中国认证认可协会文件

中认协培〔2015〕142号

关于发布《信息安全保障员考试大纲（第1版）》的通知

各相关机构及人员：

为满足CCAA《信息安全保障员注册方案》的有关要求，确保信息安全保障员水平，我会制定了《信息安全保障员考试大纲（第1版）》（见附件），现予以发布实施。

特此通知。

附件：《信息安全保障员考试大纲（第1版）》

中国认证认可协会

2015年5月28日

附件

中 国 认 证 认 可 协 会

信息安全保障员考试大纲

第 1 版

文件编号：CCAA-311

发布日期： 2015年5月28日　　实施日期： 2015年6月1日

信息安全保障员考试大纲

（第 1 版）

1．总则

本大纲依据 CCAA《信息安全保障员注册方案》（以下简称注册方案）制定，旨在通过 CCAA 统一组织的笔试，客观、公正、全面地考核参加人员满足注册方案中“2.5 考试要求”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保障员的人员。

2．考试要求

2.1 考试科目

申请基础级信息安全保障员注册需通过“基础级”科目考试；

申请专业级信息安全保障员需通过相应专业的“专业级”科目考试；

信息安全保障员考试 “基础级”科目考试由基础课程和通用课程（I 级）组成，“专业级”科目考试由基础课程、通用课程（II 级）、专业课程及附加课程组成，详见表 1、表 2。

表 1　信息安全保障员考试课程列表

序号	编号	考试课程名称	课程分类
1	B01	信息安全保障人员基本素质教育	基础课程
2	B02	信息安全意识教育	基础课程
3	B03	信息安全法律法规体系	基础课程
4	B04	风险管理基础	基础课程
5	G01	项目管理基础	通用课程
6	G02	信息安全技术	通用课程
7	G03	信息安全实验	通用课程
8	P01	安全软件技术与测试	专业课程
9	P02	信息系统安全集成	专业课程
10	P03	信息安全管理	专业课程
11	P04	安全运维技术与应用	专业课程
12	P05	安全咨询	专业课程
13	P06	风险管理	专业课程
14	P07	应急服务技术与应用	专业课程
15	P08	灾备服务技术与应用	专业课程
16	P09	业务连续性管理	专业课程
17	A01	通信技术基础	附加课程
18	A02	管理体系审核	附加课程

表 2　信息安全保障员考试课程对照表

级别和专业 / 考试课程		基础级	专业级								
			安全软件	安全集成	安全管理	安全运维	安全咨询	风险管理	应急服务	灾备服务	业务连续性
基础课程	B01	√	√	√	√	√	√	√	√	√	√
	B02	√	√	√	√	√	√	√	√	√	√
	B03	√	√	√	√	√	√	√	√	√	√
	B04	√	√	√	√	√	√	√	√	√	√
通用课程	G01	√	√	√	√	√	√	√	√		√
	G02	√	√	√	√	√	√	√	√	√	√
	G03		√	√	√	√		√	√	√	√
专业课程	P01		√								
	P02			√							
	P03				√						
	P04					√					
	P05						√				
	P06							√			
	P07								√		
	P08									√	
	P09										√
附加课程	A01			√			√	√	√		
	A02				√						

注：对应√处即为该级别及专业所应考试的课程。

参加考试时，考生需提供身份证件原件。

考生应严格遵守考场纪律（见附件），并自觉服从监考人员等考试工作人

员管理。

2.2 考试方式

“基础级”和“专业级”科目考试均为书面闭卷考试，考试试题由 CCAA 统一编制，每科（专业）考试时间 2 小时。

2.3 考试频次

CCAA 根据考试需求，组织实施考试。

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。

2.5 考试的题型及分值

2.5.1 基础级科目的题型及分值

考试课程			分值
1.信息安全保障人员基本素质教育			约占 5%
2.信息安全意识教育			约占 10%
3.信息安全法律法规体系			约占 10%
4.风险管理基础			约占 15%
5.项目管理基础（I 级）			约占 10%
6.信息安全技术（I 级）			约占 50%
题　型	数 量	单题分值（分）	小计分值（分）
单项选择题	60	1	60
多项选择题	20	2	40

