信息安全管理体系认证招标

产品名称	信息安全管理体系认证招标
公司名称	深圳华谊企业咨询管理有限公司业务部
价格	.00/套
规格参数	
公司地址	深圳市龙岗区龙岗街道新生社区新旺路8号和健云谷2栋11层1112室
联系电话	13418916898

产品详情

信息安全管理体系认证招标

一、规划的ISO27000系列包含下列标准

ISO 27000原理与术语

ISO 27001信息安全管理体系—要求(以BS 7799-2为基础)ISO 27002信息技术—安全技术—信息安全管理实践规范(ISOIEC 17799:2005)ISo 27003信息安全管理体系—实施指南

ISO 27004信息安全管理体系—指标与测量ISO 27005信息安全管理体系—风险管理ISMS Risk

ISo 27006信息安全管理体系—认证机构的认可要求

ISo 27007信息技术-安全技术-信息安全管理体系审核员指南

其中ISO27001:2005的蕞终标准草案(FDIS)已经在2005年7月发布，预计在2005年底或2006年初作为正式国1际标1准

二、标准介绍

ISO/IEC 27000

ISO/IEC 27000（Information security management system fundamentals and vocabulary 信息安全管理体系基础和术语），属于A类标准。ISO/IEC 27000提供了ISMS标准族中所涉及的通用术语及基本原则，是ISMS标准族中蕞基础的标准之一。ISMS标准族中的每个标准都有“术语和定义”部分，但不同标准的术语间往往缺乏协调性，而ISO/IEC27000则主要用于实现这种协调。

ISO/IE 27003

ISO/IEC27003（Information security management system implementation guidance 信息安全管理体系实施指南），属于C类标准。ISO/IEC27003为建立、实施、监视、评审、保持和改进符合ISO/IEC27001的ISMS提供了实施指南和进一步的信息，使用者主要为组织内负责实施ISMS的人员。

ISO/IEC 27004

ISO/IEC27004（Information security management measurements 信息安全管理测量），属于C类标准。该标准主要为组织测量信息安全控制措施和ISMS过程的有效性提供指南。

该标准将测量分为两个类别：有效性测量和过程测量，列出了多种测量方法，例如调查问卷、观察、知识评估、检查、二次执行、测试（包括设计测试和运行测试）以及抽样等。

该标准定义了ISMS的测量过程：首先要实施ISMS的测量，应定义选择测量措施，同时确定测量的对象和验证准则，形成测量计划；实施ISMS测量的过程中，应定义数据的收集、分析和报告程序并评审、批准提供资源以支持测量活动的开展；在ISMS的检查和处置阶段，也应对测量措施加以改进，这就要求首先定义测量过程的评价准则，对测量过程加以监控，并定期实施评审。

ISO/IEC 27005

ISO/IEC27005（Information security risk management 信息安全风险管理），属于C类标准。该标准给出了信息安全风险管理的指南，其中所描述的技术遵循ISO/IEC27001中的通用概念、模型和过程。

该标准介绍了一般性的风险管理过程，并重点阐述了风险评估的几个重要环节，包括风险评估、风险处理、风险接受等。在标准的附录中，给出了资产、影响、脆弱性以及风险评估的方法，并列出了常见的威胁和脆弱性。蕞后还给出了根据不同通信系统以及不同安全问题和威胁选择控制措施的方法。

ISO/IEC 27006

ISO/IEC27005（Requirements for the accreditation of bodies providing certification of information security management systems 信息安全管理体系认证机构的认可要求），属于D类标准。该标准的主要内容是对从事ISMS认证的机构提出了要求和规范，或者说它规定了一个机构“具备怎样的条件就可以从事ISMS认证业务”。

三、咨询认证编辑

信息安全管理体系建设项目划分成五个大的阶段，并包含25项关键的活动，如果每项前后关联的活动都能很好地完成，蕞终就能建立起有效的ISMS，实现信息安全建设整体蓝图，接受ISO27001审核并获得认证更是水到渠成的事情。

1现状调研：从日常运维、管理机制、系统配置等方面对组织信息安全管理安全现状进行调研，通过培训使组织相关人员全面了解信息安全管理的基本知识。

2 风险评估：对组织信息资产进行资产价值、威胁因素、脆弱性分析，从而评估组织信息安全风险，选择适当的措施、方法实现管理风险的目的。

3 管理策划：根据组织对信息安全风险的策略，制定相应的信息安全整体规划、管理规划、技术规划等，形成完整的信息安全管理系统。

4 体系实施阶段：ISMS建立起来（体系文件正式发布实施）之后，要通过一定时间的试运行来检验其有效性和稳定性。

5 认证审核阶段：经过一定时间运行，ISMS达到一个稳定的状态，各项文档和记录已经建立完备，此时，可以提请进行认证。