High risk, high reward: managing corruption risk in the global data centre boom

Published 26-Oct-2026 by
Jonah Anderson, Courtney Andrews and Darryl Lew, White & Case

Developers and hyperscalers are engaged in an arms race for land, power, water and capital to build the global data centre infrastructure necessary to support the development of AI. The resulting mega projects exceed the resources of even the largest companies, leading them to enter into public and private partnerships and seek third-party capital to fuel this rapid growth.

While much of this growth has occurred and continues to occur in the United States and Western Europe, developers and hyperscalers are turning increasingly to emerging markets to host this build-out which are often characterised by a smaller pool of under-qualified, yet often necessary, local partners and suppliers and the need for extensive government approvals amid a climate of endemic corruption.

Combined with the sheer scale and pace of construction and related spend, these factors combine to create unprecedented levels of corruption risk under anti-corruption regimes including the U.S. Foreign Corrupt Practices Act (FCPA) and the UK Bribery Act 2010. Developers and hyperscalers must therefore adopt clear strategies to manage this risk and engage effectively and compliantly with host governments, local partners, and key suppliers.

Host governments

Building data centres generally requires significant engagement with the host country's government, including in connection with land acquisition, environmental permits, grid connection approvals, tax incentive negotiations, value-adds to the host country in the form of donations or other investments, and customs clearance for imported equipment. Data centre developers and hyperscalers usually do not engage alone or directly with host governments, particularly in unfamiliar markets, and instead generally rely on a combination of local partners, general contractors and their subcontractors, and local counsel, consultants, and agents.

Anti-corruption laws such as the FCPA and UKBA prevent companies from shielding themselves from liability by using third parties as intermediaries to interact with local government officials. Indeed, illustrating how intermediary arrangements can become the vector for liability, the vast majority of enforcement actions by anti-corruption authorities have involved the use of third parties.

Developers and hyperscalers entering unfamiliar markets can mitigate corruption and related risks through an effective compliance program tailored to industry and country risks. For hyperscalers, which historically have operated in the software and cloud services industry, building mega infrastructure projects in emerging markets presents a very different risk profile. Such markets, and the compliance challenges they present, are often new for developers as well, who may be navigating cross-border compliance requirements for the first time.

Enforcement authorities on both sides of the Atlantic expect companies to calibrate their compliance programs and to allocate resources based on the risk posed by their business activities in the jurisdictions where they operate. In the United States, an effective compliance program can significantly mitigate liability in connection with an FCPA violation.

In the UK, having "adequate procedures" in place to prevent bribery goes even further and serves as a defence against liability. For both groups of companies, therefore, creating and adopting bespoke, risk-based compliance playbooks is necessary to manage effectively the corruption risk data centre projects create and ensure they are well-placed to respond if misconduct occurs and enforcement authorities come knocking.

Effective third-party management is a critical element of an effective compliance program in an industry where developers and hyperscalers must rely on multiple tiers of third parties, including:

- Ensuring periodic anti-corruption vetting of third parties engaged directly by the developer or hyperscaler and a thoughtful, defensible approach to vetting downstream suppliers, e.g., subcontractors engaged by general contractors.
- Including anti-corruption provisions, such as representations and warranties and compliance-related audit and termination rights, in third-party agreements and structuring contractual obligations with counterparties and in contracts between counterparties and downstream suppliers (with whom the developer or hyperscaler may not have contractual privity) to require information sharing and cooperation with the developer or hyperscaler to address compliance red flags should they arise.
- Implementing an active third-party audit program, including in connection with any donations or investments.

Local partners

THOMSON REUTERS™

© 2026 Thomson Reuters. No claim to original U.S. Government Works.

Many emerging markets have local content requirements that require foreign investors to partner with local companies, often resulting in joint venture or similar local project companies. Such requirements aim to keep a larger share of the project value within the host country's economy by stimulating employment, supporting local supply chains, and encouraging knowledge transfer and the generation of local operational skills.

Despite these salutary objectives, such partnerships nonetheless can pose heightened corruption risk, particularly where a local partner's value lies in its ability to navigate the local market due to government connections. Indeed, host governments may recommend — or even insist on the use of — individual local partners, creating heightened corruption and conflict-of-interest risks.

Developers and hyperscalers should assess local partner candidates' qualifications and other objective factors to confirm that such entities are qualified and add value commensurate with their equity or other stake in the project. In markets where a developer or hyperscaler is required or otherwise chooses to co-venture with a local partner, a well-considered approach from a compliance perspective is critical, including:

- Identifying competent local partner candidates and evaluating their qualifications based on pre-determined, objective criteria.
- Vetting local partner candidates to ensure they do not have disqualifying red flags, and documenting the existence of risk factors and how they were mitigated;.
- Including appropriate anti-corruption provisions, such as representations and warranties and compliance-related audit and termination rights, into transaction agreements;.
- Ensuring the local project company promptly adopts, or is integrated into an existing, risk-based compliance program; and.
- Implementing appropriate on-the-ground governance and oversight mechanisms and staffing in-country compliance gatekeeper roles with trusted and experienced personnel.

Key suppliers

Construction of mega projects, such as data centre campuses, typically involves a general contractor managing dozens of subcontractors and key suppliers. In addition to public corruption risks, large infrastructure projects also create significant commercial bribery risks. When capital is becoming increasingly scarce and expensive given the sheer volume and magnitude of data centre projects globally, a project's bottom line may also be at risk if funds are corruptly siphoned off by faithless employees or third parties.

In addition to following best practices for engaging with host governments and third parties from a public corruption perspective, developers and hyperscalers should adopt procurement and other controls to minimise the risk of commercial bribery, including by:

- Enforcing competitive procurement requirements with objective qualifications and creating documented exceptions processes.
- Defining and enforcing rigorous change order processes to avoid situations where contractors secure lucrative projects through low initial bids followed by inflated change orders.
- Implementing training and messaging for relevant company and supplier employees that corruptly directing work to a favoured supplier in exchange for cash, gifts, free services, or other things of value is prohibited - and communicating the consequences for engaging in such misconduct.
- Using data-driven solutions to test supplier invoices to identify inflated unit prices, fictitious or duplicated line items, or unjustified change orders that could serve improper purposes.

Risk management

The commercial rewards and incentives in the data centre sector are high but, as developers and hyperscalers race to build new projects in emerging markets, so are the accompanying corruption risks. Risks must be assessed and addressed actively before a project begins to avoid or at least minimise the cost, disruption, and reputational impact that eventual investigations of these projects could cause.

Jonah Anderson, Courtney Andrews and Darryl Lew, White & Case LLP

Any views expressed in this publication are strictly those of the authors and should not be attributed in any way to White & Case LLP.

Complaints Procedure

Produced by Thomson Reuters Accelus Regulatory Intelligence 27-Oct-2026

THOMSON REUTERS™

© 2026 Thomson Reuters. No claim to original U.S. Government Works.