等级测评备案注册流程

产品名称	等级测评备案注册流程
公司名称	上海道商企业服务中心
价格	.00/个
规格参数	
公司地址	浦东新区金沪路99弄3号
联系电话	15021594806 15021594806

产品详情

网络安全等级保护-系列标准 一、《信息安全技术网络安全等级保护基本要求》（GB/T22239-2019）
1.出台背景及目的 为了配合《中华人民共和国网络安全法》（一下简称「《网安法》」）的实施，同时适应云计算、移动互联、物联网、工业控制和大数据等新技术、新应用情况下网络安全等级保护工作的开展，国家标准GB/T22239-2019《信息安全技术网络安全等级保护基本要求》（以下简称「《基本要求》」和/或「GB/T22239」）应运而生。《基本要求》代替了GB/T22239-2008《信息安全技术信息系统安全等级保护基本要求》，针对网络安全共性安全保护需求提出安全通用要求，针对云计算、移动互联、物联网、工业控制和大数据等新技术、新应用领域的个性安全保护需求提出安全拓展要求，形成新的网络安全等级保护基本要求标准。 2.关键定义 网络安全：通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，并保障网络数据的完整性、保密性、可用性的能力。
安全保护能力：能够抵御威胁、发现安全事件以及在遭到损害后能够恢复先前状态等的程序。 等级保护对象：是指网络安全等级保护工作中的对象，通常是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、处理的系统，主要包括基础信息网络、云计算平台/系统、大数据应用/平台/资源、物联网、工业控制系统和采用移动互联技术的系统等。等级保护对象根据其在国家安全、经济建设、社会生活中的重要程度，遭到破化后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等，由低到高被划分为五个安全保护等级。
3.不同安全保护等级的等级保护对象应具备的基本安全保护能力 在《网络安全等级保护制度2.0：回顾与展望》中，我们介绍了根据网络在国家安全、经济建设、社会生活中的重要程度，以及其一旦遭到破坏、丧失功能或者数据被篡改、泄露、丢失、损毁后，对国家安全、社会秩序、公共利益以及相关公民、法人和其他组织的合法权益的危害程度等因素，网络分为五个安全保护等级。在这里，根据《基本要求》，我们向大家说明不同级别的等级保护对象应具备的基本安全保护能力： 4.安全要求的分类 《基本要求》将安全要求分为10个小项，分别是安全物理环节、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理。为方便各位理解与记忆，我们可以将上述10个小项分为两个大类，即网络技术安全要求与网络管理安全要求：除此以外，《基本要求》又对以上每个小项做出安全通用要求和安全拓展要求。其中，通用要求针对共性化保护需求提出，安全拓展要求针对个性化保护需求提出，根据安全保护等级和使用的特定技术或特定应用场景选择实现拓展要求。安全通用要求和安全拓展要求企共同构成了安全要求的一部分。（关于安全通用要求和安全拓展要求的选择和使用，可以参考《基本要求》附录A） 5.等级保护安全架构 开展网络等级保护是一个系统性、复杂性、细节性极强的工作，企业需要依据国家相关法律法规、政策、标

准，开展一系列组织管理、机制建设、安全规划、安全监测、通报预警、应急处置、态势感知、能力建设、监督检查、技术检测、安全可控、队伍建设、教育培训和经费保障等工作。为方便各位理解整个网络等级保护工作的架构，我们挑选了《基本要求》中的下表供参考：
二、《信息安全技术网络安全等级保护测评要求》(GB/T28448-2019) 1.出台背景及目的 《信息安全技术网络安全等级保护测评要求》（GB/T28448-2019）（以下简称「《测评要求》」和/或「GB/T28448-2019」）规定了不同级别的等级保护对象的安全测评通用要求和安全测评扩展要求。适用于安全测评服务机构、等级保护对象的运营使用单位及主管部门对等级保护对象的安全状况进行安全测评并提供指南，也适用于网络安全职能部门进行网络安全等级保护监督检查时参考使用。《测评要求》的出台替代了《信息安全技术信息系统安全等级保护测评要求》。相比于GB/T28448-2012，GB/T28448-2019细化了单项测评的规定、增加了等级测评的拓展要求，并对测评力度进行了更严格的规定。
2.《测评要求》测评方法及其框架 等级测评实施的基本方法是针对特定的测评对象，采用相关的测评手段，遵从一定的测评规程，获取需要的证据数据，给出是否达到特定级别安全保护能力的评判。具体方法有： 同时，《测评要求》将等级测评分为单项测评和整体测评，其中：
3.《测评要求》对不同安全保护等级的测评力度有不同要求 《测评要求》对不同安全保护等级的测评力度有不同要求，这主要体现在测评工作的广度和深度上。安全保护等级越高，测评广度就越大，深度就越深。其中，所谓测评广度越大，指的是测评需要在更多细节上开展，测试要求也更严格。所谓测评深度越广，指的是测评实施包含的测评对象更多。具体来说： 4.单项测评与整体测评的基本内容 单项测评针对安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理和（或）安全管理中心进行测评，测评的内容根据安全保护等级不同而有所不同，包括但不限于对防盗窃和防破坏、边界防护、可信验证、身份鉴别、数据备份恢复、服务供应商管理、安全意识教育和培训、安全事件处置、安全审计、数据保密性、资产管理等内容的测评。 整体测评主要从安全控制点、安全控制点间和区域间等方面进行测评和综合安全分析，从而给出等级测评结论。 5.等级测评报告结果 等级测评报告会对测评结果中的不符合项或部分符合项进行风险分析，评估其所产生的安全问题被威胁利用的可能性，并判断其被威胁利用后对业务信息安全和系统服务安全造成影响的程度。终，等级测评报告会给出等级保护对象的等级测评结论，确认等级保护对象达到相应等级保护要求的程度。其中， 符合，是指定级对象中未发现安全问题，等级测评结果中所有测评项的单项测评结果中部分符合和不符合项的统计结果全为0，综合得分为100分。 基本符合，是指定级对象中存在安全问题，部分符合和不符合项的统计结果不全为0，但存在的安全问题不会导致定级对象面临高等级安全风险，且综合得分不低于阈值。 不符合，是指定级对象中存在安全问题，部分符合项和不符合项的统计结果不全为0，且存在的安全问题会导致定级对象面临高等级安全风险，或中低风险所占比例超过阈值。