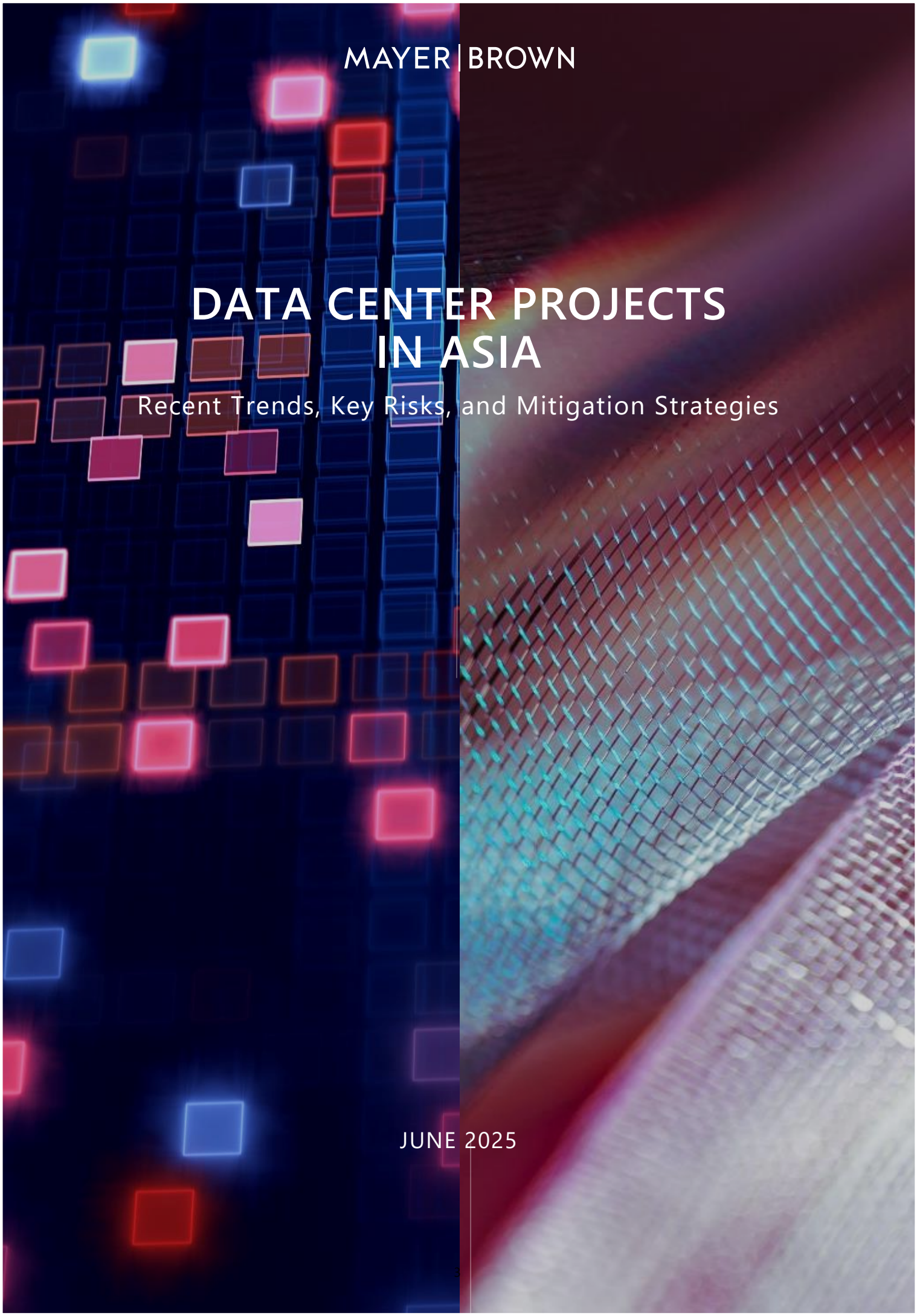
