ISO27001信息安全管理体系认证

产品名称	ISO27001信息安全管理体系认证
公司名称	海宁铭伟企业管理咨询有限公司
价格	40000.00/1
规格参数	
公司地址	海宁高新技术开发区
联系电话	13758134998

产品详情

iso27001信息安全管理体系认证

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。

随着在世界范围内，信息化水平的不断发展，信息安全逐渐成为人们关注的焦点，世界范围内的各个机构、组织、个人都在探寻如何保障信息安全的问题。英国、美国、挪威、瑞典、芬兰、澳大利亚等国均制定了有关信息安全的本国标准，国际标准化组织(iso)也发布了iso17799、iso13335、iso15408等与信息安全相关的国际标准及技术报告。在信息安全管理方面，英国标准iso27000:2005已经成为世界上应用最广泛与典型的信息安全管理标准，它是在bsi/disc的bdd/2信息安全管理委员会指导下制定完成。

iso27001标准于1993年由英国贸易工业部立项，于1995年英国首次出版bs7799-1：1995《信息安全管理实施细则》，它提供了一套综合的、由信息安全最佳惯例组成的实施规则，其目的是作为确定工商业信息系统在大多数情况所需控制范围的唯一参考基准，并且适用于大、中、小组织。

1998年英国公布标准的第二部分《信息安全管理体系规范》，它规定信息安全管理体系要求与信息安全控制要求，它是一个组织的全面或部分信息安全管理体系评估的基础，它可以作为一个正式认证方案的根据。bs7799-1与bs7799-2经过修订于1999年重新予以发布，1999版考虑了信息处理技术，尤其是在网络和通信领域应用的近期发展，同时还非常强调了商务涉及的信息安全及信息安全的责任。

2000年12月，bs7799-1：1999《信息安全管理实施细则》通过了国际标准化组织iso的认可，正式成为国际标准-----iso/iec17799：2000《信息技术-信息安全管理实施细则》。2002年9月5日，bs7799-2:2002草案经过广泛的讨论之后，终于发布成为正式标准，同时bs7799-2:1999被废止。2004年9月5日，bs7799-2:2002正式发布。

2005年，bs7799-2:2002终于被iso组织所采纳，于同年10月推出iso/iec27001:2005.

2005年6月，iso/iec17799:2000经过改版，形成了新的iso/iec17799:2005，新版本较老版本无论是组织编排还是内容完整性上都有了很大增强和提升。iso/iec17799:2005已更新并在2007年7月1日正式发布为iso/iec27002:2005，这次更新只是在标准上的号码，内容并没有改变。

现在，iso27000:2005标准已得到了很多国家的认可，是国际上具有代表性的信息安全管理体系标准。目前除英国之外，还有荷兰、丹麦、澳大利亚、巴西等国已同意使用该标准；日本、瑞士、卢森堡等国也表示对iso27000:2005标准感兴趣，我国的台湾、香港也在推广该标准。许多国家的政府机构、银行、证券、保险公司、电信运营商、网络公司及许多跨国公司已采用了此标准对自己的信息安全进行系统的管理。截至2002年9月，全球共有142家各类组织通过了iso27000:2005信息安全管理体系认证。

发展

iso27001认证好处

信息安全管理体系标准（iso27001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。iso27001是信息安全领域的管理体系标准，类似于质量管理体系认证的iso9000标准。当您的组织通过了iso27001的认证,就相当于通过iso9000的质量认证一般，表示您的组织信息安全管理已建立了一套科学有效的管理体系作为保障。根据iso27001对您的信息安全管理体系进行认证，可以带来以下几个好处:)

引入信息安全管理体系就可以协调各个方面信息管理，从而使管理更为有效。保证信息安全不是仅有一个防火墙，或找一个24小时提供信息安全服务的公司就可以达到的。它需要全面的综合管理。

通过进行iso27001信息安全管理体系认证，可以增进组织间电子电子商务往来的信用度，能够建立起网站和贸易伙伴之间的互相信任，随着组织间的电子交流的增加通过信息安全管理的记录可以看到信息安全管理明显的利益，并为广大用户和服务提供商提供一个基础的设备管理。同时，把组织的干扰因素降到最小，创造更大收益。

通过认证能保证和证明组织所有的部门对信息安全的承诺。

通过认证可改善全体的业绩、消除不信任感。

获得国际认可的机构的认证证书，可得到国际上的承认，拓展您的业务。

建立信息安全管理体系能降低这种风险，通过第三方的认证能增强投资者及其他利益相关方的投资信心。

组织按照iso27001标准建立信息安全管理体系，会有一定的投入，但是若能通过认证机关的审核，获得认证，将会获得有价值的回报。企业通过认证将可以向其客户、竞争对手、供应商、员工和投资方展示其在同行内的领导地位;定期的监督审核将确保组织的信息系统不断地被监督和改善，并以此作为增强信息安全性的依据,信任、信用及信心,使客户及利益相关方感受到组织对信息安全的承诺。

通过认证能够向政府及行业主管部门证明组织对相关法律法规的符合性。

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。

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iso17799进行了修订，修订后的标准作为iso27000标准族的第一部分——iso/iec27001，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