KPMG

等级保护2.0解读与应对

管理咨询

毕马威中国

—

2019年5月

序言

石浩然
毕马威中国
网络与信息安全咨询
服务主管合伙人

张令琪
毕马威中国
网络与信息安全咨询
服务合伙人

近年来在全球范围频发的众多网络犯罪和网络安全事件让社会对网络安全的关注度达到前所未有的高度。随着网络安全威胁和风险日益突出，中国作为拥有超过8亿网民的网络大国，网络安全已成为关系国计民生的重要影响要素之一。

中国政府已将网络安全提升至国家战略高度，明确提出“没有网络安全就没有国家安全”从立法规范的层面重视强调网络安全工作的重要性。《中华人民共和国网络安全法》（简称“网络安全法”）应运而生，在历时一年多的立法过程后，网络安全法于2016年11月由全国人大表决通过，并已于2017年6月正式生效。

网络安全法是中国首部在网络安全领域的基础性法律, 完善了国家、网络运营者、公民个人等角色的网络安全义务和责任，将原来散见于各种法规、规章中的网络安全规定上升到人大法律层面，并对网络运营者等主体的法律义务和责任进行全面规范。网络安全法第21条明确规定国家实行网络安全等级保护制度。“网络安全等级保护制度”这一概念首次从法律层面被正式提出，将成为国家网络安全基本制度。事实上，网络安全法所提到的网络安全等级保护制度与公安部运营多年的《信息安全等级保护管理办法》（简称“等保管理办法”）有着紧密关联。在《信息安全等级保护管理办法》的基础上，为贯彻落实网络安全法，深入推进实施网络安全等级保护制度，公安部会同有关部门起草了《网络安全等级保护条例（征求意见稿）》（简称“等保条例”），标志着等级保护制度也将进入到2.0时代。

近日，国家市场监督管理总局技术司召开了国标标准新闻发布会，正式发布了等级保护2.0系列国家标准文件（简称“等级保护2.0系列标准”）中的《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》、《GB/T 25070-2019 信息安全技术 网络安全等级保护安全设计技术要求》和《GB/T 28448-2019 信息安全技术 网络安全等级保护测评要求》，可有效指导网络运营者、网络安全企业、网络安全服务机构开展网络安全等级保护工作，全面提升网络运营者的安全保护能力。

© 2019 毕马威企业咨询(中国)有限公司 — 中国外商独资企业，是与瑞士实体 — 毕马威国际合作组织 ("毕马威国际") 相关联的独立成员所网络中的成员。版权所有，不得转载。中国印刷。

目录

© 2019 毕马威企业咨询(中国)有限公司 — 中国外商独资企业，是与瑞士实体 — 毕马威国际合作组织 ("毕马威国际") 相关联的独立成员所网络中的成员。版权所有，不得转载。中国印刷。

等级保护发展历程

1994

国务院颁布《中华人民共和国计算机信息系统安全保护条例》

2007

《信息安全等级保护管理办法》(公通字【2007】43号）正式发布

2008-2012

等级保护1.0系列国家标准陆续发布

2014

网络安全和信息化工作座谈会（4.19讲话）

2017

《中华人民共和国网络安全法》正式实施，且等级保护2.0国家标准草稿陆续发布

2018

《网络安全等级保护条例（征求意见稿）》公开征求意见，等级保护2.0国家标准征求意见稿陆续发布，且《公安机关互联网安全监督检查规定》（公安部第151号）正式发布

2019

等级保护2.0核心国家标准于2019年5月13日正式发布，并将于2019年12月1日正式实施

《中华人民共和国网络安全法》第21条：“国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改……”

© 2019 毕马威企业咨询(中国)有限公司 — 中国外商独资企业，是与瑞士实体 — 毕马威国际合作组织 ("毕马威国际") 相关联的独立成员所网络中的成员。版权所有，不得转载。中国印刷。

