ISO/IEC 27001:2013 信息安全管理体系+内审员培训

课程背景：

ISO/IEC 27001:2013 信息安全管理在使参与者掌握在评估和报告信息安全管理系统（ISMS ）的一致性和有效实施中所需要 的知识和技能，以保护企业免受风险。

课程目标

1、熟悉 ISO/IEC 27001:2013 的要求

2、掌握信息安全管理体系建立方法

3、掌握信息安全风险评估方法

4、理解 ISO/IEC 27001:2013 审核及注册过程，了解如何准备、执行和完成审核

5、掌握内审员应必备的知识和技巧 – 会编检查表，会审，会记，会开不符合报告

课程时长：

两天（6H/天，共 12 小时）

培训学员：

从事 IT 相关工作人员如信息安全工程师，从事企业管理的中高级管理人员、内审员和其他相关人员。

课程内容：

第一部分：信息安全管理基础知识

1 信息安全案例分析

2 信息安全是什么

3 信息安全管理体系是什么

第二部分：ISO/IEC 27001 标准

1、ISO/IEC 27001 简介

2、ISO/IEC 27001 内容简介

3、标准正文讲解（4 – 10 章）

4、附录 A 控制项讲解

第三部分：实施

1、信息安全风险评估

2、 SoA 编制

3、信息安全绩效

第四部分：审核

第一章：审核概念及原则

1、有关审核的定义

2、审核原则

练习：事实还是推理

第二章：审核的分类

1、按审核对象分

2、按审核方分

3、按审核范围分

第三章：体系审核的一般步骤

1、第一方审核

2、第二方审核

3、第三方审核

第四章：审核策划

1、审核方案管理

2、审核实施计划

（1）审核计划编制窍门

（2）建立审核小组

3、编制检查表-检查表编制窍门

4、资料准备

5、审核通知

练习：检查表编制

第五章：审核实施

1、首次会议

2、现场审核

2.1 审核证据收集

2.2 审核小窍门-审核十字要诀+PDCA

练习 4：审核十字要诀+PDCA

2.3 审核技巧

（1）聆听、验证、观察、时间管理

（2）典型情况应对技巧

（3）抽样技巧

（4）现场审核控制

2.4 审核记录

2.5 成功审核的要点

3、不合格项报告

4、审核组会议-记录与报告区别

5 末次会议

（1）案例分析：审核记录、不符合项报告、纠正措施和跟踪验证

（2）案例分析：审核记录、不符合项报告、纠正措施和跟踪验证

第六章：审核报告

1、报告内容

2、审核过程描述

3、内部审核结论

第七章：跟踪审核

1、跟踪审核内容

2、验证证据

3、验证问题处理

第八章：内审员

1、审核组长审核员任务

2、审核员资格