贯标集团-北京ISO27001建设、优化和认证指南

产品名称	贯标集团-北京ISO27001建设、优化和认证指南
公司名称	贯标集团-华北公司
价格	.00/件
规格参数	
公司地址	华北公司地址：天津市河西区南京路35号亚太大厦13层；总部地址：江苏省南京市玄武区新庄村57号二楼
联系电话	022-23125802 15502200816

产品详情

摘要：2022年10月发布的ISO/IEC 27001:2022标准取代了2013版。新版标准引入了一系列的更新，为了帮助组织理解这些修改，本文提供了关于如何基于新版本进行信息安全管理体系建设、优化和认证的指南

获取新版ISO 27001的认证。

2022版ISO27001的变化

（1）标准名称的变化

ISO 27001和ISO 27002的官方标准名称已更新为ISO/IEC 27001:2022《信息安全、网络安全和隐私保护 信息安全管理体系 要求》以及ISO/IEC 27002:2022《信息安全、网络安全和隐私保护 信息安全控制》。这表示新标准从原本的“ 信息技术 安全技术 ”扩展到了“ 信息安全、网络安全和隐私保护 ”。这个变化反映了新标准的目标是紧跟现代信息技术和信息安全的发展潮流，以便在不断进步的环境中保持领xian地位和实用性。

（2）标准内容的变化

ISO 27002:2022标准是在ISO 27002:2013的基础上进行了改进和优化。新版标准对原有的14个控制领域以及114个控制项进行了细致的审查，并进行了合并、剔除和引入新的控制项。蕞新的ISO/IEC 27002:2022标准明确列出了93个控制项，涵盖了4个主题和15个安全运营能力域。这些改动使得新版标准更加针对性和实用性，更能够满足现代信息安全管理的需求。

15个安全运营能力域

运营能力是从组织的信息安全能力角度来看待控制的一个属性。新标准ISO 27002:2022的15个安全运营能力域相较于旧版本的14个控制域有几个明显的变化。新增了“ 信息保护 ”、“ 安全配置 ”和“ 威胁和漏洞管理 ”领域；同时，部分领域的名称也有了变化，如将“ 信息系统获取、开发和维护 ”改为“ 应用安全 ”，将“ 通信安全 ”改为“ 系统和网络安全 ”。

4个主题和93个控制项

修订后的2022版信息安全控制措施将93项分配到了四大主题，即组织、人员、物理和技术。这使得组织能够更方便地选择和归类安全控制点，并通过特定主题策略来支持信息安全策略的实施。相比2013版，2022版还增加了11个安全控制项，包括威胁情报、云服务使用的信息安全、业务连续性中ICT准备、物理安全监控、配置管理、信息删除、数据脱敏、数据防泄露、监控活动、网页过滤和安全编码。这些变化进一步加强了信息安全控制的实施。

建设信息安全管理体系

强烈推荐组织参照蕞新版的ISO 27001和ISO 27002标准构建和优化信息安全管理体系。

组织需要根据自身信息安全战略进行持续改进和完善信息安全管控措施。

寻求专ye培训机构的协助能给组织带来重大益处，他们能帮助组织理解新标准要求，并提供定制化解决方案指导建设和更新信息安全管理体系。

认证培训机构在协助组织建设信息安全管理体系并获得认证过程中，通过培训和知识传递，提升组织员工的信息安全意识和技能熟练度。这将强化员工的信息安全素养，提升整个组织的信息安全防御能力，助力组织在日益复杂的信息安全环境中稳健前行。

（1）建设体系

在建设信息安全管理体系过程中，首要步骤是评估组织现有的信息安全状况，并明确可能导致信息资产泄露、破坏或丢失的威胁及其影响。评估方法多样，包括差距分析和风险评估、基于资产的风险评估、对特定业务流程或IT流程的风险评估，以及技术评估等。

基于资产的风险评估在ISO 27001认证项目中得到广泛应用。根据评估结果，参考ISO 27002的控制要求，选择适合组织实际需求的信息安全控制措施来管理风险。制定一套信息安全管理制度体系文件，指导信

