

ISO资深验厂老师告诉你：ISO/IEC27001:2005信息安全管理标准，需要注意哪些方面？

产品名称	ISO资深验厂老师告诉你：ISO/IEC27001:2005信息安全管理标准，需要注意哪些方面？
公司名称	深圳市实测通技术服务有限公司
价格	.00/件
规格参数	测试周期:5-7天 寄样地址:深圳宝安 价格费用:电话详谈
公司地址	深圳市罗湖区翠竹街道翠宁社区太宁路145号二单元705
联系电话	17324413130 17324413130

产品详情

在日趋网络化的世界里，「信息」对建立竞争优势起着举足轻重的作用。但它同时也是柄双刃剑，当信息被意外或刻意的传给恶意的接收者时，同样的信息也可能导致一所机构倒闭。在当今的信息时代，科技无疑为我们解决了不少问题。国际标准组织(ISO)应此类需求，制定了 ISO 27001:2005标准，为如何建立、推行、维持及改善信息安全管理系统提供帮助。信息安全管理系统(ISMS)是高层管理人员用以监察及控制信息安全、减少商业风险和确保保安系统持续符合企业、客户及法律要求的一个体系。ISO/IEC 27001:2005 能协助机构保护专利信息，同时也为制定统一的机构保安标准搭建了一个平台，更有助于提升安全管理的实务表现和增强机构间商业往来的信心与信任。什么机构可采用 ISO/IEC 27001:2005 标准？任何使用内部或外部电脑系统、拥有机密资料及/或依靠信息系统进行商业活动的机构，均可采用 ISO/IEC 27001:2005标准。简单的说，也就是那些需要处理信息、并认识到信息保护重要性的机构。ISO/IEC 27001 的控制目标及措施ISO/IEC 27001制定的宗旨是确保机构信息的机密性、完整性及可用性，为达成上述宗旨，该标准共提出了39个控制目标及134项控制措施，推行ISO/IEC 27001标准的机构可在其中选择适用于其业务的控制措施，同时也可增加其他的控制措施。而与ISO/IEC 27001相辅的 ISO 17799:2005 标准是信息安全管理的实务守则，为如何推行控制措施提供指引。ISO/IEC 27001:2005 的架构ISO/IEC 27001:2005 标准在 2005 年 10 月公布，同时取缔了多国采纳的英国标准 BS 7799-2:2002，但新旧标准的要求并无太大分别。ISO/IEC 27001:2005 标准以 Edward Deming 博士提出的“计划-实施-核查-采取行动”循环周期作为制定蓝图，以实现持续改善的目标。

I. 计划 计划最重要的部分是设定涵盖的范畴及区域，它可以是：覆盖整个组织并涉及多个地点的办事处及/或厂房 只涉及一个办事处或厂房 只涉及一个多元化服务供应商的其中一个业务计划的主要工作包括信息安全管理系统、风险评估、风险管理、风险处理措施和适用性报告。信息安全管理系统是运营风险整体管理系统的其中一部分，目的是建立、实施、推行、检讨、维持及改善信息安全。机构在信息的机密性、完整性和可用性三方面的目标各是什么呢？什么程度的风险是可接受的？是否存在任何限制，如法律、法规或机构内部程序？信息安全政策应该是一份由行政总监签署认可的文件。控制措施应采取由上至下的推行方式。风险评估 根据需保护的信息和可接受的风险程度来识别真正的风险，

并就这些风险出现的可能性与其影响的严重性作出评估，从而辨别出机构需要管理的风险，即下图红色部分内的风险。风险管理 / 风险处理 完成风险评估后，便要决定如何处理这些风险。适用性报告 (Statement of Applicability) 识别出所有的保安措施，指出哪些对机构而言是适用或不适用的，并说明原因。必须针对风险评估的结果来选择控制措施。II. 实施选定了控制措施后，便需落实推行，同时也需制定程序以确保能够迅速察觉到事故的发生并作出回应，并确保所有员工都了解信息安全的重要性，且确保其接受了适当的培训，及有能力执行他们负责的保安任务。此外，还要妥善管理所需的资源。I II. 核查核查的目的是确保控制措施都已推行，并能达到既定的目标。尽管有多种可行的核查方法，但只有内部审计与管理检讨是强制性的要求。IV. 采取行动最后便需对核查结果采取适当的行动，相关的行动可以是：* 修正* 预防* 改善总结ISO/IEC 27001:2005 标准为所有行业的机构都提供了一套业务工具，协助其避免信息保安的失误，从而降低了相应的风险。正式推行ISO/IEC 27001:2005 并取得有关认证的机构将受益匪浅，以下列举其中数项：由于按照国际标准实施适当的控制措施，机构便能自行将信息保安的失误率降至最低以系统化的方法处理符合法律的问题，从而减低所需承担的法律风险以系统化的方法计划及管理运营的持续性增加客户、合作伙伴和相关人士对机构的信心提升营运收入，并为机构带来更多商机。