贯标集团-天津【IT行业标配】ISO27001信息安全管理体系简介

产品名称	贯标集团-天津【IT行业标配】ISO27001信息安全管理体系简介
公司名称	贯标集团--天津公司
价格	.00/件
规格参数	
公司地址	天津市滨海高新区华苑产业区梅苑路5号金座广场-3318
联系电话	15502200816 15502200816

产品详情

PART01ISO/IEC 27001的背景知识

ISO /IEC 27001认证是信息安全管理体系认证。

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。

ISO27001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。

2000年，国ji标准化组织（ISO）在BS7799-1的基础上制定通过了ISO17799标准。BS7799-2在2002年也由BSI进行了重新的修订。ISO组织在2005年对ISO17799再次修订，BS7799-2也于2005年被采用为ISO27001:2005。

2013年修订原版本，正式使用ISO/IEC27001：2013版。

2022年10月25日正式发布实施 ISO/IEC27001:2022 《信息安全 网络安全 隐私保护信息安全管理体系要求》。

信息安全管理体系（ ISMS）是组织依据GB/T22080/ISO/IEC27001（信息技术安全技术信息安全管理体系要求）的要求，是组织整体管理体系的一个部分，是基于风险评估，来建立、实施、运行、监视、评

审、保持和改进信息安全等一系列的管理活动，是组织在整体或特定范围内建立信息安全方针和目标，以及完成这些目标所用方法的体系。

ISO/IEC27001是建立和维护信息安全管理体系的标准，它要求组织通过一系列的过程如确定信息安全管理体系范围，制定信息安全方针和策略，明确管理职责，以风险评估为基础选择控制目标和控制措施等，使组织达到动态的、系统的、全员参与的、制度化的、以预防为主的信息安全管理方式。

ISMS认证 是 针对组织 ISMS符合GB/T22080/ ISO/IEC27001要求的一种认证。这是一种通过权wei的第三方审核之后提供的保证：受认证的组织实施了ISMS，并且符合GB/T 22080/ISO/IEC 27001标准的要求。通过认证的组织，将会被注册登记。

PART02

企业如何建立ISO/IEC 27001信息安全管理体系？

ISO/IEC27001信息安全管理体系，采用PDCA循环模型，分为四个阶段：安全风险评估、规划体系建设方案（Plan），建立并实施信息安全管理体系（Do），体系运行绩效考核（Check），持续改进（Action）。我们重点说说企业在应对ISO/IEC27001认证时应该怎么建设符合标准要求的信息安全管理系统，重点从五个方面来进行：

1、确立管理系统使用的范围

◇必须覆盖到公司的每一个职能部门，或者覆盖公司信息系统相连的外部机构，例如合作伙伴、供应商等。同时从系统层次考虑覆盖网络系统、服务器平台系统、数据、安全管理、应用系统以及支撑信息系统的场所和所处的周边环境以及场所内，确保计算机系统正常运营的设施设备等。

2、安全风险评估

◇安全风险评估，主要包括企业安全管理类的评估和企业安全技术类的评估

安全管理评估的内容包括与ISO/IEC27001信息安全管理体系相关的11个方面，包括信息安全政策、安全组织、资产分类与控制、人员安全、物理与环境安全、通信与运行管理、访问控制等，系统开发和维护、安全事件管理、业务连续性管理和合规性。安全技术评估是基于资产安全等级的分类。通过对信息设备的安全扫描和安全设备的配置，对现有网络设备、服务器系统、终端和网络安全架构的安全状况和薄弱环节进行检查和分析，为安全加固提供依据。

3、规划系统建设方案

◇规划系统建设方案在风险评估的基础上，针对企业存在的安全风险提出安全建议，提高系统的安全

性和抗攻击能力。

4、信息安全体系建设与运行

◇ 系统建设以信息安全模式和企业信息化为基础，兼顾内外部安全功能。规划信息安全技术可以从安全基础设施、网络、系统和应用四个方面进行规划。

5、改进

◇ ISO/IEC27001认证标准的信息安全管理体系文件编制完成以后，按照文件控制的要求进行审核批准，向各部门发放先行有效的体系文件，保留体系运行过程中的记录，并定期进行内审和管理评审，对不符合或潜在不符合项进行纠正和预防措施，不断改进信息安全管理体系。

