

中国认证认可协会文件

中认协培〔2015〕140号

关于发布《信息安全保障员培训课程大纲》的通知

各相关机构及人员：

为积极推动信息安全保障员培训工作的开展，按照中国认证认可协会(以下简称 CCAA)《信息安全保障员注册方案》的要求，CCAA 制定了《信息安全保障员培训课程大纲》(见附件)，现予以发布，自 2015 年 5 月 29 日起实施。

附件：CCAA-312 信息安全保障员培训课程大纲



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

附件

中国认证认可协会



信息安全保障员培训课程大纲

第1版

文件编号: CCAA-312

发布日期: 2015年5月28日

实施日期: 2015年5月29日

©版权 2015-中国认证认可协会

信息安全保障员培训课程大纲

前 言

中国认证认可协会(CCAA)依据信息安全保障员注册要求,对认证培训课程提供者自愿申请从事认证培训的课程,开展认证培训课程确认工作。

本大纲是 CCAA 规范类文件,具体规定了信息安全保障员培训课程的内容、结构和实施要求,CCAA 依据培训课程确认准则及本大纲对提出申请的培训课程进行确认。培训课程通过 CCAA 确认后,申请培训课程确认的机构方可提供使用 CCAA 标志的培训课程。通过培训的检查员候选人仅有助于其获得 CCAA 信息安全保障员注册方案规定的课程知识,而不代表通过 CCAA 的统一考试或自动取得注册资格。

本大纲由中国认证认可协会制定、批准并报 CNCA 备案后发布。

所有 CCAA 文件都用中文发布。标有最近发布日期的中文版 CCAA 文件是有效的版本。CCAA 将在网站上公布所有相关规范的最新版本。

关于更多的信息,请与 CCAA 培训考试部联系,联系地址如下:

地址:北京市朝阳区朝外大街甲 10 号中认大厦 15 层。

邮编: 100020

<http://www.ccaa.org.cn>

email: info@ccaa.org.cn

1 总则

1.1 本大纲是 CCAA 规范类文件, 具体规定了信息安全保障员培训课程的内容、结构和实施要求。本大纲适用于对信息安全保障员培训课程的确认。

1.2 本大纲应与 CCAA 《认证培训课程确认准则》一同使用。《认证培训课程确认准则》规定了 CCAA 培训课程确认的要求和程序。

2 引用文件

CCAA 《信息安全保障员注册方案》

3 培训对象和目标

3.1 信息安全保障员培训课程主要适用于满足《信息安全保障员注册方案》的要求, 欲成为 CCAA 信息安全保障员的人员。

3.2 培训目标是通过完整的课程培训, 有助于学员掌握信息安全保障员所必要的知识。

4 培训方式

4.1 信息安全保障员培训课程应采用面授的方式进行。

4.2 授课教师应使用汉语普通话授课。在境内外或有其他特殊需要的培训时, 教师可根据学员需要使用相应的语言授课; 必要时, 可为教师配备翻译人员, 该翻译人员应具备提供有效翻译的能力。

4.3 培训课程提供者应确保良好的培训效果, 培训课程教学场所应与培训规模、领域相适应, 且交通便利; 应配备满足培训教学需要的培训设施, 包括声像设备、网络软硬件设备、语音设备、可视化大屏幕及其他培训设备, 应有适宜的教学环境。

4.4 培训课程应具有互动性, 使培训课程提供者能够及时得到教学效果反馈, 使学员能够及时澄清疑问。

5 培训时间

5.1 信息安全保障员培训课程的每个子课程中用于直接授课和分组活动、个人活动的全部培训课程时间应不少于表 3 中培训时间的要求; 考试、用餐、课间休息或其他自由活动的时间不应计算在课程时间内; 如果通过翻译授课, 应根据需要增加培训时间以满足培训目标。

5.2 为保证培训效果, 每期培训班的学员人数不应多于 60 人。

6 培训课程的分类

信息安全保障员培训课程根据注册级别分类对应分为基础级培训课程和专业级培训课程。

这两类培训课程共由 18 个子课程组成, 这 18 个子课程划分为基础课程、通用课程、专业课程及附加课程, 详见表 1; 其中通用课程分为两个级别: I 级和 II 级, 代表对相

