企业做ISO27001有什么用？

产品名称	企业做ISO27001有什么用？
公司名称	全球法规注册CRO-国瑞IVDEAR
价格	.00/个
规格参数	
公司地址	光明区邦凯科技园
联系电话	13929216670 13929216670

产品详情

ISO27001 信息安全管理体系认证

ISO27001 信息安全管理体系认证可有效保护信息资源,保护信息化进程健康、有序、可持续发展。

信息安全管理实用规则ISO/IEC27001的前身为英国的BS7799标准，该标准由英国标准协会（BSI）于1995年2月提出，并于1995年5月修订而成的。1999年BSI重新修改了该标准。BS7799分为两个部分：

BS7799-1，信息安全管理实施规则

BS7799-2，信息安全管理体系规范

第一部分对信息安全管理给出建议，供负责在其组织启动、实施或维护安全的人员使用。

第二部分说明了建立、实施和文件化信息安全管理体系（ISMS）的要求，规定了根据独立组织的需要应实施安全控制的要求。

适用于

信息安全对每个企业或组织来说都是需要的，所以信息安全管理体系认证具有普遍的适用性，不受地域、产业类别和公司规模限制。从目前的获得认证的企业情况看，较多的是涉及电信、保险、银行、数据处理中心、IC制造和软件外包等行业。

证书内容

认证机构名称、申请认证单位名称及产品审核通过的相关标准、证书的有效期限、证书编号、认证机构公章、认证机构负责人亲笔签字等。

定义

ISO/IEC17799-2000（BS7799-1）对信息安全管理给出建议，供负责在其组织启动、实施或维护安全的人员使用。该标准为开发组织的安全标准和有效的安全管理做法提供公共基础，并为组织之间的交往提供信任。

标准指出“ 象其他重要业务资产一样，信息也是一种资产 ”。它对一个组织具有价值，因此需要加以合适地保护。信息安全防止信息受到的各种威胁，以确保业务连续性，使业务受到损害的风险减至最小，使投资回报和业务机会最大。

信息安全是通过实现一组合适控制获得的。控制可以是策略、惯例、规程、组织结构和软件功能。需要建立这些控制，以确保满足该组织的特定安全目标。

内容

ISO/IEC17799-2000包含了127个安全控制措施来帮助组织识别在运做过程中对信息安全有影响的元素，组织可以根据适用的法律法规和章程加以选择和使用，或者增加其他附加控制。国际标准化组织（ISO）在2005年对ISO 17799进行了修订，修订后的标准作为ISO 27000标准族的第一部分——ISO/IEC 27001，新标准去掉9点控制措施，新增17点控制措施，并重组部分控制措施而新增一章，重组部分控制措施，关联性逻辑性更好，更适合应用；并修改了部分控制措施措辞。修改后的标准包括11个章节：

1）安全策略。指定信息安全方针，为信息安全提供管理指引和支持，并定期评审。

2）信息安全的组织。建立信息安全管理组织体系，在内部开展和控制信息安全的实施。

3）资产管理。核查所有信息资产，做好信息分类，确保信息资产受到适当程度的保护。

4）人力资源安全。确保所有员工，合同方和第三方了解信息安全威胁和相关事宜以及各自的责任，义务，以减少人为差错，盗窃，欺诈或误用设施的风险。

5）物理和环境安全。定义安全区域，防止对办公场所和信息的未授权访问，破坏和干扰；保护设备的安全，防止信息资产的丢失，损坏或被盗，以及对企业业务的干扰；同时，还要做好一般控制，防止信息和信息处理设施的损坏和被盗。

6）通信和操作管理。制定操作规程和职责，确保信息处理设施的正确和安全操作；建立系统规划和验收准则，将系统失效的风险降到最低；防范恶意代码和移动代码，保护软件和信息的完整性；做好信息备份和网络安全管理，确保信息在网络中的安全，确保其支持性基础设施得到保护；建立媒体处置和安全的规程，防止资产损坏和业务活动的中断；防止信息和软件在组织之间交换时丢失，修改或误用。

7）访问控制。制定访问控制策略，避免信息系统的非授权访问，并让用户了解其职责和义务，包括网络访问控制，操作系统访问控制，应用系统和信息访问控制，监视系统访问和使用，定期检测未授权的活动；当使用移动办公和远程控制时，也要确保信息安全。

8）系统采集、开发和维护。标示系统的安全要求，确保安全成为信息系统的内置部分，控制应用系统的安全，防止应用系统中用户数据的丢失，被修改或误用；通过加密手段保护信息的保密性，真实性和完整性；控制对系统文件的访问，确保系统文档，源程序代码的安全；严格控制开发和支持过程，维护应用系统软件和信息安全。

9）信息安全事故管理。报告信息安全事件和弱点，及时采取纠正措施，确保使用持续有效的方法管理信息安全事故，并确保及时修复。

10）业务连续性管理。目的是为减少业务活动的中断，是关键业务过程免收主要故障或天灾的影响，并确保及时恢复。

11）符合性。信息系统的设计，操作，使用过程和管理要符合法律法规的要求，符合组织安全方针和标准，还要控制系统审计，使信息审核过程的效力最大化，干扰最小化。

效益

ISO27001的效益

1、通过定义、评估和控制风险，确保经营的持续性和能力

2、减少由于合同违规行为以及直接触犯法律法规要求所造成的责任

3、通过遵守国际标准提高企业竞争能力，提升企业形象

4、明确定义所有组织的内部和外部的信息接口目标：谨防数据的误用和丢失

5、建立安全工具使用方针

6、谨防技术诀窍的丢失

7、在组织内部增强安全意识

8、可作为公共会计审计的证据