CISAW

信息安全保障人员认证

之

信息系统安全集成人员认证

课程介绍

信息系统安全集成人员认证

信息安全保障人员认证(Certified Information Security Assurance Worker, CISAW)体系是中国信息安全认证中心(China Information Security Certification Center, ISCCC,简称:信安中心)历经六年磨砺，集约业界专家、企业精英、高校及研究机构学者参与打磨的针对信息安全保障不同专业技术方向、应用领域和保障岗位，依据国际标准IS0/IEC 17024《人员认证机构通用要求》所建立的、不同层次的信息安全保障人员认证体系。 2014年，为进一步落实习近平总书记在网络安全和信息化领导小组第一次工作会议上提出的加强国家信息人才队伍建设的指示，信安中心加大了推广力度，针对不同专业技术方向和行业应用领域授权了一批教学管理机构，主要从事CISAW的培训体系建设、教程开发、师资建设、培训组织机构和市场渠道推广工作。

信息系统安全集成人员认证是CISAW体系中技术专业类认证的一个技术方向，主要认证对象为专业从事信息系统安全集成相关的技术人员和管理人员。

目录

第一章 CISAW认证体系

一、CISAW介绍

信息安全保障人员认证体系是中国信息安全认证中心面向信息安全保障领域不同专业、行业、岗位、不同层次信息安全技术和管理人员的培训认证体系，特别是与信息安全工作直接密切相关的中高级管理人员、专业技术人员等推出的信息安全保障人员资格认证和专业水平认证。

CISAW认证依据RB/T 202-2013 《信息安全保障人员认证准则》开展认证培训。通过CISAW认证，表明获证人员：

1.通过了ISCCC-COP-R02 《信息安全保障人员认证考试大纲》要求的相应从业方向、业务领域的技术知识水平与应用能力考试；(特别：预备级人员需通过信安中心认定的学历教育选修课程考试和基础课程考试)

2.履行了ISCCC-COP-R01 《信息安全保障人员认证规则》规定的义务；

3.达到了信息安全保障人员应具有的职业素养、教育经历、从业经历的要求(预备级无从业经历要求)；

4.证书可作为有关证书采信部门对上岗人员要求的资格证明和能力证明。

所有获证人员除符合本准则要求之外，还应遵守本国或地区的有关法律、法规。

CISAW通过考试和其它评价方式证明获证人员具备了在一定的专业方向上从事信息安全保障工作的个人素质和相应的技术知识与应用能力，以供用人单位采信，或选用具备能力资格的信息安全保障人员到合适的岗位。

表1 CISAW体系结构

<table>
<tr><td colspan="2">技术专业认证</td><td colspan="2">应用领域认证</td></tr>
<tr><td>专业高级</td><td rowspan="3">安全软件、安全集成、安全管理、安全咨询、安全运维、安全审计、风险管理、应急服务、灾备服务、工控安全、电子认证、网络攻防、云安全、业务连续性、物联网安全</td><td>管理高级</td><td rowspan="3">电子政务、电子商务、交通服务、医疗服务、教育服务、能源服务、金融服务、通信服务、宾馆服务、物流服务、 CA服务</td></tr>
<tr><td>专业级</td><td>管理级</td></tr>
<tr><td>专业资格</td><td>岗位资格</td></tr>
<tr><td colspan="4">预备级</td></tr>
</table>

CISAW体系总体分为预备人员认证和在职人员认证，在职人员认证又包括了技术专业认证和应用领域认证两个类别，如表1所示。其中：

(一)预备人员认证

预备人员认证面向对象为高等院校在校学生(大学生和研究生)，旨在为准备就业的在校学生奠定择业基础，为国家急需的信息安全专业和保障人才建设开辟出一条新的途径。

(二)应用领域认证

面向各行业在职的、从事与信息安全相关工作的人员开展的应用领域认证，具体分为专业资格、专业级和专业高级三个级别。应用领域包括了：电子政务、电子商务、交通、医疗卫生、教育、能源、金融、通信、宾馆、物流和CA服务等领域。

