

信息安全保障人员认证

关于举办《CISAW 应急处理与服务专业级》 认证培训班的通知

各相关单位：

为加强新型肺炎疫情防控，同时尽可能降低疫情对国家信息安全保障人才队伍建设的影响，信息安全保障人员认证（CISAW）“应急管理和服务”专业级培训拟通过线上网络直播结合线下面授的方式开展。现将培训与考试的具体模式通知如下：

一、 培训培训与考试模式

| 阶段 | 培训模式 | 课程内容 | 课时 |
|------|-------------|-------------------|---------------|
| 第一阶段 | 在线直播与 互动 | 理论讲解 + 云端环境 实操 | 18 课时/3 天 |
| 第二阶段 | 现场面授 | 沙盘演练 + 实操 | 9 课时/1.5 天 |
| 考试阶段 | 现场 | 笔试 + 实操考试 | 3 小时 |

*注：1）在线直播与互动通过“钉钉”视频会议的形式在线开展；

2）第一阶段：7月14-16日（3天）；

3）第二阶段：现场面授和考试时间待通知。

二、 课程介绍

CISAW 应急管理和服务认证课程根据《信息安全保障人员认证考试大纲》的要求，融合当前国内外的网络安全态势、业内专家的应急

响应实战经验，并借助包含网络安全最新攻防技术的“红黑演义应急响应演练云平台”，理论结合实践向学员授课。课程内容既包括应急管理体系规划与管理实践及案例分享的理论课程，又包括让每位学员在云端实验环境中运用红方、黑方攻防对抗技术，从正反两方面开展实战演练的实操课程。让学员充分了解和掌握应急管理知识体系和实战技术，切实提升学员网络安全应急管理和技术能力，成为国家信息安全保障人才队伍中的一员。具体课程内容可参照“附件1”。

三、 培训对象

CISAW 应急管理与服务培训适合政府部门、企事业单位的信息技术领域从业人员，特别是与网络安全、信息安全密切相关的中高级管理人员、技术人员、专业运维人员和其他相关人员。具体可参照中心网站：

<http://www.isccc.gov.cn/zxyw/shy/jcypx/xxaqbzryrz/rzfx/2019/05/897040.shtml>

四、 培训费用

(1) 培训费 6800 元/人，包含培训、培训教材、资料费、现场培训时午餐,现场培训时需要住宿的学员请提前通知班务组联系人，食宿协助安排，费用自理。

培训费交费方式： 7 月 13 日前将培训费 6800 元/人汇至以下账户：

| | |
|------|---------------------|
| 开户单位 | 广东省网络空间安全协会 |
| 开户银行 | 中国工商银行广州黄华路支行 |
| 开户账号 | 3602072509200098077 |

注：请提前通知培训机构联系人开具培训发票，并提供相关开票信息。

(2) 考试认证费网上注册后在线缴纳，并在线申请发票（网址 <http://ryrzcisaw.isccc.gov.cn>），具体缴纳时间、金额请留意认证中心通知。

五、 联系方式

联系人：成珍苑 15360402627、陈菊珍 15989296453、陈美云
18665680422、蔡瑞兰 13432358157，电话：020-83609433。

附件 1：CISAW 应急管理和服务专业级培训课程表



广东省网络空间安全协会



广州华南信息安全测评中心

2021 年 6 月 21 日

CISAW 应急管理和服务专业级培训课程表

| 日程 | 课程大纲 | 课程内容 | 课时 | 上课方式 |
|----------------------------|------------------------------|--|----|---------|
| 第一阶段 第一天 9:00-12:00 | 应急管理体系建立 | 1、建立应急管理体系的概念与目的 2、应急管理安全事件的分类 3、应急事件处理案例过程分析 4、业务战略分析与业务流程梳理 5、安全关键路径分析与风险点识别 6、威胁建模与监控指标体系建立 7、基于业务安全的应急管理如何落地 | 3 | 网络现场直播课 |
| 第一阶段 第一天 13:30-16:30 | 电子商务系统黑客破坏场景重现与企业应急响应过程重现 I | 1、SQL 注入入侵分析与应急服务重现 2、跨站入侵分析与应急服务重现 3、应急服务过程总结与回顾 | 3 | 网络现场直播课 |
| 第一阶段 第二天 9:00-12:00 | 电子商务系统黑客破坏场景重现与企业应急响应过程重现 II | 4、CSRF 高级脚本入侵分析与应急服务重现 5、高级钓鱼入侵分析与应急服务重现 6、应急服务过程总结与回顾 | 3 | 网络现场直播课 |
| 第一阶段 第二天 13:30-16:30 | 应急响应安全日志机制建立 | 1、建立日志机制的必要性有哪些 2、日常工作中如何建立安全日志机制 3、日志服务器的搭建与实操演练 4、日志异常分析实战练习 | 3 | 网络现场直播课 |
| 第一阶段 第三天 9:00-12:00 | 应急服务中的渗透测试实践 I | 1、操作系统口令安全与暴力破解实操 2、缓冲区溢出与漏洞利用实操 3、服务器渗透与检测实操 4、操作系统渗透提权实操 5、渗透实操中理解如何开展应急服务 | 3 | 网络现场直播课 |
| 第一阶段 第三天 13:30-16:30 | 应急服务中的渗透测试实践 II | 6、木马查找与病毒分析实操 7、文件上传漏洞与防御实操 8、日志分析实操 9、数据流分析 10、渗透实操中理解如何开展应急服务 | 3 | 网络现场直播课 |
| 第二阶段 第一天 9:00-12:00 | 应急响应实战案例分析与沙盘演练 | 1、大中型企业惨痛案例分析 2、惨痛案例实战演练与防范措施 3、应急响应方法论与必备工具 | 2 | 面授 |
| | 应急响应与安全事件处置 | 1、应急响应的基本内容有哪些 2、突发安全事件的应对措施有哪些 3、安全事件处置案例分析与沙盘演练 | 1 | 面授 |
| | 应急预案制定 | 1、什么是应急预案 2、制定应急预案的目的 | 2 | 面授 |

| | | | | |
|-------------------------------------|----------------------------|---|---|----|
| 第二阶段 第一天 13:30-16:30 | | 3、《网络安全法》与等级保护合规要求中的应急预案理解 4、如何制定应急预案 5、如何开展应急演练 6、应急服务安全技术基础与应用实践 7、应急服务团队技术储备和知识库建立 8、公司如何开展应急服务增值业务 | | |
| | 应急预案实施 | 1、如何根据应急预案进行实施 2、应急预案实施过程中应注意哪些问题 3、应急实施结束后的归纳与总结 4、应急案例场景分组沙盘演练 | 1 | 面授 |
| 第二阶段 第二天 9:00-12:00 | 知识升华与总结 答疑 学员经验分享与讨论 | 1、应急知识深度应用实践 2、应急实操案例总结升华 3、学员应急工作经验分享 4、应急实操强化练习 5、技术知识答疑解惑 | 3 | 面授 |