NORTON ROSE FULBRIGHT

Guide to investing in Data Centres: challenges, opportunities and funding

Norton Rose Fulbright LLP – 10 June, 2025

Foreword

-.-. --- -- -- ..- -. .. -.-. .- - .. --- -.

(Communication)

Long before Samuel Morse invented the Morse Code, humans had found ways to communicate over both time and distance. Cave paintings allowed stories to be passed down through generations, and the invention of the printing press created possibilities for these stories to travel greater distances. Modern day influencers may think they invented the idea of documenting food, but our ancestors were including depictions of food on cave walls as far back as 40,000 years ago.

Our need and desire to communicate may not have changed much over the thousands of years since our ancestors etched those drawings, but it is impossible to ignore that the way in which we communicate has changed and still continues to change. Other than face-to-face communication, our interactions largely take place in the digital world – scrolling social media, checking news sites, streaming films and TV shows, working (remotely or in the office), adjusting our smart thermostats, sending e-mails at work and at home, attending virtual meetings. These things may in themselves make up only a fraction of our day, but when combined it means we spend an average of 13 hours online every single day[1]. That's a little over half our day that is spent in the digital world.

We may access that digital world from our phones, our laptops, our TV's or our tablets. Yet these are just the gateways. Behind these gadgets sits the backbone of the digital world, the data centre. Data centres don't operate the cloud, or create AI models, or stream the content. But they do enable it, power it, streamline it, accelerate it.

It is difficult to predict with any accuracy what the future demand for data centre capacity will look like. Whilst the rate of adoption of AI will impact this, so will the types of computer chips that are used and the balance of edge and cloud computing. Whichever figures you look at though, they all predict an increase in demand, and, if we fail to meet that demand, a significant supply deficit.

In this guide we take a closer look at data centres – the types, key challenges and funding, and how securitisation can help bridge the funding gap.

[1] UK adults online for 76% of waking hours, study finds

Contents

Types of data centres

There are close to 5.6 billion internet users globally but our demands and needs for digital (virtual) ‘housing’ are as varied as our real-world housing demands and needs. What a small-scale tech-startup company needs (and is willing to pay for) is not the same as what a large tech conglomerate needs. Data centres are not, and never will be, a one-size-fits-all. If we are to have a meaningful debate around supply, demand and funding, we need to start with the subject matter and how they differ.

The table on page 5 summarises the key features of the main types of data centres, with details of average construction and operating costs.

Type	Description	Key Features	Ideal For	Additional Details	Construction Cost	Operating Cost
Enterprise Data Centres	Owned and operated by individual organisations.	Customized networks, enhanced security.	Large corporations with specific IT needs	Allows high control over infrastructure and compliance with industry regulations; Often high costs.	$600 to $1,100 per gross square foot or $7 million to $12 million per megawatt[1].	$10 million to $25 million annually[2].
Colocation Data Centres	Third-party facilities where multiple organizations rent space.	Shared infrastructure, cost savings.	Businesses needing reliable services without maintenance overhead	Offers disaster recovery solutions, hybrid IT strategies, and high-volume applications.	$10 million to over $100 million, depending on size and location[3].	Varies widely; typically includes space, power, bandwidth, and additional services[4][5].
Hyperscale Data Centres	Massive facilities supporting scalable applications and cloud services.	Efficiency, scalability.	Companies handling vast amounts of data	Typically house at least 5,000 servers, focus on energy efficiency, and high automation.	$600 to $1,100 per gross square foot or $7 million to $12 million per megawatt[1].	High operational costs due to power-intensive infrastructure[6].
Edge Data Centres	Located closer to end-users to reduce latency.	Real-time data processing.	Applications requiring real-time performance	Small, decentralized facilities, often located at telecom central offices or cell towers.	Generally lower than traditional data centres; varies by location and size[7].	Lower operating costs due to smaller size and decentralized nature[8].
Modular Data Centres	Pre-fabricated units for quick deployment and scaling.	Flexibility, rapid deployment.	Businesses with fluctuating data centre needs	Consist of standardised modules, can be containerized or prefabricated, and offer scalability.	$600 to $1,100 per gross square foot or $7 million to $12 million per megawatt[1].	$10 million to $25 million annually[2].

