信息安全管理体系（ISMS）及 ISO27000 认证咨询基本知识

一、什么是信息安全管理体系（ISMS）？

信息安全管理体系是在组织内部建立信息安全管理目标，以及完成这些目标所用方法的体系。

ISO/IEC 27001 是建立、实施和维持信息安全管理体系的标准，通过确定信息安全管理体系范围、制定信息安全方针、明确管理职责、以风险评估为基础，选择控制目标与控制方式等活动建立信息安全管理体系。

二、信息安全的必要性和好处

1、识别信息安全风险，增强安全防范意识；

2、明确安全管理职责，强化风险控制责任；

3、明确安全管理要求，规范从业人员行为；

4、保护关键信息资产，保持业务稳定运营；

5、防止外来病毒侵袭，减小最低损失程度；

6、树立公司对外形象，增加客户合作信心；

7、可以得到省信息产业厅、地方信息产业局、行业主管部门、中小企业局等政府机构的补贴，补贴额度不少于企业建立ISO27001体系的投入费用（包含咨询认证过程）。

(信息安全管理体系标准 2005 年改版后的 ISO/IEC 27001 共有 133 个控制点，39 个控制措施，11 个控制域。其中 11 个控制域包括：1)安全策略 2)信息安全的组织 3)资产管理 4)人力资源安全 5)物理和环境安全 6)通信和操作管理 7)

访问控制 8)系统采集、开发和维护 9)信息安全事故管理 10)业务连续性管理 11)符合性)

三、建立信息安全体系的主要程序

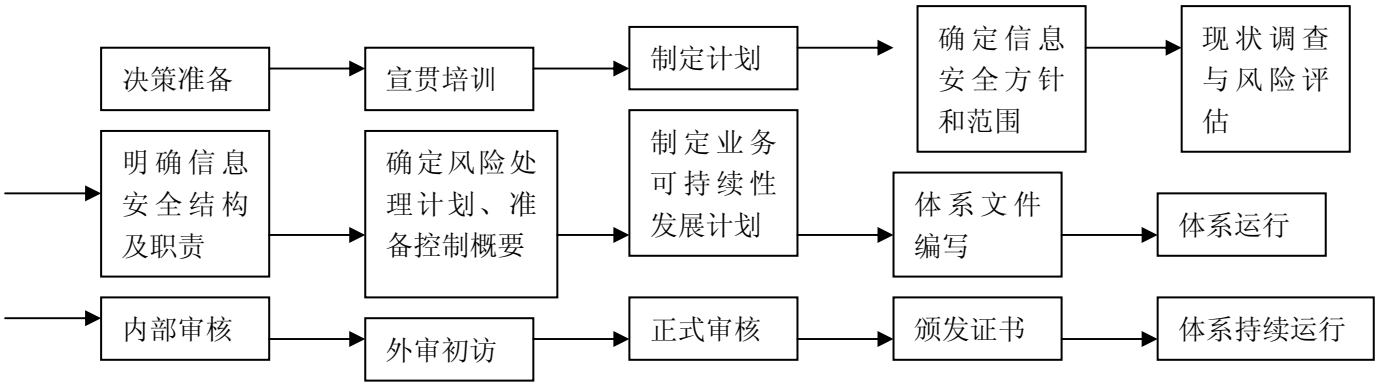
建立信息安全管理体系一般要经过下列四个基本步骤(5-7个月):

① 信息安全管理体系的策划与准备;

② 信息安全管理体系文件的编制;

③ 信息安全管理体系运行;

④ 信息安全管理体系审核、评审和持续改进。



ISMS体系建立步骤图