等级保护2.0带来的挑战

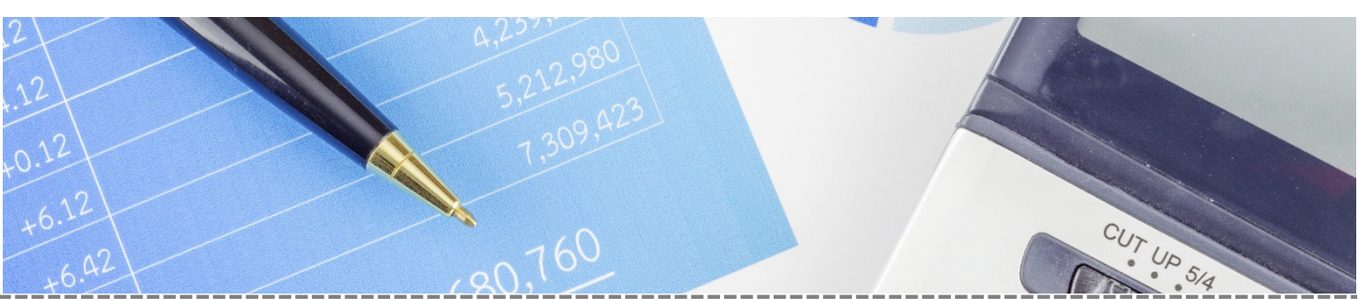
等级保护2.0是什么？

> “等保管理办法作为规范性文件，适用范围以政府部门和重点行业为主。等保条例作为条例，具备法律效力，适用于对在中国境内建设、运营、维护、使用网络的监督管理。”

对接网络安全法：《网络安全等级保护条例（征求意见稿）》（简称“等保条例”）是依据网络安全法第21条“国家实行网络安全等级保护制度”的要求制定的行政法规，其与等级保护2.0系列国家标准文件（简称“等级保护2.0系列标准”），均为确立网络安全等级保护制度的重要配套法规。等保条例为保障国家网络空间安全，维护社会公共利益、保护公民、法人的合法权益，以及应对新技术、新应用所带来的安全风险，要求网络运营者对其网络和信息系统分等级实行安全保护。等级保护2.0更加强调安全保护能力，即能够抵御威胁、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度。网络运营者应保证其不同安全保护等级的对象具有相应级别的安全保护能力。

网络“取代”系统：等保条例中所约定的“网络”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、交换、处理的系统。因此，等保条例关注的网络安全也分为“基础设施安全、运行安全、数据安全”三个层面，进而可以明确为不同的安全责任主体、不同的业务模式和系统运营方式、以及不同的安全保障方法。

监管体系加强：依据等保条例，国家网信部门负责网络安全等保工作的统筹协调，公安部门负责网络安全等级保护工作的监督管理。对网络运营者而言，等级保护工作主管部门即为法人实体所在地的公安部门。网络运营者应参照等级保护2.0相关标准的要求：1）梳理出定级对象并合理确定其安全保护等级、安全责任单位和具体责任人；2）开展网络定级备案、安全建设整改、等级测评和自查等工作；3）落实相关管理和技术措施，履行安全保护义务。



