信息系统安全注册课程

课程目标：

随着互联网的快速发展和信息化程度的不断提高，互联网深刻影响着政治、经济、文化等各个方面，保障信息安全的重要性日益凸显，加强对互联网上各类信息的管理应引起高度重视。在系统安全方面，以提高防御、应急处置能力为主的传统安全管理已经不能适应新计算、新网络、新应用和新数据为新特征的信息安全产业发展的需要。

网络信息安全是一个关系国家安全和主权、社会稳定、民族文化继承和发扬的重要问题。其重要性，正随着全球信息化步伐的加快越来越重要。网络信息安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。它主要是指网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。

适用学员：

企业信息安全主管，参与信息系统审计和管理体系规划的人员，提供信息安全咨询服务的专业人员，其他对信息安全全面的知识体系感兴趣的人员。具体培训对象包括：

- 企业信息安全主管
- 信息安全业内人士
- IT 或安全顾问人员
- IT 审计人员
- 安全设备厂商或服务提供商
- 信息安全类讲师或培训人员
- 信息安全事件调查人员
- 其他从事与信息安全相关工作的人员（如系统管理员、程序员、保安人员等）

课程设计：

授课课时:	5 天
授课条件：	学员必须具有基本的计算机操作知识
内容摘要：	**第一章 信息安全管理实务** • 什么是信息？什么是信息安全？信息安全管理和计划 • 信息安全 CIA 目标，重要的概念

- 风险管理概念和关系模型，定量和定性风险评估，风险消减和处理
- 安全策略、标准、指南和程序
- 安全管理角色和责任
- 数据分类
- 雇用策略和实务
- 安全意识（认知）、培训和教育

第二章 电信与网络安全

- 开放系统互连参考模型
- 网络通信基础
- 物理连接技术与特性，重要的电缆类型
- 局域网技术：传输方式，介质访问控制方式，拓扑，设备
- 广域网技术：链路类型，广域网交换，协议，设备
- 网络通信协议：TCP/IP，隧道技术
- 远程访问安全与管理
- 网络传输数据的安全保护：防火墙、IDS 等
- 容错和数据恢复
- 网络攻击手段与对策

第三章 操作安全

- Due diligence
- 控制措施的类型：预防性，检测性和纠正性
- 管理手段：责任分离，工作轮换，最小特权等
- 常见的 IT 任务：计算机操作，生产调度，磁带库，系统安全等
- 日常审计和监督

- 防病毒管理
- 变更管理，备份和介质处理
- 事件处理
- 常见的攻击手段，道德黑客

第四章 访问控制系统与方法

- 什么是访问控制？访问控制的功能和分类
- 身份识别与认证技术：口令、一次性口令、生物识别、SSO 等
- 访问控制技术，MAC、DAC、基于角色 AC 等
- 访问控制模型：状态机模型，BLP 模型，Biba 模型等
- 访问控制实施方法：集中式与分散式
- 访问控制管理：账号管理，权限管理，跟踪审计
- 攻击手段：口令攻击，拒绝服务，欺骗攻击
- 入侵检测，HIDS 和 NIDS
- 渗透测试

第五章 应用和系统开发

- 应用系统存在的一些问题
- 数据库和数据仓库的安全性，软件面临的攻击
- 数据/信息存储时的安全考虑
- 基于知识的系统：专家系统和神经网络
- 系统开发控制：在系统开发生命周期内考虑到安全措施
- 关于恶意代码的讨论
- 各种针对应用的攻击手段

第六章 密码学

- 密码学的定义、作用和应用
- 密码学的发展历史
- 密码学的方法：流密码、对称算法、非对称算法等
- 消息完整性，散列函数，数字签名
- 公钥基础设施 PKI，CA 证书
- 密钥管理：生成、交换、撤销、恢复
- Email 安全
- 各种应用于 Internet 的安全标准和协议
- 密码分析学和攻击手段
- 政府介入，密钥托管

第七章 BCP 和 DRP

- BCP 和 DRP 的概念
- 计划制定过程
- 业务影响分析（BIA）
- 选择应急计划策略
- 备份方案的选择
- 应急计划人员的选择和责任
- 应急计划的内容
- 应急计划测试
- 应急计划培训

第八章 法律、调查和道德

- 基本法律类型
- 关于计算机犯罪的讨论
- 计算机安全事件
- 调查取证，可信性和权威性，最佳证据规则，证据链
- 计算机辨析学

- 计算机道德

第九章 安全模型和体系结构

- 安全保护机制：分层、抽象和数据隐藏
- 计算机系统结构，硬件和软件
- 安全控制的概念，TCB，RM，安全内核，最小特权，责任分离……
- 安全模型：访问控制模型，信息流模型，
- 完整性模型等
- 系统评估标准：TCSEC、ITSEC、CC
- IPSec

第十章 物理安全

- 基本的控制措施：管理性，技术性和物理性
- 物理安全弱点和风险
- 安全设施的选择、构建和维护
- 磁带和介质库保护策略
- 文档（硬拷贝）库
- 垃圾处理
- 物理入侵检测

授课语言：	中文