中国通信企业协会文件

通企〔2022〕95 号

关于举办信息安全保障人员（CISAW）系列认证培训的通知

各会员单位：

为提升行业单位信息系统安全保障能力，培养安全运维、安全集成、风险管理、应急服务人才，满足信息系统建设及信息安全项目对投标人的资质要求，中国通信企业协会决定开展信息安全保障人员（CISAW）认证培训工作。现将认证相关情况及下半年培训安排通知如下：

一、认证简介

信息安全保障人员认证（Certified Information Security Assurance Worker，简称“CISAW”）体系是中国网络安全审查技术与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，是为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。认证体系包括信息系统安全运维、安全集成、风险管理、应急服务、软件安全开发、WEB 安全等多个方向，目前该认证体系已成为信息系统相应领域人才评价、考核的必备资质。可有效满足信息系统运维服务、安全集成、应急服务、风险管理类等各招标项目对项目人员的资质要求。

二、认证主要方向及认证对象

（一）CISAW——安全运维方向

【认证对象】:从事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，包括首席信息官（CIO)、运维部门经理、信息安全经理、运维管理人员、运行维护人员和信息技术人员等。

（二）CISAW——安全集成方向

【认证对象】: 涉及信息系统安全开发与建设、安全加固、安全优化、安全需求分析、安全设计、安全实施和安全保障等工作相关的管理人员、技术人员、维护人员和使用人员。

（三）CISAW——应急服务方向

【认证对象】: 从事网络安全、信息安全、风险管理、应急预案、应急演练、安全事件分析、应急处置等工作相关的管理人员、技术人员、维护人员。

（四）CISAW——风险管理方向

【认证对象】: 从事网络与信息安全服务的各级管理人员

和技术人员，特别是从事信息安全风险管理、信息安全风险评估的专业人员，以及与信息安全保障工作相关的人员。

（五）CISAW——安全软件方向

【认证对象】：从事软件项目管理的人员；企业各部门的设计、开发、测试、技术服务等管理和技术人员；有兴趣致力于在软件安全开发方向发展的人员。

三、申请条件及证书

CISAW 系列各方向均分为基础级、专业级、专业高级三个认证级别，各级别申请条件如下：

【基础级】满足以下条件之一且通过申请认证方向的认证考试者，可申请该方向的基础级认证：

（一）本科（含）以上学历， 1 年以上从事信息安全有关工作经历；

（二）专科毕业，3 年以上从事信息安全有关的工作经历；

（三）3.5 年以上从事信息安全有关的工作经历；

（四）具有信息技术相关专业的初级技术职称，并且至少 1 年以上从事信息安全保障相关工作经历。

【专业级】满足以下条件之一且通过申请认证方向的认证考试者，可申请该方向的专业级认证：

（一）硕士研究生（含）以上学历，2 年以上从事信息安全有关工作经历，并且至少 1 年从事与申请认证方向相关的工作经历；

（二）本科毕业，4 年以上从事信息安全有关工作经历，并且至少 2 年以上从事与申请认证方向相关的工作经历；

（三）专科毕业，6 年以上从事信息安全有关工作经历，并且至少 2 年以上从事与申请认证方向相关的工作经历；

（四）7 年以上从事信息安全有关工作经历,并且至少 2 年以上从事与申请认证方向相关的工作经历；

（五）具有信息技术相关专业的中级技术职称,并且从事至少 2 年以上与申请认证方向相关的工作经历。

【专业高级】：暂未开放。

四、培训及考试时间安排

各方向认证培训分 2 个阶段进行，第 1 阶段为线上培训，第 2 阶段为线下面授及考试。各方向培训课时及

第 1 阶段线上培训时间安排如下：

课程 / 时间	安全运维 2 天	安全集成 3 天	应急服务 3 天	风险管理 3 天	安全软件 4 天
7 月	25-26 日	20-22	27-29	18-20	12-15
8 月	29-30 日	17-19	24-26	22-24	15-18
9 月	26-27	19-21	28-30	21-23	13-16
10 月	待定	12-14	26-28	24-26	17-20
11 月	待定	23-25	28-30	21-23	15-18
12 月	待定	19-21	28-30	26-28	13-16

