

云主权

赢得信任，降低风险—— I&O负责人的三大制胜策略



引言

基础设施和运营（I&O）负责人正在承受前所未有的压力，必须调整组织的云战略，以满足日益严苛的合规、数据隐私以及数字主权需求。随着监管要求持续收紧，地缘政治变动不断重塑云市场版图，I&O团队既要守住数据驻留、安全和访问权限的合规底线，又要保持运营的敏捷性。

当前，海外云服务商占据市场主导地位，数据保护法规持续迭代，监管审查力度不断加大。在此环境下，I&O负责人必须将云主权作为战略优先事项。成功的关键在于建立跨部门协作机制，将合规与隐私要求嵌入云运营的每一个环节，同时不牺牲企业所要求的创新速度。这意味着I&O负责人既要充分理解主权相关的各项要求，又要具备落实技术管控措施的能力，并且能够灵活应对持续变化的监管规则。

I&O负责人可将合规与主权要求从阻碍因素转化为构建信任、提升韧性和打造竞争优势的驱动力。本路线图提供切实可行的行动指引，帮助企业 在监管要求与云创新之间找到平衡，赋能I&O团队在复杂、高风险的环境中自信前行、主动引领变革。

关键问题

- > 当前，哪些主要趋势正在重塑云平台的合规、隐私与主权格局？
- > I&O负责人在推进主权策略时，面临的最大挑战是什么？
- > I&O团队应采取哪些行动，确保云运营既安全合规，又保持创新活力？

为什么云主权是头等大事

数据隐私、数据驻留及数据主权相关法规层出不穷，更迭速度之快令人应接不暇。



法规持续演变



地缘政治波动



AI与数据伦理



企业信任与声誉

而人工智能的兴起，加上日益严苛的隐私要求，又让主权合规的挑战变得更加复杂。

全球局势变化以及海外云服务商的主导地位，带来了新的合规与运营风险。

企业必须具备有效的管控能力，并保持足够的透明度，才能赢得客户信任，守住竞争地位。

影响云主权格局的三大关键趋势



监管加速，全球合规局势日趋复杂

各国政府正在密集出台新的数据保护、隐私和主权法规。与此同时，海外超大规模云服务商带来了相互冲突的法律风险，I&O负责人不得不在层层叠加的监管要求和对数据驻留地的严苛审查中寻找平衡。而本地化处理、算法透明度等AI主权要求，更让合规复杂度再上一个台阶。



主权成为差异化竞争优势

企业正借助数字主权建立信任、满足客户期待，并在市场中脱颖而出。I&O团队将数据驻留、运营透明度、技术独立性等主权控制措施融入云战略，使合规不再是单纯的成本支出，而是成为创造业务价值的来源。



合规走向自动化与嵌入式管理

现代云环境的高度复杂性，正推动自动化、基础设施即代码（IaC）、策略即代码（PaC）及AI驱动合规方案的加速普及。I&O负责人借助技术控制、持续监控和智能自动化，将合规要求内嵌于云运营，确保主权与隐私政策有效落地。AI工具能够识别风险、自动执行合规策略并提供实时洞察，在降低风险的同时，推动业务创新。

I&O负责人面临的三大挑战与应对策略

挑战	应对策略
01 应对复杂的监管环境与全球法规碎片化 各地区层出不穷的数据保护、隐私和数字主权法规，令合规环境变得高度碎片化。I&O负责人既要解读和落实相互重叠、甚至彼此冲突的监管要求，又要应对海外云服务商和域外管辖法规带来的合规风险。	建立统一的合规与主权框架 组建由IT、安全、法务、合规等组成的跨职能团队，共同解读全球法规，明确主权要求，并搭建集中化的合规管理框架。借助经过研究验证的成熟模型，在法规持续变化之时，保持合规方向的一致性。同时，为所有利益相关方提供持续培训与宣导。
02 在创新与主权管控之间取得平衡 将数据驻留、运营透明度、技术独立性嵌入云运营，往往会让创新速度减缓、复杂度升高。I&O负责人需要在敏捷性、可扩展性与主权、隐私合规的严格要求之间找到恰当的平衡点。	实现合规自动化，并将其融入云运营体系 采用基础设施即代码（IaC）、策略即代码（PaC）和自动化监控手段，将合规与主权管控要求嵌入云部署流程。同时把合规检查集成到CI/CD流水线，并通过集中式仪表盘实现多云环境的实时可视化。
03 管控第三方及超大规模云服务商依赖风险 过度依赖海外超大规模云服务商或外部供应商，会令企业面临监管和地缘政治风险。I&O负责人还需在主权要求与业务连续性之间做好权衡，确保合规要求不会削弱系统的韧性与恢复能力。	多元化布局云合作伙伴，投资主权赋能技术 评估可信的本土或区域云服务商，并探索合作机会。同时投资外部密钥管理、机密计算、增强审计等技术，确保无论服务商位于何处，企业都能牢牢掌握对数据和运营的控制权。

