CISAW

信息安全保障人员认证

之

信息安全风险管理人员认证

课程介绍

信息安全风险管理人员认证

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。

信息安全风险管理人员认证是 CISAW 体系中技术专业认证类的一个技术方向,主要认证对象为专业从事信息安全风险管理及相关工作的管理和技术人员。

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技术专业认证和应用领域认证。

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。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。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；(预备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(预备人员无从业经历要求) 。

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。

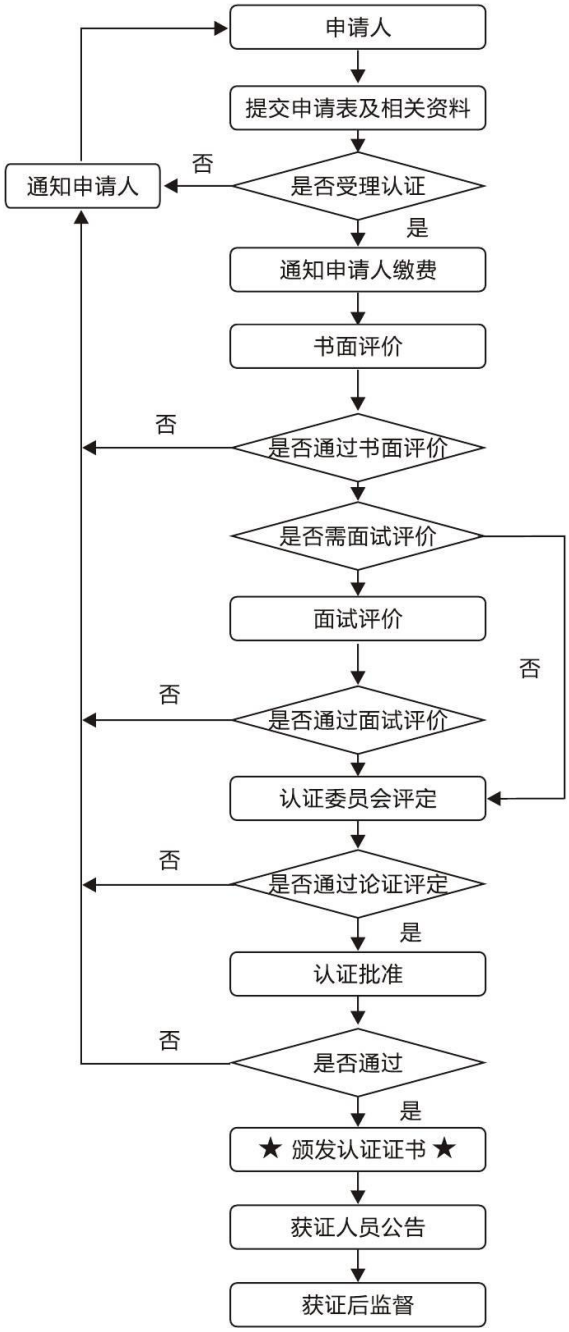

图 1 CISAW 认证流程

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、信息安全风险管理认证需求

据中国国家信息安全漏洞库(CNNVD)漏洞通报 ,近半年来漏洞通报维持在每月数百例，具体数据及其修复情况如表 2 所示。

表 2 安全漏洞通报与修复情况

年月	危急漏洞(例)/ 修复率(%)	高危漏洞(例) / 修复率(%)	中危漏洞(例) 修复率(%)	低危漏洞(例) / 修复率(%)	漏洞总数(例) / 修复率(%)
2014. 11	27/92. 59	124/95. 16	353/69. 41	41/78. 05	545/77. 06
2014. 12	32/93. 75	96/82. 29	384/75. 78	55/89. 09	567/79. 19
2015. 1	23/100	134/86. 57	542/79. 7	84/86. 9	783/82. 25
2015. 2	46/100	137/89. 78	258/82. 17	33/93. 94	474/86. 92
2015. 3	28/100	135/88. 15	437/70. 94	77/76. 62	677/76. 22