第 2 阶段线下面授及考试：开展时间待疫情防控形势稳定后，具备集中上课和考试条件后再另行通知。

安全运维	安全集成	应急服务	风险管理	安全软件
3 天	2 天	2 天	2 天	1 天

五、考试题型、时长及分值

考试形式：笔试

考试时长：150 分钟

考试题型：单选题、多选题、简答题、实验题。

满分 120 分，84 分（含）为合格分

六、申请资料提交

学员确定报名后,需由本人登陆中国网络安全审查技术与认证中心学员系统，在线提交个人学历、工作经历、项目经历等信息，并上传相关证件。

七、培训及认证费用

培训费：6800 元/人（款项需汇至中国通信企业协会账户）

认证费： 1080 元/人（款项需考前登陆中国网络安全审查技术与认证中心人员认证业务管理系统完成注册报及缴费，地址：https://ryrzcisaw.isccc.gov.cn，详见考试通知）

八、考试及证书

认证考试由中国网络安全审查技术与认证中心组织实施。通过认证考试且符合《信息安全保障人员认证准则》相关要求的认证申请人员，可以获得相应领域和级别的认证证书。证书有效期为三年，到期前 3 个月，证书持有人需要在中国网络安全审查技术与认证中心人员认证业务管理系统中完成至少 16

学时的在线继续教育学习，方可申请换发认证证书。


信息安全保障人员认证证书
Information Security Assurance Worker Certification Certificate

兹证明
This is to certify that

认证考试建培合格，并通过了认证评价，符合《信息安全保障人员认证准则》的要求，特颁此证。
Has passed the examination, certification assessment and successfully fulfilled the requirements of Certification Criteria for Information Security Assurance Worker and is hereby awarded the foundation-level in web security field.

认证方向/Certification field: Web安全（基础级）WS(F)
证书编号/Certificate No.:
序列号/Serial No.:
发证日期/Date of Issue:
有效期/Term of Validity:

九、说明

（一）学员可根据实际工作需要及课程信息，自行选择认证培训项目，并将相关信息准确填写在报名回执中；

（二）每班满25人即可开班培训和考试。如不满开班人数，将延期安排；

（三）每培训班建立学员群，由助教老师负责课程咨询、答疑、考务管理等工作。

十、报名流程

请于开班前7个工作日将填写完整的报名回执(word版)、培训考试费用汇款凭证发送至报名邮箱(ztqx_cisaw@163.com)，并注明：单位名称+项目名称+姓名。如需开具增值税专用发票，请将经单位财务核对后的开票信息

准确填写在报名回执中。

收款单位：中国通信企业协会

开 户 行：中国工商银行北京长安支行

账　　号：0200　0033　0900　5403　113

附件：1.报名回执

2.CISAW 系列各方向认证课程大纲

中国通信企业协会

2022 年 6 月 22 日

（联系方式：中国通信企业协会

宋老师　010-68200128/18612568779

王老师　010-68200127/13911072637

报名邮箱：ztqx_cisaw@163.com）

附件 1

CISAW 系列认证培训报名回执

认证方向：☐安全运维　　☐安全集成　　☐应急服务　　☐风险管理　　☐安全软件

序号	姓　名	工作单位	性别	身份证号码	手机	邮箱	毕业院校	专业	学历	工作年限	邮寄地址

发 票 信 息	1.发票抬头： 2.纳税人识别码： 3.单位注册地址：	4.开户行名称： 5.账号： 6.联系电话：
报名联系人及联系方式	部门：　　姓名：　　电话：　　邮箱：	

