CISAW

信息安全保障人员认证

之

信息系统安全运维人员认证

课程介绍

信息系统安全运维人员认证

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。

信息系统安全运维人员认证是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运维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。

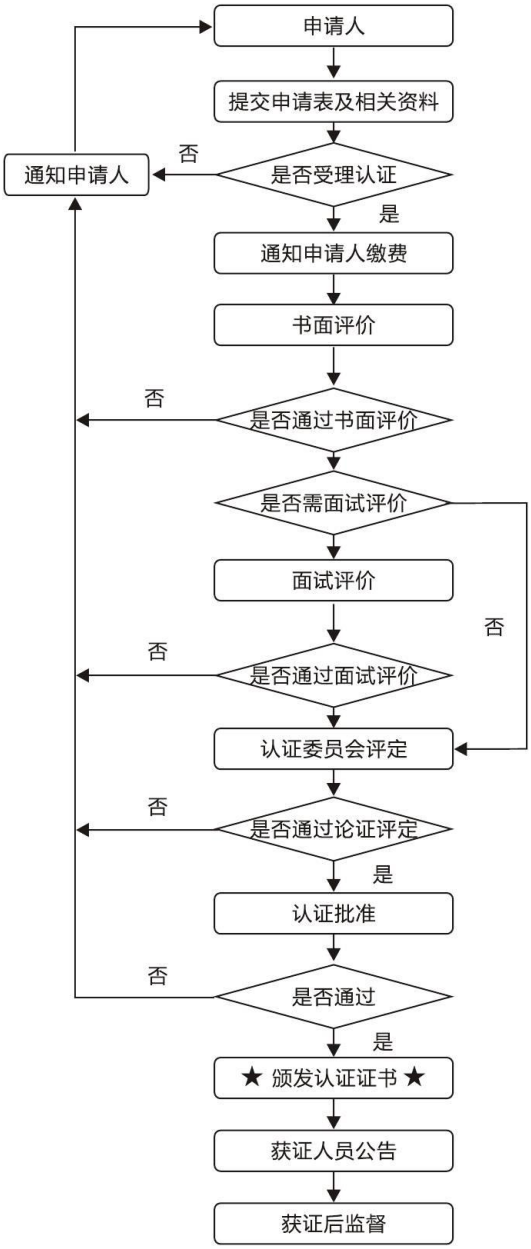

图1 CISAW认证流程

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、信息系统安全运维服务认证需求

运维一般是指对大型组织已经建立好的网络软硬件的维护，其中传统的运维是指IT运维。所谓IT运维，是指单位IT部门采用相关的方法、手段、技术、制度、流程和文档等，对IT运行环境(如软硬件环境、网络环境等)、 IT业务系统和IT运维人员进行的综合治理。随着IT建设的不断深入和完善，计算机硬软件系统的运行维护已经成为了各行各业各单位领导和信息服务部门普遍关注和不堪重负的问题。据统计，IT运维服务占到IT部门工作量的80%左右。

目前，大多数的运维服务水平处在一个被动的阶段。这主要表现在信息技术和设备的应用越来越多，但运维人员在信息系统出现安全事件的时候却茫然不知所措。究其原因，是该组织未建设成完整的运维体系。

其中问题集中体现在：

(1)众多安全设备缺乏有效的统一管理

(2)安全运维能力不足，5x8小时外的安全事件无暇顾及

（3）信息安全产品更新太快，信息安全系统建设投入太大

（4）缺乏专业的安全运维团队

（5）突发安全事件的应急处理能力不足、异常操作行为无法及时预警

（6）海量日志需要统一存储审计

（7）信息管理部门的人员有限，员工的精力有限

（8）安全管理制度体系不完善，安全责任制落实不到位

（9）安全技术能力方面或多或少的存在一定的限制

（10）外界新技术无法更快更好的应用到内网

而随着信息安全管理体系和技术体系在企业领域的信息安全建设中不断推进，占信息系统生命周期70%~80%的信息安全运维体系的建设已经越来越被广大用户重视。尤其是随着信息系统建设工作从大规模建设阶段逐步转型到"建设和运维"并举的发展阶段，运维人员需要管理越来越庞大的IT系统这样的情况下，信息安全运维体系建设已经被提到了一个空前的高度上。

目前，具有一定规模的单位已经部署相当多的安全设施，如防火墙、防病毒、远程访问设备等等。众多的安全技术与安全设备的应用却在相当程度上加重了系统与IT管理人员的负担。

另一方面，安全设备的应用越来越多，安全手段的采用也越来越多，而安全状况却不见好转。以下就是经常摆在IT管理人员面前的问题：

（1）我们已经在安全方面投入了相当多的努力，但为什么还不时出现安全问题?