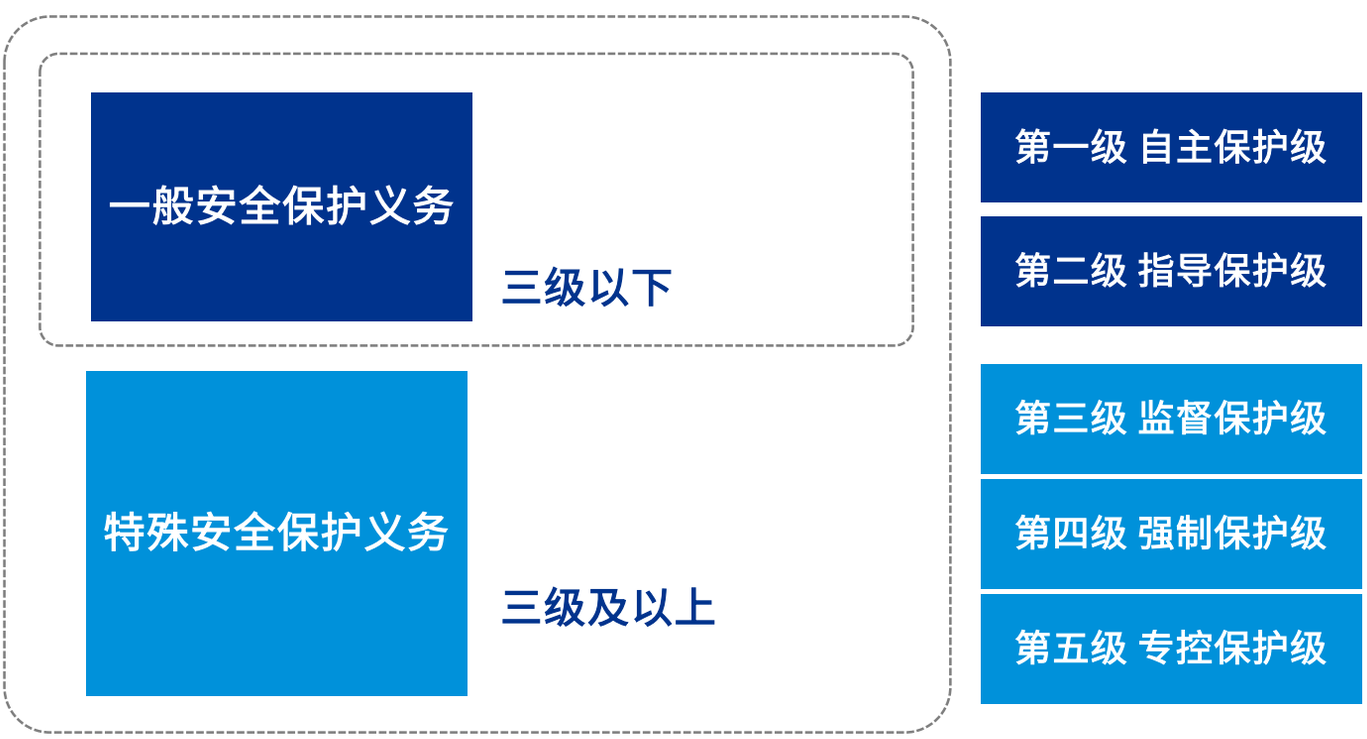
© 2019 毕马威企业咨询(中国)有限公司 — 中国外商独资企业，是与瑞士实体 — 毕马威国际合作组织 ("毕马威国际") 相关联的独立成员所网络中的成员。版权所有，不得转载。中国印刷。

网络运营者的安全保护义务

等保条例在网络安全法规定的网络运营者安全保护义务的基础上，对网络运营者针对不同安全保护等级网络的安全保护义务作了明确、细化的要求，这是等级保护2.0作为“条例”的新变化，既是公安部门的监管重点，也是网络运营者等保建设和测评的重点。