2.5.2 专业级科目的题型及分值

2.5.2.1 专业级科目的题型

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

2.5.2.2　专业级科目的分值

专业级科目依据专业划分为9个科目考试，具体分值分布见下表：

专业	考试课程	分值
安全软件	1.基础课程（B01-B04）	约占5%
	2.项目管理基础（II级）	约占10%
	3.信息安全技术（II级）	约占20%
	4.信息安全实验	约占5%
	5.安全软件技术与测试	约占60%
安全集成	1.基础课程（B01-B04）	约占5%
	2.项目管理基础（II级）	约占10%
	3.信息安全技术（II级）	约占45%
	4.信息安全实验	约占5%
	5.信息系统安全集成	约占30%
	6.通信技术基础	约占5%
安全管理	1.基础课程（B01-B04）	约占5%
	2.项目管理基础（II级）	约占5%
	3.信息安全技术（II级）	约占5%
	4.信息安全实验	约占5%
	5.信息安全管理	约占70%
	6.管理体系审核	约占10%
安全运维	1.基础课程（B01-B04）	约占5%
	2.项目管理基础（II级）	约占10%
	3.信息安全技术（II级）	约占30%
	4.信息安全实验	约占5%
	5.安全运维技术与应用	约占50%
安全咨询	1.基础课程（B01-B04）	约占5%
	2.项目管理基础（II级）	约10%
	3.信息安全技术（II级）	约占40%
	4.安全咨询	约占40%
	5.通信技术基础	约占5%

风险管理	1.基础课程（B01-B04）	约占5%
	2.项目管理基础（II级）	约占5%
	3.信息安全技术（II级）	约占20%
	4.信息安全实验	约占5%
	5.风险管理	约占60%
	6.通信技术基础	约占5%
应急服务	1.基础课程（B01-B04）	约占5%
	2.项目管理基础（II级）	约占5%
	3.信息安全技术（II级）	约占10%
	4.信息安全实验	约占5%
	5.应急服务技术与应用	约占70%
	6.通信技术基础	约占5%
灾备服务	1.基础课程（B01-B04）	约占5%
	2.信息安全技术（II级）	约占20%
	3.信息安全实验	约占5%
	4.灾备服务技术与应用	约占70%
业务连续性	1.基础课程（B01-B04）	约占5%
	2.项目管理基础（II级）	约占5%
	3.信息安全技术（II级）	约占5%
	4.信息安全实验	约占5%
	5.业务连续性管理	约占80%

2.6 考试合格判定

“基础级”科目考试及“专业级”科目考试满分均为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30天（遇法定节日顺延）内公布考试合格人员名单。

3. 考试内容

3.1 基础级考试科目的考试内容

考试课程	考试内容
1.信息安全保障人员基本素质教育	信息安全保障人员应具备的职业素养、知识结构、工作技能要求
2.信息安全意识教育	信息安全保障概念 信息安全需求识别基本方法
3.信息安全法律法规体系	我国法律法规体系 国内外信息安全法律法规建设概况 国内外信息安全标准概况 国内信息安全管理概况
4.风险管理基础	风险管理基本概念与术语 常用风险评估方法 风险处置原则与基本方法 风险管理相关标准的发展
5.项目管理基础（I 级）	项目管理的基本概念 项目管理的发展历史与现状 九大项目管理知识领域 开发类项目管理技巧 集成类项目管理技巧
6.信息安全技术（I 级）	信息安全技术发展 密码学及其应用 网络安全技术 平台安全技术 应用安全技术 数据安全技术 物理安全技术

3.2 专业级考试科目的考试范围

专业级科目依据专业划分为 9 个科目考试，具体考试范围见下表：

专业	考试课程	考试范围
安全软件	1.基础课程（B01-B04）	信息安全保障的基本概念与知识结构 信息安全需求识别的基本方法 国内法律法规体系及主要信息安全法律法规 国内外信息安全标准概况 信息安全中的风险管理基本原理
	2.项目管理基础（II 级）	项目管理的基本概念 项目管理的发展历史与现状 九大项目管理知识领域 开发类项目管理技巧 集成类项目管理技巧
	3.信息安全技术（II 级）	信息安全技术发展 密码学及其应用 网络安全技术 平台安全技术 应用安全技术 数据安全技术 物理安全技术
	4.信息安全实验	实验平台构建 网络基础实验 主机安全实验 数据库安全实验 密码学与加解密实验 访问控制实验 攻击技术实验 主动防御技术实验 安全管理实验
	5.安全软件技术与测试	GB/T18336 等业界标准与实践 安全开发生命周期 安全软件开发环境管理 安全功能架构与设计 安全漏洞分析 安全编码 密码安全模块 安全测试与实验

