中国通信企业协会文件

通企〔2022〕93号

关于开展2022年下半年度CISP系列及CISSP认证培训的通知

各会员单位：

信息安全不仅是组织持续发展的需要，更是支撑和保障国家安全的重要基础。为提升行业信息安全保障能力，培养信息安全人才，中国通信企业协会将继续在行业开展信息安全系列认证培训工作。现将2022年下半年度培训有关事宜通知如下：

一、认证项目介绍

（一）信息安全专业人员认证（Certified Information Security Professional，简称“CISP”），是经中国信息安全测评认证中心实施的国家认证，对信息安全人员执业资质的认可。该证书是面向信息安全企业、信息安全咨询服务机构、信息安全测评机构、政府机构、社会各组织、团体、大专院校以及企事业

单位信息安全专业人员所颁发的专业资质证书。目前，认证方向已涵盖信息安全各个领域，包括信息安全技术、信息安全管理、云安全、个人信息保护、大数据安全分析、数据安全治理、渗透测试等十多个方向。

（二）国际注册信息安全专家（Certification for Information System Security Professional，简称“CISSP”），由(ISC)² ——国际信息系统安全认证联盟组织与管理。该证书代表国际信息系统安全从业人员的权威认证，被业界称为信息安全中的“冠军资质”。

认证的收益与优势：

对个人而言：我国信息安全从业人员最高级别的能力认证，能帮助个人系统性提升网络安全技术和管理能力，是安全工作岗位不可或缺、广受认可的证书，也是国内拥有会员数最多的信息安全认证。

对集成服务商而言：申请信息安全服务相关资质必不可少的要求。例如常规安服项目招标都要求相关项目经理和实施人员必须具备 CISP 证书，申请信息安全服务资质（安全工程类）一级、二级和三级分别至少需要 2 名、4 名和 12 名 CISP 持证人员。

对政企事业单位而言：能够提升安全人员的综合安全能力。同时拥有一定数量的证书持证人员可以满足网络安全法对于关键信息安全岗位人员的持证上岗要求，为政企事业单位的网络安全保驾护航。

二、认证培训课程、时间安排及费用

课程名称	单价（元/人）	天数	7 月	8 月	9 月	10 月	11 月	12 月
CISP-CISE/CISO (注册信息安全工程师/ 注册信息安全管理人员)	6600 元培训费 3000 元考试费	5 天	北京 16-20 成都 27-31	直播 北京 27-31	直播 北京 24-28	直播 北京 26-30	直播 北京 26-30	直播 北京 14-18
CISP-DSG (注册数据安全治理 专业人员)	6600 元培训费 3000 元考试费	5 天	11-15	15-19	12-16	10-14	14-18	12-16
CISP-CSE (注册云安全工程师)	6600 元培训费 3000 元考试费	5 天	4 天线上培训随报随学+1 天线下考前辅导					
CISP-BDSA (注册大数据安全 分析师)	6600 元培训费 3000 元考试费	5 天	4 天线上培训随报随学+1 天线下考前辅导					
CISP-PTE (注册渗透测试工程师)	14800 元培训费 5000 元考试费	7 天	7 月 27- 8 月 2 日	8 月 27- 9 月 2 日	24-30 日	10 月 28- 11 月 3 日	11 月 26- 12 月 1 日	25-31 日
国际注册信息安全专家 CISSP 认证	7800 元培训费 5700 元考试费	5 天	16-30 周末班	6-20 日 周末班	3-24 日 周末班	15-29 日 周末班	13-27 日 周末班	17-31 日 周末班
			7 月 18-9 月 7日晚上班					

注：学员可根据个人实际情况选择其他考试时间和地点。

三、认证对象、报考条件及考试题型

课程名称	认证对象	报名条件	考试题型
注册信息安全专业人员 CISP-CISE/CISO 认证	从事信息系统（网络）建设、运行和应用管理的专业安全岗位人员	1、硕士研究生以上，具有 1 年工作经历；或本科毕业，具有 2 年工作经历；或大专毕业，具有 4 年工作经历； 2、专业工作经历:至少具备 1 年从事信息安全有关的工作经历。	考试时长：2 个小时（120 分钟） 考试题型：100 道选择题。 (注：70 分以上通过)
注册数据安全管理专业人员 CISP-DSG 认证	企业信息安全负责人、信息安全管理人员、数据管理人员、安全监管人员；数据安全部门工作人员、大数据部门的工作人员、数据信息使用者；风险管理人员、安全审计人员、运维人员、技术支持人员等。		

