LINKS Law Offices
通力律师事务所

上海
上海市银城中路 68 号
时代金融中心 16 楼和 19 楼
邮编：200120
电话：+86 21 3135 8666
传真：+86 21 3135 8600

SHANGHAI
16F/19F, ONE LUJIAZUI
68 Yin Cheng Road Middle
Shanghai 200120 P.R.China
T: +86 21 3135 8666
F: +86 21 3135 8600

北京
北京市建国门北大街 8 号
华润大厦 4 楼
邮编：100005
电话：+86 10 8519 2266
传真：+86 10 8519 2929

BEIJING
4F, China Resources Building
8 Jianguomenbei Avenue
Beijing 100005 P.R.China
T: +86 10 8519 2266
F: +86 10 8519 2929

香港
香港中环皇后大道中 5 号
衡怡大厦 27 楼
电话：+852 2592 1978
传真：+852 2868 0883

HONG KONG
27F, Henley Building
5 Queen's Road Central
Central, Hong Kong
T: +852 2592 1978
F: +852 2868 0883

伦敦
1F, 3 More London Riverside
London SE1 2RE
United Kingdom
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

LONDON
1F, 3 More London Riverside
London SE1 2RE
United Kingdom
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

www.llinkslaw.com
master@llinkslaw.com

公司及并购法律评述
2019 年 5 月

等保 2.0 要点概览及合规建议

作者：潘永建 | 邓梓珊

2019 年 5 月 13 日，在征求意见稿公开近两年半之后，“等保 2.0”国家标准正式公布，并将于 2019 年 12 月 1 日起正式实施。与 1.0 版本相比，等保 2.0 作出了较大幅度的修改，强调主动防御保护机制，并实现保护对象全覆盖。本文将对等保 2.0 体系下的网络安全等级保护制度进行解读，分析前后版本的差异，为企业网络安全等级保护的合规工作提出建议。

一、 等保 2.0 的前世今生

“等保 2.0”全称为《信息安全技术 网络安全等级保护基本要求》(GB/T 22239-2019)。从 2008 年到 2017 年，中国的网络安全等级保护技术主要应用的是“等保 1.0”版本(《信息安全技术 信息系统安全等级保护基本要求》(GB/T 22239-2008))。

随着社会的快速发展，网络已经从单纯的计算机信息系统逐步扩展至云计算、移动互联、物联网、大数据等多个领域，原有的计算机信息系统安全等级保护制度已经不能完全涵盖前述领域。因此，从 2014 年 3 月开始，由公安部牵头组织开展了信息技术新领域等级保护重点标准申报国家标准的工作，并从 2015 年开

如您需要了解我们的出版物，
请与下列人员联系：

郭建良: +86 21 3135 8756
Publication@llinkslaw.com

通力律师事务所
www.llinkslaw.com

始陆续对外发布草稿、征集意见稿，之后便开始有了“等保 2.0”的叫法。随着 2016 年《网络安全法》公布，全国信息安全标准化技术委员会秘书处于同年 11 月 3 日公布了《信息安全技术 网络安全等级保护基本要求(征求意见稿)》(“征求意见稿”)，以求与新的网络环境、新的网络治理法律体系配套。如今，等保 2.0 即为该征求意见稿的正式发布版本。

