微软《网络安全法》解读手册

2018 年 2 月 第一版

《微软<网络安全法>合规手册》之编撰目的是为了帮助微软（中国）销售团队对《中华人民共和国网络安全法》进行基础的学习，并帮助其掌握《网络安全法》的基本、核心制度要求，从而协助客户更好的落实《网络安全法》中规定的合规义务。

本手册是微软（中国）在学习并研究《网络安全法》及配套的法律法规后，根据公司自身情况总结而成，仅作为微软（中国）内部资料参考使用，不构成对客户的法律意见。

对于《网络安全法》中涉及的具体法律问题及合规要求，建议客户根据企业自身情况，并咨询客户自己的法律部门、外部律师或相关行业主管部门再做决定。

本手册相关内容根据 2018 年 1 月 30 日前发布的相关法律法规、规范性文件、国家标准及相关草案而编写，将根据立法发展不时更新。

目录

一、 《网络安全法》立法背景

《网安法》的颁布和生效

2013 年美国斯诺登事件的爆发，暴露了全球网络社会安全管理中面临的严峻形势。各国政府对于网络安全问题愈加重视，中国政府也不例外。自 2013 年起，中国在国家战略、政府机构设置、立法执法等方面全面重视和强调网络安全管理。并于 2016 年 11 月颁布《中华人民共和国网络安全法》（“《网安法》”），该法于 2017 年 6 月 1 日起生效施行。《网安法》的通过与生效，意味着中国在信息化时代的网络安全方面有法可依，并将开启一个网络安全监管的新纪元。

既然《网安法》已经生效了，其中的所有的规定是否需要立即执行

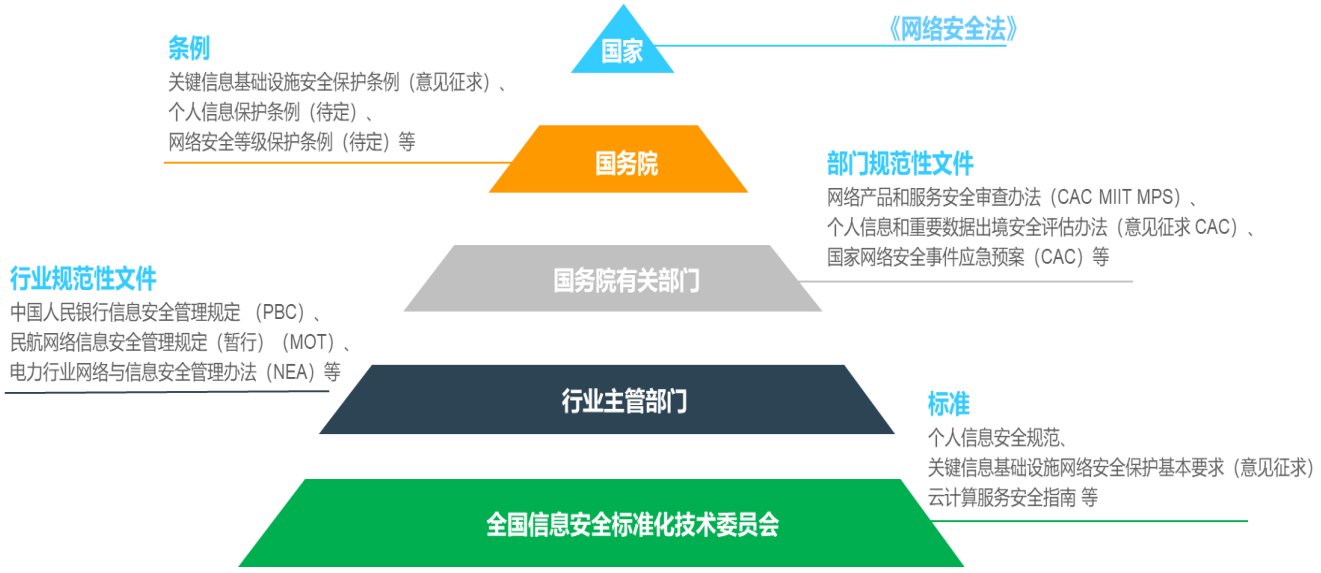
值得注意的是，《网安法》仅就网络安全的管理和保护提出了框架性的原则，这些原则是国家加强对网络空间安全管理的顶层设计，需要更具体的实施办法加以落实。根据《网安法》的规定，关于关键信息基础设施、数据本地化储存以及应急响应等制度，应当由政府有关部门在《网安法》实施的一年内做出配套规定。目前，国家相关部门已经出台了一部分的实施细则和国家标准，但部分细则和国家标准尚未出台或仅仅停留在草案阶段，有待进一步明确。因此，在实践中，由于缺乏具体可操作的细则，《网安法》的部分规定（例如数据出境安全评估）目前实际上还未能得到真正的执行。

在《网安法》体系（见下图）不断完善的过程中，一些尚未生效的细则或标准可能被有关部门作为试点执法的参考使用，因此我们建议在《网安法》体系完善的过程中，企业应跟踪立法动态，逐步完成合规要求。

既然很多细则都还没明确，本手册编写的依据是什么

本手册相关内容根据 2018 年 1 月 30 日前发布的相关法律法规、规范性文件、国家标准及相关草案而编写。其中一部分是尚未生效的草案，这些草案在最终生效前可能会被修订。如果将来相关草案发生变更，则本手册相关内容需要做相应调整。

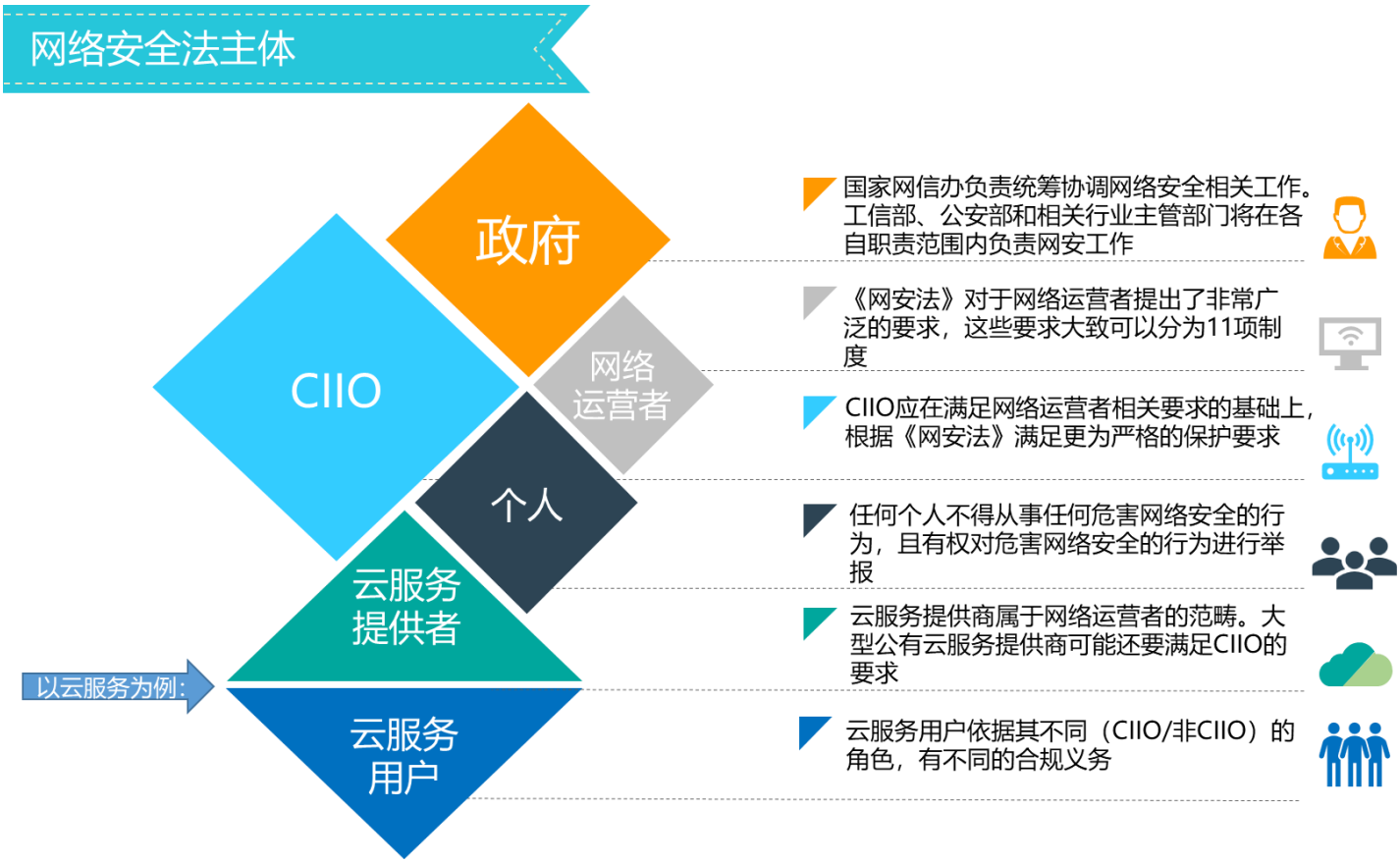
网络安全法法律体系



注：CAC-中华人民共和国国家互联网信息办公室；MIIT-中华人民共和国工业与信息化部；MPS-中华人民共和国公安部；MOT-中华人民共和国交通运输部；PBC-中国人民银行；NEA-国家能源局

