iso27001认证咨询办理机构

产品名称	iso27001认证咨询办理机构
公司名称	深圳万检通检验中心
价格	.00/件
规格参数	
公司地址	深圳市宝安区固戍一路洪辉科创空间3F
联系电话	18576464303 18576464303

产品详情

ISO27000认证 (信息安全管理体系标准)概述

ISO/IEC 27000标准是化组织专门为信息安全管理体系建立的一系列相关标准的总称，已经预留了ISO/IEC 27000到ISO/IEC 27059共60个标准号，到目前为止，正式发布的信息安全管理体系(ISMS)标准有8个，其中两个已经转化成国家标准。全部标准从ISO/IEC 27000到ISO/IEC 27037，以及ISO 27799和其他，基本可以分为以下四部分。

部分是要求和支持性指南，包括ISO/IEC 27000到ISO/IEC 27005，是信息安全管理体系的基础和基本要求;第二部分是有关认证认可和审核的指南，包括ISO/IEC 27006到ISO/IEC 27008，面向认证机构和审核人员;第三部分是面向专门行业的信息安全管理要求，如金融业、电信业，或者专门应用于某个具体的安全域，如数字证据、业务连续性方面;第四部分是由ISO技术委员会TC215单独制定的(而非和IEC共同制定)应用于健康行业的标准ISO 27799，以及一些处于研究阶段并以新项目提案方式体现的成果，比如供应链安全、存储安全等。部分标准见附表。本文向大家介绍一下ISO/IEC27000族主要标准。

ISO/IEC 27000是信息安全管理的概述和术语，是基础的标准之一。它提供了ISMS标准族中所涉及的通用术语和基本原则，由于ISMS每个标准都有自己的术语和定义，以及使用环境和行业的差别，不同标准的术语间往往会有一些细微的差异，致使在使用过程中相对缺乏协调，而ISO/IEC 27000就是用于实现这种一致性。ISO/IEC 27000标准有三个章节，章是标准的范围说明;第二章对ISO 27000系列的各个标准进行介绍，说明了各个标准之间的关系;第三章给出了共63个与ISO 27000系列标准相关的术语和定义。

ISO/IEC 27001：2005是《信息技术 安全技术 信息安全管理体系 要求》，等同转化为中国国家标准GB/T 22080-2008/ISO/IEC 27001:2005，于2008年6月19发布，同年11月1日正式实施。同ISO 9001标准的性质一样，它是ISMS的规范性标准，也是ISO/IEC 27000系列核心的两个标准之一，适用于所有类型的组织。它着眼于组织的整体业务风险，通过对业务进行风险评估来建立、实施、运行、监视、评审、保持和改进其信息安全管理体系，确保其信息资产的保密性、可用性和完整性。它还规定了为适应不同组织或部门的需求而制定的安全控制措施的实施要求，也是独立第三方认证及实施审核的依据。

ISO/IEC 27002:2005是《信息技术 安全技术 信息安全管理实用规则》，等同转化为中国国家标准GB/T 22081-2008/ISO/IEC 27002:2005，也是ISO/IEC 27000系列核心的两个标准之一。它从11个方面提出39个控制目标和133个控制措施，这些控制目标和措施是信息安全管理的佳实践。从应用角度看，该标准具有专用和通用的二重性。作为ISO 27000标准族系列的成员之一，它是配合ISO/IEC 27001标准来使用的，体现其专用性;同时，它提出的信息安全控制目标和控制措施又是从信息安全工作实践中总结出来的，不管组织是否建立和实施ISMS，均可从中选择适合自己的思路、方法和手段来实现目标，这又体现其通用性。

ISO/IEC 27003是《信息安全管理体系实施指南》，该标准适用于所有类型、所有规模和所有业务形式的组织，为建立、实施、运行、监视、评审、保持和改进符合ISO/IEC 27001的信息安全管理体系提供实施指南。它给出了ISMS实施的关键成功因素，按照PDCA的模型，明确了计划、实施、检查、纠正每个阶段的活动内容和详细指南。

ISO/IEC 27004是《信息安全管理测量》，该标准阐述信息安全管理的测量和指标，用于测量信息安全管理的实施效果，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。它分为信息安全测量概述、管理责任、测量和测量改进、测量操作、数据分析和测量结果报告、信息安全管理项目的评估和改进共6个关键部分，该标准还详细描述了测量过程机制，分析了如何收集基准测量单位，以及如何利用分析技术和决策准则来生成信息安全的临界指标等。

ISO/IEC 27005是《信息安全风险管理》，该标准描述了信息安全风险管理的要求，可以用于风险评估，识别安全需求，支撑信息安全管理体系的建立和维持。作为信息安全风险管理的指南，该标准还介绍了一般性的风险管理过程，重点阐述风险评估的重要环节。在附录中它给出了资产、影响、脆弱性以及风险评估的方法，即列出了常见的威胁和脆弱性，后给出了根据不同通讯系统、不同安全威胁选择控制措施的方法。