中国认证认可协会文件

中认协注 〔2013〕10 号

关于发布《信息安全管理体系审核员考试大纲》的通知

各相关认证机构和人员：

为满足信息安全管理体系认证需求，确保信息安全管理体系审核员水平，根据中国认证认可协会（CCAA）《信息安全管理体系审核员注册准则（第 1 版）》，我会制定了《信息安全管理体系审核员考试大纲》（见附件），现予以发布实施，请遵照执行。（附件文件也可在 CCAA 网站 www.ccaa.org.cn 查看下载。）

附件：信息安全管理体系审核员考试大纲

中国认证认可协会

2013 年 1 月 10 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

文件编号：CCAA-324

发布日期：2013 年 1 月 10 日　　实施日期：2013 年 1 月 10 日

信息安全管理体系审核员考试大纲

1. 总则

本大纲依据 CCAA-141《信息安全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“ 2.4 知识和技能要求 ”的程度，及其基本的个人素质情况，为 CCAA 评价信息安全管理体系实习审核员注册申请人的能力提供依据。本大纲适用于拟向 CCAA 申请注册为信息安全管理体系实习审核员的人员。

2. 考试要求

2.1 考试对象

已完成符合注册准则 2.2.4 要求的信息安全管理体系审核员培训的人员。参加考试时，考试人员需提供本人身份证件。

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。

考试分为基础知识和审核知识两部分，每部分考试时间为 60 分钟，总考试时间为 120 分钟，可安排在同一时段先后进行。

参加基础知识考试时，考生不能参考任何资料；参加审核知识考试时，培训机构可为考生提供 GB/T 22080-2008《信息安全管理体系 要求》文本。

考生应严格遵守考场规则（见附件）。违反考场规则者，将取

消考试资格和考试成绩。

2.3 考试费用

CCAA 根据《认证人员注册收费规则》收取考试费用。

2.4 考试的题型及分值

2.4.1 基础知识部分考试的题型及分值

分值分布	1）GB/T 22080-2008 标准理解 约占 65% 2）与 GB/T 22080-2008 有关的计算机信息安全基础知识、风险管理基础知识 约占 20% 2）法律法规知识 约占 10% 3）个人素质与审核员管理的通用要求 约占 5%		
题型	数量	单题分值	小计分值
单项选择题	60	1	60

2.4.2 审核知识部分考试的题型及分值

分值分布	1）审核及认证知识 约占 20% 2）信息安全管理体系审核 约占 80%		
题型	数量	单题分值	小计分值
简述题	2	5	10
案例分析题	5	6	30

2.5 考试合格判定

基础知识部分和审核知识部分考试的合并满分为 100 分，总成

绩 70 分（含）以上合格，达到合格分数则通过考试。

3. 基础知识部分的考试范围和内容

3.1 范围

a. 注册准则 2.3.1 个人素质

b. 注册准则 2.4.1.2 信息安全管理体系、计算机安全基础知识、风险管理基础

c. 注册准则 2.4.1.3 法律法规

3.2 内容

3.2.1 个人素质

a. 阅读理解能力

b. 观察感知能力

c. 分析判断能力

d. 逻辑推理能力

3.2.2 标准

掌握 GB/T 22080-2008 《信息安全管理体系 要求》标准全部条款。

3.2.3 信息安全基础知识

术语与概念

a. 依据 GB/T 19000 《质量管理体系 基础与术语》信息(3.7.1)。

b. 依据 GB/T 25069-2010 《信息安全技术 术语》:

口令(2.2.2.76)、访问控制（2.2.1.42）、密钥(2.2.2.106)、密码（2.2.2.92)、加密（2.2.2.60)、风险（2.3.35)、威胁（2.3.94)、脆弱性（2.3.30)、应急预案(2.2.3.4)、灾难恢复计划(2.2.3.5)、入侵检测(2.2.1.100)、访问控制列表（2.2.1.43)、物理访问控制（2.2.1.115)、远程访问（2.2.1.128)、最小特定权限（2.2.1.142)、密钥管理（2.2.2.114)、数字签名(2.2.2.176)、端口（2.2.1.37)。

c. 依据 GB/T 22080-2008 《信息安全管理体系　要求》

保密性（3.3)、完整性（3.8)、可用性（3.2)、风险分析（3.11)、风险评估（3.12)、风险处置（3.15)、风险接受（3.10)、风险管理(3.14)、残余风险(3.9)。

d. 依据 GB/T 20988-2007 《信息安全技术　信息系统灾难恢复规范》

灾难备份中心（3.1)、灾难备份（3.2)、灾难备份系统(3.3)、业务连续管理（3.4)、业务影响分析（3.5)、灾难恢复预案（3.10)、恢复时间目标（3.18)、恢复点目标（3.19)、

3.2.4　法律法规知识

a. 《中华人民共和国认证认可条例》

a) 第一章　第二条、第三条

b) 第二章　第九条、第十条、第十一条、第十三条、第十五条

c) 第三章　第二十条、第二十三条、第二十五条

d) 第四章　第三十九条

e) 第六章　第六十条、第六十三条。

b. 《认证及认证培训、咨询人员管理办法》

a) 第一条、第二条、第三条、第六条、第七条、第八条、第十条、第二十条。

c. 《中华人民共和国保守国家秘密法》

a) 第一章　总则

b) 第二章　国家秘密的范围和密级

c) 第三章　保密制度，第二十一条至第二十六条

d. 《中华人民共和国计算机信息系统安全保护条例》

a) 第一章　总则

b) 第二章　安全保护制度

c) 第五章　附则，第二十八条

e. 《信息安全等级保护管理办法》

a) 第一章　总则，第三条

b) 第二章　等级划分与保护

c) 第三章　等级保护的实施与管理，第十条，第十一条，第十四条

d) 第四章　涉及国家秘密信息系统的分级保护原理，第二十五条，第二十七条，第二十八条

e) 第五章　信息安全等级保护的密码管理，第三十五条至第三十九条

f. 《中华人民共和国商用密码管理条例》

a) 第一章　总则

b) 第二章　科研、生产管理

c) 第三章　销售管理

d) 第四章　使用管理

e) 第五章　安全保密管理

4. 审核知识部分的考试范围和内容

4.1　范围

a. 注册准则 2.3.2 审核原则

b. 注册准则 2.4.1.1 管理体系审核

c. 注册准则 2.5 注册人员行为规范

4.2　内容

4.2.1　审核过程：依据 GB/T 28450-2012 《信息安全管理体系审核指南》标准的内容：

a. 3 术语与定义

b. 4.1 审核原则

c. 4.1.1 IS 4.1 审核原则

d. 5 审核方案的管理

e. 6. 审核活动

f. 7.4 教育、工作经历、审核员培训和审核经历

4.2.2 认证过程：依据 CNAS-CC17：2012 《信息安全管理体系认证机构要求》(ISO/IEC 27006:2011)的部分内容：

a. 9.2 初次审核与认证

b. 9.3 监督活动

c. 9.4 再认证

d. 9.5 特殊审核

e. 9.6 暂停、撤销或缩小认证范围

附件 :考场规则

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：存档（2）。

中国认证认可协会　　2013年1月10日印发