息安全管理工作，并确保员工明确自身职责和任务。

编制完成后，进行审核与批准并发布实施，然后进行试运行至少3个月，检验体系运行中存在的不足并进行调整。试运行结束后，进行内部审核和管理层审查，持续优化信息安全管理体系，确保满足组织需求和目标。蕞后，邀请认证机构进行认证审核，若通过则获得ISO 27001的认证证书。

（2）优化体系

理解ISO 27001:2022与ISO 27001:2013之间的差异以及这些差异的实际意义。

对现有的信息安全管理系统进行全面审查，确定其符合新标准要求的优势和改进的需要。

制定详细的改进行动计划，包括修改政策和程序，引入新的控制措施，进行必要的额外培训等。

针对新版中新增的控制项，在现有的信息安全管理制度中进行相应的补充和完善。

进行至少3个月的试运行，并执行内部审核，确保满足了所有新版标准的要求。

管理层需要审查更新后的信息安全管理体系，确认其符合组织的业务需求和目标。

邀请认证机构进行认证审核，成功通过审核后获得ISO 27001:2022的认证证书。

（3）专项建设

设计安全体系

数据安全管理体系应当是信息安全管理体系的重要组成部分，需要与现有安全管理体系融合，并将其纳入到现有的安全体系运营中。

组织在进行数据安全管理体系建设时，可以参考相关法律法规、行业监管要求以及ISO 27002标准要求。

在深入理解关键业务流程和业务系统的基础上，组织应该梳理数据资产，明确数据的分布、流转和处理过程，并识别敏感数据的安全风险。

基于风险评估的结果，组织需要制定和实施数据安全策略，包括建立数据安全管理组织、制定数据安全管理制度流程、部署数据安全技术工具等。

数据安全管理组织架构可以参考信息安全管理体系的决策层、管理层、执行层和监督层四个层级，在原有组织体系的基础上增加对数据安全的职责。

数据安全管理制度体系分为四层架构，每一层作为上一层的支撑。第一层是管理总纲，明确数据安全治理的目标和重点。第二层是管理制度，建立各类管理内容的安全管理制度。第三层是操作流程和规范性文件，指导数据安全策略的落地。第四层是流程图和表单文件，作为执行文件支持数据安全运营。组织应根据方针策略，建立与制度流程相配套的技术和工具，并定期监控和审计数据安全措施的效果以改进管理体系。

设计外包体系

信息科技外包管理体系对于依赖外包服务商执行大量任务的组织来说非常重要，特别是对于银行和保险机构。

根据相关规定，银行和保险机构需要对信息科技外包活动进行规范，并强化对外包风险的管控。ISO 27002:2022标准中的“ 供应商关系安全 ”领域的控制要求可以作为参考，并结合外包商及其员工的安全管理实践，来构建信息科技外包管理组织架构，以及更新和完善管理体系文件。

管理体系文件应明确规定外包的种类、准入标准、尽职调查流程和内容、合同管理、监控评估、风险管理以及安全管理等方面的内容。

实施这些工作可以帮助组织更有效地识别和管理与外包商和外包人员相关的安全风险，预防可能导致的安全问题的发生。

设计生命周期

在信息安全管理体系中，信息系统开发生命周期安全管理是一个重要组成部分。组织应参考ISO 27002:2022标准中“ 应用安全 ”领域的控制要求，并结合安全开发生命周期实践，关注从需求分析、设计、编码、测试到部署和维护的整个信息系统开发过程中融入安全性的考虑。

为了进行有效的信息系统开发生命周期安全管理，组织首先需要制定明确的策略。这一策略应明确规定整个信息系统开发生命周期中的安全管理方式。具体来说，策略应包括以下内容：

安全需求识别：明确识别信息系统开发中的安全需求，确保在整个开发过程中对安全问题有所关注。

安全设计原则：明确阐述信息系统开发中的安全设计原则，指导开发人员在设计阶段将安全性考虑纳入到系统架构和功能设计中。

安全编码实践：提供安全编码的具体实践指南，确保开发人员在编码过程中采取适当的安全措施，避免常见的安全漏洞。

安全测试：定义安全测试的方法和准则，确保在测试阶段对系统的安全性进行全面评估和验证。

部署和维护中的安全管理：提供在系统部署和维护过程中的安全管理指南，确保系统在运行过程中持续保持安全状态。

对员工进行培训
：对员工进行培训是提升整个生命周期安全性的关键。培训可以确保员工具备足够的安全知识和技能。开发人员需要了解如何避免常见的安全漏洞，测试人员需要掌握安全测试方法，运维人员需要了解如何保护生产环境的安全。