注册信息安全专业人员 CISP-CSE 云安全工程师	从事云安全咨询服务、测评认证、安全建设、安全管理工作的人员； 从事云计算集成、调试、运行、维护和管理的专业人员等等； IT 技术人员、IT 运维人员从业人员等。	大专及以上学历,一年以上相关工作经历； 具备一定的相关科目基础知识； 具备一定的信息安全知识与计算机网络知识。	
注册信息安全专业人员 CISP-BDSA 大数据安全分析师	从事安全数据分析、安全产品研发的技术人员； 从事信息安全服务工作或高级安全管理工作的人员； 信息安全咨询服务机构及信息安全服务支撑机构从业人员； IT 技术人员、IT 运维人员、传统信息安全从业人员。		考试时长：2 个小时（120 分钟） 考试题型：选择+实操。 (注：70 分以上通过)
注册信息安全专业人员 CISP-PTE 渗透测试工程师认证	从事信息安全技术领域安全渗透测试工作人员； 从事规划测试方案、编写项目测试计划、编写测试用例、测试报告工作的人员； IT 技术人员、IT 运维人员、传统信息安全从业人员。		
国际注册信息安全专家 CISSP 认证	从事信息系统（网络）建设、运行和应用管理的专业安全岗位专业及管理人员。	至少五年的工作经验,拥有大学本科学历,需要四年工作经验,研究生学历仍需四年工作经验。工作经验应为 CBK 规定的 10 个知识域中的一个或多个范畴； 签署并承诺遵守(ISC)2 制定的职业守则（CodeofEthics）	考试时长：6 个小时（720 分钟） 考试题型：250 道题。 (注：700 分以上通过)

四、需提交资料(电子版)

（一）个人近期免冠 2 寸蓝底彩色照片；

（二）身份证（正反面）清晰扫描件；

（三）学历、学位证明扫描件；

（四）“注册信息安全人员考试及注册申请表”纸质盖章版1份。**（申请表电子版文件待索）**

五、考试及证书

CISP考试由中国信息安全测评中心组织实施，可在测评中心官网查询证书信息。CISP证书是面向信息安全从业人员推出的权威国家级认证，可作为能力提升、员工晋升和企业撰写招投标文件等工作提供重要参考，部分省市已将其纳入技能补贴范围。

CISSP考试由国际信息系统安全认证联盟组织与管理，可在(ISC)²官网查询证书信息。考试题目来自(ISC)²的题库，每次考试都会根据当前信息领域安全的热点有所侧重。CISSP证书是信息系统安全从业人员的权威国际级认证，被业界称为信息安全中的“冠军资质”。

六、报名流程

请于开班前10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_cisp@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.CISP及CISSP认证培训报名回执

2.CISP 及 CISSP 认证培训课程大纲

中国通信企业协会

2022 年 6 月 21 日

(联系人:中国通信企业协会

宋老师　010-68200128/18612568779)

附件 1

CISP及CISSP认证培训报名回执

单位名称					部门及职务	
序号	姓　名	性别	联系电话	电子邮箱	课程名称	培训时间
						_____月
						_____月
						_____月
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_CISP@163.COM　　电话：　010-68200128、18612568779

