辽宁网站等级保护测评备案服务

产品名称	辽宁网站等级保护测评备案服务
公司名称	河南世耀诚实业集团有限公司
价格	.00/件
规格参数	
公司地址	南阳市卧龙区工业路华龙广告二楼
联系电话	13140513661 18338218580

产品详情

等保标准具有很强的实用性：它是监管部门合规检查的依据，是我国诸多网络信息安全标准制度的重要参考体系架构，是行业主管部门对于下级部门网络安全建设的指引标准的重要依据和参考体系

由此标准衍生了诸多行业标准：例如人社行业等保标准、行业等保标准、能源行业（电力）等保标准、教育行业等保标准等行业标准。总的来说，等保制度是网络安全从业者开展网络安全工作的重要指导体系和制度。

什么是等保 1.0？

2007 年和 2008
年颁布实施的《信息安全等级保护管理办法》和《信息安全等级保护基本要求》。这部法规被称为等保 1.0。经过 10 余年的实践，等保 1.0 为保障我国信息安全打下了坚实的基础。

什么是等保 2.0？

等保 2.0 相关国家标准于 2019 年 5 月 10 日正式发布。2019 年 12 月 1
日开始实施。这是我国实行网络安全等级保护制度过程中的一件大事，具有里程碑意义。

等保 2.0 相比等保 1.0 有哪些区别 / 进步？

等保 1.0 主要强调物理主机、应用、数据、传输，而 2.0
版本增加了对云计算、移动互联、物联网、工业控制和大数据等新技术新应用的全覆盖。相较于等保 1.0，等保 2.0 发生了以下主要变化：

名称变化。等保 2.0 将原来的标准《信息安全技术信息系统安全等级保护基本要求》改为《信息安全技术网络安全等级保护基本要求》，与《网络安全法》保持一致。

第二，定级对象变化。等保 1.0 的定级对象是信息系统，现在 2.0 更为广泛，包含：信息系统、基础信息网络、云计算平台、大数据平台、物联网系统、工业控制系统、采用移动互联技术的网络等。

第三，安全要求变化。基本要求的内容，由安全要求变革为安全通用要求与安全扩展要求(含云计算、移动互联、物联网、工业控制)。

第四，控制措施分类结构变化。等保 2.0 依旧保留技术和管理两个维度。在技术上，由物理安全、网络安全、主机安全、应用安全、数据安全，变更为安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心；在管理上，结构上没有太大的变化，从安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理，调整为安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理。

第五，内容变化。从等保 1.0 的定级、备案、建设整改、等级测评和监督检查五个规定动作，变更为五个规定动作 + 新的安全要求(增加了风险评估、安全监测、通报预警、案事件调查、数据防护、灾难备份、应急处置等。)。

第六，法律效力不同。《网络安全法》第 21 条规定“ 国家实行网络安全等级保护制度，要求网络运营者应当按照网络安全等级保护制度要求，履行安全保护义务 ”。落实网络安全等级保护制度上升为法律义务。

等保 2.0 的实施对企业有哪些影响？

根据谁主管谁负责、谁运营谁负责、谁使用谁负责的原则，网络运营者成为等级保护的责任主体，如何快速高效地通过等级保护测评成为企业开展业务前必须思考的问题。

等保 2.0 有 5 个运行步骤：定级备案、差距评估、建设和整改、等级测评、检查。

同时，也分 5 个等级，即信息系统按重要程度由低到高分为 5 个等级，并分别实施不同的保护策略。

一级系统简单，不需要备案，影响程度很小，因此不作为重点监管对象；二级系统大概 50 万个左右；三级系统大概 5 万个；四级系统量级较大，比如支付宝、银行总行系统、国家电网系统，有 1000 个左右；五级系统属、国防类的系统，比如核电站、通信系统。

网络安全等级保护常见注意事项

1、等级测评并非安全认证 很多人容易把等保测评等同于安全认证。等保测评并非相当于 ISO 20000

系列的信息技术服务管理认证，也并非于 ISO27000 系列的信息安全管理体系认证。等级保护制度是国家信息安全管理的制度，是国家意志的体现。落实等级保护制度为了国家法律法规的合规需求。