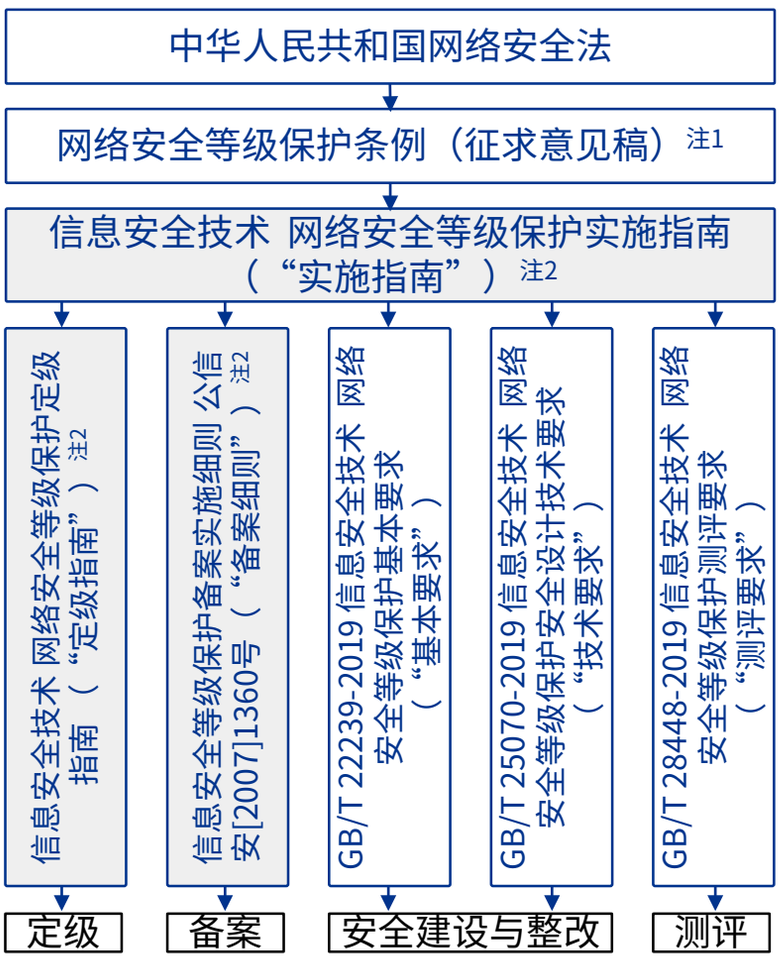
条例第20条详细规定了网络运营者应当依法履行的11项一般性安全保护义务，其中：确定安全责任人、建立和落实安全管理制度和安全技术措施、网络安全监测和网络安全事件管理、数据分类保护、个人信息保护、联网备案和实名制等，均属于基础性工作，也都是合规和监管的重点。

条例第21条详细规定了三级及以上网络的网络运营者应当依法履行的8项特殊安全保护义务，其中：制定并落实网络安全规划、网络安全管理负责人和关键岗位的人员安全背景审查、网络安全监测预警和管理平台、落实备份和恢复措施、定期开展等级测评等，更强调体系、人员、工具这些安全保护要素，也都是合规和监管的重点。



© 2019 毕马威企业咨询(中国)有限公司 — 中国外商独资企业，是与瑞士实体 — 毕马威国际合作组织 ("毕马威国际") 相关联的独立成员所网络中的成员。版权所有，不得转载。中国印刷。

等级保护2.0政策标准体系



注1：在《信息安全等级保护管理办法》的基础上，公安部会同有关部门起草了《网络安全等级保护条例（征求意见稿）》。《信息安全等级保护管理办法》为现行有效的管理办法，《网络安全等级保护条例（征求意见稿）》为新条例，目前仍在公开征求意见中。
注2：部分等保2.0系列国家标准仍在进一步修订并将陆续发布。

实施指南 – 规定了等级保护工作实施过程中的各相关方角色、基本流程和具体实施要求。等保工作的基本流程包括：定级和备案、安全规划、安全设计与实施、安全运行和维护、应急响应与保障、定级对象终止。

定级指南 – 规定了网络安全等级保护的定级方法和定级流程，新的标准中除了对定级矩阵、定级流程进行了更新之外，还增加了云计算、移动互联、物联网、工业控制系统、大数据等特定定级对象定级说明。

备案细则 – 规定了备案受理、审核和管理等流程，加强和指导等级保护备案工作。

基本要求 – 规定了第一级到第四级等级保护对象的安全通用要求和安全扩展要求，是一份由详细的安全控制要求组成的安全基线，适用于指导分等级的非涉密对象的安全建设和监督管理。