关内容掌握的程度，II 级高于 I 级。

表 1 信息安全保障员培训课程子课程列表

序号	编号	子课程名称	类别
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

6.1 基础级培训课程

基础级培训课程由基础课程及通用课程（I 级）组成，具体包括 B01、B02、B03、B04、G01（I 级）、G02（I 级）六个子课程。

6.2 专业级培训课程

根据注册方案，信息安全保障员专业级分为安全软件、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、业务连续性等 9 个专业，则信息安全保障员专业级培训课程也依据相应专业设置了 9 个专业课程，这 9 个专业课程均由基础课程、通用课程（II 级）、专业课程、附加课程组成，根据不同的专业，所涉及的子课程不同，详见表 2。

表 2 信息安全保障员培训课程（专业级）

专业 子课程		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 (II 级)	√	√	√	√	√	√	√		√
	G02 (II 级)	√	√	√	√	√	√	√	√	√
	G03	√	√	√	√		√	√	√	√
专业 课程	P01	√								
	P02		√							
	P03			√						
	P04				√					
	P05					√				
	P06						√			
	P07							√		
	P08								√	
	P09									√
附加 课程	A01		√			√	√	√		
	A02			√						

注：对应√处即为该专业级培训课程所应包含的子课程。

6.3 如学员在参加专业级培训课程前，已通过经 CCAA 确认的基础级培训课程的培训，获得相应培训合格证书，则在进行专业级培训课程时可对其免除基础课程（B01、B02、B03、B04）

的培训要求。

7 培训内容

7.1 信息安全保障人员培训课程各子课程培训内容及培训时间要求如表 3 所示:

表 3 子课程培训内容及培训时间要求

序号	子课程名称	内容		培训时间
1	信息安全保障人员基本素质教育	理解从事信息安全保障工作必备的职业素养 理解从事信息安全保障工作的特殊责任		1.5 小时
2	信息安全意识教育	了解信息安全保障的概念、形势背景 理解从事信息安全保障工作所需的基础知识结构 理解和掌握信息安全保障需求识别的基本方法		3 小时
3	信息安全法律法规体系	了解我国法律法规体系 了解国内信息安全相关法律法规建设情况 了解国内外信息安全相关的主要标准--- ISO/IEC JTC1 以及 SAC TC260 制定的系列标准 熟悉国内信息安全典型法律法规和标准--- 《中华人民共和国保守国家秘密法》、《信息系统安全等级保护管理办法》、《商用密码管理条例》、《互联网服务管理办法》、信息安全专用产品的管理要求		3 小时
4	风险管理基础	理解风险管理的术语和定义 理解风险管理的基本过程和方法 了解常用风险评估方法 了解风险处置的原则和常见处置方法		4 小时
5	项目管理基础	I 级: 掌握项目管理的基本分类 理解项目管理的生命周期过程 了解项目管理的九大知识领域 了解集成类项目生命周期过程以及项目管理的特点 了解开发类项目生命周期过程以及项目管理特点	II 级: 掌握项目管理的基本分类 理解项目管理的生命周期过程 掌握项目管理的九大知识领域 掌握集成类项目生命周期过程以及项目管理的特点 掌握开发类项目生命周期过程以及项目管理特点	各 12 小时
6	信息安全技术	I 级: 了解信息安全技术的发展 了解密码学的发展 基本理解密码学基本原理 基本掌握典型密码算法的作用与应用方法 了解密钥管理方法 了解网络边界防御原理与方法	II 级: 理解信息安全技术结构及相互关系的发展 了解密码学的发展 理解密码学基本原理 掌握典型密码算法的作用与应用方法 掌握密钥管理方法	各 12 小时

序号	子课程名称	内容	培训时间	
		了解典型的网络边界防御设备及系统的原理与应用 了解典型网络通信安全设备及系统的原理与应用 了解常用系统平台的典型安全问题 了解常用的应用支撑平台 了解各类安全漏洞的管理标准与方法 了解典型的对平台攻击手段 了解主机安全防护的主要手段 了解桌面系统的典型安全问题、保障方法与工具 了解各类常用应用系统的典型安全手段 了解安全软件开发过程与控制 了解应用软件安全测试方法与工具 了解数据安全的范畴 了解数据生命周期各阶段的安全保障技术与方法 了解数据灾备与恢复技术 了解典型的物理安全问题 了解典型的物理安全方法技术与方法 了解支持性基础设施的物理安全问题及保护措施	理解网络边界防御原理与方法 掌握典型的网络边界防御设备及系统的原理与应用 理解典型网络通信安全设备及系统的原理与应用 了解常用系统平台的典型安全问题 熟悉常用的应用支撑平台 熟悉各类安全漏洞的管理标准与方法 熟悉典型的对平台攻击手段 掌握主机安全防护的主要手段 掌握桌面系统的典型安全问题、保障方法与工具 了解各类常用应用系统的典型安全手段 熟悉安全软件开发过程与控制 了解应用软件安全测试方法与工具 理解数据安全的范畴 理解数据生命周期各阶段的安全保障技术与方法 熟悉数据灾备与恢复技术 熟悉典型的物理安全问题 掌握典型的物理安全防范技术与方法 掌握支持性基础设施的物理安全问题及保护措施	
7	信息安全实验	信息安全实验的范围和背景 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	18 小时	
8	安全软件技术与测试	了解安全软件的业界标准与实践 熟悉安全软件开发生命周期过程 熟悉安全需求分析、安全设计、安全编码、安全测试、安全生产的	18 小时	