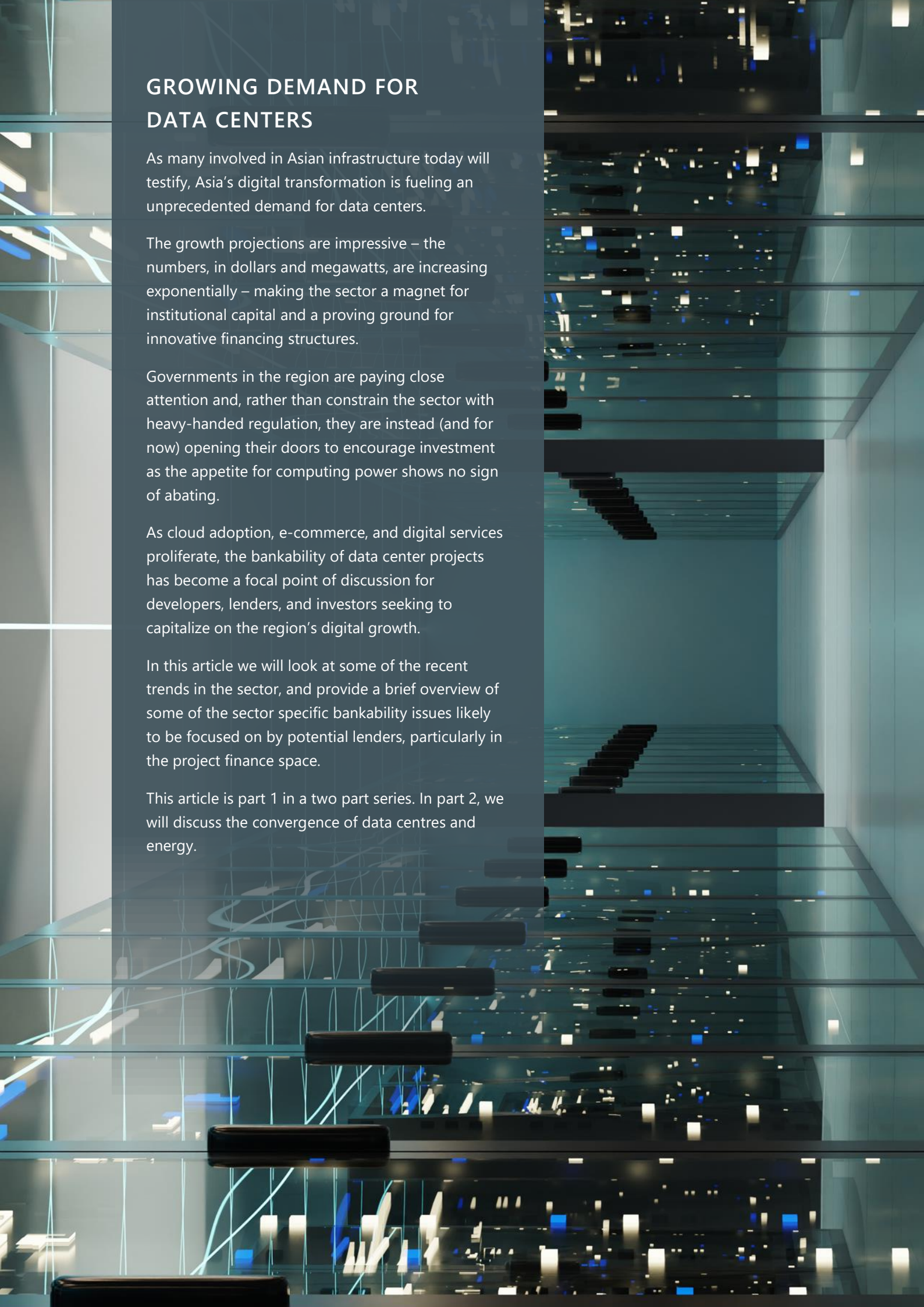

