中国认证认可协会文件

中认协培〔2015〕106号

关于发布《信息安全管理体系审核员考试大纲（第2版）》的通知

各相关机构和人员：

为满足CCAA《管理体系审核员注册准则（第1版）》的有关要求，确保信息安全管理体系审核员水平，我会制定了《信息安全管理体系审核员考试大纲（第2版）》（见附件），现予以发布实施。

特此通知。

附件：《信息安全管理体系审核员考试大纲（第2版）》

中国认证认可协会

2015年4月27日

附件

中 国 认 证 认 可 协 会

信息安全管理体系审核员考试大纲

第 2 版

文件编号：CCAA-307

发布日期： 2015年 4月 27日　　实施日期： 2015 年 5月1日

1. 总则

本大纲依据CCAA《管理体系审核员注册准则（第1版）》（以下简称注册准则）制定，旨在通过统一的笔试，客观、公正、全面地考核参加考试人员满足注册准则中“2.5知识和技能要求”的程度，为CCAA评价注册申请人的能力提供依据，适用于拟向CCAA申请注册为各级别信息安全管理体系审核员的人员。

2. 考试要求

2.1 考试科目

申请实习审核员注册需通过“基础知识”科目考试；

申请审核员注册需通过“审核知识与技能”科目考试；

申请主任审核员注册需通过 “管理理论知识与应用技能”科目考试；

参加考试时，考生需提供本人准考证和身份证件原件。

考生应严格遵守考场纪律（见附件一），并自觉服从监考人员等考试工作人员管理。

2.2 考试方式

考试为书面闭卷考试，考试试题由CCAA统一编制，每科考试时间2小时。

参加“基础知识”考试时，考生不能携带任何参考资料；参加“审核知识与技能”和“管理理论知识与应用技能”考试时，考生自带未做任何标记的GB/T 22080/ISO/IEC 27001《信息技术 安全技术 信息安全管理体系 要求》标准文本。

2.3 考试频次及地点

考试原则上每半年组织一次，在北京和选定的大中城市设立考点。CCAA在考前40天发布报名通知，申请人可在每次设立的考点范围内选择地点报名并参加考试。

2.4 考试费用

CCAA根据《认证人员注册收费规则》收取考试费用。

报名截止后，无论是否参加考试，考试费用将不予退还。

2.5 考试的题型及分值

2.5.1 基础知识科目的题型及分值

分值分布	1.信息安全管理体系标准　约占50% 2.信息安全管理领域专业知识　约占20% 3.管理体系审核　约占15% 4.法律法规　约占10% 5.个人素质　约占5%		
题　型	数 量	单题分值（分）	小计分值（分）
单项选择题	80	1	80
多项选择题	20	2	40

2.5.2 审核知识与技能科目的题型及分值

分值分布	1.信息安全管理体系审核　约占45% 2.信息安全管理领域专业知识　约占15% 3.信息安全管理体系标准和规范性文件、专业知识、法律法规的综合应用　约占40%		
题　型	数 量	单题分值(分)	小计分值（分）
单项选择题	40	1	40

多选题	5	2	10
案例分析题	5	6	30
阐述题	2	10	20

2.5.3 管理理论知识与应用技能科目的题型及分值

分值分布	1.信息安全管理体系审核实践综合能力　　约占 60% 2.信息安全管理领域专业知识　　约占 40%		
题　型	数 量	单题分值(分)	小计分值（分）
单选题	20	1	20
多选题	10	2	20
案例题	1	20	20
论述题	1	40	40