通过制定明确的策略并结合ISO 27002:2022标准中的控制要求，组织可以有效地进行信息系统开发生命周期安全管理，从而保障信息系统的整体安全性。

ISO27001认证价值

构建信息安全管理体系并获得ISO 27001认证可以为组织带来多方面的益处：

提升信息安全防护：建设信息安全管理体系可识别和管理信息安全风险，提高信息安全防御能力，减少安全事故发生的可能性。

增强信任度：ISO 27001认证代表组织达到国际信息安全管理标准，增加客户、合作伙伴及其他利益相关者对组织的信任度。

合规性：信息安全管理体系可满足法规、行业规定和合同中的信息安全要求，避免违反而产生的法律责任和经济损失。

提高效率：整合和优化信息安全控制措施可提高组织运作效率。

保护业务连续性：通过预防和应对信息安全事件，信息安全管理体系可保护组织的业务连续性，减少由安全事件导致的业务中断。

促进业务增长：对于注重信息安全的客户，组织的信息安全管理能力成为选择合作伙伴的重要因素。

能力提升：通过学习信息安全管理体系，提高员工的信息安全意识和技能，使他们更好地识别和防范信息安全风险。

应对未来挑战：持续优化的信息安全管理体系有助于组织应对新的技术、威胁和业务模式带来的挑战。

信息安全管理体系面临的挑战

以下是关于信息安全管理体系建设和认证过程中的难点和挑战：

资源投入：建设和认证信息安全管理体系需要大量的时间、人力和财力资源。这包括培训员工、购买和实施安全控制措施，以及聘请咨询服务。

组织文化和员工意识：如果组织的文化和员工对信息安全不重视，实施信息安全管理体系可能会遇到阻力。为了改变这种情况，需要进行大量宣传和教育工作。

风险评估：识别和评估信息安全风险是建设信息安全管理体系的关键步骤，但这是一项复杂的任务，需要专ye的知识和技能。

技术挑战：实施某些安全控制措施可能需要在技术上进行调整，这可能带来一些技术挑战。

合规性：满足相关法规、行业规定和合同要求可能是一项挑战。

持续改进：建设和认证信息安全管理体系不是一次性任务，而是需要持续改进的过程。然而，许多组织在初步实施信息安全管理体系后可能会发现维持和改进它是一项挑战。

变更管理：组织的业务、技术和环境可能会发生变化，这可能会影响信息安全管理体系。因此，组织需要有效的变更管理过程，以确保信息安全管理体系能够适应这些变化。

面对以上可能存在的挑战，组织可以考虑采取以下策略来应对：

确保资源：预留必要的资源，包括时间、人力和财力。获得高层管理的承诺和支持，以及各部门的积极参与和配合。

建立信息安全文化：使所有员工都理解并接受信息安全是日常工作的一部分。提供定期的安全培训和教育，增强员工的安全意识。

风险管理：建立全面的风险管理流程，包括风险识别、评估、处理和监控。持续进行风险管理，而不是一次性活动。

技术支持：考虑引入合适的技术专家或咨询服务，提供技术支持，帮助选择和实施适当的安全控制措施。

合规性考虑：规划阶段就充分考虑合规性要求，确保信息安全管理体系满足所有相关的法规、行业规定和合同要求。

持续改进：建立持续改进的文化和流程，确保信息安全管理体系能随着组织和环境的变化而改进。

变更管理：制定有效的变更管理流程，确保组织的变更能够得到恰当的处理，并且信息安全管理体系能适应这些变更。

内部和外部审计：定期进行内部和外部审计，确认信息安全管理体系的有效性，并识别出需要改进的地方。

进行ISO 27001培训
：通过学习核心概念，理解ISO27001并建立基础，了解信息安全管理的必要性和风险管理方法，并从咨询师视角掌握实施ISO27001的流程和需求分析，包括风险评估和项目实施过程，深入研究ISO27001标准条款在不同组织中的应用，并获得ISO27001Foundation认证证书以提升信息安全管理能力。