邮箱：ztqx_cisaw@163.com　　电话：010-68200128、68200127

附件 2

CISAW 系列认证课程大纲——安全运维方向

一、概述

1.信息系统　　2.系统运维
3.安全运维模型　　4.安全运维模式

二、安全运维体系

1.安全运维　　2.运维安全
3.合规性要求　　4.评审及改进

三、合规要求

1.法律法规要求　　2.信息安全标准
3.运维服务标准

四、安全策略

1.安全策略概述　　2.制定安全策略方法
3.安全策略内容　　4.案例分析

五、运维准备

1.安全运维需求分析　　2.安全运维策划
3.安全运维服务预算　　4.安全运维服务范围
5.安全运维外包　　6.案例分析

六、运维实施

1.日常运维　　2.应急响应
3.优化改善　　4.监管评估
5.案例分析

七、运维安全

1.运维安全概述　　2.风险评估
3.风险处置　　4.过程监控
5.案例分析

八、评审及改进

1.过程有效性评估　　2.过程有效性评估要点
3.过程有效性评估指标　　4.持续改进
5.案例分析

九、复习串讲

1.串讲课程重点知识点　　2.现场答疑

CISAW 系列认证课程大纲——安全集成方向

一、基础知识

1.基本概念　　2.CISAW 模型

二、数据安全

1.数据基本概念　2.动态数据与静态数据的安全技术与措施

三、载体安全

1.存储与传输数据的载体
2.物理载体和逻辑载体的安全技术与措施
3.存储安全、传输安全、安全协议

四、环境安全

1.外部环境的安全保障技术
2.物理环境和逻辑环境的安全技术和措施
3.机房安全、主机安全、访问控制、安全审计、入侵检测等

五、边界安全

1.边界安全保障技术与措施
2.物理边界和逻辑边界的安全技术与措施
3.周界安全
4.网络边界安全防火墙、网闸
5.主机边界安全等

六、安全集成概述及安全集成模型

1.安全集成基本概念
2.安全集成范畴
3.安全集成的本质
4. CISAW 安全集成模型
5.安全集成的两种模式及关键环节、差异与联系

七、系统安全工程基本理论

1.系统工程
2.系统安全工程基本概念
3.系统工程基本模型

八、SSE-CMM

1.系统安全工程成熟度模型相关概念
2.二维模型

3.三个过程域
4.11 个相关基本惯例

九、安全集成实施过程

1.集成模式及关键环节
2.安全集成实施过程要点

十、安全技术与安全集成综述及案例分析

十一、安全集成关键环节分组交流、研讨

十二、复习串讲

1.认证规范解读
2.串讲课程重点知识点
3..现场答疑

CISAW 系列认证课程大纲——应急服务方向

一、概述
二、应急响应相关法律法规
三、信息安全事件分类分级
四、网络安全事件管理与应急响应组织
五、应急响应案例分析研讨
六、典型网络安全入侵事件重现与分析
七、主机漏洞利用分析实践
八、主机入侵溯源分析实践
九、主机入侵事件检测技术总结与工具包准备
十、主机攻击特征之数据流分析实践
十一、网络层应急技术与实践
十二、数据库渗透与应急响应实践
十三、应急技术综合演练实践之 SQL 注入攻击分析实践与加固
十四、应急技术综合演练实践之 XSS 攻击分析实践与加固
十五、应急技术综合演练实践之 CSRF 攻击分析实践与加固
十六、应急安全技术保障实践之 PKI 应用
十七、应急安全技术保障实践之日志分析概念与技术
十八、应急安全技术保障实践之日志集中管理与审计系统
十九、企事业单位网络安全工作现状与困惑分析
二十、应急管理体系化建设 I
二十一、应急管理体系化建设 II
二十二、应急预案制定与管理
二十三、网络安全事件应急处理流程 I
二十四、网络安全事件应急处理流程 II
二十五、业务系统流程分析与数据流风险点识别沙盘演练
二十六、应急响应流程梳理与预案编写沙盘演练
二十七、应急演练组织与开展沙盘演练

CISAW 系列认证课程大纲——风险管理方向

一、概述
二、风险管理基本概念
三、风险管理标准体系
四、风险管理标准 ISO31000
五、信息安全风险管理标准 ISO27005
六、信息安全风险评估标准 GB/T20984
七、项目管理基础和环境建立
八、发展战略和业务识别
九、资产识别
十、威胁识别
十一、脆弱性识别
十二、已有安全措施识别
十三、风险分析
十四、风险计算
十五、风险评价和评估输出
十六、风险处置概述
十七、风险处置和风险接受
十八、沟通咨询和监视评审
十九、物理脆弱性识别
二十、网络脆弱性识别
二十一、系统软件脆弱性识别
二十二、应用中间件脆弱性识别
二十三、应用系统脆弱性识别
二十四、管理脆弱性识别
二十五、风险管理综合案例 I
二十六、风险管理综合案例 II
二十七、风险管理综合案例 III

CISAW系列认证课程大纲——软件安全方向

一、软件安全概述

软件安全相关概念、软件安全范畴及软件存在安全问题

二、软件安全开发模型

三种软件开发模型和常用的软件开发方法、典型软件安全开发模型、掌握CISAW软件安全开发模型

三、安全漏洞管理

漏洞相关概念、安全自动化协议、典型安全漏洞

四、安全功能设计

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。

五、常见安全问题

软件开发过程中常见的安全问题及出解决方案。

六、软件安全编码实践

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。

七、软件安全测试

软件安全测试的方法和过程、常见测试工具

八、新技术风险

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。

九、软件安全风险评估和软件安全管理

安全软件风险评估、运行维护管理和组织与人员管理。

中国通信企业协会秘书处　　2022年6月22日印发