二、 《网安法》的不同责任主体

我们根据《网安法》的规定，按照法律中涉及的不同责任主体，对其各自义务进行了归纳总结。



网络运营者

网络运营者定义：网络运营者的范围非常之广。任何拥有、管理网络或提供网络服务的个人或实体都属于《网安法》下网络运营者的概念，从而被要求满足《网安法》对于网络运营者提出的规定。

《网安法》对于网络运营者提出了非常广泛的要求，体现在《网安法》中的 10 项制度：

（1）网络安全等级保护制度；
（2）个人信息保护制度；
（3）安全认证和检测制度；
（4）网络安全审查制度；
（5）监测预警和信息通报制度；
（6）应急处置制度；
（7）网络运行安全保护制度；
（8）网络信息安全保护制度；

如果网络运营者属于关键基础设施运营者，那么其还应满足以下制度：

（9）关键信息基础设施保护制度；
（10）数据本地存储和出境安全评估制度。

关键信息基础设施运营者（CIIO）

关键信息基础设施的英文通常翻译为“Critical Information Infrastructure”，业内通常简称为“CII”。关键信息基础设施运营者英文通常称为“CII Operator”，简称为“CIIO”。

关键信息基础设施的运营者定义：关键信息基础设施的运营者是运营事关国家安全、国计民生、公共利益的重要网络设施的网络运营者。

CIIO 除了需要满足网络运营者的相关要求外，由于 CII 的重要性，《网安法》在以下方面：

（1）数据本地存储和出境安全评估；
（2）网络安全等级保护；
（3）网络安全审查；
（4）容灾备份；

（5）远程维护；
（6）保密协议等
提出了比一般网络经营者更为严格的保护要求。

以云服务为例

如何判定云服务提供商和云服务用户在网安法下的主体责任

- 云服务提供商
  云服务提供商属于网络运营者的范畴。另外，大型公有云（例如 Microsoft Azure）的服务提供商很有可能会被认定为是 CIIO。因此，大型公有云服务提供商通常不仅要满足一般网络运营者的要求，还要满足 CIIO 的要求。

- 云服务用户
  云服务用户依据其不同的角色，有不同的合规义务。如果某一用户自身是 CIIO，那么这一用户需要满足网安法对于 CIIO 的特别规定。如果某一用户自身只是一般的网络运营者而非 CIIO，那么这一用户满足网安法对于网络运营者一般的规定即可。

- 政府

政府不仅负责相关的审查和批准，例如网络安全审查以及针对某些产品的安全认证和检测，还负责对国家的网络安全运行进行监测。一个网络运营者是否为 CIIO，是由政府来认定的。

- 个人

任何个人不得从事任何危害网络安全的行为，且有权对危害网络安全的行为进行举报。

三、 《网络安全法》中的重要制度和要求

《网安法》中涉及的制度重点关注了网络运行安全和网络信息安全。其中网络运行安全中设立的重点制度主要包括关键信息基础设施保护制度、数据本地储存和离境安全评估制度以及等级保护制度等，而网络信息安全则规定了个人信息保护制度和违法有害信息的发现处置制度。

对于这些重要制度，《网安法》根据不同的主体做出了不同的义务要求，其中以 CIIO 与非 CIIO 为例，我们总结了下表进行对比。

	数据本地存储	数据出境安全评估	网络安全等级保护	网络安全审	安全认证和检测	用户及个人信息保护	监测预警和信息通报	应急处置	网络运行安全保护	网络信息安全	网络内容管理	容灾备份	不能远程维护	保密协议
CIIO	适用	需要审批	等保3级*	可能性高	适用	适用	适用	适用	适用	适用	适用	适用	适用*	适用
非CIIO	不强制	某些情况下上报政府*	视情况	可能性低	适用	适用	适用	适用	适用	适用	适用	不强制	不强制	不强制

注：根据现有草案和资料总结

- **网络运营者（即非 CIIO）要承担的义务大致可以分为 10 个方面：**

数据存储和数据出境安全评估：对于非 CIIO 而言，对于其掌握的重要数据和个人信息在通过安全评估的前提下，可以直接传输至境外，而无需在中国本地存储。
根据目前数据出境方面法规的相关草案，对于非 CIIO 的数据出境安全评估来说，如果出境传输的个人信息如果在一年内超过 50 万个人或者出境传输的内容涉及某些敏感数据，则应当将评估结果上报政府。目前尚不明确该等上报是否需要经政府审批。

网络安全等级保护：非 CIIO 需要对其运营的信息系统确定安全保护等级，并采取相应的安全保护措施。

用户及个人信息保护：《网安法》要求网络运营者必须切实保护用户及个人信息。

安全认证和检测：网络运营者使用的某些关键设备和安全专用产品必须通过国家要求的安全认证或安全检测。

网络安全审查：如果网络运营者采购的网络产品或服务有可能影响到国家安全，这种采购行为可能会被要求通过国家的网络安全审查 。是否影响国家安全，由国家相关机关结合具体情况具体掌握。相对 CIIO 来说，非 CIIO 采购行为被要求通过网络安全审查的可能性较低。

监测预警和信息通报：国家将建立网络安全监测预警和信息通报制度。网络运营者应当配合国家，及时报告网络安全信息。

应急处置：网络运营者应当制定网络安全事件的应急预案。一旦发生网络安全事件，网络运营者应当采取相应的措施，及时进行处置。

网络运行安全保护：网络运营者应当履行安全保护义务（例如将网络日志留存至少 6 个月，以及及时处置漏洞等），确保网络的安全运行。

网络信息安全保护：网络运营者应当履行信息安全保护义务(例如采取技术措施防止信息泄露、损毁、丢失等)，确保网络信息安全。

网络内容管理：网络运营者应当确保通过网络传播的内容符合国家法律的规定。任何人不得利用网络传播政府禁止的内容。

- **CIIO 除了要承担网络运营者的相关义务外，还需要对其运营的 CII 尽到特别的保护义务，其中比较重要的要求如下：**

数据本地存储和出境安全评估：对于 CIIO 而言，无论它是否能通过数据出境安全评估，其在境内运营中收集和产生的重要数据和个人信息都必须要在中国境内存储。此外，根据目前数据出境方面法规的相关草案，CIIO 的数据出境安全评估需要经过政府审批。

网络安全等级保护：CIIO 对 CII 的保护要以网络安全等级保护制度为基础。将来，CII 有可能被要求通过不低于等保 3 级的安全测评。

网络安全审查：如果网络运营者采购的网络产品或服务有可能影响到国家安全，这种采购行为可能会被要求通过国家的网络安全审查。是否影响国家安全，由国家相关机关结合具体情况具体掌握。相较非 CIIO 而言，CIIO 被要求进行安全审查的可能性更高。