（2）我们的安全项目已制定了很多安全制度、管理流程等，但面对一大堆的文档，怎么样才能真正地执行下去?

这类问题，几乎让每个IT管理人员头痛。面对众多的设备与手段，安全管理人员却往往感到无所适从。其根源是什么呢?

我们早就知道，安全不仅仅是一个技术问题，更是一个管理问题。实际上，在整个IT产品的生命周期中，运营阶段占了整个时间和成本的70%~80%左右，剩下的时间和成本才是花费在产品开发(或采购)上面。以往我们所说"三分技术、七分管理"是突出管理的重要性，而这个“管理”则是大部分的精力花费在"运营"方面。

效果和效率是安全运维服务的主要目标。安全运维的主要目的即是保证安全手段(产品+技术)的应用能够达到预期的良好效果和提高效率。因此，如何保证安全运维工作的有效性是摆在IT安全管理人员面前的主要难题。

正是因为目前信息系统安全运维服务中存在的弊端 ,依靠长期从事信息安全和信息系统运维服务的经验，同时结合信息安全保障体系建设中运维体系建设的要求,遵循ITIL(最佳实践指导)、 ISO/IEC 27000系列服务标准、以及国家其它相关标准，建立了一整套完善和切实可行的信息系统安全运维服务规范。

引发信息系统安全运维服务各环节安全问题的主要原因在于，即相关人员在安全意识、安全技能和安全素养上的欠缺。

CISAW《信息系统安全运维服务》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运维服务的运维管理人员、运行维护人员、运维部门经理和CIO等展开认证和培训，有效提升相关人员的安全意识、安全素养和安全技能。

CISAW《信息系统安全运维服务》人员认证中，参照的技术标准主要有：

1. 《信息技术一服务管理一第1部分：规范》(ISO/IEC 20000-1:2005)
2. 《信息技术一服务管理一第2部分：实施指南》(ISO/IEC 20000-2:2005)
3. 《信息技术一安全技术一信息安全管理体系要求》(ISO/IEC 27001:2013)
4. 《信息技术安全性评估准则》(GB/T 18336-2008)
5. 《信息系统通用安全技术要求》(GB/T 20271-2006)
6. 《信息系统安全管理要求》 (GB/T 20269-2006)
7. 《信息安全风险评估规范》(GB/T 20984-2007)
8. 《信息安全事件分类分级指南》(GB/Z 20986-2007)
9. 《信息安全管理体系要求》(GB/T 22080-2008)
10. 《信息安全管理实用规则》(GB/T 22081-2008)
11. 《信息技术服务运行维护》
12. 信息技术基础架构库(ITIL)

结合上述标准开展的《信息系统安全运维服务》人员认证，是实现信息系统安全运维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

各行业领域从事信息系统安全运维服务及相关工作的运维人员、管理人员、骨干技术人员、各级领导和核心人员。包括CIO、运维部门经理、信息安全经理、运维管理人员、运行维护人员和IT人员等。

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》对信息系统安全运维服务人员认证的要求，信息系统安全运维服务人员认证培训内容由CISAW知识体系介绍、信息安全基础知识、安全运维模型、安全运维内容、安全运维流程和安全运维的典型实例等内容构成。

