

企业如何建立ISO27001信息安全管理体系？

产品名称	企业如何建立ISO27001信息安全管理体系？
公司名称	佰事通（北京）企业管理有限公司-销售部
价格	.00/个
规格参数	
公司地址	海淀区中关村
联系电话	18201461506

产品详情

ISO27001信息安全管理体系，采用PDCA循环模型，分为四个阶段：安全风险评估、规划体系建设方案（Plan），建立并实施信息安全管理体系（Do），体系运行绩效考核（Check），持续改进（Action）。

01

确立管理系统使用的范围

必须覆盖到公司的每一个职能部门，或者覆盖公司信息系统相连的外部机构，例如合作伙伴、供应商等。同时从系统层次考虑覆盖网络系统、服务器平台系统、数据、安全管理、应用系统以及支撑信息系统的场所和所处的周边环境以及场所内，确保计算机系统正常运营的设施设备。

02安全风险评估

企业技术类的评估和主要包括企业安全管理类的评估。

安全管理评估的内容包括与ISO27001信息安全管理体系相关的11个方面，包括信息安全政策、安全组织、资产分类与控制、人员安全、物理与环境安全、通信与运行管理、访问控制等，系统开发和维护、安全事件管理、业务连续性管理和合规性。

安全技术评估是基于资产安全等级的分类。通过对信息设备的安全扫描和安全设备的配置，对现有网络设备、服务器系统、终端和网络安全架构的安全状况和薄弱环节进行检查和分析，为安全加固提供依据。

03规划系统建设方案

规划系统建设方案在风险评估的基础上，针对企业存在的安全风险提出安全建议，提高系统的安全性和抗攻击能力。

04信息安全体系建设与运行

系统建设以信息安全模式和企业信息化为基础，兼顾内外部安全功能。规划信息安全技术可以从安全基础设施、网络、系统和应用四个方面进行规划。

05改进

ISO27001认证标准信息安全管理体系文件编制完成后，按文件控制的要求进行评审和批准，有效的体系文件下发到各部门，保持体系运行过程中的记录，定期进行内部审核和管理评审，对不符合或潜在不符合项采取纠正和预防措施，不断完善信息安全管理体系。