**中 国 认 证 认 可 协 会**



信息安全管理体系基础考试大纲

# 第 1 版

文件编号：CCAA-TR-110-01:2021

发布日期：2021 年 3 月 2 日 实施日期：2021 年 4 月 1 日

# 信息安全管理体系基础考试大纲（第 1 版）

1. 总则

本大纲依据 CCAA《管理体系审核员注册准则》制定，适用于拟向 CCAA 申请注册信息安全管理体系审核员实习级别的人员。

1. 考试要求
   1. 考试科目

申请注册信息安全管理体系审核员实习级别的人员，需通过“信息安全管理体系基础”科目考试。

* 1. 考试方式

“信息安全管理体系基础”科目考试为闭卷考试，考试试题由 CCAA统一编制，考试时间 1.5 小时。

* 1. 考试频次及地点

考试原则上每年组织 2 次，CCAA 在考前 40 天发布报名通知，申请人可在每次考试设立的考点范围内选择报名并参加考试。

* 1. 考试的题型及分值

|  |  |  |  |
| --- | --- | --- | --- |
| 题型 | 数量 | 单题分值（分） | 小计分值（分） |
| 单项选择题 | 40 | 1.5 | 60 |
| 多项选择题 | 15 | 2 | 30 |
| 判断题 | 10 | 1 | 10 |

* 1. 考试合格判定

“信息安全管理体系基础”科目考试的满分为 100 分，考试成绩

70 分（含）以上为合格。

* 1. 考试结果发布

CCAA 将在考试结束后 45 天（遇法定节日顺延）内发布考试结果，申请人可在CCAA 官方指定渠道查询考试成绩。

1. 考试内容
   1. 信息安全管理体系标准
      1. 了解 ISO/IEC 27000 系列标准发展概况；
      2. 了解 GB/T 28450《信息安全技术 信息安全管理体系审核指南》的内容；
      3. 了解 ISO/IEC 27006《信息技术 安全技术 信息安全管理体系审核认证机构的要求》的目的、意图以及第 9 章的内容；
      4. 理解GB/T 29246 《信息技术 安全技术 信息安全管理体系 概述和词汇》中的术语，以及术语所涉及的相关技术、产品及其应用。 e)理解和掌握GB/T 22080《信息技术 安全技术 信息安全管理体

系 要求》的内容和要求；

1. 了解 ISO/IEC 27000 系列标准的部分规范性文件和指南，如：
   1. GB/T 22081《信息技术 安全技术 信息安全控制实用规则》；
   2. ISO/IEC 27004《信息技术 安全技术 信息安全管理 监视，测量，分析和评估》；
   3. ISO/IEC 27005《信息技术 安全技术 信息安全风险管理》。 g)理解信息安全有关标准的要求。
2. GB 17859《计算机信息系统安全保护等级划分准则》；
3. GB/Z 20986《信息安全技术 信息安全事件分类分级指南》。
   1. 信息安全管理领域专业知识 a)掌握相关管理知识和技术：
4. 常用统计技术方法；
5. 风险管理方法；
6. 测量和监视技术；
7. 顾客满意的监视和测量、投诉处理、行为规范、争议解决；
8. 持续改进、创新和学习。 b)理解信息安全领域的专业知识；

重点理解如下专业知识:网络结构与通信基础、数据安全、载体安全、环境安全、边界安全、应用安全等相关技术；掌握与组织业务活动相关的知识，例如：流程、资产、风险、安全要求、控制措施以及信息安全技术和信息技术在业务活动中的特定应用等；

c)了解信息安全管理相关工具、方法、技术以及在审核过程中的综合运用。

* 1. 法律法规和其他要求
     1. 理解信息安全管理相关法律法规的要求，如： 1)《中华人民共和国保守国家秘密法》；

1. 《中华人民共和国网络安全法》；
2. 《中华人民共和国密码法》；
3. 《中华人民共和国计算机信息系统安全保护条例》；
4. 《信息安全等级保护管理办法》；
5. 《互联网信息服务管理办法》；
6. 《网络安全审查办法》。
   * 1. 理解中国认证认可协会相关人员注册与管理要求。

注：本大纲中的标准和法律法规以现行有效的为准。