容灾备份：CIIO 应当对重要系统和数据库进行容灾备份。

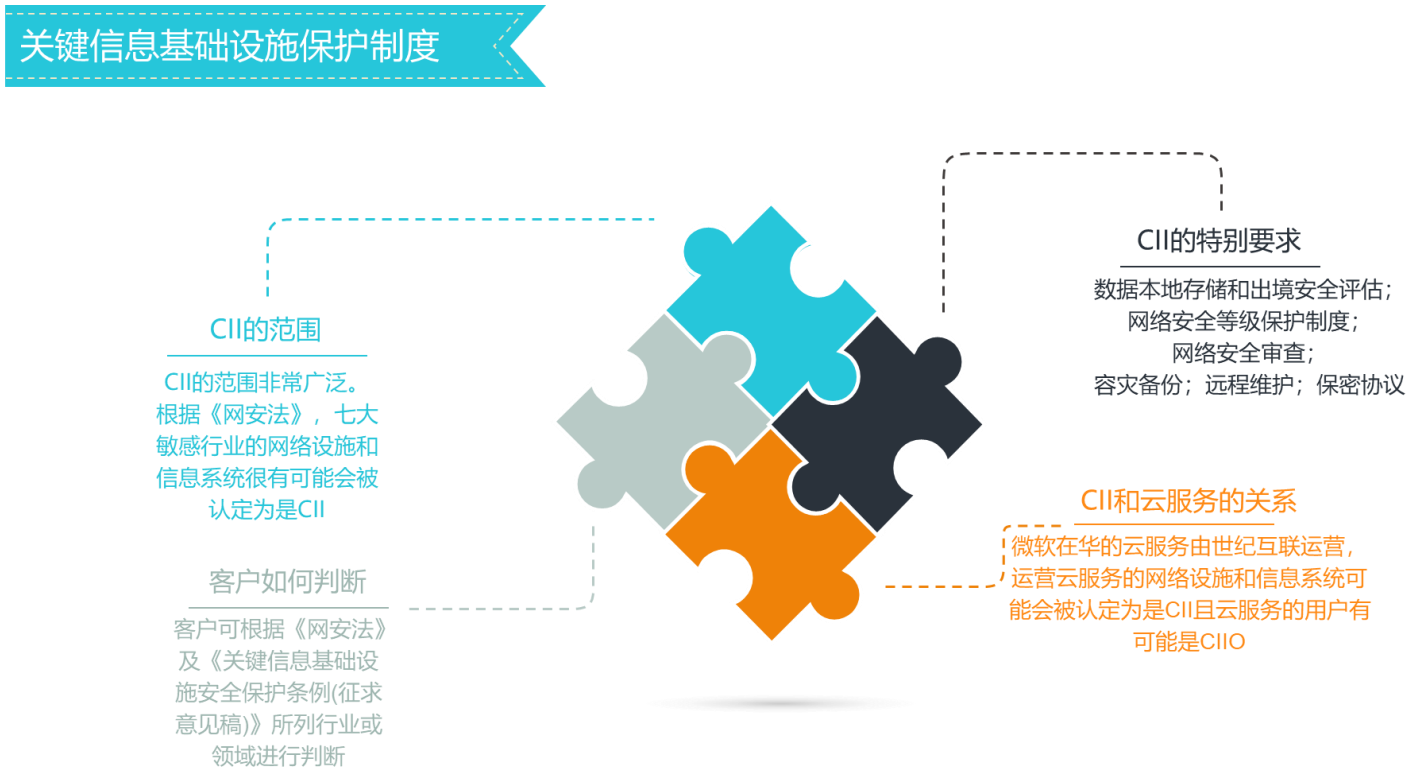
远程维护：根据目前数据出境方面法规的相关草案，对于 CII 的维护应当在中国境内进行。如果需要进行境外远程维护的，需要事先上报政府。

保密协议：CIIO 采购网络产品和服务，应当和供应商签署保密协议。

下面我们在关键信息基础设施保护制度、数据本地化储存和离境安全评估制度、等级保护制度以及个人信息保护制度这四个方面着重进行介绍，并在本章最后一部分对其他重点制度做简单的归纳总结。

A. 关键信息基础设施保护制度

“关键信息基础设施”，亦即“CII”，指的是那些对国计民生非常重要的信息基础设施。CII 可以是 IT 基础设施，比如中国的电信网络，也可以是控制重要基础设施的信息系统，比如国家电网调度电力的信息系统。



CII 的范围

根据《网安法》，七大敏感行业包括：（1）公共通信和信息服务，（2）能源，（3）交通，（4）水利，（5）金融，（6）公共服务，以及（7）电子政务等重要行业和领域的网络设施和信息系统很有可能会被认定为是 CII。

此外，根据国务院即将出台的《关键信息基础设施安全保护条例（征求意见稿）》以下行业或领域内的相关单位的网络设施和信息系统也很有可能被认定为是 CII：（1）电信网、广播电视网、互联网等信息网络，以及提供云计算、大数据和其他大型公共信息网络服务的单位；（2）国防科工、大型装备、化工、食品药品等行业领域科研生产单位；以及（3）广播电台、电视台、通讯社等新闻单位。

客户如何判断其运营的网络和信息系统属于 CII

CII 的认定程序如下：国家相关机关会制定一份 CII 识别指南，但该指南很可能不会对外公开。相关行业主管部门会根据该识别指南认定其行业内的 CII 并通知被认定为 CII 的有关单位。

CII 和云服务的关系

微软在中国的 Azure 和 Office 365 云服务由其合作伙伴北京世纪互联宽带数据中心有限公司的全资子公司上海蓝云网络科技有限公司（“世纪互联”）运营。运营公有云服务本身很有可能会被认定为是 CII。相应地，世纪互联会被认定为 CIIO。世纪互联会被要求履行 CIIO 的义务，对其运营的网络设施和信息系统采取更为严格的保护措施。

此外，公有云服务的用户有可能也会是 CIIO，从而会对云服务提供商有更高的合规要求。这个时候，如果云服务的提供商本身是一个 CIIO，且满足了相关要求，例如通过等级保护 3 级的安全测评，则将更有助于云服务用户满足其自身的合规要求。

对 CII 有哪些特别保护要求

CIIO 需要对其运营的 CII 尽到特别保护义务，其中比较重要的要求如下：

（1）数据本地存储和出境安全评估：对于一般网络运营者而言，对于其掌握的重要数据和个人信息在通过安全评估的前提下，可以直接传输至境外，而无需在中国本地存储。但对于 CIIO 而言，无论它是否能通过数据出境安全评估，其在境内运营中收集和产生重要数据和个人信息都必须要在中国境内存储备份。
此外，根据目前数据出境方面法规的相关草案，CIIO 的数据出境安全评估需要经过政府审批，而一般网络运营者的数据出境安全评估仅需在某些特定情况下上报政府。数据本地存储和出境安全评估的具体内容参见 B

（2）网络安全等级保护：CIIO 对 CII 的保护要以网络安全等级保护制度为基础。将来，CII 有可能被要求通过不低于等保 3 级的安全测评。而一般的网络经营者无此要求。网络安全等级保护制度的具体内容参见 C

（3）网络安全审查：CIIO 采购网络产品和服务，如果可能影响国家安全，应当通过国家的安全审查。是否影响国家安全，由国家相关机关结合具体情况具体掌握。
CIIO 在某些特殊情况下，有可能也会被要求就其某一采购行为进行安全审查。不过，总体而言，CIIO 的采购行为被要求通过网络安全审查的可能性更高。

（4）容灾备份：容灾指指在相隔较远的异地，建立两套或多套功能相同的系统。当一处系统因意外（如火灾、地震等）停止工作时，整个应用系统可以切换到另一处，使得该系统功能可以继续正常工作。《网安法》要求 CIIO 应当对重要系统和数据库进行容灾备份。