安全集成	1.基础课程（B01-B04）	信息安全保障的基本概念与知识结构 信息安全需求识别的基本方法 国内法律法规体系及主要信息安全法律法规 国内外信息安全标准概况 信息安全中的风险管理基本原理
	2.项目管理基础（II 级）	项目管理的基本概念 项目管理的发展历史与现状 九大项目管理知识领域 开发类项目管理技巧 集成类项目管理技巧
	3.信息安全技术（II 级）	信息安全技术发展 密码学及其应用 网络安全技术 平台安全技术 应用安全技术 数据安全技术 物理安全技术
	4.信息安全实验	实验平台构建 网络基础实验 主机安全实验 数据库安全实验 密码学与加解密实验 访问控制实验 攻击技术实验 主动防御技术实验 安全管理实验
	5.信息系统安全集成	GB/T 20261 等安全集成业界标准与实践 安全集成过程 安全集成工具使用 典型安全保障手段 安全集成实例
	6.通信技术基础	通信和网络安全技术的基本原理 主要通信协议及应用
安全管理	1.基础课程（B01-B04）	信息安全保障的基本概念与知识结构 信息安全需求识别的基本方法 国内法律法规体系及主要信息安全法律法规

		国内外信息安全标准概况 信息安全中的风险管理基本原理
	2.项目管理基础（II 级）	项目管理的基本概念 项目管理的发展历史与现状 九大项目管理知识领域 开发类项目管理技巧 集成类项目管理技巧
	3.信息安全技术（II 级）	信息安全技术发展 密码学及其应用 网络安全技术 平台安全技术 应用安全技术 数据安全技术 物理安全技术
	4.信息安全实验	实验平台构建 网络基础实验 主机安全实验 数据库安全实验 密码学与加解密实验 访问控制实验 攻击技术实验 主动防御技术实验 安全管理实验
	5.信息安全管理	ISO/IEC 27000 族标准等业界安全管理标准与实践 安全管理的实施过程 典型安全管理工具 典型安全保障手段 安全管理实例 风险管理在信息安全管理中的应用
	6.管理体系审核	审核的概念与术语 审核的过程与方法 审核员的能力要求
安全运维	1.基础课程（B01-B04）	信息安全保障的基本概念与知识结构 信息安全需求识别的基本方法 国内法律法规体系及主要信息安全法律法规

		国内外信息安全标准概况 信息安全中的风险管理基本原理
	2.项目管理基础（II 级）	项目管理的基本概念 项目管理的发展历史与现状 九大项目管理知识领域 开发类项目管理技巧 集成类项目管理技巧
	3.信息安全技术（II 级）	信息安全技术发展 密码学及其应用 网络安全技术 平台安全技术 应用安全技术 数据安全技术 物理安全技术
	4.信息安全实验	实验平台构建 网络基础实验 主机安全实验 数据库安全实验 密码学与加解密实验 访问控制实验 攻击技术实验 主动防御技术实验 安全管理实验
	5.安全运维技术与应用	安全运维的业界标准与实践 安全运维的分类、过程与方法 项目管理在运维管理中的应用 典型的安全运维工具和手段
安全咨询	1.基础课程（B01-B04）	信息安全保障的基本概念与知识结构 信息安全需求识别的基本方法 国内法律法规体系及主要信息安全法律法规 国内外信息安全标准概况 信息安全中的风险管理基本原理
	2.项目管理基础（II 级）	项目管理的基本概念 项目管理的发展历史与现状 九大项目管理知识领域 开发类项目管理技巧

