ISO27001 标准实施与内部审核员培训课程大纲

【课程天数】2 天

【培训对象】信息安全管理系统推动人员、 进行内部审核的人员、资深经理、IT 经理、系统经理、IT 安全经理、其他想把信息安全管理体系引入组织的人员、敏感岗位员工等

【课程简介】

基于国际标准 ISO/IEC 27001:2005 和 ISO/IEC 27002:2005 的信息安全管理体系（ISMS-Information Security Management System）是管理体系思想和方法在信息安全保障方面的具体应用。建立和实施信息安全管理体系，是目前许多组织解决信息安全问题的有效方法和手段。

信息安全管理体系标准实施与内审员培训课程的目的是使学员了解信息安全管理体系基础知识，熟悉信息安全管理体系标准实施，内审的基本内容，掌握内审的流程和方法，培训合格者可获得本中心颁发的合格证书。

【课程目标】

理解 ISO/IEC 17799 对组织的意义和信息安全的重要性

了解信息安全基本常识、基本观念等

理解标准的目的

理解信息安全控制目标和控制措施

强调信息安全重要控制措施的重要性

【课程主要内容】

1.信息安全概述----信息及信息安全基本观念和重要性，信息安全保护的基本常识、信息安全保护的基本责任和义务、CIA 目标，信息安全需求来源，信息安全管理

2.风险评估与管理----风险管理要素，过程，定量与定性风险评估方法，风险消减等

3.ISO27001 标准简介----ISO27001 标准发展历史、现状和主要内容，信息安全标准族、ISO27001 标准认证

4.信息安全管理实施细则（实现信息安全的方法）----从十个方面介绍 ISO17799 的各项控制目标和控制措施--信息安全需要保护或控制措施的相关内容(结合企业实际案例)

5.信息安全管理体系标准--------ISO/IEC 27001：2005 正文部分内容解读，PDCA 管理模型，ISMS 建设方法和过程--信息安全管理的相关规定(结合企业实际案例)

ISO/IEC 27001：2005 正文解读

A5 安全策略（Security Policy）

A6 组织信息安全(Organizing Information Security)

A7 资产管理(Asset Management)

A8 人力资源安全（human resources security ）

A9 物理与环境安全（Physical and environ- ment security）

A10 通信与运行安全（Communication and Operation security

A12 信息系统获取、开发与维护（Information system acquisition, Development and maintenance)

A11 访问控制 （Access Control)

A13 信息安全事件管理（Information Security Incident Management)

A14 业务连续性管理(Business Continuity Management)

A15 符合性(Compliance)

6.**信息安全异常发生时的报告流程**(结合企业案例)、 **违反信息安全管理规定的相关处罚**(结合企业实际案例) 、相关案例

6.内部审核的策划、准备和实施

7.信息安全管理体系认证----认证和认可，认证的好处，认证的过程，认证准备

【颁布证书】考试合格者，将获得“ISO27000 信息安全管理体系内部审核员培训合格证书”。