(三)技术专业认证

面向信息安全技术各专业人员的技术专业认证，分为专业资格、专业级和专业高级三个级别。专业方向包括了：安全软件、安全集成、安全管理、安全咨询、安全运维、安全审计、风险管理、应急服务、灾备服务、网络攻防、业务连续性、云安全、物联网安全、工业控制安全和电子认证等。

CISAW正式开展的认证，每年根据社会实际需求和技术发展情况进行一次审定。

二、 认证流程

CISAW认证依据图1所示进行。

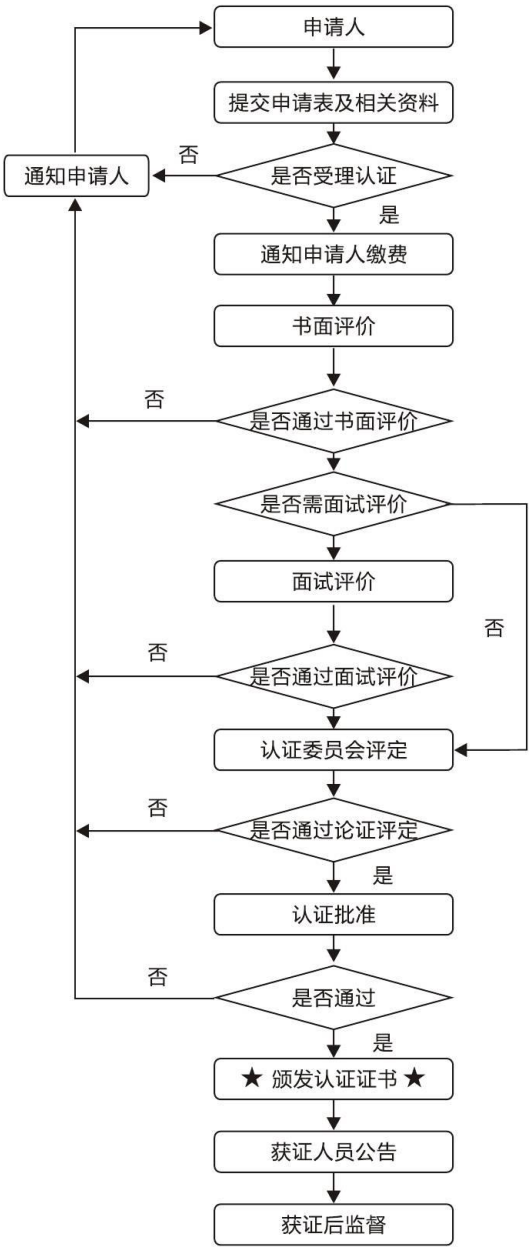

图1 CISAW认证流程

注：申请者通过www.isccc.gov.cn网站提交电子版申请资料。

三、认证考试

CISAW认证考试依据ISCCC-COP-R02《信息安全保障人员认证考试大纲》的要求开展。

考试形式：采用笔试、操作、论文、答辩等形式进行。其中笔试采用单项选择题组卷，满分100分；

考试机构：中国信息安全认证中心为唯一考试机构；考试机构可以依据考试需求授权其他合作机构组织实施；

考试流程：按照《信息安全保障人员考试管理细则》执行；

考试结果：考试70分(含)及格，通过者将获得中国信息安全认证中心颁发的《考试合格证书》，该证书是信息安全保障人员认证注册的有效证明文件之一。

四、证书管理

依据ISCCC-COP-R04 《信息安全保障人员认证证书与标识使用细则》的相关规定进行证书的使用和管理。

证书有效期为3年，有效期从发证之日起计算，有效期到期前3个月，持有证书人员须经后续教育培训，合格者可申请证书保持。

五、信息系统安全集成认证需求

信息系统安全集成是信息系统安全工程的一种具体形式。信息系统安全集成是将安全单元、产品部件进行集成的行为或活动，包括在新建信息系统的结构化设计中考虑信息安全保证因素，也包括在已有信息系统的基础上额外增加信息安全子系统或信息安全设备等，即所谓的安全优化或安全加固。