等级保护测评没有相应的证书，如何才能证明信息系统已经符合等级保护安全要求了呢？目前这主要是由授权委托的全国一百多家测评机构，对信息系统进行安全测评，测评通过后出具《等级保护测评报告》，拿到了符合等保安全要求的测评报告就证明该信息系统符合了等级保护的安全要求。

2、等保制度只是基本要求 等保制度只是基线的要求，通过测评、整改，落实等级保护制度，确实可以规避大部分的安全风险。但就目前的测评结果来看，几乎没有任何一个被测系统能全部满足等保要求。一般情况下，目前等级保护测评过程中，只要没发现高危安全风险，都可以通过测评。注意如果有高危漏洞，立刻不合格， 但是，安全是一个动态而非静止的过程，而不是通过一次测评，就可以一劳永逸的。企业通过落实等保安全要求，并严格执行各项安全管理的规章制度，基本能做到系统的安全稳定运行。但依然不能保证系统的安全性。

3、内网系统也需要做等级测评 首先，所有非涉密系统都属于等级保护范畴，和系统在外网还是内网没有关系；《网络安全法》规定，等级保护的对象是在境内建设、运营、维护和使用的网络与信息系统。因此，不管是内网还是外网系统，都需要符合等级保护安全的要求。

其次，在内网的系统往往其网络安全技术措施做的并不好，甚至不少系统已经中毒不浅。2017 年肆虐全球的永恒之蓝勒索 病毒攻击，导致了大量内网系统瘫痪，这提醒我们内网系统的安全防护同样不能马虎。所以不论系统在内网还是外网都得及时开展等保工作。

4、系统上云或者托管在其他地方就也需做等级测评
目前，比较多的小型企业客户偏向于把系统部署在云平台与 IDC 机房。这些云平台、IDC 机房一般都通过了等级测评。不过，根据“ 谁运营谁负责，谁使用谁负责，谁主管谁负责 ”的原则，系统责任主体仍然还是属于网络运营者自己，所以，还是得承担相应的网络安全责任，该进行系统定级的还是得定级，该做等保的还是得做等保。

部署在云平台的系统还需要购买云平台的安全服务或者第三方安全服务，部署在 IDC 机房的系统还需要购买相应的安全设备以满足等保安全要求。

在云计算环境中，将云计算平台作为基础设施、云租户系统作为信息系统，分别作为定级对象进行定级。对于大型云计算平台，当运管平台共用时，可将云计算基础设施与运管平台系统分开定级，责任分离，分别定级、各自备案。云计算基础设施的安全保护等级不低于其所支撑的业务系统的等级。

针对私有云用户，也要按照云平台和云租户信息系统，分别进行定级。并且云平台的安全等级不低于其所支撑的业务系统的等级。

对于云计算平台和云租户信息系统，则分别依据等保 2.0 基本要求中的通用要求和云计算安全扩展要求来开展等级保护工作。对于私有云，定级流程为云平台先定级测评，再将已定级应用系统向云平台迁移。（云平台等级必须高于等于系统等级）

5、不可根据自己的主观意愿来定级 目前的等级保护对象（信息系统）的安全级别分为五个等级：1级为别，5 级为别（5 级为预留级别，市面上已定级的系统为 4 级）。如果定了 1级，不需要做等级测评，自主进行保护即可。定 2 级以上就需要进行等级测评。系统级别的确定需要根据系统的重要性进行决定。如果定高了，有可能造成投资的浪费；定低了则有可能造成重要信息系统得不到应有的保护，应该谨慎定级。

等保 1.0 的要求是自主定级，有主管部门的需要主管部门审核，报送公安机关进行审核。等保 2.0 之后定级流程新增了“ 专家评审 ”和“ 主管部门审核 ”两个环节，这样定级过程将会变得更加规范，定级也会更加准确。

6、系统备案场所 《信息安全等级保护管理办法》规定，等级保护的主体单位为信息系统的运营、使用单位。备案主体一般不会是开发商、系统集成商，而是用户方。

目前有些单位的注册地跟运营地不一致，正常情况下需要去运营地区的网安部门办理备案手续。比如客户注册地在北京海淀区，运营部门在北京朝阳区，需要到北京朝阳区办理定级备案手续，当然，前提是北京朝阳区必须有正规办公地址。

