

汉坤法律评述

2026 年 9 月 15 日

北京 | 上海 | 深圳 | 杭州 | 武汉 | 海口 | 香港 | 新加坡 | 纽约 | 硅谷 | 伦敦

云上方圆（七）：从芯片到云端 — 云服务管制制裁合规风险治理

作者：权威 | 蒋睿馨 | 熊祎 | 郑博 | 叶田振

从云服务形态的多元演进，到算力成为新型交易标的，再到数据中心与智算中心的投资建设，本系列文章此前已经从不同角度介绍了云产业链中的主要业务模式和交易场景。在这些业务场景中，出口管制与制裁合规始终贯穿上下游各环节：企业在上游获取先进芯片与算力资源时，需要关注供应链、部署地点、最终用户和最终用途等因素；在中游进行设备部署、运维及服务模式设计时，需要评估是否会涉及物项转移、技术出口等限制；在下游提供持续服务过程中，则还需关注客户身份、服务流向、实际用途以及相关限制性清单和监管要求的变化。

根据具体交易安排，云服务产业链条中的企业可能同时承担一个或多个角色，并面临来自上下游不同程度的合规要求。因此，如何在交易准入、合同安排及后续运营中识别和管理出口管制与制裁风险，已经成为云服务业务中需要持续关注的问题。本文将围绕中国和美国出口管制及制裁、反制裁相关规则，结合云服务产业链的主要业务环节，梳理其中可能涉及的管制要求和典型风险场景，并进一步讨论合作方尽调、合同安排及持续合规管理等方面的实务应对。

一、云服务重点环节适用的管制制裁规则

（一）算力资源获取与应用的管制限制

当前，美国针对先进计算物项的出口管制，是中资企业获取先进算力资源时需要重点关注的合规限制。关于美国《出口管理条例》（Export Administration Regulations，“EAR”）的具体规则介绍，可参见我们之前发布的《汉坤·观点 | AI 管制前沿 — 美国出口管制政策观察》与《汉坤·观点 | AI 企业出海（三）：全球出口管制合规与应对策略》。在此就云服务相关的主要关注点概括如下：

- **先进计算物项采购限制。**根据 EAR 针对先进计算物项的相关规则，向总部或最终母公司总部位于 D:5 组国家/地区或澳门等实体提供特定先进计算芯片、服务器等物项，原则上可能面临许可证要求¹。因此，中国企业即使通过境外子公司或其他海外主体采购先进计算资源，也需要关注总部所在地、最终母公司及实际最终用户等因素。

¹ 参见：<https://www.bis.gov/media/documents/bis-guidance-may-31-2026.pdf>。

- **特定 AI 模型训练用途限制。**美国商务部工业与安全局（Bureau of Industry and Security, “BIS”）近年来亦持续关注先进计算物项被用于特定 AI 模型训练的风险。根据其 2025 年发布的相关指引，如受 EAR 管辖的先进计算物项被用于支持与军事情报、大规模杀伤性武器等敏感最终用户或最终用途相关的 AI 模型训练，可能触发进一步的许可证要求²。

对云服务企业而言，这意味着先进算力采购不能只关注设备实际部署在哪个国家，还需要结合采购主体、集团总部、最终用户及实际用途进行综合判断。

（二）远程提供服务的管制判断

与硬件直接交付不同，远程提供云服务往往不涉及底层物理硬件的实际转移，在客户仅取得远程算力、软件功能或计算结果的情况下，一般不会构成对芯片、服务器等货物的出口行为。

但云服务种类多样，是否触发出出口管制不能仅依据“SaaS”、“MaaS”等业务名称判断，而应结合客户实际获得的权限和服务内容进行分析。

与此同时，中美两国的出口管制规则都逐渐从传统的物理转移扩展到“技术、能力和远程访问”。中国方面，2026 年 7 月 1 日正式实施的《国务院关于对外投资的规定》第 13 条明确限制投资者在对外投资活动中出口或使用受管制的货物、技术、服务及相关数据，并明确列示以跨境派遣技术人员、提供技术指导等为重点转移方式。因此境内企业在为境外客户提供模型微调、私有化部署、交付权重或安排技术团队跨境工作时，也需要关注是否涉及受管制技术、服务等。