MAYER | BROWN
DATA CENTER PROJECTS IN ASIA
Recent Trends, Key Risks, and Mitigation Strategies
JUNE 2025



GROWING DEMAND FOR DATA CENTERS

As many involved in Asian infrastructure today will testify, Asia's digital transformation is fueling an unprecedented demand for data centers.

The growth projections are impressive – the numbers, in dollars and megawatts, are increasing exponentially – making the sector a magnet for institutional capital and a proving ground for innovative financing structures.

Governments in the region are paying close attention and, rather than constrain the sector with heavy-handed regulation, they are instead (and for now) opening their doors to encourage investment as the appetite for computing power shows no sign of abating.

As cloud adoption, e-commerce, and digital services proliferate, the bankability of data center projects has become a focal point of discussion for developers, lenders, and investors seeking to capitalize on the region's digital growth.

In this article we will look at some of the recent trends in the sector, and provide a brief overview of some of the sector specific bankability issues likely to be focused on by potential lenders, particularly in the project finance space.

This article is part 1 in a two part series. In part 2, we will discuss the convergence of data centres and energy.

RECENT TRENDS IN DATA CENTER FINANCING IN ASIA

The financing landscape for data center projects in Asia has evolved rapidly in recent years, reflecting both the sector's dynamic growth and the increasing sophistication of market participants.

Developers have access to a whole range of financing options and structures, and at different levels of the capital stack, with increasing leverage in negotiating the terms as lenders compete in the space.

Each financing is deal-specific, but several notable trends have emerged, shaping how data center projects are structured, funded, and delivered.

SURGE IN INSTITUTIONAL AND INTERNATIONAL CAPITAL

Institutional investors, including global private equity funds, infrastructure investors, and sovereign wealth funds, have shown heightened interest in Asian data center assets. This influx of capital is driven by the sector's stable, long-term cash flows (once operational), and its critical role in supporting digital economies. International lenders and export credit agencies are also increasingly active, often partnering with local and regional banks to provide large-scale, multi-currency financing packages. In short, there is no shortage of financiers lining up to provide support, leaving developers spoiled for choice to some degree.

RISE OF GREEN AND SUSTAINABILITY-LINKED FINANCING

Environmental, social, and governance ("**ESG**") considerations are now central to data center financings. For example, many in the sector have emphasized their commitment to carbon-free power, and there is a marked increase in the use of green loans and sustainability-linked financing structures, where loan pricing is tied to the achievement of specific ESG targets such as energy efficiency, carbon-free electricity supply, or water conservation. This trend is supported by both lender requirements and the growing demand from tenants – particularly the global technology companies – for sustainable infrastructure. Whether the sector can continue to live up to its 100% carbon-free energy ambition whilst meeting the insatiable levels of electricity demanded by the data centers is the big question. We will explore more of this topic in detail in our second upcoming article on the convergence of energy and data centers.

SHIFT TOWARD HYPERSCALE AND EDGE DATA CENTRES

Financing structures are adapting to the rise in the region of hyperscale data centres, which require significant upfront capital and are often anchored by long-term contracts with major cloud service providers and AI developers. At the same time, there is growing interest in edge data centers – smaller facilities located closer to end-users to reduce latency. These projects may involve different risk profiles and financing approaches, including smaller ticket sizes and more flexible structures.

INCREASED USE OF PROJECT FINANCE STRUCTURES

While corporate balance sheet funding remains common, there is a clear trend toward project finance structures, particularly for larger or greenfield developments. Project finance allows developers to ring-fence project

risks and leverage non-recourse or limited-recourse debt, supported by robust contractual frameworks and security packages. This approach is attractive to both developers and lenders, as it aligns risk allocation with project fundamentals. However, for developers, it is crucial to understand which financing approach a prospective lender is assessing for its project, particularly to avoid being pulled in too many different directions by differing credit analyses.

GREATER EMPHASIS ON PRE-LEASING AND ANCHOR TENANCY

Lenders are placing increased emphasis on pre-leasing levels and the presence of creditworthy anchor tenants before committing to financing, reflecting the need for predictable revenue streams and the desire to mitigate demand risk. As a result, developers are prioritizing the early negotiation and execution of long-term, take-or-pay contracts – often with global cloud service providers, hyperscalers, or large enterprise clients – well before construction commences. These contracts typically guarantee a minimum level of committed revenue regardless of actual usage. Under a take-or-pay contract, the tenant agrees to pay for a specified amount of capacity or service whether or not they actually use it, ensuring a minimum revenue stream for the developer.

Developers are also seeking to diversify their tenant base to reduce reliance on a single customer and further de-risk the project from a revenue perspective. Lenders may require that a certain percentage of the facility's capacity be pre-leased to multiple tenants under take-or-pay contracts, and will closely scrutinize the creditworthiness of each counterparty. Lenders could also insist on parent company guarantees or letters of credit from tenants, especially those that are not sufficiently capitalized or may not have sufficient cash-flows to fulfil their payment obligations.

REGIONAL DIVERSIFICATION AND LOCAL PARTNERSHIPS

Data center development is expanding rapidly beyond the more evolved and traditional digital hubs such as Singapore, Hong Kong, and Tokyo. Although Singapore remains a regional leader in Southeast Asia, Malaysia and Indonesia have developed as new hubs in the region as well. Additionally, Thailand is attracting major interest from hyperscalers, and Vietnam is an emerging hub following favorable legislative developments (most notably the removal of the foreign ownership cap in July 2024).