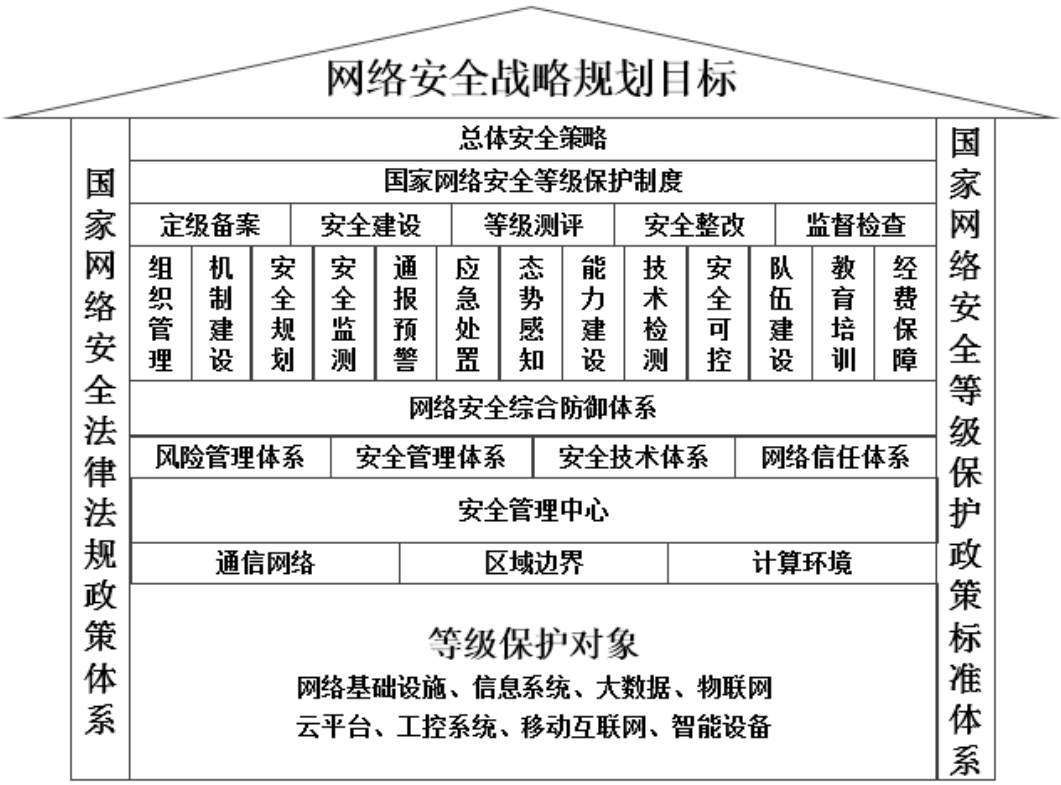
等保 2.0 体系中还包括《信息安全技术 网络安全等级保护测评要求》(GB/T28448-2019)、《信息安全技术 网络安全等级保护安全设计技术要求》(GB/T 25070-2019)等国家标准。

二、 法律效力提升

根据等保 1.0、等保 2.0 的引言以及制定/修改依据，前后两个版本所参照的规范性文件完全不同。以国务院行政法规(《计算机信息系统安全保护条例》)为顶层设计，公安部、国家保密局、国家密码管理局、国务院信息化工作办公室共同发布的部门规范性文件《信息安全等级保护管理办法》确立核心体系的“信息安全等级保护”为等保 1.0 时代；以《网络安全法》、《保守国家秘密法》等法律为顶层设计的等保 2.0，其核心体系将是《网络安全等级保护条例》(已于 2018 年 6 月发布征求意见稿)。

无论是自身法律效力亦或法律依据的效力位阶，等保 2.0 均高于等保 1.0，等保 1.0 到 2.0 不仅仅是制度修订，技术的升级，更是法律效力的提升。

网络安全等级保护制度框架



三、 保护对象范围扩大

等保 1.0 主要应用于传统架构下的信息系统安全，而 2.0 版本的保护范围将从“信息系统”扩展为“网络空间”，且将云计算、大数据、物联网、工业控制系统等新兴技术和应用场景纳入了等级保护范围。相较于征求意见稿，等保 2.0 不再针对不同等保对象制定五个单独标准，而是对所有等保对象采用统一标准，而针对不同等保对象采用序号标识增加扩展要求，具体包括：安全通用要求、云计算安全扩展要求、移动互联安全扩展要求、物联网安全扩展要求以及工业控制系统安全扩展要求。各扩展部分的内容亦有所精简。

