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 版第 1 次修订

文件编号：CCAA-307
发布日期： 2017年7月28日　　实施日期： 2017年 7 月28 日

信息安全管理体系审核员考试大纲

第 2 版第 1 次修订

1．总则

本大纲依据CCAA《管理体系审核员注册准则》（以下简称注册准则）制定，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。

2.2 考试方式

考试为书面考试，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”考试时，考生自带未做任何标记的GB/T 22080-2016/ISO/IEC 27001:2013《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报名并参加考试。

2.4 考试的题型及分值

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.信息安全管理体系审核　约占 15% 4.法律法规和其他要求　约占 15%		
题　型	数 量	单题分值（分）	小计分值（分）
单项选择题	50	1	50
判断题	10	1	10
多项选择题	20	2	40

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知识及应用　约占 45% 2.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% 3.信息安全管理领域专业知识　约占 15%		
题　型	数 量	单题分值（分）	小计分值（分）

单项选择题	30	1	30
多项选择题	10	2	20
阐述题	2	10	20
案例分析题	5	6	30

2.5 考试合格判定

基础知识科目满分为 100 分，80 分（含）以上合格；

审核知识与技能科目考试满分为 100 分，70 分（含）以上合格。

2.6 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：访问控制、攻击、身份鉴别、真实性、可用性、保密性、符合性、后果、控制措施、控制目标、纠正、纠正措施、决策准则、形成文件的信息、事态、外部环境、信息安全治理、信息处理设施、信息安全、信息安全连续性、信息安全事态、信息安全事件、信息安全事件管理、信息系统、完整性、相关方、内部环境、风险水平、可能性、不符合、不可否认性、过程、可靠性、要求、残余风险、评审、风险、风险接受、风险分析、风险评估、风险沟通和咨询、风险准则、风险评价、风险识别、风险管理、风险责任者、风险处置、安全实施标准、威胁、脆弱性；

c）理解 GB/T 22080-2016/ISO/IEC 27001:2013 的要求；

d）了解 GB/T 22081-2016/ISO/IEC 27002：2013《信息技术 安全技术 信息安全控制实践指南》标准的结构、适用范围及其与 GB/T 29246/ISO/IEC 27000《信息安全管理体系 概述与词汇》、GB/T 22080-2016/ISO/IEC 27001:2013 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 、6 章及第 5 章 5.4 的内容；

b） 理解 CNAS-CC170《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 法律法规和其他要求

a）掌握信息安全管理相关法律法规和其他要求：

1)《中华人民共和国保守国家秘密法》;

2)《中华人民共和国网络安全法》;

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》)。

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》。

c）理解中国认证认可协会相关注册要求。

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知识及应用

a）掌握GB/T 28450 标准第3、4、6 章及第5 章5.4 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-CC170 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 22080-2016/ISO/IEC 27001:2013 标准要求;

c）掌握 ISO/IEC 27000 族标准部分规范性文件和指南的内容（ GB/T 22081-2016/ISO/IEC 27002:2013、 ISO/IEC 27004、 ISO/IEC27005）;

d）掌握信息安全有关标准的要求：

1）GB 17859《计算机信息系统安全保护等级划分准则》;

2）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

a）理解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;

b）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方面的知识。