有些单位的系统部署在云平台，云平台的实际物理地址往往和云系统网络运营者不在同一地址。而且，有些单位的运维团队和注册经营地址也不一致。这种情况下，云系统应当在系统实际运维团队所在地市网安部门进行系统备案，因为这样会方便属地公安对系统进行监管。

所以，大部分情况下，还是需要到系统的运维人员实际所在地进行定级备案。当然也有一些特殊行业的要求，比如一些涉及到安全的行业，比如互联网系统、支付系统需要属地化管理，这些系统需要在注册地办理定级备案手续，以满足本地的监管要求。

7、等保测评做完不一定需要花很多钱去整改 整改花多少钱取决于你的信息系统等级、系统现有的安全防护措施状况以及网络运营者对测评分数的期望值，不一定要花很多钱甚至不花钱。

整改的内容大体分为：安全制度完善、安全加固等安全服务以及安全设备的添置。在安全制度及安全加固上网络运营者自己可以做很多整改工作或者委托系统集成方进行加固，往往这是不需要额外付费的或者是包含在你和系统集成方合同约定中的，这两块内容整改好，加上你有一定的安全技术措施，基本上是可以达到基本符合的结论的。所以花多少钱看你怎么去做或者你的期望值是多少。

8、单位如何开展等级保护建设的相关工作？ 等级保护工作是一个系统性工程，根据网络安全等级保护相关标准，等级保护工作总共分五个阶段，分别为：系统定级、系统备案、建设整改、等级测评、监督检查。

（1）系统定级 对拟定为第二级及以上的对象，其运营者应当组织专家评审；有行业主管部门的，应当在专家定级评审后报请主管部门核准；跨省或者全国统一联网运行的网络由行业主管部门统一拟定安全保护等级，统一组织定级评审。

（2）系统备案 定级对象的运营使用单位应准备定级备案材料，材料包括：定级报告、等级保护备案表、单位基本情况、信息系统情况等材料。第二级以上网络运营者应当在定级对象安全保护等级确定后 10 个工作日内，到县级以上公安机关备案。

公安机关在接到备案材料后，于 10
个工作日内完成材料审查，并对定级对象安全等级进行初步审核，并出具网络安全等级保护备案证明。

（3）建设整改 对于新建的等级保护对象，要按照等级保护相关标准，撰写等级保护建设方案，并根据建设方案组织集成实施。

对于已有的等级保护对象，等级保护对象运营使用单位负责对其进行风险评估和整改建设工作，
重要等级保护对象的运营使用单位应形成等级保护整改建设方案，并根据整改方案组织集成建设。

对于三级以上的等级保护对象建设整改方案，要组织专家进行评审，形成专家评审意见，并形成等级保护整改建设方案。

（4）等级测评 等级保护对象的运营使用单位应落实等级测评资金保障工作，同时开展等级测评工作。

等级保护对象建设完成后，运营使用单位或者其主管部门应当选择符合资质要求的第三方测评机构，依据《网络安全等级保护测评要求》等技术标准，定期对等级保护对象开展等级测评。

第三级及以上定级对象应当每年至少进行一次等级测评（等保 1.0 标准里面等级保护四级系统需要每半年一次，现在调整为每年一次），第五级定级对象应当依据特殊安全需求进行等级测评。

9、对于工业控制系统如何开展等级保护工作？
依据等保基本要求中的安全通用要求和工控扩展要求来对工业控制系统开展等级保护工作。

工业控制系统主要包括现场采集 / 执行、现场控制、过程控制和生产管理等特征要素。其中，现场采集 / 执行、现场控制和过程控制等要素应作为一个整体对象定级，各要素不单独定级；生产管理要素可单独定级。

对于大型工业控制系统，可以根据系统功能、责任主体、控制对象和生产厂商等因素划分为多个定级对象。

工控扩展要求保护主要包括：室外控制设备防护、工业控制系统、网络架构安全、拨号使用控制无线使用控制、控制设备安全、漏洞和风险管理、恶意代码防范管理等方面内容。

工业控制系统安全扩展要求主要针对现场控制层和现场设备层提出特殊安全要求，其他层次使用安全通用要求条款，对工业控制系统的保护需要根据实际情况使用基本要求。