2

[2] [1] How Much Does it Cost to Build a Data Center? - Dgtl Infra
[2] Breaking Down Data Center Cost: Building vs. Outsourcing
[3] An Overview of Data Center Costs (All You Need to Know)
[4] Understanding Colocation Data Center Pricing in 2024
[5] Data Center Colocation Costs: Price Guide - DataCenterAndColocation
[6] North America Data Center Trends H2 2024 - CBRE
[7] Data Center Development Cost Guide - Cushman & Wakefield
[8] What is an Edge Data Center? (With Examples) - Dgtl Infra

A closer look at construction costs

As the above table demonstrates, construction costs can vary from as low as $200 per square foot to over $1000 per square foot. The key factors that influence the construction cost variance are:

1 **Location**

Land price: Variances between urban and rural locations, and between different countries significantly influences overall construction cost;

Labour costs: Areas with higher living costs and living standards will attract higher labour costs;

Energy availability: Distance to power grids and water sources (necessary for cooling) can impact costs;

Local regulations: the cost of complying with building and environmental regulations can increase costs;

2 **Size and scale**

Construction costs are measured by square foot (or metre), with larger data centres necessarily increasing the cost;

3 **Security and compliance**

Jurisdictional variances in industry standards and regulations (and the necessity to comply with these) can increase costs. The scale of physical security, surveillance systems and access control that are required also impact this.

4 **Energy efficiency**

Energy efficient technology, whilst reducing longer term operating costs, can increase initial construction costs.

5 **IT infrastructure**

The specification of the required IT equipment is another key component to overall costs, high-end servers and specialised hardware will increase construction costs.

A closer look at operating costs

With operating costs we see a similar variance, with costs ranging from $10 million to $25 million per annum[3]. Here the key factors driving the variance are:

1 **Energy consumption**

Unsurprisingly this features very heavily in the factors to be considered. The amount of energy needed for things like cooling will vary depending on the region and variance of outside temperatures, as well as on the energy costs.

2 **Maintenance and repairs**

Regular maintenance can be anticipated at the outset, which will increase as the data centres ages. However unexpected maintenance may arise and the higher the initial specification of the IT equipment, the more costly repairs will be. Labour costs, especially for out-of-hours repairs also significantly impact costs.

3 **Staffing**

Data centres need to be operated by skilled personnel, and labour costs will vary depending on location and level of expertise required. Physical security measures (such as security personnel) will also impact operating costs.

4 **Software and licensing**

Licensing fees for software will vary depending on the software utilised. Any updates and upgrades to software over time will also feature in operating costs.

5 **Facility costs**

Insurance premiums for data centres can be a significant part of the operating costs, with certain types of data centre and locations seeing very high premiums.

[3] https://encoradvisors.com/data-center-cost/

Key risks facing data centres

The construction and operation of a data centre is only one side of financing piece. Ultimately, whether you are running a business or working from home, the resiliency of the data centre hosting your operations will be critical. This is where the concept of data resiliency comes in: the ability to predict, prepare for and survive key threats. Without data resilience the data centre becomes a redundant shell with very expensive equipment inside it.

The types of risks data centres may face can broadly be divided into three categories: External, internal and digital.

External risks

The defining feature of an external risk is one that is outside of the control of the data centre itself.

Natural disasters (earthquakes, storms, floods and fires), civil unrest, extreme high or low temperatures and supplier outages are some examples of external risks.

Risk type	Impact	Mitigant
Power	Natural disasters will likely cause a power outage, but there can be other disruptions to power. Loss of power would bring the data centre to standstill.	Multiple power sources, including back-up generators.
Water	There are two key risks here: 1 Given the vast electrical nature of data centres, even the slightest ingress of water can cause malfunction. 2 Water is also critical for cooling, and loss thereof can lead to overheating and malfunction.	1 Building design to protect against water ingress; 2 Access to multiple water sources for cooling.
Climate	Data centres need to maintain a constant temperature, without humidity and without swings in temperature.	High-quality and reliable air conditioning systems, with back-up systems in place.
Structure	The structure of the building is the first line of defence against natural disasters and also human threats (like civil unrest).	The location of the data centre will necessitate use of materials that provide resilience against these threats.
Fire	External fires (even if prevented from spreading to the inside) can cause damage (through raising the outside air temperature, preventing employees from reaching the data centre, ingress of pollutants and damaging power or other critical supplies).	Back-up cooling and power systems and efficient disaster back-up plans.
Civil unrest and physical security breaches	Civil unrest can impact not only the structure of the building but also the ability (and willingness) of staff to attend the data centre.	As far as possible only locating data centres in areas where civil unrest is less likely.

