什么是ISO27001认证，怎么办理？

产品名称	什么是ISO27001认证，怎么办理？
公司名称	深圳市天润标准技术服务有限公司
价格	.00/件
规格参数	服务1:包通过 服务2:包整改 服务3:一次性收费
公司地址	深圳市龙华区龙华街道富康社区东环一路100号良基大厦101C04
联系电话	13828872873 13828872873

产品详情

ISO27001信息安全管理体系认证市场现状

随着信息化水平的不断提高，信息本身的价值越来越高，信息安全风险始终存在，同时由于诸如敏感信息泄露、网络非法劫持、核心系统宕机等信息安全事件时有发生，国家出台了如《中华人民共和国网络安全法》、《互联网个人信息安全保护指南》、《加强工业互联网安全工作的指导意见》、《中华人民共和国密码法》、《电信和互联网行业提升网络数据安全保护能力专项行动方案》等意见法规文件，对企业实施信息安全管理提出了更高的要求。实施信息安全管理体系（ISO27001）并通过第三方认证，重要性日渐凸显。

附信息安全管理体系认证数据（截止2022.10）:

本文之后将围绕体系标准介绍、标准实施收益、如何通过信息安全管理体系认证三个方面，给大家做简要介绍。

1

信息安全管理体系标准介绍

信息安全管理体系（Information Security Management System，简称ISMS）的概念*初来源于英国标准学会制定的BS7799-1：1995《信息安全管理实施细则》。2002年，英国标准学会发布了BS7799-2：2002《信息安全管理体系规范》，2005年10月，该规范通过了****化组织ISO的认可，正式成为****，被广泛接受。这套标准是建立信息安全管理体系的一套需求规范，其中详细说明了建立、实施和维护信息安全管理体系的要求，指出实施机构应该遵循的风险评估标准。

目前现行的ISO27001：2013标准于2013年10月19日由****化组织（ISO）正式颁布实施。

2

通过信息安全管理体系认证的收益

组织实施信息安全管理体系，通过ISO27001标准认证，表示企业已经建立了一套科学有效的体系作为保障，为企业带来全面的价值提升，包括但不限于以下五个方面:

1.提升企业品牌形象

企业实施信息安全管理体系并通过第三方认证机构相关认证，能向公众和外部客户展示自身的管理水平，能向外部证明自身管理能力符合相关信息安全标准及相关法律法规的要求，体现企业较于同业企业的竞争优势。

2.获取政府财务支持

为相应国家相关行业政策，推进区域企业高质量发展，鼓励企业提升自身信息安全管理能力，各地主管部门对本地区通过第三方认证的企业有不同的财务补贴政策。详情咨询销售人员

3.其他资质前置条件

目前有许多IT行业内通用的证书如业务连续性管理体系（ISO22301）、 云服务信息安全管理体系、（ISO27017）云隐私保护体系、（ISO27018）隐私信息安全管理体系（ISO27701）、个人身份信息保护管理体系（ISO21951）、国际云安全认证（C-STAR）等，在申报这些认证证书时，申报企业需要提前建立ISO27001管理体系并通过第三方认证。

4.提高企业信息安全管理能力

通过实施ISO27001，按照PDCA模型建立信息安全管理自我约束机制，有助于企业识别信息安全风险并加改进规避，减少可能存在的安全隐患，降低潜在安全事件发生给企业带来的损失，规范企业各个部门各个岗位的职责，提升员工信息安全意识，不断改善，有效预防，*终实现组织的良性发展。

5.满足市场准入需求

各类体系认证证书是IT行业招投标的敲门砖，不同证书在不同的投标标的会有不同的分数占比。部分项目标的甚至明确要求ISO27001认证证书作为准入门槛。

如何通过ISO27001体系认证

01｜获证流程

我们以ISO/IEC27001标准为指导，结合信息安全体系认证优秀实践，充分考虑国内企业的信息安全管理现状，总结归纳出适宜电子信息行业快速通过ISO27001认证的六大流程：

01

差距分析

从人员、环境、技术、管理四个方面对企业进行评估调研，发掘组织信息安全需求，分析与标准之间差距，明确体系实施的目标、范围和要点。

02

培训导入

开展信息安全基础知识培训、项目专题培训、体系建立指导等，导入信息安全管理思想，明确各岗位信息安全管理职责。

03

体系建立

结合组织信息安全目标和方针，指导、协助编写ISO27001程序文件、管理手册，制定合乎规范的管理规程和控制措施。

04

推广实施

在企业内部推进体系运行，识别信息安全风险资产，在适宜时间开展有效的内部评审和管理评审，保留体系有效运行证据。

05

现场审核

向第三方认证机构申请信息安全管理体系认证，协助企业完成现场审核，整改或纠正审核过程中产生的不符合项。

06

改进维持

规划体系年度审核计划及方案，按照PDCA原则，结合企业实际需求，继续完善和改进信息安全管理体系。

咨询认证流程规划图如下：

02｜审核前需准备的材料

在进行管理体系审核之前，需要准备和提交完备的体系材料。通常我们将这些材料分为管理手册、程序文件、制度策略、运行记录等四级文件。

03｜审核员一般会关注的点

在进行文件审核时，外部审核员主要关注信息安全管理体系文件是否符合ISO27001标准，关注文件的适宜性和完整性是否符合要求。着重关注的文件包括但不限于：

法律地位证明、组织简介、组织机构图、人员情况说明、管理手册、程序文件、信息安全方针和目标、信息安全管理体系的规程和控制措施、SOA适用性声明、风险评估报告、残余风险声明、风险处置计划、资产识别表、法律法规清单

现场审核

关注要点

现场审核时，外部审核员主要关注组织信息安全管理体系执行的程度及有效性，除着重关注各部门信息安全资产识别与风险管理相关记录外，对应不同部门或角色，着重关注的体系运行记录分别为：

行政人事部门：

1.来访人员登记记录2.人员保密协议3.与信息安全相关的法律法规清单、符合性评价4.与相关相关的培训计划、培训签到记录

IT相关部门：1.服务器管理（包括设备点检、测试日志记录与审查）2.机房管理等重点区域进出管理3.对各部门定期杀毒、屏保、密码等监督检查表单4.公司软件使用清单、容量标注5.重要数据备份记录6.上网安全检查7.各类信息系统如邮箱、OA权限及权限时效性管理记录

市场业务部门：

1.合同、订单2.业务连续性资料（计划、验证）3.访问区域限制如未经授权人员可能进入的地点管理记录

研发部门：

1.产品技术资料（设计开发资料，应包括信息安全风险评估）2.研发人员保密协议3.生产工艺流程图

采购部门：

1.合格供应商名录2.供应商调查表3.供应商签署安全要求的文件协议

4.供应商基本资料（如营业执照、ISO9001证书等）

管理层：

1.目标达成统计表2.文件清单（手册、程序、作业指导书）3.文件发布记录4.外来文件清单5.全公司资产识别与风险管理汇总表6.内审、管审过程记录