信息系统安全集成工程涉及集成方案设计、开发、实施和管理等诸多环节，每个环节都面临着相应的安全风险。

设计环节直接关系着系统的安全功能和安全性能。频频出现在各类网站中的用户验证和口令找回的安全隐患暴露出了系统在安全设计上的弱点；12306网站在上线的第一天就暴露出了信息泄露隐患和重复订票错误逻辑问题。这些安全问题主要源于系统在安全设计方案上

存在的漏洞。

开发环节更多的是编码实现与测试所面临的安全问题。缓冲区溢出、格式化字符串、SQL注入等各种网络攻击都是利用了信息系统代码实现上的漏洞。诸多漏洞型病毒也是利用了操作系统核心进程的缓冲区溢出漏洞得以实现大规模传播和破坏。

实施环节的安全隐患主要体现在系统和设备的配置环节，如防火墙、入侵检测、网闸等安全系统和部件的配置上存在策略漏洞造成。

引发信息系统安全集成在设计、开发、实施和管理等环节安全问题的主要原因在于人，即相关人员在安全意识、安全技能和安全素养上的欠缺。

CISAW《信息系统安全集成》人员认证依据国家相关的政策和国内外相关标准对从事信息系统安全集成的安全设计、安全开发、安全实施和安全管理人员展开认证和培训,有效提升相关人员的安全意识、安全素养和安全技能。

CISAW《信息系统安全集成》人员认证中，参照的技术标准主要有：

1.《系统安全工程能力成熟度模型》(GB/T20261-2006/IS021827：2002)

2.《信息系统安全工程管理要求》(GB/T20282-2006)

3.《信息技术安全性评估准则》(GB/T18336-2008)

3.《信息技术安全性评估准则》(GB/T 18336-2008)

4. 《信息系统通用安全技术要求》(GB/T 20271-2006)

5.《信息系统安全管理要求》(GB/T 20269-2006)

6.《信息安全风险评估规范》(GB/T 20984-2007)

7.《信息安全事件分类分级指南》(GB/Z 20986-2007)

8.《信息安全管理体系要求》(GB/T 22080-2008)

9.《信息安全管理实用规则》(GB/T 22081-2008)

结合上述标准开展的《信息系统安全集成》人员认证，是实现信息系统安全集成和信息安全保障的有力手段。

第二章认证培训

一、CISAW知识体系

中国信息安全认证中心针对信息安全保障人员认证各专业技术方向和行业应用领域的不同要求，建立了信息安全基础知识、信息安全专业技术知识和行业应用领域管理知识的模块式组合培训体系。整个知识体系以CISAW信息安全保障模型为主线展开。主要包括：

1)信息安全基础知识：信息安全技术、信息安全技术应用、信息安全实验；

2)信息安全专业知识：软件安全开发、信息系统安全集成、信息安全管理、信息安全咨询、信息系统安全运维、信息系统安全审计、信息系统安全集成、网络攻防技术、业务连续性管理、云计算安全、物联网安全、工业控制安全和电子认证技术；

3)行业应用领域管理知识：电子政务安全、电子商务安全、能源服务信息安全、交通服务信息安全、医疗卫生信息安全、教育服务信息安全、金融服务信息安全、通信服务信息安全、宾馆服务信息安全、物流服务信息安全和CA服务信息安全。

二、培训组织

CISAW认证培训采取统一课程建设、统一教师管理、统一教学管理、分散教学实施的模式开展培训。统一课程建设是指由中国信息安全认证中心统一召集行业专家、高校教师和企业代表组成课程建设组，编制教材、编写教案等。统一教师管理是指依据《信息安全保障人员认证培训教师注册准则》要求，对教师进行注册管理，并委托教学主管机构进行派遣。统一教学管理机构是指每一认证方向的认证培训由中国信息安全认证中心授权唯一的组织作为课程建设、教师派遣和市场推广的责任单位。