序号	子课程名称	内容	培训时间
		主要方法 熟悉安全软件开发环境的管理 了解典型的安全功能及实现模型 熟悉典型的安全漏洞机理 熟悉典型的加密算法及密码应用 熟悉软件安全功能测试的基本手段 熟悉软件安全性测试工具	
9	信息系统安全集成	了解安全系统集成的业界标准 掌握 GB/T 20261 对安全集成的要求 掌握安全集成工程的过程和方法，包括安全需求分析、安全设计、安全集成实施、安全集成保证 熟悉典型的安全集成工具 熟悉安全集成方案的基本内容结构 熟悉常用的信息安全产品 行业典型安全集成实例	12 小时
10	信息安全管理	理解信息安全管理相关基本概念和术语 了解信息安全标准的历史与发展— ISO/IEC 27000 族标准构成及其应用中的关系 理解信息安全管理中的风险管理基本方法 理解信息安全管理的实施过程 掌握典型信息安全保障手段	12 小时
11	安全运维技术与应用	熟悉安全运维的业界标准与实践 熟悉项目管理在运维管理中的应用 熟悉安全运维的分类、过程与方法 熟悉典型的安全运维工具和手段	12 小时
12	安全咨询	熟悉国内外主要的信息安全标准框架和核心标准 掌握安全咨询过程与方法 掌握安全咨询实施框架与保障方案的设计 熟悉安全咨询过程中的项目管理 掌握安全咨询中的知识库管理 掌握安全咨询中的信息安全管理体系建设 掌握安全咨询中的风险评估 熟悉典型的安全分析工具	12 小时
13	风险管理	理解风险管理的术语和定义 理解风险管理的基本过程和方法 了解风险评估方法的基本过程和方法 理解和掌握典型风险评估方法 理解和掌握常用风险处置方法 熟悉国内外风险管理相关标准	4 小时

序号	子课程名称	内容	培训时间
14	应急服务技术与应用	熟悉 ISO 22301 标准的过程与方法 熟悉应急服务的安全要求 熟悉应急服务准备、回退计划、风险评估、资源协调、服务升级、现场保护与取证等过程与方法 熟悉典型的安全分析工具的使用	4 小时
15	灾备服务技术与应用	熟悉灾备中心建设、灾备等级分类等业界标准与实践 熟悉灾备中心运维管理的生命周期过程 熟悉数据存储技术、数据管理技术、系统迁移技术、系统恢复技术 熟悉灾备服务的规划、组织与实施的主要方法	4 小时
16	业务连续性管理	理解 ISO 22301 标准要求及业务连续性管理的过程与方法 掌握 ISO 22301 在信息安全连续性管理中的应用 掌握常用业务影响分析方法 掌握业务连续性计划框架要求及计划的制定 掌握业务恢复策略与指标的制定的原则及方法	4 小时
17	通信技术基础	熟悉通信和网络安全技术的基本原理，主要通信协议及应用	2 小时
18	管理体系审核	1. 了解“管理体系审核指南”的历史和背景 2. 理解和掌握“管理体系审核”基本概念 3. 理解和掌握“管理体系审核”原则 4. 理解和掌握“管理体系审核”方案管理 5. 理解和掌握“管理体系审核”过程 6. 理解和掌握“管理体系审核”人员能力要求及评价	12 小时

7.2 CCAA 鼓励申请者在开发培训课程时，适当增加有助于丰富学员知识、提高技能等实用性的内容，体现申请者自身的特色和针对性。

8 附则

本大纲由中国认证认可协会负责解释。

