CISAW

信息安全保障人员认证

之

软件安全开发保障人员认证

课程介绍

软件安全开发保障人员认证

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/IEC17024《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。

软件安全开发保障人员认证是CISAW体系中的一个应用领域，主要认证对象为政府机关、各行业及企事业单位从事软件项目管理、设计、开发、测试、技术服务等管理和技术人员。

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体系具体包括:

(一)预备级

面向在校学生(大学生和研究生)开展的CISAW预备级认证,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)管理类

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管理类认证,发放管理级和管理高级认证证书。管理类认证包括：电子政务、能源、金融、交通、通信、教育、医疗卫生、物流、电子商务等领域；

(三)技术类

面向信息安全技术各专业人员的专业水平认证,分为专业级和专业高级。专业方向包括：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、网络攻防、业务连续性、云安全、物联网安全、工业控制安全等。

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。

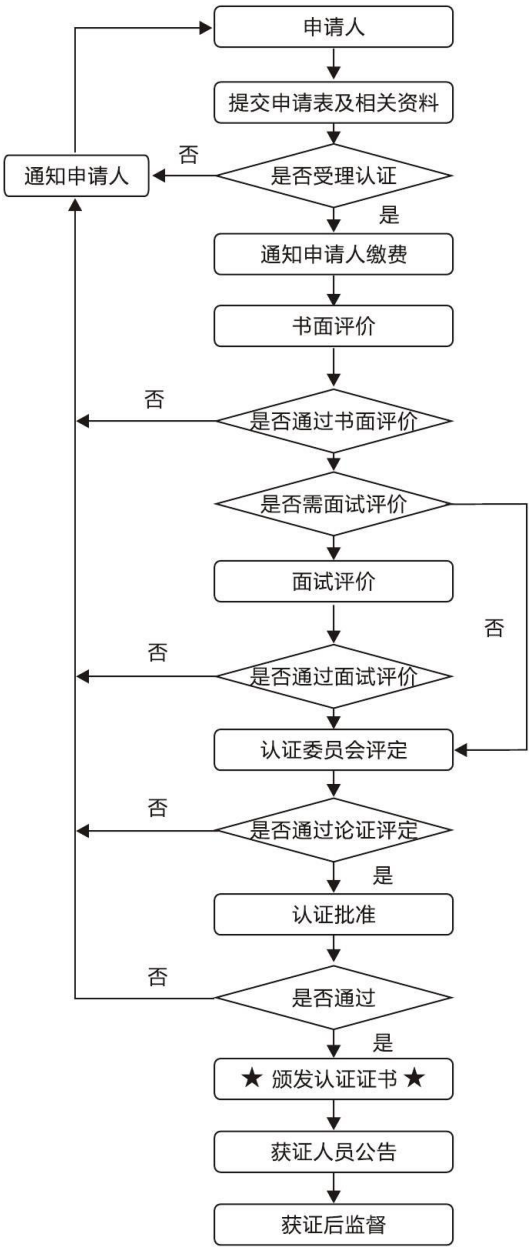

图1 CISAW认证流程

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、软件安全开发认证需求

短短几十年的发展 ,软件已经作为构成现代社会基础设施的要素 ,融入社会的每个角落，而软件的复杂度也随着规模的增大而成指数级增长。在软件技术不断进步、规模不断扩大的过程中，安全问题无法回避而且贯穿始终。从全球范围看，由于软件系统受到攻击而造成的损失也在逐年增加。

2014年2月28日，全球最大Bitcoin交易平台Mt.Gox申清破产。由于比特币软件中存在一个漏洞，黑客可以利用该漏洞修改交易信息。比如让一个本来已经发生的比特币交易看起来像没发生，这会导致系统重新发送比特币，最终造成85万个比特币被盗，损失4.67亿美元。

2014年5月22日, eBay要求近1.28亿活跃用户全部重新设置密码，此前这家零售网站透露黑客能从该网站获取密码、电话号码、地址及其他个人数据。

2014年12月25日，12306网站被黑客攻击，导致131653名用户信息泄露，包括用户帐号、明文密码、身份证、邮箱等用户数据在互联网上疯传。

继人人网、天涯等网站用户信息被公布之后，2014年京东商城又曝安全漏洞，用户住址电话均"裸奔"。携程泄露用户银行卡信息，安全支付日志可被遍历下载。余额宝被盗刷6万多元，支付宝让失主"耐心等待"……

上述事例表明，软件的安全已经是世界范围内关注的问题，而保证软件的安全开发无疑会降低造成产生漏洞的风险，对软件从业人员进行软件安全开发的培训与认证也至关重要。中央网络安全和信息化领导小组组长习近平强调，建设网络强国，要把人才资源汇聚起来，建设一支政治强、业务精、作风好的强大队伍。

我国已经颁布了800多条与信息技术相关的国家标准及相关政策，这些标准还远远不能满足软件安全发展的需要。CISAW《软件安全开发》保障人员认证中，参照的已颁布的与软件安全开发相关的标准及政策如下：

1.《2006-2020年国家信息化发展战略》全面加强国家信息安全保障体系建设。坚持积极防御、综合防范，探索和把握信息化与信息安全的内在规律，主动应对信息安全挑战，实现信息化与信息安全协调发展。