Risk type	Impact	Mitigant
	Physical security breaches lead to loss of data.	Creating perimeter areas beyond the data centre to allow safe entry/exit for staff. Appropriate physical security measures and screening.
Environmental impact	Pollution, chemical spills, poor air quality can impact both staff and the cost of operating the facility. It can, in extreme cases, impact the operation itself.	Only mitigant is to choose locations with lower environmental contaminants.

Internal risks

Internal risks are ones that (should) be more within the control of the data centre operator (although a lot of the external risks can in turn create an internal risk so there is no bright line between the two sets of risks).

Risk type	Impact	Mitigant
Human	Human error and sabotage are the most likely sources for this type of risk.	Properly screened and trained staff, with appropriate controls in place.
Fire	Internal fires can be caused by any number of ignition sources.	Fire suppressant systems and adequate risk assessment for fires. Staff training (on fire prevention and suppression).
Staff safety	These will include anything that puts staff safety at risk, in including: tripping hazards, electrical hazards, risks associated with heavy equipment, working at elevated platforms, accessing overhead equipment, poor air quality, temperature fluctuations, exposure to hazardous materials, malfunctioning fire suppression systems, inadequate emergency evacuation plans. Failure to adequately protect staff may lead to a higher attrition rate and can increase risk of human error.	Staff training, risk assessments and adequate controls.

Digital risks

This is perhaps the key risk that springs to mind, as it encompasses threats from cyber-attacks. However these are not the only ways in which digital risks present themselves.

Risk type	Impact	Mitigant
Viruses	This can cause loss of data, ransom demands and corruption of data.	Various lines of defence need to be in place: 1 Training: to increase awareness of potential threats and ensure staff do not introduce viruses or open door to cyber-attacks; 2 Software: anti-virus and similar software to screen for and negate threats; 3 Education: staying up to date with potential threats and possible mitigants.
Data backup and storage	Given the variety of potential risks data centres face, it is impossible to remove these entirely. Recovering data after downtime is crucial for business continuity.	Timely back-up of data with minimum recovery time.
Software	This is likely third-party operated so not entirely within the control of the data centre.	Understanding best practices, bug-fixes and deployment of updates.
Communication networks	Like power these can fail due to a number of reasons.	Back-up / multiple network connectivity with automatic switchover to reduce downtime.
Shared servers	The use of cloud-technology and shared servers means there is a potential for cross-contamination of cyber-attacks/viruses.	Ensuring effective isolation of accounts hosted on same server.

Taking stock

There are at least 5 different headline types of data centre, each of which will face differing degrees of at least 14 types of risk. Location of the data centre is perhaps still the most significant variable in this, dictating material costs, labour costs, planning and building regulation compliance costs and the extent of external risks they are likely to face.

For example, Florida experienced 34 billion-dollar related natural disasters in the 5-year period from 2020-2024[4]. California, by contrast, experienced 8 such natural disasters during the same period. So even before we consider the type of data centre, there are already inherent differences between build and operational costs for data centres located in those two regions. The solution doesn't lie in relocating all data centres to regions with lower costs and/or lower risks as proximity is crucial to minimise latency and allow fast data transfer. Location is everything – both in terms of costs and also in terms of performance.

For now (at least until such time as we can utilise space data centres) we will continue to need to build and operate data centres in a variety of locations, in a variety of sizes and with their own unique hierarchy and concentration of risk factors. These data centres will continue to require both up front funding for construction and also funding for operational costs and any funding will have to be sensitive enough to anticipate and manage the inherent risks. They also, crucially, have to anticipate and adapt to evolving environmental regulation which may increase costs or ultimately increase the risk of redundancy.

What does any of this have to do with securitisation?