PART03ISO/IEC 27001认证项目实施

一、项目前期准备阶段

● 将实施ISO27001项目的决定、目的、意义、要求在组织内传达，这也是体现内部沟通，提高全体员工意识的必要手段。

● 组织建设，包括任命管理者代表、成立贯标组织机构、各级信息安全管理人员，明确其职责。

二、现场调研诊断

目的： 了解组织的现状，寻找与ISO27001标准的差距。

内容： 实施调研诊断。

三、人员培训

目的： 提升各级领导和全员的信息安全意识，使内审员具备相应能力。

内容： 动员会、ISO27001标准培训、信息安全管理体系文件编写培训、培训是落实要求的重要手段。

四、整合体系文件架设计

目的： 策划覆盖各个业务流程的系统的文件化程序。

内容： 根据现场诊断的结果，梳理所有管理活动流程，根据ISO27001标准要求形成信息安全管理体系文件清单。

五、确定信息安全方针和目标

目的： 明确信息安全方针和目标，为信息安全管理体系提供导向。

内容： 根据业务要求及组织实际情况，制定安全方针和目标。

六、建立管理组织机构

目的： 建立完善的内控组织架构，为整合体系提供支持。

内容： 良好的组织架构是确保各项管理活动落实的根本。

七、信息安全风险评估

目的： 实施风险评估，识别不可接受风险，明确管理目标。

内容： 风险评估是整个风险管理的基础，本阶段将根据前期策划的风险评估方法。

八、ISMS体系文件编写

目的： 建立文件化的信息安全管理体系。

内容： 根据文件体系策划的结果，编写信息安全管理体系文件。

九、ISMS管理体系记录的设计

目的： 设计科学的信息安全管理体系记录，保证各管理流程的可控性和可追溯性。

内容： 根据各个管理流程和文件对管理过程的记录要求，设计记录表格格式。

十、ISMS管理体系文件审核

目的： 确保ISMS信息安全管理体系文件的系统性、有效性和效率。

内容： 对信息安全管理体系文件进行评审。

十一、ISMS体系文件发布实施

目的： 发布ISMS信息安全管理体系文件，落实管理要求。

内容： 由蕞高管理者组织发布管理文件，并提出管理要求。

十二、组织全员进行文件学习

目的：确保信息安全管理体系文件要求在各个层级、各个岗位均得到有效的沟通和理解。

内容：培训是提升信息安全意识，明确信息安全要求的有效途径，组织全员参与到体系的运行维护中，发挥每一个员工的重要作用。

十三、业务连续性管理

目的：确保在任何情况下，核心业务均可保持提供连续提供服务的能力。

内容：根据标准要求，对重大的灾难性事件发生时所引发的业务中断进行应急响应和灾难恢复的设计。

十四、审核培训及内审

目的：实施内部审核，发现信息安全管理体系运行中的不符合，寻找改进的机会。

内容： 根据项目计划实施内部审核。

十五、管理体系有效性测量

目的： 根据量化指标，测量信息安全管理体系的有效性。

内容： 制定测量的方法论，根据 ISO27004指南的内容，进行信息安全管理体系有效性测量。

十六、管理评审

目的： 将体系运行过程中的成效和问题向管理层汇报，由蕞高管理者提出改进的要求和资源的支持。

内容： 根据管理评审流程的要求实施管理评审。

十七、认证机构正式审核

目的： 由第三方权wei机构审核信息安全管理体系的有效性。

内容： 由认证机构对建立的信息安全管理体系进行进一步的审核验证，发现改进机会。

PART04企业申请ISO/IEC 27001认证的基本条件1、中国企业持有工商行政管理部门颁发的《企业法人营业执照》、《生产许可证》或等效文件；外国企业持有关机构的登记注册证明。

2、申请方的信息安全管理体系已按ISO/IEC 27001: 2013标准的要求建立，并实施运行3个月以上。

3、至少完成一次内部审核，并进行了管理评审。

4、信息安全管理体系运行期间及建立体系前的一年内未受到主管部门行政chu罚。

PART05企业申请ISO/IEC 27001认证的文件清单

1、组织法律证明文件，如营业执照及年检证明复印件（盖公章）；2、组织机构代码证书复印件、税务登记证复印件（盖公章）；3、申请认证组织的信息安全管理体系有效运行的证明文件（如体系文件发布控制表，有时间标记的记录等复印件）；4、申请组织的简介：
4.1、组织简介（1000字左右）； 4.2、申请组织的主要业务流程； 4.3、组织机构图或职能表
述文件；5、申请组织的体系文件，需包含但不jin限于（可以合并）：
5.1、信息安全管理体系ISMS方针文件； 5.2、风险评估程序； 5.3、适用性声明；
5.4、风险处理程序； 5.5、文件控制程序； 5.6、记录控制程序；
5.7、内部审核程序； 5.8、管理评审程序； 5.9、纠正措施与预防措施程序；
5.10、控制措施有效性的测量程序； 5.11、职能角色分配表；
5.12、整个体系文件结构与清单。6、申请组织体系文件与GB/T22080-2016/ ISO/IEC 27001:2013要求的文件对照说明；7、申请组织内部审核和管理评审的证明资料；8、申请组织记录保密性或敏感性声明；9、认证机构要求申请组织提交的其他补充资料。