In these markets, developers often form joint ventures or partnerships with local players to navigate regulatory requirements, secure land, and access local financing sources.

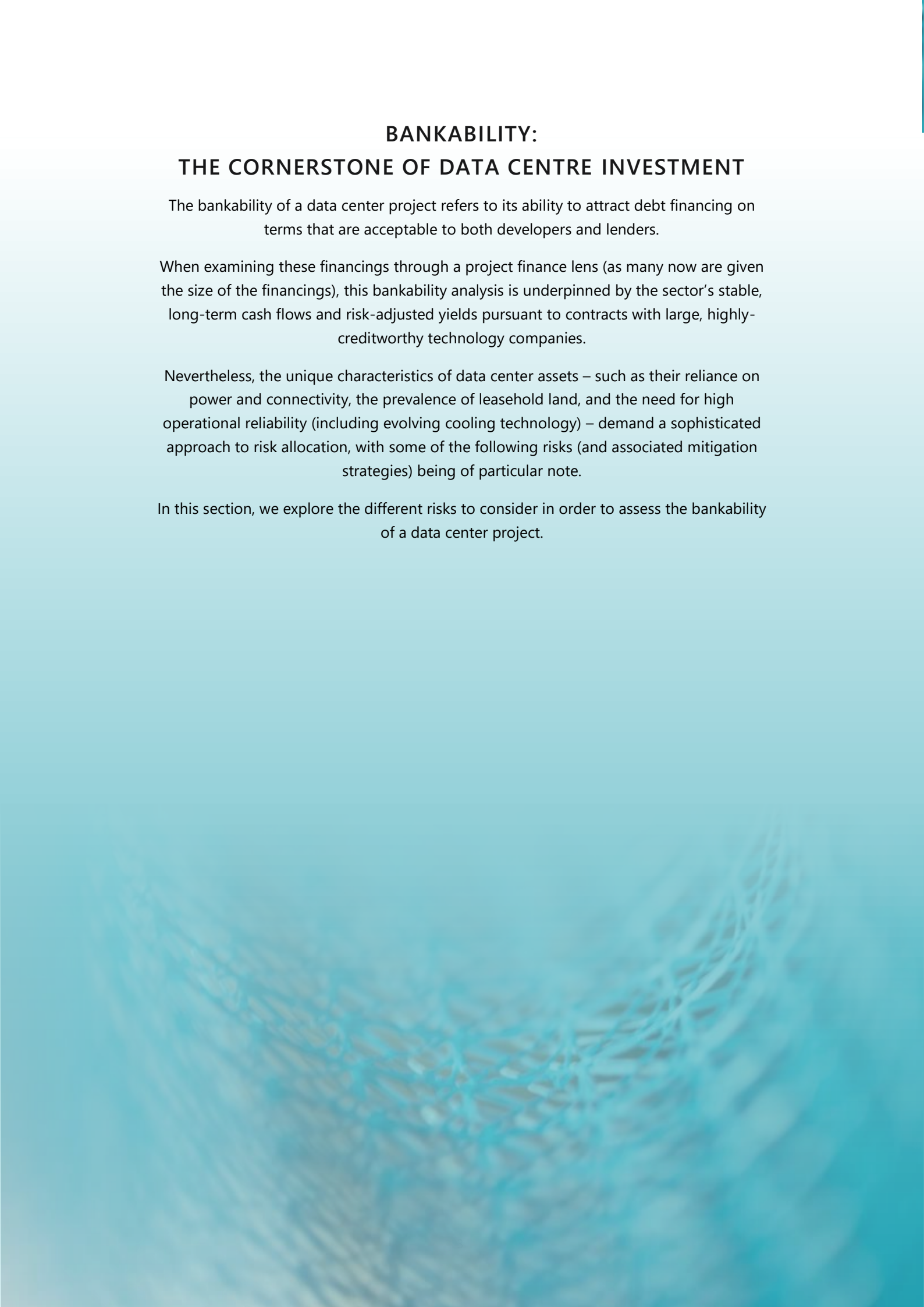
BANKABILITY:
THE CORNERSTONE OF DATA CENTRE INVESTMENT

The bankability of a data center project refers to its ability to attract debt financing on terms that are acceptable to both developers and lenders.