三、培训对象

专业资格级培训对象：各行业领域从事信息系统安全集成及相关工作的人员。

专业级培训对象 :各行业领域从事信息系统安全集成及相关工作的的骨干技术人员和管理人员。

专业高级培训对象：各行业领域从事信息系统安全集成及相关工作的核心人员。

四、培训内容

为满足ISCCC-COP-R02《信息安全保障人员认证考试大纲》对信息系统安全集成人员认证的要求，信息系统安全集成人员认证培训内容由信息安全技术、信息安全技术应用和信息系统安全集成等内容构成。

具体内容及安排，见表3和表4。

(一)专业高级认证培训

专业高级认证培训以研讨为主，讲授为辅，为期3天，具体研讨培训内容如下：

表3专业高级认证培训课程内容

天	内容标题	时间
第一天(上午)	安全意识	9: 00-12: 00
安全意识	讨论和分析当前信息安全形势和发展趋势,探讨信息系统安全集成模型 。	
第一天(下午)	相关标准	1:30-4:30
标准实施	讨论与交流信息系统安全工程相关标准及实施	
第二天(上午)	工程实施	9: 00-12: 00
实施过程	讨论与交流安全集成工程各个环节的实施	
项目组织	讨论与交流安全集成项目组的组织和管理	
第二天(下午)	安全的集成	1:30-4:30
案例分析	安全的集成模式下典型案例分析与共享交流	
第三天（上午）	集成的安全	9: 00-12: 00
案例分析	集成的安全模式下，典型案例分析与共享交流	
第三天（下午）	开题辅导	1:30-4:30
论文开题	介绍和提出论文题目,对论文的撰写、关注点等进行必要的辅导和讨论。	

(二)专业级认证培训

专业级认证培训，以讲授为主，讨论与测试为辅。专业级认证培训为期5天，具体培训内容如表4所示 。

专业高级认证培训以研讨为主，讲授为辅，为期3天，具体研讨培训内容如下：

表4 专业级认证培训课程内容

天	内容标题	时间
第一天(上午)	安全意识	9: 00-12: 00
基本知识	介绍信息安全发展形势，介绍基本概念和基本模型，给出国家相关法律法规和技术标准等	
第一天(下午)	数据与载体安全	1: 30-4: 30
数据安全	介绍数据安全的概念、范畴,介绍和分析数据面临的典型安全问题,并针对安全问题介绍数据安全的技术与解决措施	
载体安全	介结裁体安全的概念、范畴，介绍和分析各类载体面临的典型安全问题，并针对安全问题介绍相关的技术与解决措施	
第二天(上午)	环境与边界安全	9: 00-12: 00
环境安全	介绍环境安全的概念、范畴，介绍和分析机房等物理环境、操作系统等逻辑环境面临的典型安全问题，并针对安全问题介绍相应的技术与措施	
边界安全	介绍边界安全的概念、范畴，介绍和分析机房边界、网络边界、系统边界等面临的典型安全问题，并针对安全问题介绍边界安全的技术与措施	
第二天(下午)	应用技术	1: 30-4: 30
云计算	介绍云计算的基本概念，云计算的典型安全问题，以及解决这些安全问题所采取的安全措施	
物联网	介绍物联网的基本概念，物联网的典型安全同题，以及解决这些安全同题所采取的信息安全技术和物联网安全措施	
第三天(上午)	基础知识	9: 00-12: 00
基本概念	介绍并解析安全集成的基本概念	
相关模型	详细分析和介绍信息系统安全模型，讲解模型各元素的关系和安全集成的基本理论	
第三天(下午)	理论基础	1: 30-4: 30
信息系统安全工程综述	对系统安全工程、信息系统安全工程的基本概念、范畴进行介绍,详细讲解系统安全工程成熟度模型 SSE-CMM	
第四天(上午)	安全集成实施	9: 00-12: 00
符合性要求	讲解安全集成的相关约束的识别，达到对法律法规、标准规范、行业规定的符合	
风险评估	介绍通过识别信息资产，识别资产所面临的风险，并进行风险分析与评估，从而提出系统的安全需求	
安全设计	讲解在安全需求的基础上进行的安全设计,识别和评审安全设计方案，盘点安全措施，制定措施计划	
第四天(下午)	安全集成实施	1: 30-4: 30
工程实施	讲解依据安全设计方案进行的安全开发和依据措施计划而开展的措施实施	
监测与评价	讲解对系统安全态势的监视，评价系统方案的有效性、安全实施的正确性	
改进	讲解系统持续改进的方式方法和建议	
第五天(上午)	总结	9: 00-12: 00
案例分析	结合两种模式的案例，讲解安全集成的具体过程	
培训总结	培训内容内容总结，问题提问与回答	