Quite simply, everything. If there is no single type of data centre, and no single quantification of risk then there can be no singular solution to the funding requirement – funding ultimately exists because investors are willing to accept a level of risk to achieve a potential return. And those investors are not homogenous. Whilst project finance may be the traditional route to financing (data centres are, at least in the construction phase, very similar to other project-finance assets), securitisation can offer a diversified investor base which may ultimately result in lower-cost capital.

[4] https://www.ncei.noaa.gov/access/billions/state-summary/FL

CMBS, ABS or project finance

The first data centre securitisation was executed in the US in 2018, but the first European transaction was 6 years further down the line. During that period the US market saw over $21 billion of issuance[5]. The growth in data centre securitisation is in part a function of the rating agencies. At the outset we saw wholesale securitisation, with key tenants, on long-term contracts, at their centre. This was, and remains, a relatively low-risk structure. But over time, as the agencies have become more accustomed and comfortable with the asset, retail and colocated transactions have emerged.

Data centre securitisations, at least in the US, may seem to be well established but the issuance total somewhat masks the differences in ratings approach.

S&P, for example, uses one of four main analytical approaches when rating data centre transactions: ABS, CMBS, corporate/REIT, or project finance[6]. Fitch ratings uses the business risk profile, debt structure finance and exposure to completion and construction risks to evaluate whether the transaction should be rated under its Infrastructure and Project Finance Rating Criteria, Corporates or Structured Finance rules.

It should perhaps come as no surprise that rating agencies, much like the asset they are assessing, do not share a common structure.

Taking S&P as an example again, if the issuing entity is also the operator of the data centre, that lends itself to using the corporate criteria. An SPV ring-fenced style structure will lean towards using the CMBS or ABS criteria. However, if there is unmitigated construction risk, the project finance criteria will come into play. Using the project finance criteria will also though bring into play an assessment of the refinancing risk. This is in contrast to the structured finance criteria, where refinancing risk isn't part of the assessment.

In an ideal world the variety of rating approaches would mirror the variety of data centres. What we find in practice though is a 'best fit' approach is utilised.

Does this matter?

Depending on which criteria are used, certain features or risks will be given a greater or lesser weighting. That is inherent in the very nature of a rating methodology: it takes certain features and applies assumptions to them to create a risk framework, which may or may not be mitigated by certain other features. If too much focus is placed on the wrong risks or features, it distorts the end product - the rating. It is a bit like those toy sorters that toddlers are a fan of: if the shape (the type of data centre) isn't a perfect fit for the slot we are trying to force it into we will ultimately have to accept an imperfect fit, or worse still, 'cut' the shape to make it fit. Either that or we become frustrated and lose interest.

Therein, perhaps, lies the concern. The data centre market is likely to require anywhere between $3.7 trillion and $7.9 trillion of funding over the next 5 years[7]. That funding ultimately comes from investors and they in turn need a clear understanding of the risk profile of the investment they are acquiring if they are to invest in meaningful volumes. It is difficult to assess how investors approach data centre transactions, these criteria are commercially sensitive, but those that do publish information on this[8] stress the importance of a thorough assessment of the transaction, the underlying assets and deal structures that not only go beyond the ratings provided by the agencies but also include factors not considered by the rating agencies.

Are we ready to think outside the box?

Unless investors are willing look beyond the label (be it ABS, CMBS or any other label) we may ultimately see the market for data centre financing becoming

[5] Research Report
[6] https://www.spglobal.com/ratings/en/research/articles/240613-the-four-main-approaches-for-rating-data-center-financings-13135603#:~:text=When%20rating%20transactions%20or%20companies,most%20notably%20the%20financing%20vehicle.

[7] The cost of compute power: A $7 trillion race | McKinsey
[8] See for example: https://www.troweprice.com/financial-intermediary/uk/en/thinking/articles/2024/q3/ai-and-fixed-income-booming-demand-for-data-center-abs-and-cmbs.html

constrained. To reach even the conservative target of $3.7 trillion of funding by 2030 we will need all the investors: the project finance investors, the ABS, the CMBS, the esoterics – the ABS market alone cannot possibly absorb the funding need alone. Yet to date approximately 74% of issuance is in the ABS market, with only 26% in the CMBS market.