（5）远程维护：根据目前数据出境方面法规的相关草案，对于 CII 的维护应当在中国境内进行。如果需要进行境外远程维护的，需要事先上报政府。

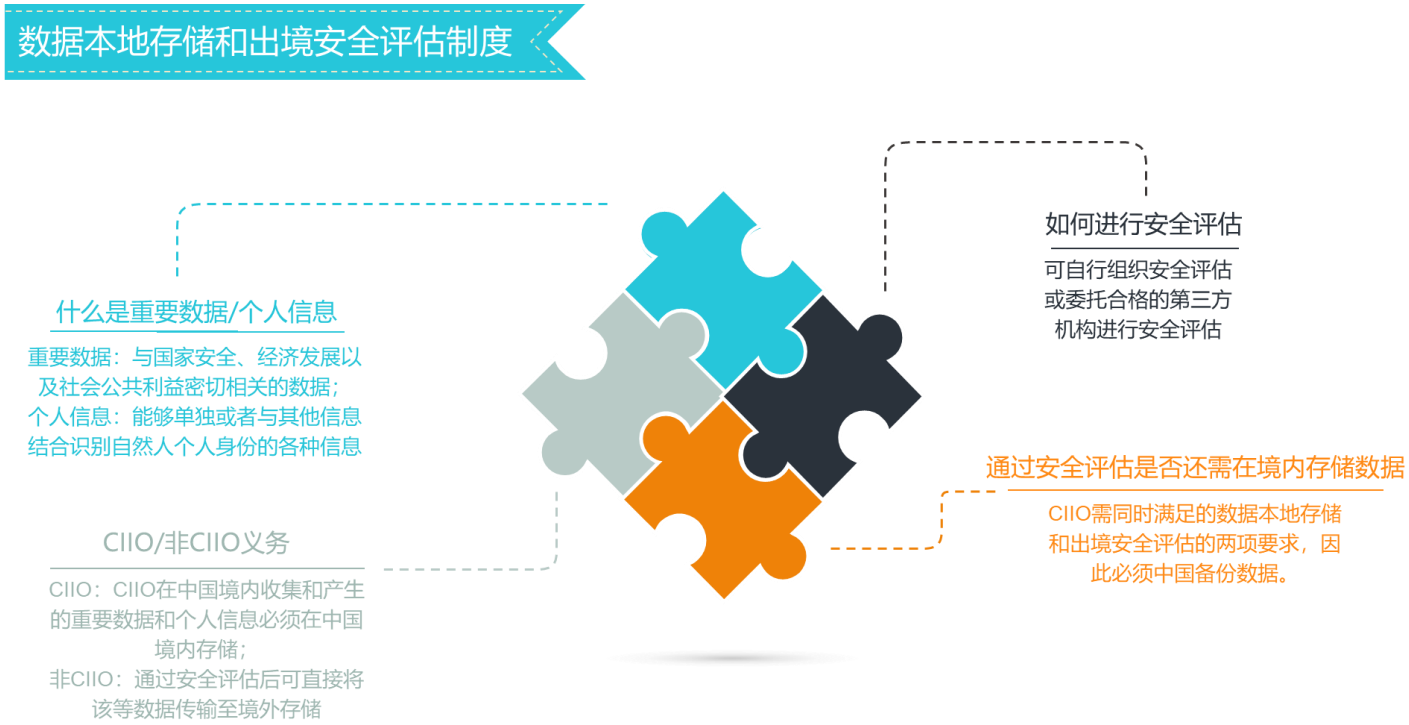
（6）保密协议：CIIO 采购网络产品和服务，应当和供应商签署保密协议。

CII 的配套管理条例出台时间

根据《网安法》第三十一条规定："关键信息基础设施的具体范围和安全保护办法由国务院制定"，截止至 2018 年 2 月 8 日，《关键信息基础设施安全保护条例》尚未正式出台，其意见征求稿已于 2017 年 7 月公示。根据《立法法》相关规定，本条例有望在 2018 年 6 月（即《网安法》正式生效一周年）前出台。

B. 数据本地化储存和出境安全评估制度

《网安法》规定在中国境内运营中收集和产生重要数据以及个人信息在特定情况下，必须存储在中国。如果这些数据要出境，则必须通过相应的安全评估。



什么是重要数据/个人信息

“重要数据”指的是那些与国家安全、经济发展以及社会公共利益密切相关的数据。目前相关部门正在起草《重要数据识别指南》作为《数据出境安全评估指南》的附录 A。根据该《重要数据识别指南》草案，重要数据的范围非常之广泛，涉及许多敏感行业的数据均有可能被认定为是重要数据。该识别指南尚处于草案阶段，目前（截止至 2018 年 2 月）尚未生效。

“个人信息”指的是以电子或其他方式记录的，能够单独或者与其他信息结合识别自然人个人身份的各种信息，典型的如自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。《网安法》对于个人信息的定义与国际上常用的“Personally Identifiable Information”（个人可识别信息）相类似。因此，在英文翻译中，通常以“Personally Identifiable Information”的缩写“PII”指代《网安法》下的个人信息。

CIIO 在数据本地存储和出境安全评估方面有什么义务

CIIO 在中国境内收集和产生的重要数据和个人信息必须在中国境内存储。实践中，CIIO 既可以自己部署服务器存储这些数据，也可以使用满足合规要求的云服务存储这些数据。

如果 CIIO 确实需要将上述数据传输到境外，那么这样的跨境传输必须事先进行安全评估。之后，CIIO 才能进行数据的跨境传输。安全评估的具体要求参见下文。

客户如何进行安全评估

根据目前数据出境方面法规的相关草案，无论是 CIIO 或非 CIIO，均可以自行组织安全评估或委托合格的第三方机构进行安全评估。评估的频率为每年一次，当出境数据的规模和数量有变化时需要再次进行评估工作。安全评估结果和出境数据传输日志需要保存不少于 2 年。

根据目前数据出境方面法规的相关草案，CIIO 和非 CIIO 的安全评估略有不同：CIIO 的评估结果应当上报政府，经批准后方可开展数据跨境传输。非 CIIO 出境传输的个人信息如果在一年内超过 50 万个人数据或者涉及其出境传输的内容涉及某些敏感数据，则应当将评估结果上报政府。目前尚不明确该等上报是否需要经政府审批。

CIIO 通过安全评估后，是否还需要在中国境内部署服务器或购买云服务存储数据

CIIO 需要同时满足的数据本地存储和出境安全评估的两项要求。这意味着，即便 CIIO 能够满足安全评估的要求，可以将数据传输至境外，也必须要在中国境内部署服务器或购买云服务存储这些数据。

非 CIIO 在数据本地存储和出境安全评估方面有什么义务

不同于 CIIO 需要同时满足的数据本地存储和出境安全评估的两项要求，非 CIIO 仅仅需要遵守安全评估的义务。这意味着，如果非 CIIO 能够通过安全评估，其不需要在中国本地存储重要数据和个人信息，而可以直接将该等数据传输至境外存储。

数据本地储存及安全评估相关办法正式出台时间

《个人信息和重要数据出境安全评估办法（征求意见稿）》自 2017 年 4 月起已经过 3 次意见征求，截止至 2018 年 2 月正式版本尚未出台。并且由于《个人信息和重要数据出境安全评估办法（征求意见稿）》会有很大的改动，因此具体的评估需等相关办法的正式实施。同时，作为数据出境安全评估的国家推荐性标准，《信息安全技术数据出境安全评估指南（草案）》也具有一定的参考意义。

C. 安全等级保护制度

信息系统的运营者应根据相关规定确定其信息系统安全保护等级，并采取相应的保护措施。英文中，通常将等级保护制度翻译为“Multi-Level Protection Scheme”（“MLPS”）

网络安全等级保护制度

什么是等保1.0和等保2.0

《网安法》出台前，公安部已经在执行计算机信息系统的等级保护制度。《网安法》中，将“计算机信息系统等级保护制度”的概念升级为“网络安全等级保护制度”。
因此，原有的计算机信息系统等级保护制度称为“等保1.0”，而将网安法下的网络安全等级保护制度称为“等保2.0”。

云服务通过等保3级的意思

根据信息系统对国家安全的重要程度被依次分为1到5级，定级越高越严格，由世纪互联运营的Microsoft Azure 和Office 365均已经通过了等保3级的安全测评，意味着世纪互联运营的这些云服务已经满足了等保3级的保护要求，可以为客户提供高安全等级的云服务。

什么是等保 1.0 和等保 2.0

在《网安法》出台之前，国家公安部便已经在执行计算机信息系统的等级保护制度。网安法中，将“计算机信息系统等级保护制度”的概念升级为“网络安全等级保护制度”。因此，在业内，通常将原来计算机信息系统等级保护制度称为“等保 1.0”，而将网安法下的网络安全等级保护制度称为“等保 2.0”。