对应《信息安全技术 网络安全等级保护定级指南》，定级对象也根据上述扩展要求进行了细化：

1. 云计算平台方面，定级对象分为服务的提供方和租户方；

2. 物联网方面，感知、网络传输和处理应用等特征因素不单独定级，将作为一个整体进行评定；

3. 移动互联方面，移动终端、移动应用、无线网络、相关有线网络业务系统等也将统一定级；

4. 大数据方面，安全责任主体相同的平台和应用将整体定级，除此之外为单独定级。

四、 保护思路变化

等保 1.0 的保护重点更多的关注系统、人员、物理环境的安全，而等保 2.0 的保护重点已经变更为围绕数据、网络、系统、人员的网络空间体系的安全。在等保 2.0 的要求中，已经没有“技术要求”、“管理要求”的表述。可以预见，在未来的网络安全建设中技术、管理将深度融合。在我们接受企业关于网安数据合规咨询时也发现，企业网络安全管理人员不懂技术是寸步难行的，而技术人员不懂管理亦是无法挑起网安合规重任的。如何有效搭建网络安全管理体系，选定符合资质要求的人员进行运维管理将成为企业网络安全合规的关键。

对比等保 1.0，等保 2.0 更为强调了安全运维的概念：在传统的资产管理、设备运维的基础上，将安全运维的范畴扩充到了安全事件的响应和高级安全威胁的发现，如果考虑到定期的审计和有效性验证，安全运维的范畴将进一步扩充。所以我们可以看到，等保 2.0 中所提到的安全运维的概念正在逐步向安全运营的概念转变。

五、 定级与测评要求变化

等级保护是我国信息安全保障的基本制度，是对网络和信息系统按照重要性等级分级别保护的一种制度。安全保护等级越高，要求安全保护能力就越强，既不能保护不足，也不能过度保护。

等保 2.0 体系定级要素与安全保护等级的关系

受侵害客体	对客体的危害程度		
	一般	严重	特别严重
用户自身利益	一级	二级	三级
公众利益、社会秩序	二级	三级	四级
国家安全	三级	四级	五级

相比等保 1.0 要求企业进行“自主定级，自主保护”，等保 2.0 将定级模式修改为“申请批准”。企业应以书面形式说明保护对象的安全保护等级以及确定等级的方法和理由，并组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定，最终报定级结果经过相关部门的批准。

此外，对于基础信息网络、云计算平台、大数据平台等支撑类网络，其安全保护等级原则上应不低于其承载的等级保护对象的安全保护等级。按照这一原则，大数据安全保护等级不低于第三级；对于关键信息基础设施，原则上其安全保护等级不低于第三级。

六、 安全管理机构岗位设置及职能

等保 1.0、等保 2.0 均在“安全管理机构”部分提出了设立网络安全管理工作职能部门的要求，且要求应设立安全主管、安全管理各个方面负责人的岗位，定义各负责人的职责。在等保 2.0 中，主要岗位由“系统管理员”“网络管理员”以及“安全管理员”变更为“系统管理员”“审计管理员”和“安全管理员”，并做出了进一步细化。例如，在新增控制点“安全管理中心”部分，对前述岗位人员的职责、系统接入权限和工作规范设置详细要求:

1. 系统管理

   a) 应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计;

   b) 应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。

2. 审计管理

   a) 应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计;

b) 应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。

3. 安全管理

a) 应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计;

b) 应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。

七、 新增“个人信息保护”要求项

等保 2.0 中新增了个人信息保护的要求。随着欧盟《通用数据保护条例》(GDPR)的出台以及近期个人信息安全事件频发，个人信息保护已经成为执法部门关注的重点。值得企业注意的是，公安部网络安全保卫局、北京网络行业协会、公安部第三研究所于 2019 年 4 月 10 日联合发布了《互联网个人信息安全保护指南》(“《指南》”)在技术要求方面较大程度借鉴了等保 1.0、等保 2.0 的内容。该《指南》是公安机关结合其办理大量真实案例的执法经验，并基于监管过程中掌握的情况而制定的，其不仅可供企业在个人信息保护工作中参考使用，亦可供**网络安全监管职能部门**依法进行个人信息保护**监督检查**时参考使用。因此，虽然关于个人信息保护的部分在等保 2.0 中只有寥寥几语，但严格按照等保技术要求落实个人信息保护仍应引起企业的重视。(关于《指南》的内容及其影响，详见通力法评文章《<互联网个人信息安全保护指南>简评》)