技术要求 – 规定了第一级到第四级等级保护安全设计的技术要求，适用于指导系统运营使用单位、信息安全企业、信息安全服务机构开展网络安全等级保护安全技术方案的设计和实施，也可作为信息安全职能部门进行监督、检查和指导的依据。

测评要求 – 规定了第一级到第四级等级保护对象的安全通用测评要求，以及移动互联、大数据、云计算、物联网和工业控制等新技术、新应用的保护对象的安全扩展测评要求。

与现行公安部门颁布的法规的关系

《公安机关互联网安全监督检查规定》、《计算机信息网络国际联网安全保护管理办法》是公安部门为加强对计算机信息网络国际联网的安全保护，预防网络违法犯罪，维护公共秩序和社会稳定制定的法规文件。等级保护2.0与现行法规相辅相成，均为国家网络安全的保障，因此网络运营者也应遵循现行公安部门颁布的相关法规。

与关键信息基础设施保护的关系

《网络安全等级保护条例》、《关键信息基础设施安全保护条例（征求意见稿）》（简称“关保条例”）是网络安全法最主要的支持性法律文件。两者分别对应的是《网络安全法》的第21条和第31条，所有的网络运营者均应遵守等保条例及相关标准要求，而关键信息基础设施运营者除了要满足等保要求之外，还需要遵守关保条例及相关标准要求，实行重点保护。等保条例作为网络安全保障领域一项普适性的基本制度，是关键信息基础设施保护的基础，所以在等保条例中并未直接提及“关键信息基础设施”，但是关键信息基础设施的安全保护等级建议不能低于三级。

© 2019 毕马威企业咨询(中国)有限公司 — 中国外商独资企业，是与瑞士实体 — 毕马威国际合作组织 ("毕马威国际") 相关联的独立成员所网络中的成员。版权所有，不得转载。中国印刷。

等级保护2.0主要变化与实施要点

等级保护2.0在监管和实施流程上与等级保护1.0相比有较大的变化，整体体现为“宽”和“严”两个字。

监管范围和手段拓宽

等级保护2.0监管范围将从传统的网络信息系统拓宽到网络基础设施、重要信息系统、网站、大数据中心、云计算平台、物联网、工控系统、公众服务平台、移动互联等。与之对应的监管手段，除了定级备案和等级测评之外，增加了更多的执法检查手段，如：远程监测、现场检查、事件调查、负责人约谈、责令整改、通报处罚、紧急断网等。

监管内容和强度趋严

无论从流程还是要求上，等级保护2.0均比等级保护1.0有较大提升，尤其是针对原先的第二级网络，有了更明确具体的实施要求，如“个人信息保护”，对第三级以上网络则较大程度地融合了网络安全法和关键信息基础设施保护条例中关于“网络产品和服务安全”、“系统境内维护”等特定要求。

© 2019 毕马威企业咨询(中国)有限公司 — 中国外商独资企业，是与瑞士实体 — 毕马威国际合作组织 ("毕马威国际") 相关联的独立成员所网络中的成员。版权所有，不得转载。中国印刷。

等级保护2.0新增或加强的内容主要包括：

01/ 等级确定

- 等级保护2.0的信息系统安全保护等级矩阵表和业务信息安全保护等级矩阵表中，均将“对公民、法人和其他组织的合法权益侵害造成特别严重损害”的保护等级从“第二级”修改为“第三级”。 因此网络运营者需要客观评估其定级对象受到破坏时所侵害的客体，以及对客体可能造成的侵害程度（如：业务能力下降、引起法律纠纷、导致财产损失、造成社会不良影响等）。
- 等级保护1.0仅要求第三级及以上系统的等级确定应组织专家评审，而等级保护2.0则要求第二级系统的等级确定也应组织专家评审。

02/ 新技术新应用的风险管控

- 等级保护2.0要求网络运营者充分评估其所采用的云计算、大数据、人工智能、物联网、工控系统和移动互联等新技术、新应用带来的安全风险，并参照等保2.0系列国家标准，在“通用要求”的基础上，依据相应的“扩展要求”，采取安全管控措施，保护新技术、新应用。