2.《国务院关于大力推进信息化发展和切实保障信息安全的若干意见》（ 国发〔2012〕23号)提高风险隐患发现、监测预警和突发事件处置能力。加强信息共享和交流平台建设，健全网络与信息安全信息通报机制。

3.《国家信息化领导小组关于加强信息安全保障工作的意见》(中办发[2003]27号)信息安全监控是及时发现和处置网络攻击，防止有害信息传播，对网络和系统实施保护的重要手段。基础信息网络的运营单位和各重要信息系统的主管部门或运营单位要根据实际情况建立和完善信息安全监控系统， 提高对网络攻击、病毒入侵、网络失窃密的防范能力，防止有害信息传播。

4.《全国人民代表大会常务委员会关于加强网络信息保护的决定》

5.《关于进一步加强互联网管理工作的意见》

软件安全开发依据包括政策文件和技术标准两个部分。

(一)政策文件

1.《国家信息化领导小组关于加强信息安全保障工作的意见》(中办发[2003]27号)

2.《国务院办公厅关于加强政府信息系统安全和保密管理工作的通知》（国发办[2008]17号)

3.《国务院办公厅关于印发国家网络与信息安全事件应急预案的通知》(国办函[2008]168号)

4.《关于加强党政机关计算机信息系统安全和保密管理的若干规定》(国保发[2007]13号)

(二)技术标准

1. 《信息系统保护轮廓和信息系统安全目标产生指南》（GB/Z 30286-2013）

2. 《信息安全服务分类》(GB/T 30283-2013)

3. 《安全漏洞等级划分指南》(GB/T 30279-2013)

4. 《信息安全漏洞管理规范》(GB/T 30276-2013)

5. 《信息系统安全保障通用评估指南》（GB/T 30273-2013）

6. 《安全漏洞标识与描述规范》(GB/T 28458-2012)

7. 《应用软件系统通用安全技术要求》（GB/T 28452-2012）

8. 《信息安全风险管理指南》(GB/Z 2436-2009)

9. 《信息系统安全等级保护基本要求》（GB/T 22239-2008）

10. 《信息安全管理体系要求》(GB/T 22080-2008)

11. 《信息安全管理实用规则》(GB/T 22081-2008)

12. 《信息安全风险评估规范》(GB/T 20984-2007)

13. 《信息安全事件分类分级指南》(GB/Z 20986-2007)

14. 《信息系统安全管理要求》 (GB/T 20269-2006)

15. 《信息系统通用安全技术要求》(GB/T 20271-2006)

综上所述，实现软件的安全开发主要依赖软件安全开发保障人员的信息安全意识、素质和技能，软件安全开发保障人员认证是实现这一目标的有力手段。

第三章认证培训

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、信息安全风险管理、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、统一教学管理机构、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

政府机关、各行业及企事业单位从事软件项目管理、设计、开发、测试、技术服务等管理和技术人员。

四、培训对象

为满足ISCCC-COP-R02《信息安全保障人员认证考试大纲》对软件安全开发保障人员认证的要求，软件安全开发保障人员的培训内容由软件安全开发模型、安全漏洞管理、安全功能设计、安全编码实践和软件安全测试等内容构成。

具体内容及安排,见表2。

表2 软件安全开发专业级认证培训课程内容

天	内容标题	时间
第一天(上午)	软件安全概述、软件安全开发模型	9: 00-12: 00
软件安全概述	介绍软件及软件安全的相关概念，了解软件安全的范畴及软件存在的安全问题。	
软件安全开发模型	介绍三种软件开发模型和常用的软件开发方法讲解典型的软件安全开发模型及 CISAW 软件安全开发模型。	
第一天(下午)	安全漏洞管理	1:30-4:30
安全漏洞管理	介绍漏洞的分类、等级等相关知识，讲解安全自动化协议，介绍典型的安全漏洞。	
第二天(上午)	安全功能设计	9：00-12：00
安全功能设计	介绍安全审计、安全通信、密码支持、用户数据保护、标识与识别(身份认证)、安全管理、隐私保护、安全功能的保护、资源利用、系统子系统的访问记忆可信路径/信道等安全功能。	
第二天(下午)	软件安全测试	1：30-4：30
软件安全测试	介绍软件安全测试的方法和过程讲解软件安全测试的组织过程结合例子介绍几种常见的测试工具。	
天	内容标题	时间
第三天(上午、下午)	常见安全问题	9： 00-12：00 1：30-4：30
常见安全问题	分别从整型、字符串、数组、指针、函数、多线程、文件、内存、面向对象、和 web 等方面讲解软件开发过程中常见的安全同题并给出解决方案。	
第四天(上午、下午)	软件安全编码实践	9：00-12：00 1：30-4：30
软件安全编码实践	讲解软件开发过程中常见的安全漏洞 包括输入输出验证和数据合法性校验、声明和初始化、表达式、多线程编程和序列化等。	
第五天（上午)	复习	9：00-12：00
第五天（下午)	考试	1：30-3：30

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、安全素养和安全技能，整体提高软件安全开发保障能力。

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。

第四章 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。