		集成类项目管理技巧
	3.信息安全技术（II 级）	信息安全技术发展 密码学及其应用 网络安全技术 平台安全技术 应用安全技术 数据安全技术 物理安全技术
	4.安全咨询	安全相关标准 咨询的过程管理 安全方案设计 安全咨询工具的使用 安全咨询知识库管理
	5.通信技术基础	通信和网络安全技术的基本原理 主要通信协议及应用
风险管理	1.基础课程（B01-B04）	信息安全保障的基本概念与知识结构 信息安全需求识别的基本方法 国内法律法规体系及主要信息安全法律法规 国内外信息安全标准概况 信息安全中的风险管理基本原理
	2.项目管理基础（II 级）	项目管理的基本概念 项目管理的发展历史与现状 九大项目管理知识领域 开发类项目管理技巧 集成类项目管理技巧
	3.信息安全技术（II 级）	信息安全技术发展 密码学及其应用 网络安全技术 平台安全技术 应用安全技术 数据安全技术 物理安全技术
	4.信息安全实验	实验平台构建 网络基础实验 主机安全实验

		数据库安全实验 密码学与加解密实验 访问控制实验 攻击技术实验 主动防御技术实验 安全管理实验
	5.风险管理	ISO 31000、ISO/IEC 27005 等业界标准与实践 风险管理的概念与术语 风险管理的实施过程 风险管理工具使用 风险处置的方法
	6.通信技术基础	通信和网络安全技术的基本原理 主要通信协议及应用
应急服务	1.基础课程（B01-B04）	信息安全保障的基本概念与知识结构 信息安全需求识别的基本方法 国内法律法规体系及主要信息安全法律法规 国内外信息安全标准概况 信息安全中的风险管理基本原理
	2.项目管理基础（II 级）	项目管理的基本概念 项目管理的发展历史与现状 九大项目管理知识领域 开发类项目管理技巧 集成类项目管理技巧
	3.信息安全技术（II 级）	信息安全技术发展 密码学及其应用 网络安全技术 平台安全技术 应用安全技术 数据安全技术 物理安全技术
	4.信息安全实验	实验平台构建 网络基础实验 主机安全实验 数据库安全实验 密码学与加解密实验

		访问控制实验 攻击技术实验 主动防御技术实验 安全管理实验
	5.应急服务技术与应用	应急服务相关标准与规范 应急服务过程管理 安全技术工具的使用
	6.通信技术基础	通信和网络安全技术的基本原理 主要通信协议及应用
灾备服务	1.基础课程（B01-B04）	信息安全保障的基本概念与知识结构 信息安全需求识别的基本方法 国内法律法规体系及主要信息安全法律法规 国内外信息安全标准概况 信息安全中的风险管理基本原理
	2.信息安全技术（II 级）	信息安全技术发展 密码学及其应用 网络安全技术 平台安全技术 应用安全技术 数据安全技术
	3.信息安全实验	实验平台构建 网络基础实验 主机安全实验 数据库安全实验 密码学与加解密实验 访问控制实验 攻击技术实验 主动防御技术实验 安全管理实验
	4.灾备服务技术与应用	灾备服务的业界标准与实践 灾难恢复技术 灾备服务过程管理 灾备工具使用域管理
业务连续性	1.基础课程（B01-B04）	信息安全保障的基本概念与知识结构 信息安全需求识别的基本方法 国内法律法规体系及主要信息安全法律法规

		国内外信息安全标准概况 信息安全中的风险管理基本原理
	2.项目管理基础（II 级）	项目管理的基本概念 项目管理的发展历史与现状 九大项目管理知识领域 开发类项目管理技巧 集成类项目管理技巧
	3.信息安全技术（II 级）	信息安全技术发展 密码学及其应用 网络安全技术 平台安全技术 应用安全技术 数据安全技术
	4.信息安全实验	实验平台构建 网络基础实验 主机安全实验 数据库安全实验 密码学与加解密实验 访问控制实验 攻击技术实验 主动防御技术实验 安全管理实验
	5.业务连续性管理	ISO 22301 等业界标准与实践 业务连续性管理结构 业务连续性管理过程与方法 业务连续性管理程序与计划 业务连续性管理在信息安全连续性管理中的应用

附件：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）考生应在规定时间和地点参加考试，并将身份证件原件放在指定位置以便核验。

（三）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。

（四）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。

（五）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。

（六）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。

（七）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。

（八）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）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。

（三）在考试过程中旁窥、交头接耳、互打暗号或者手势。

（四）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。

（五）未经考试工作人员同意在考试过程中擅自离开考场。

（六）将试卷(含答题纸等)、草稿纸等考试用纸带出考场。

（七）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。

（八）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5月28日印发