目前国家正在制定等保 2.0 的相关实施细则。

根据《网安法》中等级保护的相关要求，网络运营者应采取监测、记录网络运行状态、网络安全时间的技术措施，并规定留存相关的网络日志不少于六个月。

微软在中国由世纪互联运营的云服务通过等保 3 级安全测评具体是什么意思

根据信息系统对国家安全的重要程度，国家将信息系统的安全保护等级依次分为 1 到 5 级。定级为 1 级和 2 级的信息系统即便遭到破坏也不会危害国家安全。定级为 3 级或 3 级以上的信息系统，如果遭到破坏，将会危害国家安全。因此，等级保护的定级越高，说明对于国家安全越重要，其所需要采取的保护措施也越严格。

由世纪互联运营的 Microsoft Azure 和 Office 365 均已经通过了等保 3 级的安全测评，意味着世纪互联运营的这些云服务已经满足了等保 3 级的保护要求，可以为客户提供高安全等级的云服务。

D. 个人信息保护制度

- **网络运营者个人信息保护的重要原则（下图）**

云服务的客户，作为其所收集的个人信息的控制者，应当遵循这些个人信息保护的原则，并对其收集并存储在云服务上的个人信息履行主要的保护义务。

世纪互联作为云服务的运营者，对于客户收集的 个人信息承担信息处理者的责任。由世纪互联运营的 Microsoft Azure、Office 365 和 Power BI 采用最先进的安全措施和安全机制，将从技术上为保障信息安全提供有力的支持。

E. 网络运营者的其他重要义务

除了关键信息基础设施保护制度、数据本地存储和出境安全评估制度、网络安全等级保护制度和个人信息保护制度之外，网络运营者还需履行以下制度中的重要义务：

其他重要义务

安全认证和检测制度
网络运营者使用的某些关键设备和安全专用产品必须通过国家要求的安全认证或安全检测

应急处置制度
网络运营者应当制定网络安全事件的应急预案。一旦发生网络安全事件，网络运营者应当采取相应的措施，及时进行处置

网络安全审查制度
若网络运营者采购的网络产品或服务可能影响到国家安全，则采购行为可能被要求通过安全审查。而非CIIO对于CII的采购行为被要求通过审查的可能性更高

网络运行/信息安全保护制度
网络运营者应当履行各项义务（例如将网络日志留存至少6个月，以及及时处置漏洞等），确保网络的安全运行；网络运营者应当确保网络信息安全

监测预警和信息通报制度
国家将建立网络安全监测预警和信息通报制度。网络运营者应当配合国家，及时报告网络安全信息

网络内容管理制度
网络运营者应当确保通过网络传播的内容符合国家法律的规定。任何人不得利用网络传播传播政府禁止的内容

四、 微软对客户的合规帮助——以世纪互联运营的中国的可信云为例

微软可信云服务在全球获得众多的合规认证

微软在全球任何一个国家或地区的经营均符合当地的法律法规。微软在中国的运营均遵守中国的法律、法规和强制标准。微软认真学习、研究了《网安法》，并持续跟踪相关实施配套法规和标准。微软在中国的产品和服务也毫无疑问符合《网络安全法》、相关法规和强制标准。

在实践中，如果客户业务属于指定的关键信息基础设施行业、指定的重点单位或服务、涉及敏感数据或大量“重要数据”或“个人信息”，我们建议客户认真考虑实现数据本地化存储，并对其数据出境安全评估和《网安法》要求的其它安全、管理措施做审慎评估。

可信云在中国为客户的《网安法》合规提供全方位支持

微软在中国由世纪互联运营的云服务将为客户的《网安法》合规提供全方位的支持。由世纪互联运营的 Microsoft Azure 、Office 365 和 Power BI 的客户数据在本地存储。由世纪互联运营的 Microsoft Azure 和 Office 365 均通过了等保 3 级的安全测评。世纪互联和微软会对客户自身的等保测评工作提供支持。

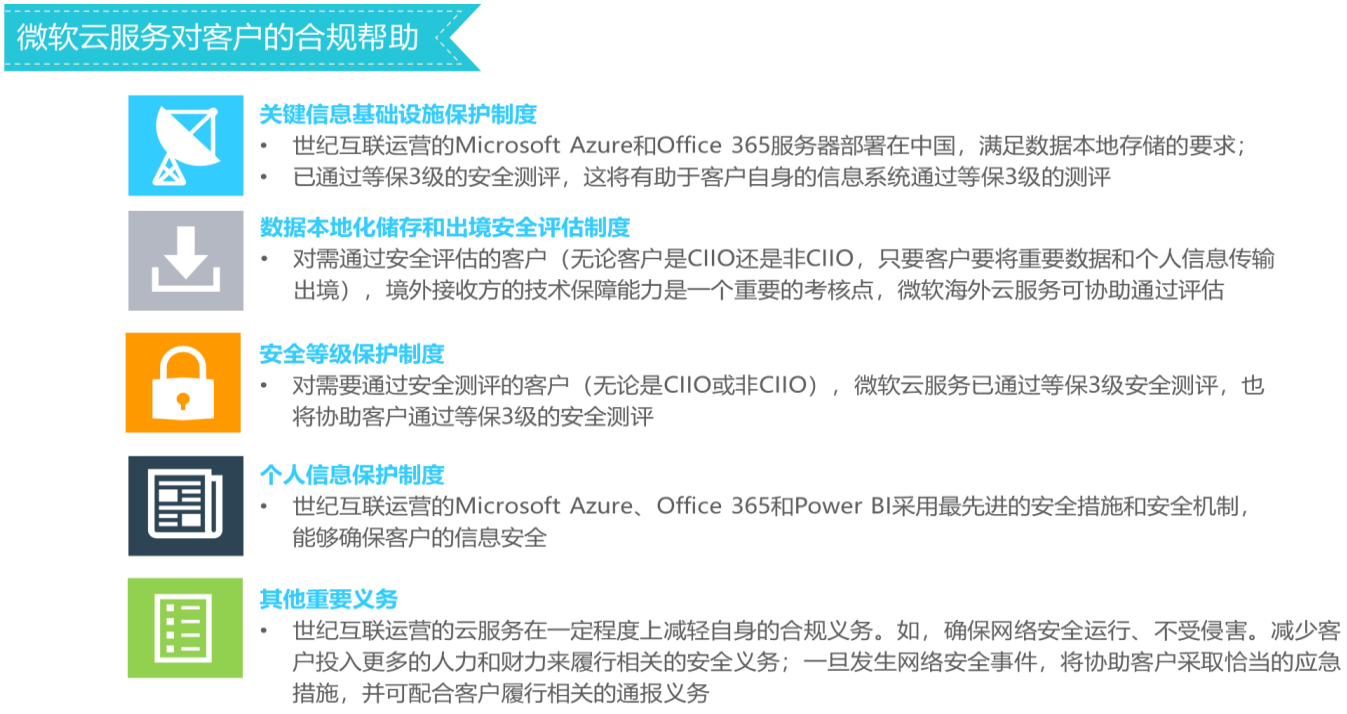
此外，由世纪互联运营的 Microsoft Azure、Office 365 和 Power BI 具备最先进的安全措施、应急机制和管理机制，均满足国际、国内和行业特定的合规性标准，拥有 ISO/IEC20000 和 ISO/IEC27001 认证，同时也符合 GB 18030 信息技术中文编码字符国家标准以及可信云服务认证（TCS）。

此外，世纪互联在数据中心运维和支持各种规模的商业、企业、和政府客户方面拥有丰富经验。世纪互联和微软了解商业运行软件的关键需求，包括认证、数据主权性、安全性和隐私性的要求。采用世纪互联云计算服务来处理客户的业务，可以进一步满足客户业务的合规需求。

微软海外云服务提供更为丰富的的服务种类

无论对于有在华业务的跨国公司还是有海外业务的中国公司，微软通过其海外云服务和在中国由世纪互联运营的云服务，为客户提供多种选择。客户可以购买世纪互联运营的中国云服务，以满足数据本地存储的要求。同时，在满足合规要求或在海外运营客户业务时，客户还可以购买微软的海外云服务，享受更丰富的服务种类。

