《ISO/IEC 27001:2022》升级转版介绍

产品名称	《ISO/IEC 27001:2022》升级转版介绍
公司名称	贯标集团
价格	.00/件
规格参数	
公司地址	南京市仙林大道10号三宝科技园1号楼B座6层
联系电话	4009992068 13382035157

产品详情

近日，随着ISO/IEC27001:2022新版信息安全管理体系的正式发布，为各行各业的组织提供了一个更新框架，助力应对日益复杂的威胁环境。此次新版标准将控制措施按四方面进行分类，其中包括组织、人员、技术和物理，帮助组织更有效地管理控制措施。

新标准也呼应了最近更新的ISO 27002:2022所列出的信息安全控制措施。现在控制措施已由原先的114项减少为93项，其中11项为新增措施，其它的则多被合并或删除。

?ISO/IEC 27001:2022???? ????????? ????????

????2022?10?25???????????2013??114???93??93?????????????ISO/IEC 27002:2022 ????

????????? ?????????????ISO/IEC

27002:2022???2022??2?15?????????????????????????????ISO/IEC

27002:2022?????????????????????ISO/IEC

27002:2022????????????????????????????????????

?????????

2个标准的新旧版名称分别如下：新版：《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》《ISO/IEC 27002:2022 信息安全 网络安全和隐私保护 信息安全控制》旧版：《ISO/IEC 27001:2013 信息技术 安全技术 信息安全管理体系 要求》《ISO/IEC 27002:2013 信息技术 安全技术 信息安全控制实践指南》注释： 标准名称由“ 信息技术 安全技术 ”变为“ 信息安全 网络安全和隐私保护 ”，新版加大了对“ 网络安全和隐私保护 ”的控制深度，增加了相关的条款和控制措施。二、《ISO/IEC 27002:2022》的文件结构发生变化文件结构如下： 人员控制（第6章）；---》人员，如果涉及到单独的个人 物理控制（第7章）；---》物理，如果涉及到物理对象； 技术控制（第8章）；---》技术，如果涉及到技术； 组织控制（第5章）；---》其他均归类为组织2个资料性附录： 附录A 属性的使用； 附录B 本文件与GB/T 22081—2016的对应关系。三、《ISO/IEC 27002:2022》增加了属性表的使用对每个条款的5个属性进行赋值，方便读者日后控制措施的选择。5个属性介绍如下：1、控制类型：是从控制何时和如何改变信息安全事件发生风险的视角来看控制的一种属性，属性值如下： 预防（旨在防止信息安全事件发生的控制） 检测（作用于信息安全事件发生时的控制） 纠正（作用于信息安全事件发生后的控制）。2、信息安全属性：是从控制有助于保护哪些信息特征的视角来看控制的一种属性，属性值如下： 保密性、完整性、可用性3、网络空间安全概念：是从控制与网络空间安全概念关联的视角来看控制的一种属性，属性值如下： 识别、防护、发现、响应和恢复4、运行能力：是从从业者信息安全能力的视角来看控制的一种属性，属性值如下： 治理、资产管理、信息保护、人力资源安全、物理安全、系统和网络安全、应用安全、安全配置、身份和访问管理、威胁和脆弱性管理、连续性、供应商关系安全、合规性、信息安全事件管理和信息安全保障。5、安全领域是从四个信息安全领域的视角来看控制的一种属性，属性值如下： 治理和生态体系（“ 信息系统安全治理和风险管理 ”和“ 生态系统网络空间安全管理 ”（包括内外部相关方）） 防护（IT安全架构 ”、IT安全管理 ”、身份和访问管理 ”、IT安全维护 ”及“ 物理和环境安全 ”） 防御（检测 ”和“ 计算机安全事件管理 ”） 弹性（运行的连续性 ”和“ 危机管理 ”）四、《ISO/IEC 27002:2022》强调了“ 安全开发 ”工作的重要性。新版的安全开发理念与2013版完全不同。1、新版的“ 5.1信息安全策略 ”中较2013版增加了“ 安全开发 ”特定主题策略。2、“ 8.27 安全体系架构和工程原则 ”较2013版变化很大，开发理念和开发要求更加能够应对dingjian恶意攻击，如提出了在软件设计开发过程中要应用“ 零信任原则 ”，如下：安全体系架构和工程原则组织宜考虑“ 零信任 ”原则，如：a) 假设该组织的信息系统已经遭到破坏，因此不单单依赖网络周界安全；b) 采用“ 从不信任，总是验证 ”的方法访问信息系统；c) 确保对信息系统的请求进行端到端加密；d) 验证向信息系统发出的每个请求时，宜将请求视同为开放外部网络发来的请求，即便这些请求来自组织内部（即不自动信任其周界内或周界外的任何东西）；e) 使用“ 最小权限 ”和动态访问控制技术（见5.15、5.18和8.2）。这包括基于应用语境信息（如认证信息（见5.17）、用户身份（见5.16）、与用户终端设备有关的数据和数据分级（见5.12））对信息或系统的请求进行鉴别和授权；f) 始终基于包括身份鉴别信息（参见5.17）和用户身份（参见5.16）、与用户终端设备有关的数据和数据分级（参见5.12）在内的信息，对请求者进行身份鉴别，并始终验证对信息系统的授权请求，例如强制实施强身份鉴别（如多因素，参见8.5）。3、提出了“ 防篡改 ”技术，实践了《GB/T 22239-2019 信息安全技术 网络安全等级保护 基本要求》的“ 可信验证 ”要求。 《ISO/IEC 27002:2022》的“ 防篡改 ”技术相关内容如下：8.27 安全体系架构和工程原则8.27.5 其他信息安全工程原则可应用于一系列技术的设计或配置，例如：—— 容错和其他弹性技术；—— 隔离（例如通过虚拟化或容器化）；—— 防篡改。安全虚拟化技术可用于防止在同一物理设备上运行的应用程序之间的干扰。如果应用程序的虚拟实例受到攻击者的攻击，则只有该实例受到影响。该攻击对任何其他应用程序或数据都没有影响。防篡改技术可用于检测信息容器的篡改，无论信息容器是物理形式（如防盗报警器）还是逻辑形式（如数据文件）。这种技术的特点是可以产生试图篡改容器的记录。此外，这种安全控制还可以通过销毁数据来防止成功提取数据（如可以删除设备内存）8.7 恶意软件防范d)定期自动验证系