03/ 个人信息安全保护

- 等级保护1.0约定了数据安全方面的通用要求，而等级保护2.0遵循《网络安全法》明确了 “个人信息保护”相关管理要求，明确网络运营者应建立并落实个人信息安全保护制度，在数据生命周期各个环节采取安全保护措施。此外，个人信息保护的具体要求可以参照《个人信息安全规范》、《个人信息安全影响评估指南（征求意见稿）》等国家标准。

04/ 网络产品和服务 （三级及以上）

- 等保条例依据《网络产品和服务安全审查办法（试行）》和《网络关键设备和网络安全专用产品目录》，要求第三级及以上网络的网络运营者应采用与其安全保护等级相适应的网络产品和服务，对重要部位使用的网络产品应通过专业机构的测评或认证。此外，等级保护2.0系列国标也提出了信息安全产品和密码产品与服务的采购和使用应符合国家有关规定的要求。因此，网络运营者必须明确自己采购、使用或租用的产品的合规情况，以及外部网络服务提供者的相关资质，了解可能存在的安全风险。

05/ 安全管理中心 （二级及以上）

- 等级保护2.0明确将“安全管理中心”作为5大技术领域之一，充分体现“一个中心（安全管理中心）和三重防御（安全通信网络、安全区域边界和安全计算环境）”的思想：二级的“安全管理中心”包含“系统管理”和“审计管理”相关要求；三级及以上的“安全管理中心”包含了“系统管理”、“审计管理”和“安全管理”等相关要求。

© 2019 毕马威企业咨询(中国)有限公司 — 中国外商独资企业，是与瑞士实体 — 毕马威国际合作组织 ("毕马威国际") 相关联的独立成员所网络中的成员。版权所有，不得转载。中国印刷。

06/ 可信验证

- 等级保护2.0基本要求中，从一级到四级的“安全通信网络”、“安全区域边界”和“安全计算环境”中均新增了部分“可信验证”控制点，建议在关键执行环节开展动态可信验证，并进行有效的跟进处置和记录。

07/ 上线检测

- 等保条例新增第二级及以上系统上线检测要求，新建的第二级网络上线运行前应当按照网络安全等级保护有关标准规范，对网络的安全性进行测试，公安部门有权要求提供检测报告。

08/ 技术维护（三级及以上）

- 等保条例要求第三级及以上网络应当在境内实施技术维护，不得境外远程技术维护。因业务需要，确需进行境外远程技术维护的，应当进行网络安全评估，并采取风险管控措施。实施技术维护，应当记录并留存技术维护日志，并在公安机关检查时如实提供。因此，对于网络运营者而言，第三级及以上网络的保护强度事实上类同于关键信息基础设施的保护要求。

09/ 安全自查

- 等保条例新增要求网络运营者应当每年对本单位落实网络安全等级保护制度情况和网络安全状况至少开展一次自查，发现安全风险隐患及时整改，并向备案的公安机关报告。因此，这将成为网络运营者的日常安全工作之一。此外，公安机关对拥有三级及以上网络的网络运营者每年至少开展一次安全检查。

10/ 检测预警和事件通报（三级及以上）

- 等保条例要求三级及以上网络的网络运营者应当建立健全网络安全监测预警和信息通报制度，按照规定向同级公安部门报送网络安全监测预警信息，报告网络安全事件。因此，网络运营者在其网络安全管理制度中，应结合网络安全应急预案，制定合理的事件分类分级策略和处置流程，并建立与公安部门的通报路径。

© 2019 毕马威企业咨询(中国)有限公司 — 中国外商独资企业，是与瑞士实体 — 毕马威国际合作组织 ("毕马威国际") 相关联的独立成员所网络中的成员。版权所有，不得转载。中国印刷。

