CISAW

信息安全保障人员认证

基本介绍

CISAW 信息安全保障人员认证体系

基本介绍

认证认可

根据中华人民共和国认证认可条例第二条的规定：

认可，是指由认可机构对认证机构、检查机构、实验室以及从事评审、审核等认证活动人员的能力和执业资格，予以承认的合格评定活动，也是对从业者和从业单位专业性的肯定。认可是对认证机构、检查机构、实验室等机构满足所规定要求的一种证实，这种证实大大增强了政府、监管者、公众、用户和消费者对合格评定机构的信任，以及对经过合格评定机构认可的产品、过程、体系、人员的信任。

认证，是指由认证机构证明产品、服务、管理、体系、人员符合相关技术规范、相关技术规范的强制性要求或者标准的合格评定活动，是一种第三方公正机构和法人实体提供的信用保证形式。

认可机构依据 CC03《人员认证机构通用要求》（等同采纳 ISO/IEC 17024 ）对人员认证机构进行认可。

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。

目录

第一章概述

一、引言

2014 年 2 月 27 日，中央网络安全和信息化领导小组宣告成立，习近平总书记亲自担任组长。这是中央落实十八届三中全会精神的重大举措，是中国网络安全和信息化国家战略迈出的重要一步，体现了中国最高领导层全面深化改革、加强顶层设计的意志，显示出国家在保障网络安全、维护国家利益、推动信息化发展的决心。"没有网络安全，就没有国家安全；没有信息化，就没有现代化。〃网络安全已经成为国家安全的重要组成部分，建设坚固可靠的国家网络安全体系，是中国必须做出的战略选择。

国家认监委在《国家认证认可事业发展"十二五〃规划》中，针对信息安全认证认可工作，提出了内容丰富、任务具体、目标明确的全面要求，其中特别强调："完善信息安全认证认可体系，进一步健全涵盖产品、管理体系、服务、人员、信息系统的信息安全认证体系。建立国家推行的信息安全服务资质认证制度，努力探索建立信息安全保障人员认证制度，推动信息安全认可领域国际互认。实现信息安全认证认可制度与国家信息安全相关管理制度的有效衔接，促进认证结果的社会采信，充分发挥认证认可在国家信息安全保障工作中的基础性作用。”

2014 年 10 月 23 日闭幕的十八届四中全会以"依法治国”为主题，首次审议通过了《中共中央关于全面推进依法治国若干重大问题的决定》。中央网信办在随后的贯彻落实会议精神中，提出了最近几年要制订的涉及网络空间的法律法规：《电信法》、《网络安全法》、《电子商务法》、《个人信息保护法》、《互联网信息服务法》、《电子政务法》和《未成年人网络保护条例》。今后 5 至 7 年，网络空间法律体系将逐步形成。这也为信息安全认证认可体系的完善和发展奠定了法律依据和政策保障。

随着移动互联网、物联网、云计算、大数据等新技术、新商业模式的飞速发展，给网络及信息化建设的发展带来新的产业机遇。同时也给网络安全和信息安全的保障提出更加严峻的挑战。

二、信息安全形势

2013 年 6 月,前美中情局(CIA)职员爱德华-斯诺登将两份绝密资料交给英国《卫报》和美国《华盛顿邮报》,标志着"棱镜门"事件的爆发,至今其影响还在持续发酵。该事件暴露出美国全球监听丑闻,引发全球信息安全热潮,凸显了我国在信息安全上的软肋,引发了高层的担忧,反映出我国在网络空间这一新疆域面临的巨大安全威胁,为世界各国敲响了警钟,充分印证了"没有网络安全就没有国家安全"这一深刻的道理,也使得国家高层领导从政治思想上进一步高度重视信息安全。网络空间的安全已经成为影响国家政权稳固、国防安全、社会稳定、经济发展和科技进步的重要因素。

2014 年 12 月 3 日中国软件评测中心发布 2014 年中国政府网站绩效评估结果显示，在评估范围内的 900 余家政府网站中，超过 93%存在各种危险等级安全漏洞，其中 97%的区县网站被监测到有安全隐患。近 50%的网站被监测到的安全漏洞超过 30 个，70 余家网站安全漏洞数量超过 100 个。从漏洞类型上看，破坏力大、影响范围广的信息泄露、跨站请求伪造等漏洞在 27%的网站中被监测到。当前政府网站安全形势严峻，安全防护能力亟待提升。