统的软件和数据内容，尤其是支持关键业务过程的系统；调查是否存在任何未经批准的文件或未授权的修改；8.7.5其他信息在某些系统（如某些工业控制系统）上，并不总是能够安装防范恶意软件的软件。某些形式的恶意软件会感染计算机操作系统和计算机固件，以致常见的恶意软件控制将系统无法清理干净，这就有必要对操作系统软件，有时还包括对计算机固件进行完全重新镜像，以恢复到安全状态。8.16 监视活动d)检查正在执行的代码是否被授权在系统中运行，并且未被篡改（例如通过重新编译添加不必要代码）；增加了“ 8.28 安全编码 ”条款，对“ 规划和编码前 ”、“ 编码期间 ”、“ 评审和维护 ”3个阶段活动进行了要求。强调了开发人员对安全编码掌握并实践到编码活动中的重要性。增加了“ 8.12 数据防泄露 ”条款，重视了“ 网络安全和隐私保护 ”，提出了“ 逆向社会工程或蜜罐 ”技术的使用，如下：8.12 数据防泄露在备份数据的位置，宜确保使用加密、访问控制和对保存备份的存储媒体进行物理保护等措施来保护敏感信息。数据防泄露还宜考虑用于防止对手的情报活动获取保密或秘密信息（地缘政治、人力、金融、商业、科学或任何其他信息），这些信息可能利于间谍活动或对社会至关重要。无论作为独立措施还是对对手情报活动的回应，数据防泄露措施宜着眼于混淆对手的决策，如将真实信息替换为虚假信息。此类措施例如逆向社会工程或使用蜜罐吸引攻击者。五、增加了“ 8.16 监视活动 ”条款《ISO/IEC 27002:2022》为加强软硬件运维人员的运维监视工作，增加了“ 8.16 监视活动 ”条款。六、加强了“ 隐私保护 ”工作《ISO/IEC 27002:2022》加强了“ 隐私保护 ”工作的要求，增加了“ 8.11 数据脱敏 ”条款、“ 8.10 信息删除 ”，并对“ 5.34 隐私和个人可识别信息保护 ”条款增加了“ 隐私影响风险评估（PIA） ”要求，隐私影响风险评估（PIA）也是我国的《中华人民共和国个人信息保护法》的要求。七、增加“ A.8.9 配置管理 ”条款《ISO/IEC 27002:2022》为加强项目实施中的配置管理工作、在软件设计开发中的安全配置设计的要求，增加了“ A.8.9 配置管理 ”条款。八、增加“ 8.23 网页过滤 ”条款《ISO/IEC 27002:2022》为加强网络安全工作，要求操作员规范上网行为，增加了“ 8.23 网页过滤 ”条款。注：其他条款变化也很多，需要大家学习《ISO/IEC 27002:2022 信息安全 网络安全和隐私保护 信息安全控制》，我司可以给企业提供落地实施信息安全管理体系咨询、培训，按岗位进行培训，让各岗位知道按照信息安全管理体系的要求，自己该如何开展工作。欢迎保密要求较高、需要通过落地实施信息安全管理体系解决企业困境的单位可后台私信留言，我们定能提供达到预期结果的服务。