等级保护合规建议

等级保护是国家信息安全保障工作的基本制度；是督促合规性要求，开展网络安全工作的基本方法；是促进信息化、维护网络安全的根本保障。企业必须在系统建设、改造完成后，选择具备资质的测评机构，依据网络安全等级保护合规性要求，开展等级保护建设工作，以有效规避企业所面临的网络安全风险。

我们建议的等级保护合规路径如下：

等级保护合规路径

01 系统梳理和定级

- 基于企业运营现状和规划开展内部系统梳理，识别并形成系统清单
- 根据等级保护相关要求，按业务重要程度、系统对外服务可用性、数据的类型和规模等要素，梳理网络和系统及其边界，明确信息安全责任主体和定级对象，对内部系统进行初步定级

02 自查整改

- 根据确定的定级对象和对应级别，参照等级保护相关要求，进行差距分析，形成自查报告
- 针对不符合项，确定整改策略，开展整改工作，包括技术措施落实和管理制度完善等
- 按需开展网络安全法相关要求的合规性评估、风险评估和技术检测等，作为等级保护合规的必要补充

03 第三方测评和备案

- 按要求编制定级报告，并组织必要的外部专家评审（二级及以上），完成主管部门审核（如有）后，进一步完成公安部门备案
- 选择公安部授权的测评机构开展测评，根据初测结论进行安全整改，并通过复测以获得备案证明（三级及以上）
- 三级系统要求每年需测评1次，二级系统建议每2年测评1次

04 持续改进

- 围绕信息安全治理目标，结合等保工作发现，制定安全规划，明确网络安全工作任务，以及各项任务的优先级、成本和资源
- 参照等级保护2.0和行业最佳实践，完善网络安全技术保障体系（识别、保护、检测、响应、恢复等），并按要求定期开展年度测评工作
- 持续关注网络安全法及相关法律、政策、标准的动态，及时对应新的监管要求

© 2019 毕马威企业咨询(中国)有限公司 — 中国外商独资企业，是与瑞士实体 — 毕马威国际合作组织 ("毕马威国际") 相关联的独立成员所网络中的成员。版权所有，不得转载。中国印刷。

毕马威中国网络安全服务

网络安全服务概览

战略及治理	安全转型	网络防御	网络响应
帮助您了解如何更好地将网络安全管理工作与动态业务和合规性优先事项保持一致。	在正确的组织和技术支持下，帮助您构建及完善程序和流程，从而改善网络安全管理工作。	通过对持续变化的安全风险提供更有效的可视化管理和分析，帮助您在业务和技术持续发展过程中有效落实网络安全管理工作。	帮助您有效并高效地应对网络安全事件，并进行法证分析及详细调查。

安全事件发生前 → 安全事件发生后

毕马威网络安全团队**从您的角度**看待网络安全管理工作，为不同级别的组织提供网络安全管理的业务背景。

帮助您实现网络安全管理转型，促使网络安全管理为业务发展赋能，使您能够充分了解，设立优先序，并有效管理网络安全风险；控制不确定性，提高灵活性并将风险转化为优势。

© 2019 毕马威企业咨询(中国)有限公司 — 中国外商独资企业，是与瑞士实体 — 毕马威国际合作组织 ("毕马威国际") 相关联的独立成员所网络中的成员。版权所有，不得转载。中国印刷。

等级保护合规咨询服务

现状梳理与差距评估	基于等级保护2.0相关合规要求，协助企业开展现状梳理，形成定级备案的基础材料和输入，并据此开展进一步差距评估与风险分析，识别现有差异，依据风险评估结果和企业实际安全管理、业务和技术运营要求，制定和明确整改策略和方案。
制度体系优化与技术措施改进	基于等级保护2.0相关合规要求，结合企业的业务和技术现状及发展战略，参考其他适用的行业标准和最佳实践，开展网络安全管理制度体系的优化与技术措施改进工作，协助企业搭建既符合监管要求，又具备落地可行性的网络安全管理体系，形成并归档测评和备案所需的制度文档，操作手册，执行记录等。
项目管理与辅导协助	在企业开展等级保护系统梳理和定级、自查整改、第三方测评和备案、持续改进等合规工作的过程中，为企业提供项目管理与辅导，协助企业进行内部、外部各利益相关者的协调和沟通，进行定级、备案、测评所需材料准备辅导，助力企业有效达成合规目标。