三、我国信息安全人才现状

来自教育部的统计调查资料表明 ,我国各行各业每年掌握信息安全技能的人员缺口数以百万计。来自工信部中国电子信息产业发展研究院发布的我国信息安全专业人才缺口超过

50 万。截至 2013 年底，我国培养信息安全专业人才总共约为 6 万人左右，距 50 多万的需求差距很大。今后五年，社会对信息安全的人才需要量大约为每年增加 1.2 万人左右。目前无论是学校教育还是社会培训都与社会需求极不相称。每年我国信息安全专业毕业生不足 1 万人，社会培训学员数量也不足 2 万人，信息安全人才匮乏的现象将长期存在。

2014 年 8 月 14 一 15 日 ,中国第八届信息安全学科专业建设与人才培养研讨会在上海召开。中国信息安全认证中心魏昊主任出席会议并做了题为"完善信息安全认证认可体系，助力国家信息安全人才培养”的大会专题演讲。

魏昊主任在演讲中，介绍了国际上人员认证认可行业的发展情况，并从认证机构、认证范围、市场占有率等方面与国内人员认证认可行业现状进行了对比，提出了建立完善我国信息安全保障人员认证制度的建议。中国信息安全认证中心(ISCCC)作为从事信息安全认证的专业机构，严格按照国际通行标准开展了自主品牌的信息安全保障人员认证（CISAW),得到业内的广泛认可。魏昊主任特别提出：下一步中国信息安全认证中心将发挥专业技术优势，继续致力于建立覆盖不同专业、行业、岗位、不同层次信息安全技术和管理人员的培训认证服务体系，为建立和完善人员认证制度、培养和造就我国信息安全人才队伍发挥应有作用。

第二章 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。

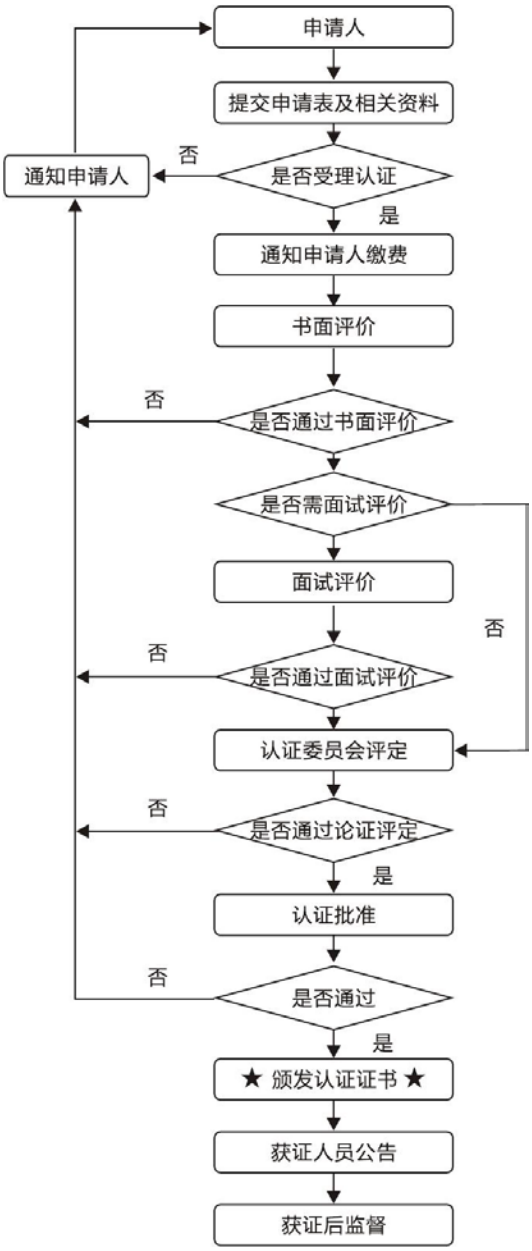

图 1 CISAW 认证流程

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。

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。