美国方面，近年来亦持续讨论如何应对通过境外数据中心远程获取受控先进算力的问题。2026 年以来，美国国会及 BIS 均出现进一步规范先进计算资源远程访问的立法及政策动向³。目前，相关立法尚未正式颁布为法律，但远程访问先进计算资源已经成为美国出口管制政策的重要关注方向。

（三）开展云服务的制裁风险

与出口管制主要关注受管制物项的跨境流动不同，经济制裁规则更关注交易本身是否违反有关规定。

因此，云服务商在向下游客户持续提供服务时，需要重点关注客户是否属于受制裁主体，是否位于制裁地区，以及相关云服务、技术支持等是否属于被禁止提供的类型。

例如，美国针对俄罗斯采取的部分制裁措施已经明确限制美国人士向俄罗斯境内主体提供特定受管控软件的 IT 支持服务和云服务⁴。对跨境云服务商而言，这意味着即使底层硬件并未发生跨境转移，持续提供账户、算力、软件、技术支持等服务本身仍可能触发制裁合规问题。

除美国等国家的出口管制和经济制裁要求外，中国企业还需同步遵守我国反外国制裁相关规则。对云服务企业而言，一方面需要结合境外管制制裁要求开展必要的客户和交易筛查；另一方面，也应避免简单、机械地依据境外制裁或限制性清单拒绝交易、终止服务或采取其他限制措施，而忽视中国反制裁及相关规则可能提出的相反要求。因此，在设计客户准入、持续筛查及服务终止机制时，需要兼顾不同法域规则之间可能存在的冲突。

² 参见：<https://www.bis.gov/media/documents/ai-policy-statement-training-ai-models-may-13-2025>。

³ 参见：<https://www.theinformation.com/articles/trump-administration-working-ai-rule-curb-chinas-remote-access-chips>。

⁴ 参见：<https://ofac.treasury.gov/media/932951/download?inline>。

二、云服务场景下管制制裁的重点风险信号

结合 BIS 与 OFAC 发布的合规指导文件⁵，云服务业务中值得重点关注的风险信号可以从算力资源获取及下游服务提供两个环节进行进一步总结：

风险环节	重点风险信号
先进算力资源获取	■ 采购规模、频率或产品类型与采购方既有业务情况明显不匹配； ■ 采购方、最终用户或实际部署地点等关键信息不完整或存在异常； ■ 交易安排、交付路径或相关主体之间的关系缺乏合理商业解释； ■ 交易涉及受限制国家、地区、主体或其他高风险因素。
下游云服务提供	■ 无法充分识别实际用户、最终用途、访问地点或相关控制主体； ■ 签约客户、付款方、实际使用方等交易参与主体不一致，且缺乏合理解释； ■ 服务账号、访问权限或算力资源可能被转供、共享或由未经审查的第三方使用； ■ 客户股权、控制关系、业务用途等关键信息发生变化，或相关限制性清单及监管规则更新后未及时重新评估。

需要明确的是，风险信号的出现并不意味着直接构成违规，其作用更多在于提示企业进一步核实交易背景、客户身份、最终用途及实际服务安排，并根据核查结果决定是否继续交易、采取附加控制措施或开展进一步合规评估。

因此，对云服务企业而言，从全面合规的角度来看，建议建立能够覆盖交易准入、持续服务及异常情形处置的合规机制。

三、云服务交易尽职调查与持续合规治理路径

（一）交易尽职调查

云服务交易链条通常涉及资源提供方、平台运营方、数据中心、多级服务商、渠道经销商、最终用户等参与主体。具体交易还可能存在签约方、付款方、租户主体⁶、管理员、实际使用方相互分离的情况。各主体的身份、属地与各环节所涉的物项与服务模式均可能影响整体交易的合规判定。

因此，企业可结合交易规模、算力资源的敏感程度及具体合作模式，对不同交易采取相应的尽职调查措施：

- 对于一般交易对手，可重点了解主体名称、注册及经营地址、联系方式、股权及控制关系、总部所在地、主营业务、经营网站、实际交易角色等基本信息；
- 涉及敏感算力资源或较高风险交易，还可进一步了解最终受益所有人、最终母公司，以及服务部署方式、访问权限和预期用途等情况。