毕马威的优势

全球化的专业团队： 毕马威全球网络有助于协助企业在进行网络安全管理体系的本地化建设过程中充分考虑企业现有的全球化管理机制与体系。

丰富的实施经验： 毕马威团队拥有丰富的网络安全法合规、等级保护合规、信息安全管理体系、数据安全合规管理等方面有丰富的实施经验，已辅导多家企业成功通过等级保护3级测评与备案。

良好的资源体系： 毕马威已建立与网络安全国家与地方监管部门、行业主管部门、第三方检测和认证机构的紧密联系，参与国家和行业信息安全和信息化政策研讨和标准制定，初步形成涵盖网络安全产品和服务提供商、行业和领域专家的生态圈，有能力为企业带来更多本地合规的增值服务。

© 2019 毕马威企业咨询(中国)有限公司 — 中国外商独资企业，是与瑞士实体 — 毕马威国际合作组织 ("毕马威国际") 相关联的独立成员所网络中的成员。版权所有，不得转载。中国印刷。

联系我们

石浩然
毕马威中国
网络与信息安全咨询
服务主管合伙人
Tel: +852 2143 8799
henry.shek@kpmg.com

张令琪
毕马威中国
网络与信息安全咨询
服务合伙人
Tel: +86 (21) 2212 3637
richard.zhang@kpmg.com

赫荣科
毕马威中国
网络与信息安全咨询
服务合伙人
Tel: +86 (755) 2547 1129
jason.rk.he@kpmg.com

黄财明
毕马威中国
网络与信息安全咨询
总监
Tel: +852 2140 2823
patrick.c.wong@kpmg.com

Bhagya Perera
毕马威中国
网络与信息安全咨询
总监
Tel: +852 2140 2825
bhagya.perera@kpmg.com

张倪海
毕马威中国
网络与信息安全咨询
副总监
Tel: +852 2847 5062
brian.cheung@kpmg.com

邬敏华
毕马威中国
网络与信息安全咨询
副总监
Tel: +86 (21) 2212 3180
fm.wu@kpmg.com

李振
毕马威中国
网络与信息安全咨询
副总监
Tel: +86 (10) 8508 5497
jz.li@kpmg.com

沈俊伟
毕马威中国
网络与信息安全咨询
副总监
Tel: +852 2847 5044
darryl.sim@kpmg.com

周文韬
毕马威中国
网络与信息安全咨询
副总监
Tel: +86 (21) 2212 3149
kevin.wt.zhou@kpmg.com

罗圣涛
毕马威中国
网络与信息安全咨询
副总监
Tel: +86 (755) 2547 3421
stuart.luo@kpmg.com

黄芃芃
毕马威中国
网络与信息安全咨询
副总监
Tel: +86 (21) 2212 2355
quin.huang@kpmg.com

郝长伟
毕马威中国
网络与信息安全咨询
副总监
Tel: +86 (10) 8508 5498
danny.hao@kpmg.com

kpmg.com/cn

所载资料仅供一般参考用，并非针对任何个人或团体的个别情况而提供。虽然本所已致力提供准确和及时的资料，但本所不能保证这些资料在阁下收取时或日后仍然准确。任何人士不应在没有详细考虑相关的情况及获取适当的专业意见下依据所载资料行事。

© 2019 毕马威企业咨询 (中国) 有限公司 — 中国外商独资企业，是与瑞士实体 — 毕马威国际合作组织 (“毕马威国际”) 相关联的独立成员所网络中的成员。版权所有，不得转载。中国印刷。

毕马威的名称和标识均属于毕马威国际的商标或注册商标。