That is even before we take into consideration financing the AI build out. This hasn't really started yet, but the ratings do not properly account for this nuanced asset class. One key difference is that AI data centres may include weaker tenants (in the sense of start-ups without credit histories or proven business model). Size wise they will be more akin to hyperscale data centres, but if the key tenant is a start-up that's a very different risk profile to the wholesale hyperscale transactions that we saw at the start. To date the ABS data centre transactions have been typically structured as master trusts, with the ability to add collateral over time. The CMBS transactions typically follow a SASB structure, with the collateral pool fixed at the outset. AI transactions at first blush lend themselves to an SASB structure but with the weaker credit quality of the tenant may need to be pooled in a master trust structure to spread the risk.

The data centre shape is already an imperfect fit for the 'slot' defined by the rating agency criteria, and this is only going to increase as the AI build out ramps up. There is much scope for creative financing here and we would be delighted to discuss these further.

In the meantime, take a look at our article '*Are we forgetting the 'Y' in AI*?' for an in depth look at AI in financial services.

EMEA Contacts

Christian Lambie
Partner
Tel +44 (20) 7444 5139
christian.lambie@nortonrosefulbright.com

David Shearer
Partner
+44 (20) 74442215
david.shearer@nortonrosefulbright.com

London
Farmida Bi
Partner
Tel +44 (20) 7444 5842
farmida.bi@nortonrosefulbright.com

Nigel Dickinson
Partner
Tel +44 (20) 7444 5714
nigel.dickinson@nortonrosefulbright.com

Kirstin Russell
Partner
Tel +44 (20) 7444 3505
kirstin.russell@nortonrosefulbright.com

Jennie Dorsaint
Partner
Tel +44 (20) 7444 3095
jennie.dorsaint@nortonrosefulbright.com

Yusuf Battiwala
Partner
Tel +44 (20) 7444 2696
yusuf.battiwala@nortonrosefulbright.com

James Kent
Partner
Tel +44 (20) 7444 5104
james.kent@nortonrosefulbright.com

Andrea Salsi
Counsel
Tel +44 (20) 7444 2235
andrea.salsi@nortonrosefulbright.com

Mirella Hart
Knowledge Of Counsel
+44 (20) 74445875
mirella.hart@nortonrosefulbright.com

Amsterdam
Omar Salah
Partner
Tel +31 (20) 4629482
omar.salah@nortonrosefulbright.com

Joris Ravelli
Partner
Tel +31 (20) 4629405
joris.ravelli@nortonrosefulbright.com

Dubai
Hamed Afzal
Partner
Tel +971 (4) 3696324
hamed.afzal@nortonrosefulbright.com

Frankfurt
Oliver Sutter
Partner
Tel +49 (69) 505096223
oliver.sutter@nortonrosefulbright.com

Hamburg
Veit Sahlfeld
Partner
Tel +49 (40) 970799192
veit.sahlfeld@nortonrosefulbright.com

Luxemburg
Stéphane Braun
Partner
Tel +352 (28) 5739210
stephane.braun@nortonrosefulbright.com

Paris
Jeremy Grant
Partner
Tel: +33 (1) 56595090
jeremy.grant@nortonrosefulbright.com

Athens
Yianni Cheilas
Partner
Tel +30 (21) 09475345
yianni.cheilas@nortonrosefulbright.com

Warsaw
Piotr Zawislak
Consultant
Tel +48 887 087 001
piotr.zawislak@nortonrosefulbright.com

Milan
Nunzio Bicchieri
Partner
Tel +39 02 8635 9412
nunzio.bicchieri@nortonrosefulbright.com

Singapore
Colin Rice
Partner
Tel +65 63095421
colin.rice@nortonrosefulbright.com

NORTON ROSE FULBRIGHT

Norton Rose Fulbright provides a full scope of legal services to the world's preeminent corporations and financial institutions. The global law firm has more than 3,000 lawyers advising clients across more than 50 locations worldwide, including Houston, New York, London, Toronto, Mexico City, Hong Kong, Sydney and Johannesburg, covering the United States, Europe, Canada, Latin America, Asia, Australia, Africa and the Middle East.

nortonrosefulbright.com