2.6 考试合格判定

基础知识科目满分为 120 分，96 分（含）以上合格；

审核知识与技能科目考试的满分为 100 分，70 分（含）以上合格；

管理理论知识与应用技能科目满分 100 分，70 分（含）以上合格。

2.7 考试结果发布

CCAA 将在考试结束后 45 天（遇法定节日顺延）内公布考试合格人员名单。

3．基础知识科目的考试内容

3.1 信息安全管理体系标准

a. 了解 ISO/IEC 27000 族标准的发展概况及相关国家标准；

b. 理解 GB/T 29246/ISO/IEC 27000《信息安全管理体系 概述与词汇》中的部分术语，重点理解以下术语：

1)访问控制、2)攻击、3)身份鉴别、4)保密性、5)完整性、6)可用性、7)不可否认性、8)信息处理设施、9)信息安全、10)信息安全连续性、11)事态、12)信息安全事态、13)信息安全事件、14)信息安全事件管理、15)信息系统、16)管理体系、17)最高管理者、18)风险、19)威胁、20)脆弱性、21)可能性、22)后果、23)风险责任人、24)风险识别、25)风险分析、26)风险评价、27)风险评估、28)风险处置、29)残余风险、30)风险接受、31)风险管理、32)方针、33)控制措施、34)控制目标、35)过程、36)形成文件的信息、37)不符合、38)纠正措施、39)信息共享社区、40)可信信息沟通实体、41)利益相关方、42)内部环境、43)外部环境。

c. 理解 GB/T 22080/ISO/IEC 27001 的要求；

d. 了解 GB/T 22081/ISO/IEC 27002 标准的结构、适用范围及与 GB/T 29246/ISO/IEC 27000 《信息安全管理体系 概述与词汇》、GB/T 22080/ISO/IEC 27001 标准的关系；

e. 理解 ISO/IEC 27000 族标准的部分规范性文件和指南，如：

--- ISO/IEC 27004《信息技术 安全技术 信息安全管理 测量》

--- ISO/IEC 27005《信息技术 安全技术 信息安全风险管理》

3.2 信息安全管理体系审核

a. 理解 GB/T 28450《信息安全管理体系审核指南》标准第 3、4 章及第 6 章 6.3 和 6.4 的内容；

b. 理解 CNAS-CC17《信息安全管理体系认证机构要求》的目的、意图以及第 9 章的部分内容。

3.3 信息安全管理领域专业知识

a. 熟悉并掌握相关管理专业知识

1) 常用统计技术方法

2) 测量和监视技术

3) 顾客满意的监视和测量、投诉处理、行为规范、争议解决

4) 风险管理方法

5) 持续改进、创新和学习

b. 了解信息安全管理相关工具、方法、技术及其应用

3.4 法律法规

a. 掌握信息安全管理相关法律法规的要求

1) 《中华人民共和国保守国家秘密法》

2) 《中华人民共和国计算机信息系统安全保护条例》

3) 《信息安全等级保护管理办法》

4) 《互联网信息服务管理办法》

b. 了解国家认证认可法规、规章要求和国家认证认可体系

《中华人民共和国认证认可条例》

4. 审核知识与技能科目的考试内容

4.1 信息安全管理体系审核

a. 掌握GB/T 28450标准第3、4、6章及第5章及第5章5.4.2、5.4.4的要求，并能应用到审核实践中；

b. 掌握GB/T 28450标准附录B的内容，并能应用到审核实践中；

c. 掌握CNAS-CC17 第9章的内容，并能应用到审核实践中；

d. 掌握信息安全管理体系要求；法律法规、认可准则要求；信息安全应用工具、方法、技术及其在审核过程中的综合运用。

4.2 信息安全管理体系标准和规范性文件

a. 理解 GB/T 29246/ISO/IEC 27000 标准中的术语和信息安全管理体系基础;

b. 理解 GB/T 22080/ISO/IEC 27001 标准要求;

c. 掌握 GB/T 29246/ISO/IEC 27000 族标准部分规范性文件和指南的内容（ GB/T 22081/ISO/IEC 27002、 ISO/IEC 27004、 ISO/IEC 27005）

