

# 中国认证认可协会文件

中认协注[2011]81号

---

## 关于发布《信息安全管理体系 认证审核员确认方案（第2版）》的通知

各相关认证机构：

为进一步做好信息安全管理体系的认证工作，我会在原《信息安全管理体系认证审核员确认方案》的基础上，制订了《信息安全管理体系认证审核员确认方案（第2版）》，现予以发布。于2011年7月1日起实施，原《信息安全管理体系认证审核员确认方案》同时废止。

特此通知。

附件：信息安全管理体系认证审核员确认方案（第2版）

二〇一一年六月十三日

附件：

## 信息安全管理体系认证审核员确认方案（第2版）

### 一、目的

为满足国家质量监督检验检疫总局《认证及认证培训、咨询人员管理办法》（总局令2004年第61号）第六条“属于认证及认证培训、咨询新领域、国家尚未建立执业资格注册制度的，由相应认证及认证培训、咨询机构建立执业人员评价制度，并统一向中国认证人员与培训机构国家认可委员会申请办理相关人员执业资格的确认，未经确认的，不得从事相关活动”规定的要求，中国认证认可协会（CCAA）根据《新领域认证及认证培训、咨询人员确认程序规则》的有关规定，制定本确认方案。

### 二、确认范围与级别

1. 本方案适用于信息安全管理体系（以下简称 ISMS）审核员的确认。

2. 确认分 ISMS 审核员和 ISMS 高级审核员两个级别。

### 三、确认要求

（一）对确认申请人推荐机构的要求

1. 经 CNCA 批准的认证机构；

2. 建立了与所从事的认证活动相适应的认证人员选择、培训、评价、聘用和管理的制度或程序并形成文件；

3. 按照机构建立的评价制度对申请人的专业能力作出评价和证实，并形成记录。

（二）对确认申请人的基本要求

1. 个人素质

申请人应具备以下个人素质：

- 有道德：公正、可靠、忠诚、诚实和谨慎；
- 思想开明：愿意考虑不同意见或观点；
- 善于交往：灵活地与人交往；
- 善于观察：主动地认识周围环境和活动；
- 有感知力：能本能地了解和理解环境；
- 适应力强：容易适应不同情况；
- 坚韧不拔：对实现目的坚持不懈；
- 明断：根据逻辑推理和分析及时得出结论；
- 自立：在同其他人交往中独立工作并发挥作用。

## 2.行为准则

经确认的 ISMS 审核员有义务严格遵守以下行为准则：

- 遵纪守法、敬业诚信、客观公正；
- 努力提高审核技能和信誉；
- 帮助其监督管理的人员提高管理水平、专业和审核技能；
- 不承担本人不具备能力的审核；
- 不介入冲突或利益竞争，不向审核员聘用机构隐瞒任何可能影响公正判断的关系；
- 除非审核员聘用机构和受审核方书面授权或有法律要求，不讨论或透露任何有关审核的信息；
- 不接受受审核方及其工作人员或任何相关方的回扣、礼品及其他任何形式的好处，也不应在知情时允许同事接受；
- 不有意传播任何错误的或易产生误解的信息，以防影响审核或审核员注册/确认过程的信誉；
- 在任何情况下，不损坏 CCAA 及其注册/确认过程的声誉，与针对违背本准则的行为而进行的调查给予充分的合作；
- 不对受审核方既进行咨询又进行认证审核。

## 3.知识要求

### 3.1 管理体系审核

- 理解 GB/T19011 标准 3、4、6 章的内容；
- 理解审核原则、程序和技术的应用；
- 理解受审核方管理体系与审核准则的关系；
- 理解如何确定组织的信息安全管理体系范围,以及在受审核方组织环境中实施有效的审核；
- 理解审核中运用抽样技术的适宜性和后果；

### 3.2 信息安全管理体系

- 理解 GB/T 22080-2008 / ISO/IEC27001:2005 标准每项条款的内容和要求；
- 理解 GB/T 22080-2008 / ISO/IEC27001:2005 标准中的术语；
- 理解信息安全特性（保密性、可用性、完整性以及真实性、可核查性、不可否认性和可信性）之间的联系；
- 理解信息安全管理体系在不同类型组织中的应用，包括：
  - a)不同类型组织信息资产的识别以及与组织业务的关系；
  - b)不同类型组织资产脆弱性与威胁的识别以及与组织业务的关系；
  - c)不同类型组织信息安全技术应用以及与组织业务的关系；
  - d)保障物理区域安全的常用技术；
  - e)通信设施及信息处理设施运行中的信息安全；
  - f)信息系统的开发、获取和维护；
  - g)访问控制；
  - h)信息安全领域的业务连续性管理与容灾；

i)信息安全技术符合性测试及 IT 系统审计;

j)理解 GB/T 22080-2008 / ISO/IEC27001:2005 标准中控制措施的选择以及删减原则。

- 理解风险管理的基本原理和常用风险评估技术以及在信息安全管理中的应用;

- 了解用于文件、数据和记录的授权、安全、发放、控制的信息系统和技术。

### 3.3 法律法规

- 了解我国法律法规体系的构成;