在基础的信息核查之外，企业还可要求对手方出具合规声明等书面承诺文件，以强化合规约束。以

⁵ 参见：<https://ofac.treasury.gov/media/935441/download?inline>；<https://www.bis.gov/media/documents/ai-counter-diversion-industry-guidance-may-13-2025.pdf>。

⁶ “租户”是指云服务商为客户组织建立的逻辑隔离服务空间。一个租户可以包含多个账号、管理员、项目和云上应用和计算任务（即“工作负载”）。具体分析时应识别租户持有人、管理员、实际用户及工作负载所属主体。

最终用户证明为例，文件一般载明最终用户身份、服务及算力资源的真实最终用途、不转移承诺、严格遵守出口管制及制裁合规要求等核心承诺。

（二）持续合规治理

云服务具有持续提供的特征，客户准入时的尽职调查并不能覆盖服务存续期间可能发生的全部变化。例如，限制性清单可能更新，客户的股权和控制关系可能发生变化，实际用户、访问地点和服务用途也可能与最初了解的情况不同。因此在交易完成后，企业需要实施持续合规治理，并在发现异常及时采取处置措施。

1. 物理资产与服务访问的追踪留痕

对于自持或托管的算力芯片、服务器等硬件的企业，应建立资产台账，覆盖采购、部署、变更、维修退换、报废处置等流程，并在退出环节执行规范的数据擦除并留存硬件去向记录，确保资产流向可追溯。

对于云服务交付场景，建议服务方建立 IP 访问管控与访问日志留痕机制，并开展异常行为监测（包括访问地域异常、用量波动异常、访问时段异常等）与设置暂停、退出服务的配套流程。

2. 持续更新尽调信息及开展清单筛查

企业应在合作协议中明确约定合作方的信息真实性保证与持续更新义务，用以维护尽职调查信息的完整性与准确性。在完成对交易对手及下游用户准入式筛查后，建议企业依中美等重要辖区管制制裁清单重大更新、尽职调查信息重大变更、定期时间节点等事件设置存量筛查机制，确保对合作方及下游用户的风险判断能够及时更新。

3. 向下游传导必要的合规要求

为实现对交易链条的合规管控，企业可选择通过合同约定将管制制裁合规要求传导至下游交易参与方，尤其是通过经销商、渠道商转售算力或提供云服务的场景。具体而言，合同中可明确约定转售限制、审计权与服务终止权，并要求开展制裁筛查、反馈筛查结果、收集下游主体的合规承诺等内容。此外，企业还可对下游合作方开展定期独立审查，确保合规要求得到落实。

四、结语

云服务领域的管制制裁合规义务，需同时兼顾中美等辖区关于出口管制、经济制裁及反制裁的合规要求。企业需要结合自身在交易中的角色、以及算力与技术来源、用户地域分布、最终用途场景等多重因素动态判断。相关经营者应当在准入式尽职调查的基础上，按需建立覆盖资产追踪、持续筛查、下游义务传导与风险事件处置的持续治理机制，确保合规状态在服务存续期间得以维持。

随着算力服务和云服务跨境应用的进一步发展，相关监管规则预计仍将持续变化。对于云服务企业而言，在业务模式设计和交易落地过程中尽早识别出口管制与制裁问题，并预留必要的合规安排，将有助于减少后续业务调整和交易中断的风险。

特别声明

汉坤律师事务所编写《汉坤法律评述》的目的仅为帮助客户及时了解中国或其他相关司法管辖区法律及实务的最新动态和发展，仅供参考，不应被视为任何意义上的法律意见或法律依据。

如您对本期《汉坤法律评述》内容有任何问题或建议，请与汉坤律师事务所以下人员联系：

权威

电话： +86 21 6080 0946

Email: wei.quan@hankunlaw.com

蒋睿馨

电话： +86 10 8524 5808

Email: ruixin.jiang@hankunlaw.com