具体内容及安排，见表3。

专业资格认证培训以研讨为主，讲授为辅，为期5天，具体研讨培训内容如下：

天	内容标题	时间
第一天(上午)	安全运维知识体系	9:00- 12:00
CISAW 知识体系	讨论信息安全形势，介绍信息安全基本概念和发展历程、法律法规。介绍 CISAW 知识体系的核心理念，重点讲解 CISAW 信息安全保障模型和基本内容等	
安全运维模型	讨论运维过程中的安全事件，介绍安全运维和运维安全两种模式的基本概念、 详细分析信息系统安全运维模型，讲解模型各元素的关系和安全运维和运维安全两种模式关系	
第一天(下午)	信息安全技术知识	14:00-17:00
数据安全域	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，以及数据安全相关的密码技术、身份认证、访问控制、 PKI 技术、信息隐藏、容错容灾、反垃圾邮件技术等	
载体安全域	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,介绍存储介质安全、恶意代码与防范、传输载体安全技术等内容	
第二天(上午)	信息安全技术知识	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，介绍机房安全、主机安全、漏洞管理、安全审计、取证技术等内容	
边界安全	介绍边界要全的概念、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同题，并针对安全问题介绍边界安全的技术与措施，讲解防火墙技术、入侵检测技术、隔离技术、网络攻击与防范等技术内容	

第二天(下午)	安全运维知识	14:00- 17:00
安全运维综述	介绍安全运维的方法论,详细讲解方法论的基本框架、服务与服务管理、流程、功能与角色的基本概念和各元素的关系,详细介绍安全运维的实施目标、实施对象、运维方式和运维支撑系统	
合规要求	介绍安全运维领域相关的法律法规、标准,以案例方式进行讨论的安全管理要求	
第三天(上午)	安全运维知识	9:00- 12:00
安全策略	讲解安全运维工作安全策略制定方法并说明典型安全策略的制定	
运维准备	讲解安全运维准备的具体工作内容和各环节的工作方法,包括需求调研、运维规划、运维导入等，从而确定运维的范围、策略和基线等安全需求,案例讨论安全运维规划的具体工作内容和流程	
第三天(下午)	安全运维知识	14:00- 17:00
运维实施	讲解依据运维规划的内容如何开展有效的安全运维工作，包括技术准备、工具准备、环境建立、人员准备、流程建立等,案例讨论主要的安全运维工作内容和流程	
第四天(上午)	安全运维知识	9:00- 12:00
运维评审	讲解对系统运维过程的质量监视,评价系统安全运维的有效性、运维安全的正确性,评审阶段的具体工作内容和流程，案例讨论服务生命周期每一个阶段进行评估和分析。	
持续改进	介绍安全运维改进阶段的具体工作内容和流程,案例讨论改业务流程的信息系统安全运维服务，以及与业务需求变化的适应过程。	
第四天(下午)	安全运维知识	14:00- 17:00
运维安全	介绍运维安全的基本概念、范围、目标、方式等内容。	
风险评估	讲述运维过程的风险评估方法与基本流程,对运维活动所面临的风险进行识别、评价、处置与管理进行详细分析和讲解	
风险处置	对运维过程的安全保障措施的选择、部署、管理等进行具体分析和介绍	
过程监控	讲解对风险处置过程和采取的安全保障措施如何进行质量监视,如何评价安全保障措施给运维安全带来的有效性和正确性	
第五天(上午)	安全运维知识	9:00- 12:00
案例分析	结合安全运维活动的典型案列，以 CISAW 安全运维保障模型为依据,讨论和分析安全运维保障各个环节的实现,讨论运维安全的风险和风险规避措施 。	
第五天(下午)	考前辅导	14:00-1630
考前辅导	全面复习所学习的内容，梳理知识点	
总结讨论	培训总结、专题讨论、交流心得体会	

五、培训收益

针对提供运维服务的人员：

1.运维人员掌握最佳安全运维实践方法，提升个人的业务能力和处理效率；

2.运维人员了解和掌握运维安全的概念和实例，避免在运维过程中的安全事件，提升客户满意度；

3.掌握安全运维服务体系的流程和方法，提高服务意识，采用的管理措施和技术手段建立一套信息系统安全运维服务的管理流程和管控方法。

对系统运营单位的管理者：

1.了解运维活动中的安全风险，熟悉安全运维工作方法，获得信息系统安全运维服务体验；

2.确保安全运维流程支持业务流程，提高企业整体业务运营的质量；

3.了解和熟悉运维监控和运维评审活动，追求安全运维活动的持续改善。

对系统运营单位的运维管理者：

1.了解业界领先的信息系统安全运维服务管理模式，熟悉业界领先的信息系统安全运维服务最佳实践；

2 .了解和熟悉处于运行阶段的信息系统在运维过程中的安全性和避免信息系统运维过程面临的风险；

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。