世纪互联运营的云服务对于客户履行《网络安全法》中合规要求的帮助



A. 关键信息基础设施保护

如果客户从事敏感行业的业务，则该客户的网络或信息系统很可能会被认定为是 CII，因此需要采取更高的安全保护措施。

客户如果采购世纪互联运营的 Microsoft Azure 和 Office 365 云服务，将有助于其满足《网安法》对 CIIO 的要求。例如，世纪互联的运营的 Microsoft Azure 和 Office 365 云服务服务器部署在中国，这能够满足 CIIO 必须将数据在本地存储的要求。此外，世纪互联的运营的 Microsoft Azure 和 Office 365 云服务本身已经通过了等保 3 级的安全测评，这将有助于客户自身的信息系统通过等保 3 级的测评。

B. 数据本地化储存和出境安全评估制度

如果客户是 CIIO，那么该客户必须将重要数据和个人信息在中国存储。世纪互联运营的 Microsoft Azure 和 Office 365 将服务器部署在中国，能够帮助客户满足本地存储的要求。

如果客户是非 CIIO，需要具体结合相关行业和客户的具体业务进行判断。国家对于某些行业的某些数据必须在中国境内存储做出了特别规定。此外，如果客户需要购买云服务在中国从事增值电信业务（比如互联网信息服务），则根据中国政府的电信管理规定，这些客户必须在中国部署服务器。如果客户的业务不涉及上述特殊数据或增值电信服务，那么该客户不需要在中国部署服务器存储数据。因此，如果其能满足安全评估的要求，可以购买微软的海外云服务，并直接将数据传输至境外。

此外，根据目前数据出境方面法规的相关草案，无论客户是 CIIO 还是非 CIIO，只要客户需要将重要数据和个人信息传输出境，就必须通过安全评估。在安全评估的过程中，境外数据接收方的技术保障能力将是一个重要的考核点。微软提供的云服务在全球获得众多合规认证。微软有能力在信息安全方面为客户提供充分的保障。微软将全力协助客户通过安全评估。

C. 安全等级保护制度

由世纪互联运营的 Microsoft Azure 和 Office 365 均已经通过了等保 3 级的测评，意味着世纪互联运营的这些云服务已经满足了等保 3 级的保护要求，可以

为客户提供高安全等级的云服务。其采购世纪互联运营的云服务将有助于其自身通过等保 3 级的安全测评。同时，微软和世纪互联也将协助客户通过网络安全等级保护的安全测评。

如果客户的信息系统不需要通过等保 3 级的安全测评，由于其采购的世纪互联运营的云服务已经通过了等保 3 级的安全测评，这将大大增强其系统的安全性。

D. 个人信息保护制度

个人信息保护制度中技术保障的要求意味着客户必须采取充分技术措施，防止信息泄露、损毁或丢失。此外，本地存储和出境安全评估的要求意味着在某些情况下，客户必须要在中国境内存储个人信息。

由世纪互联运营的 Microsoft Azure、Office 365 和 Power BI 采用最先进的安全措施和安全机制，能够确保客户的信息安全。此外，该等云服务的服务器位于中国，能帮助客户满足本地存储的要求。

E. 网络运营者的其他重要义务

由世纪互联运营的 Microsoft Azure 和 Office 365 和 Power BI 采用了先进的技术手段确保网络安全运行，并确保相关的网络信息不受侵害。如果客户自己运营相关网络，势必需要投入更多的人力和财力来履行相关的安全义务。此外，一旦有网络安全事件发生，微软和世纪互联也将协助客户采取恰当的应急措施，避免损失扩大，并可配合客户履行相关的通报义务。

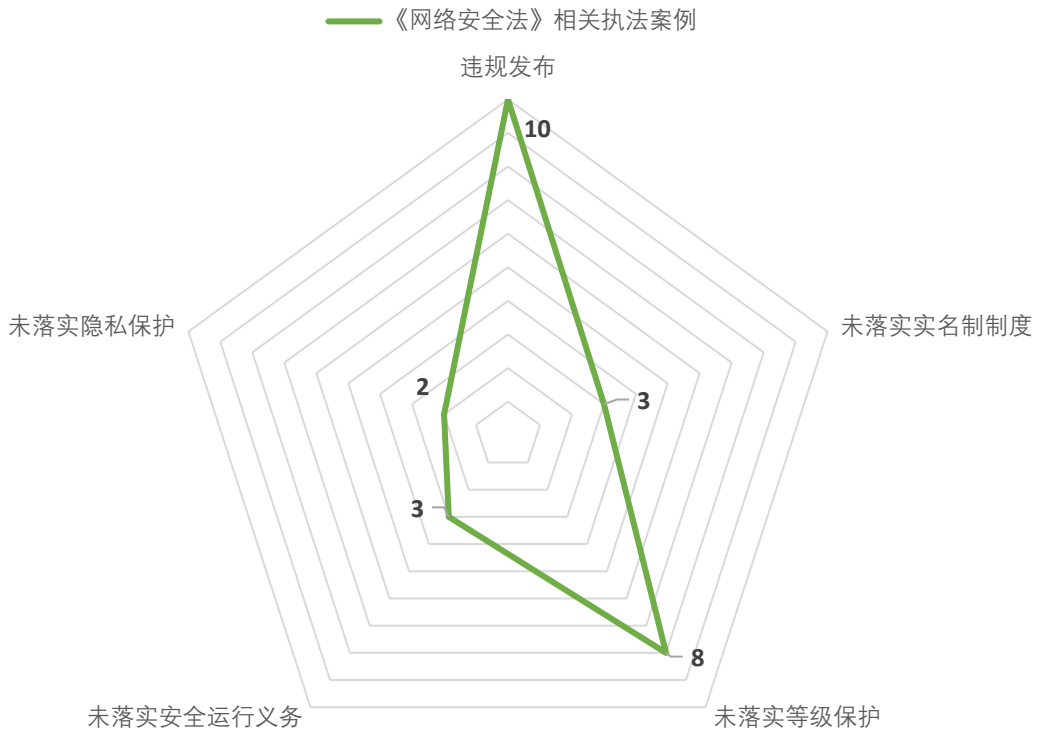
五、 《网络安全法》相关执法案例

执法案例统计

根据《网安法》实施之后的执法案例统计，执法相关案例可大致分为五类，包括含有违规发布内容、未落实实名制制度、未落实等级保护制度、未落实安全运行义务以及未落实隐私保护的案件，具体案件数量分布见下图。其中因未按要求管理用户发布的信息而被做出处罚案例的数量最多，其次则为网络安全等级保护制度相关案例。

主要处罚措施

在处罚措施方面，根据《网络安全法》第六章，对未履行《网安法》义务的主体做出的处罚措施，最主要的为责令整改；其次为罚款，对单位的罚款从一万到五十万不等，在实际案例中，腾讯公司、新浪微博、百度贴吧这三家公司因未按要求管理用户发布的信息受到过较重罚款处罚，分别给予了两个50 万的“最高罚”以及一个“从重罚”。



《网安法》具体执法案例列表（截止至：2018 年 2 月）

A. 违规发布相关案例

法律要求：

【第四十六条】任何个人和组织应当对其使用网络的行为负责，不得设立用于实施诈骗，传授犯罪方法，制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组，不得利用网络发布涉及实施诈骗，制作或者销售违禁物品、管制物品以及其他违法犯罪活动的信息。

【第四十七条】网络运营者应当加强对其用户发布的信息的管理，发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告。

法律责任：

【第六十七条】违反本法第四十六条规定，设立用于实施违法犯罪活动的网站、通讯群组，或者利用网络发布涉及实施违法犯罪活动的信息，尚不构成犯罪的，由公安机关处五日以下拘留，可以并处一万元以上十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处五万元以上五十万元以下罚款。关闭用于实施违法犯罪活动的网站、通讯群组。

单位有前款行为的，由公安机关处十万元以上五十万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

【第六十八条】网络运营者违反本法第四十七条规定，对法律、行政法规禁止发布或者传输的信息未停止传输、采取消除等处置措施、保存有关记录的，由有关主管部门责令改正，给予警告，没收违法所得；拒不改正或者情节严重的，处十万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