八、 其他主要变化

以《信息安全技术 网络安全等级保护基本要求》及《信息安全技术 信息系统安全等级保护基本要求》规定的三级要求为例，我们概括等保 2.0 的新要求如下。

章节名称	等保 2.0 新要求
技术要求	
安全物理环境部分	明确提出机房视频监控系统的要求，等保 1.0 中未提及。
	防静电要求明确举例说明采用静电消除器、防静电手环；对于静电防护要求更为细节化。
	供电部分不再要求备用供电系统，但保留冗余电力电缆的要求。
	在云计算扩展要求中新增，物理机房必须要在境内。
安全通信网络部分	减少了结构安全、边界完整性检查、网络设备防护三个控制点，增加了网络架构、通信传输两个控制点，增加“可信验证要求”。
	删除了重要系统不能直接外连外部网络的要求，删除了按业务优先级

	分配带宽的 SLA 服务；新标准只要求通信线路、关键网络设备冗余性。
	在边界完整性间检查中，提出了无线网络的安全要求，无线网络接入必须要通过受控边界。
	访问控制中新增内容过滤管理，要求在关键网络节点处对进出网络的信息内容进行过滤，实现对内容的访问控制。
	入侵防范的新要求，能够检测由内对外和由外对内的攻击。
	恶意代码防范的新要求，第一次明确要求对垃圾邮件进行防护。
	日志审计方面要求变化由以前的留存 6 个月改为符合法律法规要求。
安全区域边界	将边界防护、访问控制、入侵防范、恶意代码防范和安全审计整合作为安全区域边界的要求子类，新增可信验证要求项。
安全计算环境	将设备和计算安全、应用和数据安全合并，改为安全计算环境。
	设备计算及安全子类: a) 身份鉴别中两种鉴别方式有明显变化，采用两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用动态口令、密码技术或生物技术来实现。 b) 恶意代码防范要求也有明显变化，应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。
	应用和数据安全子类: a) 减少了通信完整性、通信保密性和抗抵赖三个控制点，增加了个人信息保护控制点。 b) 新增应强制用户首次登录时修改初始口令的要求。 c) 新增用户身份鉴别信息丢失或失效时，应采用技术措施确保鉴别信息重置过程的安全的要求。 d) 新增在故障发生时，应自动保存易失性数据和所有状态，保证系统能够进行恢复的要求。 e) 新增模块，个人信息保护: f) 应仅采集和保存业务必需的用户个人信息; g) 应禁止未授权访问和非法使用用户个人信息。
管理要求	
安全管理中心	新增控制项，包括：系统管理、审计管理、安全管理和集中管控。详细明确了系统管理员、审计管理员和安全管理员的具体职责，强调了岗位的重要性，包括身份鉴别、特殊的操作权限，资源配置等。
安全管理制度	对于制定和发布，不再要求论证和审定过程，不再要求注明发布范围并且收发文要登记，只要控制好版本，正式有效发布即可。 评审和修订，去掉了必须由领导小组进行评审的要求。
安全管理机构	授权和审批方面，去掉了过程文档记录的要求。 沟通合作方面，不再要求要与供应商、专家、安全公司保持沟通，不需

	要每年聘请安全顾问指导安全工作。
安全管理人员	删除人员考核要求。
	新增对外部人员接入网络访问系统的审批要求。
安全建设管理	简化了系统安全方案设计的要求，比如不再要求做系统的近期和长期安全建设计划，不再要求定期调整和修订总体安全策略、框架等配套文件。
	自行软件开发，增加了新的要求点: a) 应确保具备软件设计的相关文档和使用指南，并对文档使用进行控制; b) 应确保在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测; c) 应确保开发人员为专职人员，开发人员的开发活动受到控制、监视和审查。
	强调安全在开发层面的重要性，要求必须进行安全测试。
	简化外包开发、工程实施、测试验收和系统交付的流程。
安全运维管理	资产管理控制点下不再要求建设资产安全管理制度。
	介质管理要求由 6 个要去项缩减为 2 个 a) 应确保介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点; b) 应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。
	设备维护管理要求新增两项: a) 应确保信息处理设备必须经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要数据必须加密; b) 含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，确保该设备上的敏感数据和授权软件无法被恢复重用。
	删除管理和安全管理中心，新增漏洞和风险管理。
	恶意代码防范管理，去除了查杀记录保存的要求，去除了升级、杀毒等过程的分析记录要求；新增一条要求，定期检验技术措施的有效性。
	新增配置管理控制点，要求备份系统配置信息，至少要包含：网络拓扑、设备安装的组件、软件版本和补丁信息、设备和软件的配置参数。