d. 掌握信息安全有关标准的要求（GB 17859《计算机信息系统安全保护等级划分准则》、GB/Z 20986 《信息安全技术 信息安全事件分类分级指南》）

4.3 信息安全管理领域专业知识

理解网络与通信基础、数据安全、载体安全、环境安全、应用安全等相关技术。

5. 管理理论知识与应用技能科目的考试内容

5.1 信息安全管理体系审核

精通并熟练掌握和准确应用信息安全管理体系审核原则及相关技术，并在审核实践中具有综合评价和风险控制的能力。

5.2 信息安全管理领域专业知识：

掌握网络与通信基础、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。

5.3 掌握现代信息安全管理前沿技术和动态

附件一：考场纪律及考试违规认定与处理

一、考场纪律

考生应严格遵守以下考场纪律，并自觉服从监考人员等考试工作人员管理，不得以任何理由妨碍监考人员等考试工作人员履行职责，不得扰乱考场及其他考试工作地点的秩序。

（一）考生应重道德、讲诚信，互相尊重。

（二）考生应携带《准考证》等规定证件，在规定时间和地点参加考试。

（三）考生应按规定向监考人员出示相关证件，并按准考证号（座位号）入座。将《准考证》等相关证件放在指定位置以便核验。

（四）考生进入考场除考试用蓝、黑签字笔外，其他任何物品不准带入考场。

严禁携带各种通讯工具（如手机、电脑及其他无线接收、传送设备等）、电子存储记忆录放等设备进入考场。严禁随身夹带文字材料及其他与考试无关的物品。

（五）考生在领到试卷后，应在指定位置清楚地填写姓名、准考证号、座位号等信息。

（六）考生应使用蓝、黑签字笔作答，不得使用红色等其他颜色笔或铅笔答题。

考生应将答案书写在试卷指定位置，不准在答卷上做任何标记。

使用规定以外的笔答题或未在试卷指定位置作答的答案，均视为无效答案，不记成绩。

（七）考生在考场内必须保持安静。不准吸烟，不准喧哗，不准交

头接耳、左顾右盼、打手势、做暗号，不准夹带、旁窥、抄袭或有意让他人抄袭，不准传抄答案或交换试卷、草稿纸。考场内不得自行传递文具、用品等。

（八）考试结束前要离开考场的考生须先将试卷反扣在桌面上，再举手提出离场，经监考人员允许后才准离开考场。离开考场后不得再次进场续考，也不准在考场附近逗留、交谈、喧哗。

（九）考生不得将试卷、草稿纸等考场上所发的任何考试材料带出考场。

二、违规认定与处理

考生不遵守考场纪律，不服从考试工作人员的安排与要求，有下列行为之一的，认定为考试**违纪行为：**

（一）携带规定以外的物品进入考场或者未放在指定位置。

（二）未在规定的座位参加考试。

（三)考试开始信号发出前答题或者考试结束信号发出后继续答题。

（四）在考试过程中旁窥、交头接耳、互打暗号或者手势。

（五）在考场或者禁止的范围内，喧哗、吸烟或者实施其他影响考场秩序行为。

（六）未经考试工作人员同意在考试过程中擅自离开考场。

（七）将试卷(含答题纸等)、草稿纸等考试用纸带出考场。

（八）用规定以外的笔或者纸答题或者在试卷规定以外的地方书写姓名、考号或者以其他方式在答卷上标记信息。

（九）其他违反考场规则但尚未构成作弊的行为。

考生违背考试公平、公正原则，以不正当手段获得或者试图获得

试题答案，有下列行为之一的，认定为考试**作弊行为**：

（一）携带与考试内容相关的文字材料或者存储有与考试内容相关资料的电子设备参加考试。

（二)抄袭或者协助他人抄袭试题答案或者与考试内容相关的资料。

（三）抢夺、窃取他人试卷、答卷或者强迫他人为自己抄袭提供方便。

（四）在考试过程中使用通讯设备。

（五）由他人冒名代替参加考试。

（六）故意销毁试卷、答卷或者考试材料。

（七）在答卷上填写与本人身份不符的姓名、考号等信息。

（八）传、接物品或者交换试卷、答卷、草稿纸。

（九）其他作弊行为。

考生如有考试违纪行为之一的，取消该科目的考试成绩；考生如有考试作弊行为之一的，取消其当次报名参加考试的各科成绩；考生如扰乱考试工作场所秩序，拒绝、妨碍考试工作人员履行管理职责的，终止其继续参加该科目考试，其当次报名参加考试的各科成绩无效。

违规考生如具备 CCAA 认证人员注册资格的，还将按照《注册人员资格处置规则》进行相应的资格处置。

抄送：国家认监委认可监管部，存档（2）。

中国认证认可协会　　2015 年 4 月 27 日印发