电子信息发送服务提供者、应用软件下载服务提供者，不履行本法第四十八条第二款规定的安全管理义务的，依照前款规定处罚。

序号	案例	日期
1	上海网信办要求万豪国际集团，ZARA，美敦力（上海）及花椒直播对将港澳台和西藏列为“国家”的行为进行整改	2018 年 1 月
2	北京网信办在国家网信办指导下，约谈微博负责人并将部分板块暂时下线一周	
3	北京网信办在国家网信办指导下，要求今日头条和凤凰网收集客户端停止违规内容传播	2017 年 12 月
4	广东省网信办调查阿里云未落实实名制制度和荔支 FM 平台违规传播有害信息并责令立即整改	2017 年 9 月
5	北京网信办对新浪微博、百度贴吧，广东网信办对腾讯传播违规内容进行调查并依法处罚	2017 年 9 月
6	北京网信办对 58 同城、赶集网、百度违法发布租房信息责令整改	2017 年 8 月
7	广东网信办对腾讯公司微信公众号平台存在用户传播违法信息作出最高处罚并要求整改	
8	北京网信办联合天津网信办约谈直聘网要求停止违规内容传播并落实实名制制度	

序号	案例（接上页）	日期
9	安徽铜陵网警对一网民传播不实谣言、组织非法集会依法处以拘留十日	2017 年 7 月
10	浙江网信办对淘宝、同花顺金融网、蘑菇街互动网等网站违规售卖 VPN 工具限期责令改正并依法处罚	2017 年 6 月

B. 未落实等级保护相关案例

法律要求：

【第二十一条】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：

（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；

（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；

（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；

（四）采取数据分类、重要数据备份和加密等措施；

（五）法律、行政法规规定的其他义务。

法律责任：

【第五十九条】 网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。

序号	案例	日期
1	合肥公安部门对对其辖区内某网站未落实网络安全保护责任的行为下达整改通知书，并处以警告处罚	2017 年 10 月
2	安徽网信办对一学校网站未进行等级保护、留存数据，导致身份信息泄漏责令改正	2017 年 9 月
3	安徽公安局查实当地一学校网站未进行等级保护，遭黑客攻击，责令改正并处罚款	2017 年 8 月
4	哈尔滨公安局查实当地一农业服务网站未进行等级保护，遭黑客攻击，责令改正并处罚款	
5	宜宾网安部门对一教师培训与教育研究中心未落实等级保护处一万元罚款并对法人代表处五千元罚款	
6	汕头公安分局查实当地某公司未进行等保评测并责令依法改正	2017 年 7 月
7	重庆公安分局调查当地一公司并认定未留存用户登陆日志并责令依法改正	
8	山西忻州市、县两级公安机关网安部门针对山西忻州市某省直事业单位网站进行行政处罚	2017 年 6 月

C. 未落实实名制制度相关案例

法律要求：

【第二十四条 第一款】网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通讯等服务，在与用户签订协议或者确认提供服务时，应当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务。

法律责任：

【第六十一条】网络运营者违反本法第二十四条第一款规定，未要求用户提供真实身份信息，或者对不提供真实身份信息的用户提供相关服务的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

序号	案例	日期
1	广东省网信办调查阿里云未落实实名制制度和荔支 FM 平台违规传播有害信息并责令立即整改	2017 年 9 月
2	广东省工信部调查三人网络科技有限公司未要求用户提供真实身份信息并提供网络电话服务，责令停业整顿	
3	北京网信办联合天津网信办约谈直聘网要求停止违规内容传播并落实实名制制度	2017 年 8 月

D. 未落实隐私保护相关案例

法律要求：

【第二十二条 第三款】 网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。

【第四十一条】网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。
网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。

【第四十二条】网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。
网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

【第四十三条】个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。

法律责任：

【第六十四条】网络运营者、网络产品或者服务的提供者违反本法第二十二条第三款、第四十一条至第四十三条规定，侵害个人信息依法得到保护的权利的，由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；情节严重的，

并可以责令暂停相关业务、停业整顿、关闭网站、
吊销相关业务许可证或者吊销营业执照。

序号	案例	日期
1	工信部约谈百度，支付宝及今日头条要求三家企业本着充分保障用户知情权和选择权的原则立即进行整改	2018 年 1 月
2	网信办会同工信部、公安部、国家标准委三部门于 2017 年 7 月开展了针对首期十个网络产品和服务隐私保护的评审公司：微信、淘宝网、支付宝、滴滴打车、京东商城、航旅纵横、百度地图、高德地图、携程网、新浪微博： •前八款产品做到向用户主动提示，并提供更多选择权； •前五款服务还提供了一站式撤回和关闭授权，在线访问、更正、删除个人信息， 在新注销账户等功能； •参与企业还共同签署了个人信息保护倡议书	2017 年 7 月

E. 未落实安全运行义务相关案例

法律要求：

【第二十二条】网络产品、服务应当符合相关国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。
网络产品、服务的提供者应当为其产品、服务持续提供安全维护；在规定或者当事人约定的期限内，不得终止提供安全维护。
网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。

法律责任：

【第六十条】违反本法第二十二条第一款、第二款和第四十八条第一款规定，有下列行为之一的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款：
（一）设置恶意程序的；
（二）对其产品、服务存在的安全缺陷、漏洞等风险未立即采取补救措施，或者未按照规定及时告知用户并向有关主管部门报告的；
（三）擅自终止为其产品、服务提供安全维护的。

序号	案例	日期
1	广东工信部调查 UC 浏览器发现存在安全漏洞	2017 年 9 月
2	四川一教育网站因存在高危安全漏洞遭入侵被处以罚款并限期改正	2017 年 7 月
3	山西一事业单位网站因不履行网络安全保护义务存在漏洞被依法处罚	2017 年 6 月

六、 Q&A

我们梳理了目前《网络安全法》在企业的合规过程中遇到的常见问题，并给出微软的建议供参考。收集到的问题共分为两大类，一类为《网络安全法》中的常规问题，另一类则是客户针对微软所提供的云服务在《网安法》合规中的一些疑惑。

A. 关于《网络安全法》的常规问题

什么是关键信息基础设施运营者（Critical Information Infrastructure Operator，简称“CIIO”）？怎么判断自己是否属于 CIIO？

- CIIO 指的是关键信息基础设施 （Critical Information Infrastructure，即“CII”）的运营者
- CII 范围很广
  - 七大敏感行业的网络设施和信息系统
  - 其他敏感行业或领域内的网络设施和信息系统
- 国家相关机关会制定一份 CII 识别指南
  - 不一定对外公开
- 相关主管部委再根据 CII 识别指南来认定
- 行业主管部门会通知被认定为 CII 的有关单位
- 具体请参照前文第三章 A

什么类型数据的跨境传输受《网安法》的禁止或者限制？

- CIIO：重要数据和个人信息本地存储以及出境安全评估
- 非 CIIO：重要数据和个人信息出境安全评估
- “重要数据”及“个人信息”的概念
  - “重要数据”指的是那些与国家安全、经济发展以及社会公共利益密切相关的数据
  - “个人信息”指的能够单独或者与其他信息结合识别自然人个人身份的各种信息：自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等
- 企业应当在做数据的跨境传输之前，审慎检视其需要传输的数据
- 具体请参照前文第三章 B

哪些情况属于数据的跨境传输？从境外传入数据需要注意哪些问题？

- 《网安法》主要针对的是将数据往中国地区以外传输的情况
  - 从中国地区以外往中国传输数据，《网安法》没有明确规定。
- 数据出境的定义
  - 指的是网络运营者通过网络等方式，将个人信息和重要数据提供给境外的机构或个人
  - 存在中国地区以内的数据如果能被境外的机构、组织、个人远程访问查看的（公开信息、网页访问除外），通常也会被认定为数据跨境传输，因此也需要通过安全评估。
- 不在中国境内收集和产生的个人信息和重要数据，如果未作处理而仅仅经过中国出境，或者虽有处理但是不涉及在中国境内收集和产生的重要数据和个人信息的，不视为数据出境。在上述情况下，不需要做数据出境安全评估。

什么是网络安全等级保护制度？目前世纪互联运营的云服务的安全等级是几级？

- 信息系统的运营者应根据相关规定确定其信息系统安全保护等级，并采取相应的保护措施
  - 英文翻译为“Multi-Level Protection Scheme”（“MLPS”）
- 信息系统的安全保护等级依次分为 1 到 5 级

- 由世纪互联运营的 Microsoft Azure 和 Office 365 均已经通过了等保 3 级的测评
- 客户如果被认定为 CIIO，通常会被要求通过等保 3 级的测评