结语

等保 2.0 公布后，与其他制度一起共同构建了中国网络安全等级保护体系。

网络安全等级保护体系	效力层级
《网络安全法》	法律
《网络安全等级保护条例》	行政法规
《网络安全等级保护备案办法》	部门规章
网络安全等级保护国家标准: ➢ 《信息安全技术 网络安全等级保护基本要求》(GB/T 22239-2019) ➢ 《信息安全技术 网络安全等级保护测评要求》(GB/T28448-2019) ➢ 《信息安全技术 网络安全等级保护安全设计技术要求》(GB/T 25070-2019)	国家标准

随着网络安全法执法的深入，网安及等保合规已不仅仅是跨国公司的关注重点，国内企业也日益重视这一领域的合规工作。

以国有企业为例，去年 WannaCry 蠕虫病毒在全球范围大爆发，在数小时内影响近 150 个国家，政府机关、高校、医院都纷纷中招。国家政府、教育、医院、能源、通信、交通等诸多关键信息基础设施对社会稳定运行起关键性作用，但也极易成为不法分子攻击的目标。

随着与中国国企、政企、事业单位有关的网络安全事件频发，国有资产监督管理委员会(“国资委”)在 2019 年 4 月 1 日生效的《中央企业负责人经营业绩考核办法(2019 修订)》中增加了一个全新的业绩考核指标——网络安全事件，以建立重大事项报告制度等为主要表现。企业法定代表人及相关负责人违反国家法律法规和规定，导致发生较大及以上网络安全事件，造成重大不良影响或国有资产损失的，国资委将视具体情节给予降级或扣分处理。

在此背景下，央企需要关注跟进等保 2.0 的新要求，及时开展等级保护工作；同时应确定网络安全负责人，落实网络安全保护责任。关键信息基础设施单位需要额外做好重要系统和数据库的容灾备份工作。

如需进一步信息，请联系:

作　者	
潘永建 电话: +86 21 3135 8701 david.pan@llinkslaw.com	

上　海	
俞卫锋 电话: +86 21 3135 8686 david.yu@llinkslaw.com	**刘贇春** 电话: +86 21 3135 8678 bernie.liu@llinkslaw.com
佘　铭 电话: +86 21 3135 8770 selena.she@llinkslaw.com	**娄斐弘** 电话: +86 21 3135 8783 nicholas.lou@llinkslaw.com
钱大立 电话: +86 21 3135 8676 dali.qian@llinkslaw.com	**孔焕志** 电话: +86 21 3135 8777 kenneth.kong@llinkslaw.com
吴　炜 电话: +86 21 6043 3711 david.wu@llinkslaw.com	**潘永建** 电话: +86 21 3135 8701 david.pan@llinkslaw.com
姜　琳 电话: +86 21 6043 3710 elyn.jiang@llinkslaw.com	
北　京	
俞卫锋 电话: +86 10 8519 2266 david.yu@llinkslaw.com	**刘贇春** 电话: +86 10 8519 2266 bernie.liu@llinkslaw.com
杨玉华 电话: +86 10 8519 1606 yuhua.yang@llinkslaw.com	
香　港(与方緯谷律师事务所联营)	
俞卫锋 电话: +86 21 3135 8686 david.yu@llinkslaw.com	**吕　红** 电话: +86 21 3135 8776 sandra.lu@llinkslaw.com
伦　敦	
杨玉华 电话: +44 (0)20 3283 4337 yuhua.yang@llinkslaw.com	