When examining these financings through a project finance lens (as many now are given the size of the financings), this bankability analysis is underpinned by the sector's stable, long-term cash flows and risk-adjusted yields pursuant to contracts with large, highly-creditworthy technology companies.

Nevertheless, the unique characteristics of data center assets – such as their reliance on power and connectivity, the prevalence of leasehold land, and the need for high operational reliability (including evolving cooling technology) – demand a sophisticated approach to risk allocation, with some of the following risks (and associated mitigation strategies) being of particular note.

In this section, we explore the different risks to consider in order to assess the bankability of a data center project.



CONSTRUCTION-STAGE RISKS

Data center projects can be capital-intensive and technically complex, with tight timelines and high specifications for power, cooling, and security. Delays, cost overruns, supply chain constraints, permitting delays or technical failures during construction can jeopardize project delivery, delay revenue generation, and increase financing costs.

TECHNICAL COMPLEXITY AND RAPIDLY EVOLVING SPECIFICATIONS

Data centers require extremely high technical specifications, especially for power density, cooling, and security. The sector is marked by fast-paced technological change, with specific requirements often evolving even during construction. The integration of advanced cooling technologies (like liquid or direct-to-chip cooling) and scalable power infrastructure to support AI and hyperscale computing can introduce additional complexity and the risk of scope changes or obsolescence. The need to future-proof facilities against emerging technologies is an ongoing challenge.

MITIGANTS

TAILORED EPC CONTRACTS

Lenders will expect EPC contracts to be tailored to the unique technical and operational requirements of data centers, with detailed performance specifications for power usage effectiveness (PUE), cooling efficiency, system redundancy (N+1/N+2), and uptime guarantees.

PROVISION FOR DESIGN FLEXIBILITY

EPC contracts should be structured to provide sufficient flexibility for the integration of emerging technologies and evolving technical requirements (such as the adoption of new cooling systems, increased power density, or enhanced redundancy features) through clearly defined change-order procedures. Developers are also moving towards phased construction and modular design approaches, which provide flexibility to adapt to changing requirements and reduce the risk of large-scale rework if technology standards shift during the construction phase.

ROBUST LIQUIDATED DAMAGES REGIME FOR DELAY AND DATA CENTRE PERFORMANCE

Contractors are generally expected to be liable for liquidated damages for both delay in completion and failure to meet key technical performance guarantees. For data centers, these guarantees should specifically address sector-specific metrics such as PUE, cooling capacity, system redundancy, and uptime.

SUPPLY CHAIN AND EQUIPMENT LEAD TIMES FOR MISSION-CRITICAL COMPONENTS

The global supply chain for data center-specific equipment, such as high-capacity generators, switchgear, precision cooling units, UPS systems, and specialist IT infrastructure, is often stretched, especially during sectoral growth or geopolitical disruption.

Delays in delivery of these critical components can threaten project schedules and increase costs. The specialized nature of this equipment, often sourced from a limited pool of international suppliers, also exposes projects to currency fluctuations,

import/export restrictions, and quality-assurance risks.

MITIGANT

CONTINGENCY PLANNING AND RESERVES

Financing structures should include contingency reserves not only for generic cost overruns as is usual, but also for technology upgrades, supply chain disruptions, and regulatory changes.

PERMITTING, UTILITY CONNECTIONS, AND REGULATORY DELAYS

Data center construction requires a complex array of permits and regulatory approvals, including those related to land use, environmental impact, and, crucially, utility connections for high-capacity power and fiber. Delays in obtaining these approvals or in securing sufficient power and connectivity can significantly stall project commencement or progress, particularly in jurisdictions where regulatory frameworks are still adapting to the sector's rapid growth. Permitting remains an under-appreciated delay risk factor.

MITIGANTS

EARLY AND PROACTIVE ENGAGEMENT

Developers need to engage with regulatory authorities and utility providers early in the project lifecycle and on an ongoing basis to identify and address potential permitting or utility connection issues. This is especially important for securing long-term power purchase agreements (PPAs) and ensuring access to reliable, scalable power, and connectivity.

INTERFACE AND COORDINATION RISK AMONG SPECIALIST CONTRACTORS

Data center projects typically involve a number of specialist contractors and suppliers working in parallel – civil, electrical, mechanical, IT systems, security, and fire suppression. Coordination risk exists whether the project is built under a single EPC contract or split into multiple work packages.

