处理复杂安全事件。
网络安全攻防	端口扫描、漏洞利用、内网渗透技术、流量分析与协议解析。	具备实际的网络攻防和检测能力。
系统与Web安全攻防	操作系统提权、后门植入、内核级攻击。高级Web漏洞利用（如反序列化、SSRF）、代码审计。	掌握系统和Web应用层面的进阶攻防技术。
新兴领域安全	云计算安全 （虚拟化安全、云平台安全配置）、 大数据安全 （数据脱敏、隐私保护）、 物联网安全 （设备认证、通信安全）。	了解并掌握新兴技术领域特有的安全挑战和解决方案。
业务与数据安全	业务逻辑漏洞、数据分类分级、数据生命周期安全管理。	掌握数据安全和业务连续性保障的关键技术。

四、考试形式与要求

CCSC认证的考试形式和要求因等级而异，技术II级尤其注重实操能力。

1. I级考试（管理I级/技术I级）

项目	详情
考试形式	线上考试（闭卷上机考试），采用双平台双机位。
考试时长	1.5小时（90分钟）。
题型与分值	单选题：60道，每题1分。多选题：20道，每题2分。判断题：20道，每题1分。 总分：120分。
合格标准	84分及格 （总分的70%）。

2. II级考试（技术II级）

项目	详情
考试形式	笔试 + 实操（均为机考），采用双平台双机位。
考试时长	4个小时（笔试1小时，实操3小时）。
笔试部分	占总分比例40%。题型：单选题40道（每题2分），判断题20道（每题1分）。总分100分。
实操部分	占总分比例60%。题型：10道实操题（分值不同）。总分100分。

五、学习建议

- 明确方向**：根据职业规划选择**管理**或**技术**方向，建议从**I级**开始打基础。
- 管理方向**：重点在于**法律法规**、**标准体系**（如等保2.0）和**风险评估**方法论。
- 技术方向**：I级侧重**基础技术原理**，II级核心是**实操能力**。必须通过实验环境进行攻防演练。
- 系统学习**：严格按照知识大纲，逐一攻克，构建完整的知识图谱。
- 模拟测试**：利用模拟题熟悉考试节奏和题型，确保在规定时间内达到合格分数。