- 了解组织所属行业和行业性法律法规要求;

- 与信息安全管理体的关系以及在审核中的应用;

- 了解国家认证认可法规、规章要求;

- 了解相关的国际条约和公约、合同和协议等;

- 了解组织遵守的其他要求;

- 了解 CCAA 审核员行为规范要求。

### 4.教育经历

申请人应具有国家承认的信息安全相关专业(见附件)或相近专业大学本科(含)以上学历,并获得国家承认的学士(含)以上学位或与信息安全和信息技术相关的中级(含)以上技术职称。

注:信息安全相近专业指与信息安全和信息技术相近的专业,如光电子技术科学、集成电路设计与集成系统、智能科学与技术、信息显示与光电技术、数字媒体技术、测绘工程、遥感科学与技术、电子商务、网络工程、广播电视工程、建筑设施智能技术、电气工程及自动化等。必要时须向 CCAA 提供相关证明材料。

## 5.工作经历

申请人应具有至少 4 年全职工作经历。

工作经历应是在取得大学本科（含）以上学历之后获得的。

## 6.专业工作经历

具有信息安全相关专业学历的申请人在全部工作经历中应具有至少 2 年与信息安全相关的工作经历。

具有信息安全相近专业学历的申请人在全部工作经历中应具有至少 4 年与信息安全相关的工作经历。

信息安全相关工作经历包括信息安全管理（如 ISMS 的研究、实施、运作、咨询、审核、教学经历），信息安全技术工作（如信息安全科研教学、工程设计与实施、产品研发与测试和网络管理工作等）。

其中，ISMS 的实施经历是指组织中业务管理部门的人员和组织中信息安全管理体系实施部门的负责人具体实施管理体系的经历。ISMS 的运作经历指组织中最高管理层、信息安全主管部门的人员策划、运行管理体系的经历。

专业工作经历与工作经历可以同时发生。

## 7. 培训考试

申请人应成功地完成 CCAA 确认的、不少于 40 小时的 ISMS 审核员培训课程，并经 CCAA 考试合格。

## 8. 审核经历

审核员申请人应完成至少 3 次审核经历，审核经历可以是 ISMS 见习审核经历或与信息技术有关的 QMS 正式审核经历（即质量管理体系认证业务范围分类表中第 33 大类的审核经历）；

高级审核员申请人应在取得 ISMS 审核员资格后，作为审核组长，领导审核组完成至少 3 次 ISMS 审核经历，并具有 CCAA QMS 高级审核员注册资格 1 年以上或与信息安全和信息技术相关的高级技术职称。

## 9. 聘用

确认申请人应与推荐机构(且仅与此一个机构)建立认证人员聘用关系。

### 四、确认过程

#### (一) 申请

确认申请应由聘用申请人的认证机构统一向 CCAA 申报。

#### (二) 申报资料

##### 1. 认证机构应提交:

- 机构的批准文件复印件;
- 机构的营业执照复印件;

##### 2. 确认申请人应提交:

● 《CCAA 认证人员确认申请表》，申请表应经聘用机构盖章确认;

- 身份证复印件;
- 学历和学位证明复印件;
- 培训和考试合格证明文件复印件;
- 聘用合同复印件;
- 聘用机构按照其建立的人员评价制度为申请人出具的专业能力评价记录;

● 审核经历记录(包括 CCAA《审核经历记录表》和审核计划);

● QMS 高级审核员证书或公告复印件(适用时);

● 与信息安全和信息技术相关的技术职称证书复印件(适用时)。

3、申请人应按 CCAA-201《认证人员注册、培训认可收费规则》缴纳相应费用。

#### (三) 评价

CCAA 对认证机构的相关证明和文件进行审核, 确认机构的申

报资格；

CCAA 评价人员对申请人的申请资料进行评价，提出确认意见；  
CCAA 注册部负责人审查评价过程和确认意见，作出确认决定；  
CCAA 秘书长批准确认决定并签发确认文件。

## 五、确认结果

CCAA 将向申报机构公布审核人员资格确认文件。

确认资格自确认文件批准之日起生效，有效期 3 年；出现以下情况时，有效期自动终止，确认资格即行失效：

- 确认人员与申报机构解除聘用关系；
- 确认人员违反法律法规、认证规范文件和审核员行为准则，经 CCAA 查实并予资格处置的；
- CCAA 建立覆盖确认业务范围的审核员注册制度满 3 个月后。

附件：信息安全相关专业涵盖的专业目录

一、教育部《普通高等学校本科专业目录》中有关专业

专业代码	专业名称
071201	电子信息科学与技术
071202	微电子学
071203	光信息科学与技术
071205W	信息安全
080603	电子信息工程
080604	通信工程
080605	计算机科学与技术
080606	电子科学与技术
081606	信息对抗技术
110102	信息管理与信息系统

二、教育部《授予博士、硕士学位和培养研究生的学科、专业目录》中有关专业

专业代码	专业名称
080903	微电子学与固体电子学
081001	通信与信息系统
081002	信号与信息处理
081020	信息安全
081202	计算机软件与理论
081203	计算机应用技术
110505	密码学