上述表格说明，漏洞的修补情况并不理想，同时也意味着这些尚未修补的漏洞将持续给信息系统、组织的业务开展带来无法确定的影响和损失。这给信息安全风险管理提出了需求和挑战。而信息安全风险管理工作的开展依赖于风险管理、分析、评价、实施、处置等相关人员的安全意识、安全素养和技术能力。CISAW《信息安全风险管理》人员认证依据国家相关的政策和国内外相关标准，对从事信息安全风险管理的相关人员展开认证和培训，有效提升风险管理相关人员综合素质。

CISAW《信息安全风险管理》人员认证中，参照已颁布的与信息安全预防、信息安全风险管理相关政策主要有：

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》

技术标准主要参照：

1. 《信息系统安全管理要求》 (GB/T 20269-2006)

2. 《信息安全风险评估规范》 (GB/T 20984-2007)

3. 《信息安全事件分类分级指南》(GB/Z 20986-2007)

4. 《信息安全管理体系要求》 (GB/T 22080-2008)

5. 《信息安全管理实用规则》 (GB/T 22081-2008)

6. 《信息安全风险管理指南》 (GB/Z 2436-2009)

结合上述标准开展的《信息安全风险管理》人员认证 ,是实现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、交通服务信息安全、医疗卫生信息安全、教育服务信息安全、能源服务信息安全、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。

预备级人员认证培训以信息安全基础知识为主，旨在巩固和梳理在校学生所学信息安全基础知识，增强实战技能，提高信息安全保障能力。

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、领域从事信息安全风险管理及相关工作的人员。

专业级培训对象：各行业、领域从事信息安全风险管理及相关工作的骨干技术人员和管理人员。

专业高级培训对象：各行业、领域从事信息安全风险管理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》对信息安全风险管理人员认证的要求，信息安全风险管理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安全风险管理等内容构成。

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，探讨信息安全风险的特征及信息安全风险管理模型 。	
第一天（下午）	相关标准	1: 30-4: 30
标准讨论	探讨信息安全风险管理相关标准及其应用	
第二天(上午)	风险评估	9: 00-12: 00
风险识别	探讨风险评估框架，交流和讨论风险识别的各项工作	
分析与评估	交流与探讨风险分析、分析评估工作的开展和评估报告的组织	
第二天（下午)	风险处置	1: 30-4: 30
风险处置	交流与探讨风险处置方法、处置过程实施	
监督与评审	探讨对风险处置进行监督和评审工作的开展	
第三天(上午)	案例分析	9: 00-12: 00
案例分析	介绍和交流具体风险管理案例，讨论案例中风险识别、分析、评估、评价以及处置各个环节中的管理问题	
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 。

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，并针对安全同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采取的信息安全技术和物联网安全措施	
第三天（上午)	风险管理基础	9: 00-12: 00
基础知识	介绍信息安全风险的由来、基本概念、特征及信息安全风险管理模型。	
第三天(下午)	相关标准	1: 30-4: 30
技术标准	介绍信息安全风险管理相关标准及其应用	
第四天(上午)	风险评估	9: 00-12: 00
风险识别	介绍风险评估框架，介绍与分析风险识别的各项工作	
分析与评估	交流与探讨风险分析，分析评估工作的开展和评估报告的组织	
第四天(下午)	风险处置	1: 30-4: 30
风险处置	介绍风险处置方法，讲解处置过程实施	
监督与评审	详细介绍对风险处置进行监督和评审工作的开展	
第五天(上午)	总结	9: 00-12: 00
案例分析	结合具体风险管理案例，讲解案例中风险识别、分析、评估、评价以及处置各个环节工作的开展	
培训总结	总结培训内容	
第五天(下午)	认证考试	14:00-16:30

(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）	新技术	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）	风险管理综述	9: 00-12: 00
基础知识	介绍基本概念、特征及信息安全风险管理模型、相关标准	
风险识别	简介风险评估框架，与分析风险识别的各项工作	
分析与评估	简介风险分析、分析评估工作的开展和评估报告的组织	
风险处置	简介风险处置方法，说明处置过程实施	
监督与评审	简介介绍对风险处置进行监督和评审工作的开展	
案例分析	结合具体风险管理案例，说明案例中风险识别、分析、评估、评价以及处置各个环节工作的开展	
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、安全素养和风险识别、分析、评估和处置能力，整体提高信息安全风险管理能力。

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。