Even with a single EPC contract, where the head contractor is responsible for delivering the whole project on a turnkey basis, it must still manage and coordinate many specialist subcontractors. There is no single EPC contractor that has all the in-house skills needed to deliver every part of a data center. This means that integrating systems like building management (BMS), fire suppression, and security with the core IT infrastructure remains complex, and delays or mistakes in one area (such as late delivery of cooling units or switchgear) can affect the whole project.

Lenders will prefer a single turnkey EPC contract (especially for hyperscale data centres) because the head contractor is ultimately responsible for all coordination risks. There are however recent examples of smaller or specialized data center projects being deployed under a multi-work package approach, with key systems (such as cooling and power) being split into separate contracts, often because of specialized vendor requirements or to address supply chain bottlenecks.

MITIGANT

COMPREHENSIVE INTERFACE MANAGEMENT FOR SPECIALIST CONTRACTORS

Regardless of the delivery model, lenders will expect robust interface management protocols to be put in place, including clear delineation of responsibilities, regular coordination meetings, and the use of digital project management tools to track progress and manage dependencies. In the case of a single turnkey arrangement, this is usually done by the head contractor, and in the case of a multi-package approach, this is done by the developer.

OPERATIONS-STAGE RISKS

STRINGENT UPTIME AND RELIABILITY REQUIREMENTS

Data centers must deliver extremely high levels of operational reliability, often targeting "five nines" (99.999%) uptime or higher. Any operational failure, even of a short duration, can result in significant financial losses for tenants, reputational damage for the operator, and potential liability under service agreements.

MITIGANT

ENGAGEMENT OF SPECIALIST DATA CENTRE OPERATORS

Lenders expect developers to engage operators with a proven track record in managing mission-critical data center environments. The operator's experience should specifically include managing high-density power and cooling loads, implementing advanced monitoring and automation systems, and maintaining compliance with international data center standards (such as Uptime Institute Tier certifications or ISO 27001).

Developers may also opt to operate the facility themselves under a "data center as a service" model, in which case lenders will have the same requirements.

Structuring the power supply arrangements to maintain such operational reliability is obviously crucial, and is a topic we will explore in more depth in our next article.

RAPID TECHNOLOGICAL CHANGE AND OBSOLESCENCE

The pace of technological advancement in IT hardware, cooling, and energy efficiency means that operational practices and systems must be continuously updated. Failure to keep pace can result in higher operating costs, reduced competitiveness, and difficulty attracting or retaining tenants.

MITIGANT

ADVANCED MONITORING, AUTOMATION, AND PREDICTIVE MAINTENANCE

Data center operations increasingly rely on sophisticated building management systems (BMS) and data center infrastructure management (DCIM) platforms. These systems provide real-time monitoring of power, cooling, and environmental conditions, enabling early detection of anomalies and predictive maintenance. Automation can reduce human error and improve response times to incidents. Lenders will require evidence of such systems being in place and regularly updated.

NETWORK CONNECTIVITY RISK

Reliable, high-capacity network connectivity is essential for any data center. This is particularly so if the facility relies on a single network provider or has limited fiber routes, as any disruption – such as a cable cut or equipment failure – can impact all tenants. Inadequate bandwidth or high latency can also make the data center less attractive to tenants, especially those with demanding applications like cloud services, financial trading, or AI workloads.

In some jurisdictions, regulatory restrictions on network infrastructure or cross-border data flows can further complicate connectivity.

MITIGANTS

MULTIPLE NETWORK PROVIDERS AND DIVERSE ROUTES

Data centers typically contract with several independent fiber providers and ensure that network cables enter the facility through different physical routes. This reduces the risk of a single point of failure and helps maintain service even if one provider or route is disrupted.

CARRIER-NEUTRAL DESIGN

Many data centers are designed to be carrier-neutral, allowing multiple network providers to operate within the facility. This gives tenants more choice and reduces dependency on any single provider.

DIRECT CLOUD AND INTERNET EXCHANGE CONNECTIONS

Establishing direct connections to major cloud platforms and internet exchanges is now standard practice. This ensures low-latency and high-reliability access to global cloud services, which is a key requirement for many tenants.

STRINGENT SERVE LEVEL AGREEMENTS (SLAS)

As with PPAs, contracts with network providers should include strict SLAs covering uptime, latency, repair response times, and bandwidth guarantees. These SLAs are often backed by liquidated damages for non-performance.