(三)专业资格认证培训

专业资格认证培训形式以讲授为主。培训为期3天，内容以岗位基础培训为主，具体培训内容如表5所示。

表5专业资格认证培训课程内容

天	内容标题	时间
第一天(上午)	安全意识	9: 00-12: 00
基本知识	介绍信息安全发展形势，介绍基本概念和基本模型，给出国家相关法律法规和技本标准等	
第一天(下午)	数据与裁体安全	1: 30-4: 30
数据安全	介绍数据安全的概念、范畴，介绍和分析数据面临的典型安全问题，并针对安全问题介绍数据安全的技术与解决措施	
载体安全	介绍载体安全的概念、范畴，介绍和分析各类载体面临的典型安全问题，并针对安全问题介绍相关的技术与解决措施	
第二天(上午)	环境与边界安全	9: 00-12: 00
环境安全	介绍环境安全的概念、范畴，介绍和分析机房等物理环境、操作系统等逻辑环境面临的典型安全问题，并针对安全问题介绍相应的技术与措施	
边界安全	介绍边界安全的概念、范畴，介绍和分析机房边界、网络边界、系统边界等面临的典型安全问题，并针对安全问题介绍边界安全的技术与措施	
第二天(下午)	应用技术	1: 30-4: 30
云计算	介绍云计算的基本概念，云计算的典型安全问题，以及解决这些安全问题所采取的安全措施	
物联网	介绍物联网的基本概念，物联网的典型安全问题，以及解决这些安全问题所采取的信息安全技术和物联网安全措施	
第三天（上午)	安全集成综述	9: 00-12: 00
基础知识	概念、模型、相关标准	
基本理论	信息系统安全工程综述	
两种模式	信息系统安全集成实施过程	
案例分析	两种模式的案例综合介绍和重点讲解	
第三天(下午)	认证考试	14:00-16：30

五、培训收益

通过培训有效提升管理和技术人员的安全意识、安全素养和信息系统安全集成的风险评估、措施应用、安全设计、工程实施和安全测评与改进等相关能力，整体提高信息系统安全集成能力。

考试通过后可获得由中国信息安全认证中心统一颁发的认证证书。

获证人员为信息系统安全集成服务资质认证提供支撑，是服务资质认证的审查条件之一。

第三章机构介绍

一、认证机构

中国信息安全认证中心是经中央编制委员会批准，2006年11月正式挂牌成立，是我国信息安全保障的重要机构之一。信安中心是由公安部、安全部、工业与信息化部、国家保密局、国家密码管理局、国务院信息化工作办公室、国家质检总局、国家认证认可监督管理委员会八部委授权，依据国家有关强制性产品认证、信息安全管理的法律法规，负责实施信息安全领域有关产品、体系、服务资质、保障人员认证的专门机构，是中央网信办指定的办事服务机构。

信安中心为国家质检总局直属公益一类事业单位，系第三方公正机构和法人实体。其职能为：在批准的工作范围内按照认证基本规范和认证规则开展认证工作；受理认证委托、实施评价、做出认证决定，颁发认证证书，负责认证后的跟踪检查和相应认证标志的使用监督；受理有关的认证投诉、申诉工作；依法暂停、注销和撤销认证证书；对认证及与认证有关的检测、检查、评价人员进行认证标准、程序及相关要求的培训；对提供信息安全服务的组织、人员进行资质认证和培训；根据国家法律、法规及授权参加相关国际组织信息安全领域的国际合作；依据法律、法规及授权从事相关认证工作。在业务上接受国家网络与信息安全协调小组办公室指导。