附件 2

CISP 系列认证培训课程大纲

——CISE（信息安全工程师）及 CISO（信息安全管理人员）

一、信息安全保障

1.信息安全保障基础　　2.安全保障框架模型

二、信息安全监管

1.网络安全法律体系建设　　2.国家网络安全政策

3.网络安全道德准则　　4.信息安全标准

三、信息安全管理

1.信息安全管理基础　　2.信息安全风险管理

2.信息安全管理体系建设　　3.信息安全管理体系最佳实践

4.信息安全管理体系度量

四、业务连续性

1.业务连续性　2.信息安全应急响应　3.灾难备份与恢复

五、安全工程与运营

1.系统安全工程　　2.安全运营

3.内容安全　　4.社会工程学与培训教育

六、安全评估

1.安全评估基础　　2.安全评估实施

3.信息系统审计

七、安全支撑技术

1.密码学　　2.身份鉴别　　3.访问控制

八、物理与网络通信安全

1.物理安全　　2.OSI 通信模型　　3.TCP/IP 协议安全

4.无线通信安全　5.典型网络攻击防范　6.网络安全防护技术

九、计算环境安全

1.操作系统安全　　2.信息收集与系统攻击

3.恶意代码防护　　4.应用安全　　5.数据安全

十、软件安全开发

1.软件安全开发生命周期　　2.软件安全需求及设计

3.软件安全实现　　4.软件安全测试

5.软件安全交付

CISP 系列认证培训课程大纲
——DSG（数据安全治理专业人员）

一、信息安全保障

1.安全保障框架模型　　2.信息安全保障基础

二、信息安全支撑技术

1.密码学　　2.身份鉴别　　3.访问控制

三、信息安全监管

1.网络安全法律体系建设　　2.网络安全国家政策

3.网路安全道德准则　　4.信息安全标准

四、信息安全评估

1.信息安全评估基础　　2.信息安全评估实施

五、数据安全基础

1.结构化数据应用　　2.非结构化数据应用

3.大数据应用　　4.数据安全基础

六、数据安全治理

1.数据安全治理与保障框架　　2.数据安全管理要求

七、数据安风险全评估

八、数据安全策略

1.数据安全策略要求　　2.数据安全技术要求

3.数据安全运营要求　　4.数据安全合规测评要求

九、数据安全技术

1.数据防泄漏技术　　2.数据库安全技术

3.数据可用性保障技术　　4.大数据安全防护技术

CISP 系列认证培训课程大纲
——CSE（云安全工程师）

一、云计算基础知识

云计算的基本概念、云计算参考架构、云计算的关键技术及系统实现、云计算运营模式和市场格局。

二、云安全模型与风险分析

云安全基本概念、云计算安全风险、云计算面临的威胁、云计算存在的隐患以及云安全需求。

三、云平台和基础设施安全

从安全攻防的角度介绍了云平台和基础设施身份访问管理、攻击防护、入侵检测、恶意代码检测、虚机镜像防护等五类安全防护措施。

四、云数据安全与隐私保护

云计算中数据安全治理方法模型、数据安全治理步骤以及云计算中数据安全防护技术。

五、云应用安全

应用安全的管理要求与技术措施。

六、云安全运维

日常运维与事件应急两大类安全运维活动。资产管理、安全配置、恒能管理、日志管理、业务连续性/灾难恢复管理、变更管理、电子取证等方面的运维操作。

七、云安全服务

八、云安全治理

CISP 系列认证培训课程大纲
——BDSA（大数据安全分析师）

一、大数据安全分析预备知识

大数据、大数据分析、大数据安全分析、机器学习、深度学习、有监督学习、无监督学习等基本概念和组成。

二、大数据安全分析概述

大数据安全分析思路、大数据分析的过程和大数据分析一般方法、大数据安全分析项目实施的主要步骤及主要内容、常用分析技术。

三、大数据安全分析理论

大数据安全分析中用到的各种算法原理，包括相似性分析、关联分析、预测分析、分类、聚类、机器学习、深度学习等。

四、大数据安全分析工程

数据采集、数据存储、数据搜索、实时计算、批量计算、计算任务管理及调度，和数据可视化。

五、大数据安全分析应用

大数据安全分析的应用场景、分析思路、安全建模和实例介绍等

六、大数据安全相关政策法规

CISP 系列认证培训课程大纲

——PTE（渗透测试工程师）

一、操作系统安全基础

Windows 安全账户、Windows 文件系统安全、Windows 日志分析、Linux 安全账户、Linux 文件系统安全、Linux 日志分析

二、数据库安全基础

关系型数据库 MSSQL 角色与权限、关系型数据库 MSSQL 存储过程安全、MYSQL、Oracle 权限与设置、MYSQL 内置函数风险、Oracle 角色与权限及安全风险，非关系型数据库 Redis 权限与设置、非关系型数据库 Redis 未授权访问风险

三、中间件安全基础

Apache 服务器的安全设置、服务器文件名解析漏洞、服务器日志审计方法；IIS 服务器的安全设置、服务器常见漏洞、服务器日志审计方法；Tomcat 服务器的安全设置、服务器的日志审计方法；Weblogic 的安全设置、Websphere 的漏洞利用与防范、Websphere 的日志审计方法；Jboss 的安全设置、Jboss 的漏洞利用与防范

四、web 安全基础

HTTP 协议、SQL 注入漏洞、XML 注入漏洞、代码注入漏洞；存储式 XSS 漏洞、反射式 XSS 漏洞、DOM 式 XSS 漏洞；请求伪造漏洞、文件处理漏洞、访问控制漏洞、会话管理漏洞

CISSP 国际注册“信息安全专家”培训课程大纲

一、安全和风险管理

安全基本原则、安全定义、控制措施类型、安全框架、反计算机犯罪法律的难题、数据泄露、基线、风险管理、威胁建模、风险评估与分析、供应链风险管理、风险管理框架、业务连续性和灾难恢复、人员安全、安全治理

二、资产安全

信息生命周期、数据分级、管理责任层级、资产留存策略、隐私保护、保护资产、数据泄露

三、安全架构与工程

系统架构、计算机架构、系统安全架构、安全模型、开放式系统和封闭式系统、密码运算类型、加密方法、对称和非对称密码系统的种类、公钥基础架构、对密码技术的攻击、设计场所与基础设施安全、场所安全设计过程

四、通信与网络安全

网络架构原则、开放系统互联参考模型、TCP/IP 模型、传输介质、无线网络、网络基础、网络协议和服务、网络组建、内联网和外联网、城域网、广域网、通信信道、远程连接、网络加密、网络攻击

五、身份与访问管理

身份表示、身份验证、授权与可问责性、访问控制方法和技术、控制物理与逻辑访问、访问控制实践、访问控制面临的威胁

六、安全评估与测试

评估、测试、和审计策略、审计技术控制措施、审计管理控制措施报告、管理评审和批准

七、运营安全

八、软件开发安全

中国通信企业协会秘书处　　2022 年 6 月 21 日印发