CYBERSECURITY AND PHYSICAL SECURITY THREATS

Data centers are prime targets for both cyber and physical security threats. Operational lapses in security protocols can expose tenants to data breaches, service interruptions, and regulatory penalties.

MITIGANT

COMPREHENSIVE SECURITY FRAMEWORKS

Industry practice dictates that data center operators implement robust physical and cyber security measures, including multi-factor access controls, 24/7 surveillance, biometric authentication, and regular penetration testing of IT systems. Lenders will also expect security protocols to be aligned with international best practices and subject to regular audit, including maintenance of third-party security certifications.

CONTRACTUAL AND PERFORMANCE RISKS IN OPERATIONS

Operational failures can result in breaches of SLAs with customers, leading to financial penalties, tenant claims, and reputational harm.

MITIGANTS

COMPREHENSIVE, DATA CENTER-SPECIFIC O&M CONTRACTS

Operations and maintenance (O&M) contracts should be tailored to the unique requirements of data centers. This includes detailed SLAs that specify not just generic uptime, but also metrics such as PUE, response times for critical incidents, and maximum allowable temperature or humidity deviations. Performance liquidated damages should be calibrated to reflect the true cost of downtime or underperformance in a data center context.

DIRECT AGREEMENTS AND STEP-IN RIGHTS

Lenders typically require direct agreements with the data center operator, granting them step-in rights in the event of persistent underperformance or default. These agreements should be tailored to the data center context, ensuring that lenders can appoint a qualified replacement operator with minimal disruption to ongoing operations and tenant services.

CHURN AND TECHNOLOGY OBSOLESCENCE

The financial viability of a data center project is fundamentally dependent on securing robust, long-term demand from creditworthy tenants. Unlike many traditional infrastructure assets, data centers face a unique set of revenue risks due to the rapid pace of technological change, evolving tenant requirements, and the highly competitive landscape for digital infrastructure.

The rapid evolution of IT hardware and cloud architectures means that tenants may seek to relocate or consolidate their operations as technology advances. This creates a risk of higher churn rates and shorter average contract tenures compared to other infrastructure asset classes.

MITIGANTS

FUTURE-PROOFING FACILITY DESIGN

As highlighted in the construction section above, developers are increasingly adopting modular, scalable designs with advanced cooling/power infrastructure to accommodate evolving tenant requirements and reduce the risk of obsolescence.

ACTIVE ASSET MANAGEMENT

Ongoing engagement with tenants to anticipate future needs and proactively offer upgrades or expansions can help retain key customers and maintain high occupancy rates.

ENVIRONMENTAL AND SOCIAL RISKS

Data centers have a significant environmental footprint, particularly in terms of energy and water usage, and are increasingly subject to related scrutiny from regulators, investors, tenants, and local communities. In particular, traditional data center cooling systems can consume large volumes of water, which is a growing concern in water-stressed regions.

MITIGANT

ADVANCED COOLING SOLUTIONS

The industry is seeing a move towards the adoption of water-efficient or waterless cooling technologies (e.g., direct-to-chip, liquid immersion, or closed-loop systems) to minimize water consumption and reduce environmental impact. Implementation of greywater recycling and rainwater harvesting systems can also contribute to further reduce reliance on municipal water supplies.

CONCLUSION

The bankability of data centrer projects in Asia is being shaped by a confluence of strong sector fundamentals, innovative financing structures, and sophisticated risk mitigation strategies.

As the market continues to mature, developers and their lenders are demonstrating a growing ability to adapt and structure financings that focus on bankability fundamentals, whilst being flexible and pragmatic enough to accommodate the particularities and fast moving nature of the sector.

By embracing innovation, sustainability, and comprehensive risk management, data centers in Asia are poised to play a pivotal role in the region's digital future.

KEY CONTACTS

If you would like to learn more on how we can help and support you in the data center and energy space in Asia, please reach out to our key contacts listed below.

HEAD OF PROJECTS & INFRASTRUCTURE (ASIA)
PARTNER

BEN THOMPSON

SINGAPORE +65 6922 2248

BEN.THOMPSON@MAYERBROWN.COM

REGISTERED FOREIGN CONSULTANT

MATTHEW CHOW

HONG KONG +852 2977 1766

MATTHEW.CHOW@MAYERBROWN.COM

MAYER|BROWN