**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——软件安全开发方向**

**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。