01

应对策略

建立统一的合规与主权框架

构建稳健的云主权战略，离不开IT、安全、法务和合规团队的紧密协作。I&O负责人必须统筹各方，解读全球法规，明确主权要求，确保管控措施落地执行，及时跟上不断变化的监管要求。这种统一协作的方式，能在复杂的监管环境中有效降低风险、保持业务敏捷性，并切实守护数据隐私。

不同地区的监管要求存在差异，各利益相关方对风险、运营透明度和技术独立性的看法也不尽相同。为克服这些障碍，企业应建立一套集中化的合规框架，整合各职能部门的意见，清晰传达合规预期，并能灵活适配新的法律法规。

跨职能团队与统一的合规模式，为云主权打下了坚实基础。I&O负责人需要主动应对监管变化，减少合规碎片化，赢得客户与监管机构的信任，从而支撑安全、有韧性且富有创新力的云运营。

主权云战略必备特征



来源：Gartner

02

应对策略

实现合规自动化，并将其融入云运营体系

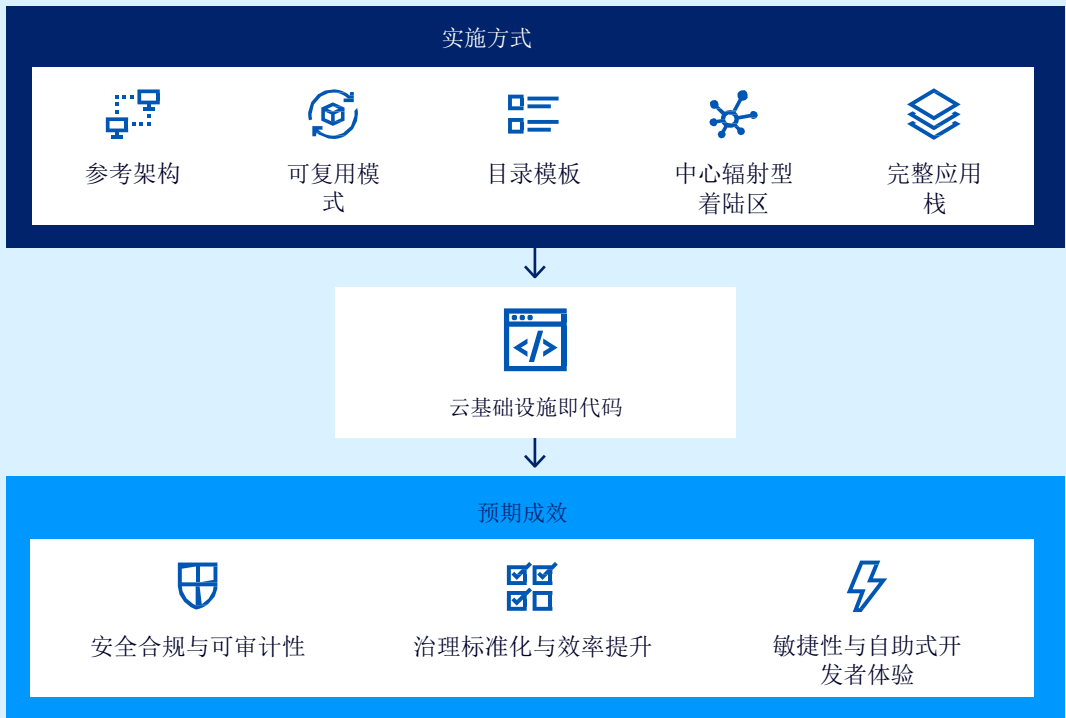
要在创新与主权管控之间取得平衡，I&O负责人必须将监管要求直接嵌入云运营，彻底告别依赖人工的合规管理方式。

