信息安全意识管理

课程背景：

ISO 27001 标准的更新已在 2013 年正式发布。2016 年 11 月 7 日中国发布了《中华人民共和国网络安全法》。随后 2018 年 5 月 25 日欧洲联盟出台《通用数据保护条例》GDPR。 2019 年 7 月 8 日，英国信息监管局发表声明说，英国航空公司因为违反《一般数据保护条例》被罚 1.8339 亿英镑（约合 15.8 亿元人民币）。

随着信息化和数字化的不断深入，各国家和企业纷纷重视信息安全保障工作，从战略、组织结构、科技等各个方面加强信息安全保障工作力度。本课程从当前隐私保护，数据泄露，网络入侵等案例入手，引入信息安全管理的重要性，分析安全管理与安全技术的关系。剖析组织中信息安全管理的核心要点和关键环节，分享在由各行业实际安全管理工作中总结出来的信息安全的重要原则，使管理人员对信息安全的理念、规律有清晰的认识，便于在组织信息安全管理过程中把握核心要点，有效地推动整个组织的信息安全管理工作。

课程收益：

- 领悟信息安全管理的重要性
- 了解行业相关信息安全法规
- 掌握信息安全管理的规律和特点
- 理解信息安全管理的作用和责任
- 掌握信息安全建设的重点和难点

课程时间：2 天，6 小时/天
课程对象：企业信息安全、信息部、IT 开发、运维人员、信息安全审计人员
课程方式：理论讲授+案例分析+现场演练

课程大纲

第一讲：信息安全管理的认知

一、信息和信息资产分类

信息：是一种资产，就像企业其它资产一样重要，对企业具有重要的价值，因此需要受到适当的保护

1. 数据资产（纸本文件、电子文件）
2. 软件资产（业务系统、OA 软件、操作系统、数据库软件、办公软件、压缩工具等）
3. 实物资产（服务器、笔记本电脑、打印机、手机、光盘等）
4. 人员资产（正式员工、临时员工、外聘员工等）
5. 服务资产（保洁服务、安保服务、桌面帮助服务、通信服务等）
6. 环境（物理环境、业务环境、组织环境）

二、信息安全三大属性 CIA

1. 机密性（Confidentiality）：信息不可被未经授权之个人、实体、流程所取得或揭露的特性
2. 完整性（Integrity）：确保信息不被非授权修改的特性
3. 可用性（Availability）：基于需要可由授权者存取及使用的特性。

三、信息安全管理模型

1. 信息安全管理定义
2. 信息安全目标和方针
3. 信息安全问题发生原因及其解决之道

案例：数据泄露-思科诉华为知识产权侵权案以和解告终
案例：可用性-某离港系统主机发生故障
案例：电商行业安全案例分析

第二讲：信息安全与业务发展的关系

1. 业务安全基础
2. 业务安全问题和威胁
3. 业务安全风险评估
4. 业务安全解决之道

案例：分组讨论业界有关业务安全问题

第三讲：国内外互联网行业信息安全法规与标准

1. ISO27001 信息安全管理体系（ISMS）

1）策划：建立 ISMS 范围&风险评估
2）实施：设计&实施 ISMS
3）检查：监控&评审 ISMS
4）改进：改进 ISMS

2. 网络安全法解析
3. 网络安全等级保护制度介绍
4. GDPR 欧盟个人隐私保护法案

案例：某证券公司信息安全管理体系建设实施计划

第四讲：信息安全组织工作范围及其职责分工

1. 信息安全组织规划和建设

2. 信息安全职责分工

1）信息安全委员会
2）信息安全负责人
3）业务负责人
4）用户
5）审计师

小组模拟：究竟谁管谁？

3. 信息安全组织工作内容

案例：业界著名公司信息安全组织结构和职责介绍

第五讲：信息安全风险评估

一、风险评估的认知

1. 风险风险评估分析

1）风险分析
2）风险评价
3）剩余风险

2. 风险来源
3. 风险管理原则
4. 风险评估要素

二、风险评估过程

1. ISO31000 风险处理过程

2. 信息安全风险评估过程

1）环境构建
2）风险识别
3）风险分析
4）风险评价
5)风险处置
练习：识别资产，威胁，弱点，可能性，影响，现有控制措施
3. 选择和实施安全控制
案例：分组讨论信息安全的风险评估