- **客户使用的软件不合规（例如为盗版软件），是否不符合等级保护要求？**
  - 客户使用盗版软件或过期软件将使其信息系统更容易遭受网络攻击
  - 客户可能因此无法满足等级保护测评的要求
  - 微软强烈推荐客户使用在有效期内的正版软件
    - 客户自己的义务
    - 世纪互联可以提供协助

- **《网安法》对企业运营的影响：《网安法》涉及哪些问题？其中哪些与企业的日常运营有关？**
  - 其主要涉及的问题包括关键信息基础设施的保护、数据本地存储和数据出境安全评估、网络安全等级保护和个人信息保护
  - 上述各方面是有机结合的，都会对企业的日常运营造成影响

B. 关于云服务的问题

- **在华企业使用微软海外的云服务（服务器在境外）：《网安法》是否会影响客户使用外国母公司订阅的云服务？**
  - 如果客户是 CIIO
    - 数据本地存储和出境安全评估
    - 安全评估结果需政府审批
    - 网络安全审查
    - 等级保护
  - 如果客户是非 CIIO
    - 数据出境安全评估
      - 如果超过某一数额的个人信息或涉及敏感数据，安全评估结果需要上报政府
    - 其它行业和业务相关的限制
  - 客户应当结合自身的情况，做综合审慎的评估
  - 微软将为客户的数据出境安全评估提供帮助

拓展阅读

《网安法》对使用海外云服务方面的主要影响视客户的具体情况而定。

如果客户是 CIIO，那么客户通常需要考虑使用世纪互联运营的境内云服务：

1. CIIO 必须将重要数据和个人信息存储在中国。此外，客户的上述数据出境的安全评估要经过政府的审批。
2. CIIO 采购云服务可能需要进行网络安全审查。海外云服务可能无法通过网络安全审查。
3. CII 通常可能需要通过等级保护的 3 级安全测评。海外云服务可能无法通过该项测评。

如果客户是非 CIIO，需要具体结合相关行业和客户的具体业务进行判断：

1. 根据目前数据出境方面法规的相关草案，非 CIIO 的重要数据和个人信息也需要通过出境安全评估。如果出境传输的个人信息如果在一年内超过 50 万 个人或者出境传输的内容涉及某些敏感数据，则应当将评估结果上报政府。目前尚不明确该等上报是否需要经政府审批。
2. 国家对于某些行业的某些数据必须在中国境内存储有特别规定 。此外，如果非 CIIO 需要购买云服务在中国从事增值电信业务（比如互联网信息服务），则根据中国政府的电信管理规定，这些客户必须在中国部署服务器。如果某一非 CIIO 的业务不涉及上述特殊数据或增值电信服务，那么该非 CIIO 通常不需要在中国部署服务器存储数据，而仅需满足数据出境安全评估的要求。

无论客户是 CIIO 还是非 CIIO，应当结合自身的情况，做综合审慎的评估。

在安全评估的过程中，境外数据接收方的技术保障能力将是一个重要的考核点。微软提供的云服务在全球获得众多的合规认证。微软有能力在信息安全方面为客户提供充分的保障。

- **在华企业使用由世纪互联运营的的云服务（服务器在境内）相关问题**
  - 微软中国地区的云服务 是否由微软提供？
    - 微软在中国地区的云服务由微软合作伙伴北京世纪互联宽带数据中心有限公司的全资子公司上海蓝云网络科技有限公司 （以下简称 “世纪互联”）运营
  - 如果微软中国地区的云服务是由世纪互联运营，那微软在该服务中扮演了什么样的角色？
    - 微软系技术提供方
      - 将相关云技术许可给世纪互联
    - 微软与世纪互联相互独立
      - 不参与运营
      - 不接触客户数据
      - 提供技术支持
  - 由世纪互联运营的云服务与微软在全球其他地区提供的云服务的关联是什么？两者在物理和逻辑上是否相互独立，能否实现数据交换和转移？
    - 物理上和逻辑上相互独立
    - 不能实现数据的交换和转移
    - 香港地区的数据中心由微软自身经营
    - 中国内地的云服务由世纪互联经营

拓展阅读

在中国地区由世纪互联运营的 Microsoft Azure、Office 365 和 Power BI 与全球其他地区由微软运营的云服务在物理上和逻辑上都是独立的。

正如微软无权访问世纪互联云服务中的客户数据一样，世纪互联也无权访问中国地区以外的由微软运营的云服务中的客户数据，更不能实现数据的交换和转移。

香港特别行政区的数据中心是由微软运营的全球服务，而非由世纪互联在中国地区运营的云服务。

- 《网安法》的风险主要是由云服务运营商承担，还是由用户自己承担？
  - 云服务运营商负责云平台合规
    - 获得针对云平台的相关证照
    - 针对云平台进行等级保护安全测评
    - 针对云平台的产生和收集的数据进行本地存储和出境安全评估
    - 针对云平台收集的个人信息进行保护
  - 用户负责自行部署的应用程序、数据内容、虚拟机、访问凭据以及遵守适用于其特定行业和区域的法规
    - 获得针对用户的相关证照
    - 针对用户自身信息系统进行等级保护安全测评
    - 针对用户产生和收集的数据进行本地存储和出境安全评估
    - 针对用户的产生和收集的个人信息进行保护
- 世纪互联承诺不会访问 Microsoft Azure 和 Office 365 上的客户数据。但是政府有关部门要求接触世纪互联运营的 Microsoft Azure 和 Office 365 上的客户数据，一般是怎么操作？
  - 配合政府部门的执法要求，前提是政府的行动：
    - 符合行政法律法规要求的书面行政命令
    - 符合行政执法的法定程序
  - 向某一第三方披露客户数据
    - 立即通知客户
    - 提供相应要求的副本
- 用户停止使用由世纪互联运营的 Microsoft Azure、Office 365 和 Power BI 等服务后，世纪互联会如何处理用户保存在云中的数据？
  - 客户删除数据
    - 覆盖写入
  - 客户停止使用服务
    - 保存 90 天
    - 删除
- 世纪互联运营的云服务可以在哪些方面帮助企业用户实现网络运营的合规？
  - 世纪互联运营的云服务有如下优势：
    - ISO/IEC20000 和 ISO/IEC27001 认证
    - GB 18030 信息技术中文编码字符国家标准
    - 可信云服务认证（TCS）
    - 等保 3 级的安全测评
    - 丰富经验

拓展阅读

世纪互联在数据中心运维和支持各种规模的商业、企业、和政府客户方面拥有丰富经验。世纪互联了解商业运行软件的关键需求，包括认证、数据主权性、安全性和隐私性的要求。采用世纪互联云服务来处理客户的业务，可以进一步满足客户业务的合规需求。

- 在华的跨国公司或有海外业务的中国公司，在选择云服务的时候，对于如何选择海外云服务和国内的云服务，微软有什么建议？
  - 推荐世纪互联运营的云服务，如果：
    - 客户有可能被认定为是 CIIO
    - 客户的主要服务对象可能是 CIIO
  - 推荐海外云服务，如果：
    - 客户被认定为 CIIO 的可能性较小
    - 跨境传输的数据中不包含重要数据、个人信息或其它政府要求必须在中国境内存储的数据

- 客户对其自身通过安全评估非常有信心
- 对于跨境传输的稳定性要求较低
- 公司业务在海外运营

拓展阅读

此问题这需要结合客户自身业务的性质，进行综合分析。通常，我们可以考虑如下因素：

如果客户有可能被认定为是 CIIO 或者客户的主要服务对象可能被认定为是 CIIO，则其必须在中国存储重要数据和个人信息。那么在这种情况下，推荐客户使用中国地区由世纪互联运营的云服务可以更好地帮助客户满足《网安法》的合规要求。

如果客户被认定为 CIIO 的可能性较小，且其跨境传输的数据中不包含重要数据、个人信息或其它政府要求必须在中国境内存储的数据，或者客户对其自身通过安全评估非常有信心。这种情况下，客户可以结合自身业务和财务状况选择是否使用境外的云服务 。

在客户使用海外云服务的过程中，对于跨境传输的稳定性要求也是客户需要考虑的因素之一。

必须说明的是，目前数据跨境传输的安全评估制度（包括相关的安全评估标准）仅停留在草案阶段，因此在实践中尚未开始实施，客户可在具体选择海外或是中国地区的云服务时充分考虑上述因素后，做出适合其企业自身业务需求的 决定