通过自动化、基础设施即代码（IaC）、策略即代码（PaC）和自动化监控，确保无论部署规模多大、使用哪家云服务商，合规与主权要求都能在所有环境中得到一致执行。

这一方式兼顾了敏捷性与控制力。在CI/CD流水线中内嵌自动化合规检查，结合实时监控的集中式仪表盘和持续审计能力，有助于企业主动识别并修复风险。内嵌的管控措施既能减少人为失误、加快部署节奏，并确保默认符合主权与隐私要求，无需额外干预。

当合规成为云生命周期中的内建属性，I&O负责人就能在最小化监管风险和运营复杂度的同时，赋能团队快速创新。

借助云基础设施即代码实现预期成效



来源：Gartner

03

应对策略

多元化布局云合作伙伴，投资主权赋能技术

管理第三方及超大规模云服务商依赖带来的风险，需要一套前瞻性策略，将运营控制力和法规遵从放在首位。I&O负责人应积极评估多元化布局云合作伙伴的机会，例如借助可信的本土或区域服务商，建立符合主权要求的战略联盟。但需要留意的是，服务商数量增多也可能导致云资源分散和管理复杂度上升。

投资主权赋能技术（如外部密钥管理、机密计算、高级审计工具），可帮助企业掌控敏感数据和关键业务运营，无论云工作负载部署于何处。这些技术有助于化解外国政府访问、服务中断以及监管政策变动带来的风险。

通过将多元化的服务商策略与一流的技术管控相结合，I&O负责人既能降低依赖风险、增强运营韧性，确保满足当前及未来的主权合规要求，也能时刻警惕服务商数量膨胀与系统集成带来的新挑战。

实现运营主权的解决方案



来源：Gartner

Gartner相关洞察推荐



[《构建主权云战略》 ↗](#)

[《主权云：理解并应对主权合规要求》 ↗](#)

[《如何选择最合适的自愿性隐私框架》 ↗](#)

[《利用基础设施平台工程与基础设施即代码保障云安全》 ↗](#)

[《紧跟美国网络安全监管变化，保持数据中心与云合规》 ↗](#)

[《隐私趋势2026：如何通过数据伦理、主权云与无摩擦用户体验建立信任》 ↗](#)

[《数字主权解决方案市场指南》 ↗](#)

[《提升政府的数字主权与韧性》 ↗](#)



[Gartner IT领导者服务](#)

[成为客户](#)

切实可行的客观洞察

探索更多面向I&O领导者的免费资源与工具：

网络研讨会

《企业生成式人工智能基础设施战略与部署实践》

探讨如何制定高效的 GenAI 基础设施战略，助力企业构建灵活、可扩展的 AI 支撑体系。

立即观看



电子书

《CIO首席信息官如何应对AI规模化、云成本与安全挑战》

了解 CIO 如何应对 AI 规模化、云成本与安全挑战，推动企业实现高效创新与可持续增长。

现在下载



路线图

AI就绪数据要点

确保数据能够支持拟推进的具体AI项目，并帮助利益相关方统一理解数据实现AI就绪所需具备的条件。

立即阅读



工具

针对基础设施和IT运营的IT Score评价模型

对标绩效基准，制定关键行动举措，助力高效的基础设施和IT运营领导者脱颖而出。

了解更多



已是Gartner客户？通过Gartner客户服务平台获取更多资源。[登录↗](#)

联系我们

获取客观公正、切实可行的商业与技术洞见，驱动关键任务领域的智慧决策与卓越绩效。

点击以下链接，了解关于Gartner I&O领导者服务的更多信息：
gartner.com/cn

成为客户