quocirca

Business and IT Analysis

Data Centre Co-location: An easy decision; a difficult choice

For many organisations, co-location is the logical way forward for hosting, securing and connecting the IT infrastructure. However not all co-location providers are the same, and it is often the subtle differentiators that can make the difference between a successful or a stressful partnership.

February 2014

Differentiating one co-location provider from another can be a challenge. They all promise much the same service and it is tempting to select the one offering the lowest cost. However this choice can be catastrophic for the business, resulting in low system availability and ongoing arguments over problems that should not have occurred in the first place. Not all co-location providers are the same – when selecting a co-location provider you are engaging with one of your business' most important on-going partners and the correct choice is critical.

This paper provides guidelines for those both within IT and within the business who are looking to move to a co-location facility and who want to make sure that their selection procedures cover all the criteria required to make the appropriate choice.

Clive Longbottom
Quocirca Ltd
Tel : +44 118 948 3360
Email: Clive.Longbottom@Quocirca.com

Bernt Ostergaard
Quocirca Ltd
Tel: +45 45 50 51 00
Email: Bernt.Ostergaard@Quocirca.com

Datum BUSINESS CRITICAL DATA CENTRES

Copyright Quocirca © 2014

quocirca

Contents

Section	Topic	Page
Executive Summary	Data Centre Co-location – An easy decision; a difficult choice	3
Introduction	Co-location considerations	4
	A long term partnership	4
	The whole package	4
	Service management	5
	Physical location	7
	Value-added ecosystem	7
The Differentiators	Differentiating your co-location partner The Differentiation Checklist	8
Conclusion	Business Impact	11
Appendix	Basics for Data Centre Provision	12

© Quocirca 2014

Data Centre Co-location: An easy decision; a difficult choice

For many organisations, co-location is the logical way forward for hosting, securing and connecting the IT infrastructure. However not all co-location providers are the same, and it is often the subtle differentiators that can make the difference between a successful or a stressful partnership.

Co-location is not just about the facility	If the choice of co-location provider was solely down to the facility, life would be simpler. As it is, the relationship between your organisation and the co-location provider will be critical in ensuring that the total package - including the facility, the technology, the operations and client service - fully supports your business. Getting the choice wrong is not just a minor problem: this is a long term commitment with far-reaching consequences.
The location of the facility is a core concern for security and resilience	Whilst a data centre facility may be secure, consider the external environment. Look for a location that offers additional multiple layers of security within the larger area outside the facility - and opt for a controlled and secure environment. This ensures utility feeds and other services will be planned and fully mapped over a wide area, and avoids service interruptions through accidental damage such as ground works by external contractors.
Both sides have to work on the trust relationship	It may seem hackneyed, but a co-location relationship has to be built on trust. Ensure that your chosen partner has the levels of service management and support that your business requires. Look for named service management staff to be assigned to you; make sure that interactions will be regular and meaningful and check that the co-location provider's team will provide advice and rapid support when you need it.
The contract must not be one-way	If the provider tries to insist that you sign a standard contract, walk away. Your needs will be individual and your contract should reflect this. Look for flexibility in approach; look for a contract that works towards fully supporting your organisation. Don't look to write in harsh penalties where operational problems occur – instead, include clauses that aim to avoid such problems in the first place.
Any agreement has to be viewed as long term	Bear in mind that once you are up and running in one facility, it is not that simple to move equipment to another. Any move will require business workloads to be switched off while the IT equipment is transported, or a parallel system to be built in a new facility with new equipment. Neither option will be painless – the best option is to select the right co-location provider in the first place.
The wrong decision can be career limiting	Without over-dramatising, if a business identifies problems with the data centre, first in line for blame will be the IT team; second is likely to be all those who made decisions that put in place a poorly-performing platform. Even if blame is finally attributed to the provider, a residual feeling of failure will remain with the people who made the choice. Ensuring that you have carried out due diligence could ensure that you safeguard your job.
The implications of ownership	Not all co-location providers own the facility which means you may be signing a contract with an intermediary who has no control over how the facility is managed or the strategy for its future. If things go wrong, the in-house data centre staff may have no knowledge of you, your business or your priorities – and you won't know them.

Conclusions

The decision to move from in-house to a co-location facility should not be a difficult one. Increasing compute power demands additional complexity, cost, capacity flexibility and scalability that do not in general warrant the risk and effort required to build and subsequently maintain an in-house facility. However it is not advisable to rush the selection of co-location provider without full due diligence to ensure you understand exactly what is involved. Cost should be low on the list. Choosing a cheap provider for the wrong reasons could be ruinously expensive and business-limiting in the long term, whereas choosing the right one should turn out to be highly cost-effective and an enabler for business growth. The key to success lies in the ability to build a trusted relationship with a co-location provider who will work with you to support your business, now and in the future.

© Quocirca 2014

Co-location considerations

The arguments for moving to a co-location facility are getting stronger as the demands on the IT infrastructure increase. The up-front costs of building a new private data centre can be prohibitive, not to mention the increasing costs of maintaining it to meet the changing needs of the business and new technical architectures. However, making the right choice of co-location partner can mean the difference between a highly successful business – and its failure.

A long term partnership

Due diligence upfront is key to fully understanding what the co-location provider has to offer your business

Although in theory you can move your equipment if you are unhappy with your provider, in practice it is not that simple and the initial decision has long-term implications. Many co-location providers promise much, but deliver little - problems often only come to the fore after the decision is made and your IT platform is installed. As with any ongoing partnership, it is vital to take time to truly understand what is behind the promises and the impact that could have for the future. Due diligence is crucial to ensure that the selected provider will meet all the requirements that your business will need from the facility and the platform within it, not forgetting the support that the provider will extend so that you have the information and assistance you need to put things right if a problem arises.

Co-location can only really deliver on its promise when the contact points between the two parties are completely seamless and a trusted relationship can be established. By asking the right questions up-front of a proposed co-location provider, the possible level of relationship can be gauged – and if you do not believe that it will be seamless, walk away. Where great technology and a trusted relationship meet, the business has a stronger and better technology foundation, and discussions with the technologists will be more business-centric. All of which means that the business can make more effective decisions and can use the IT platform to support the business in its long-term strategy.

For successful co-location, consider what happens now and in the future – both when times are good and when things might go wrong.

To put it simply, moving to the wrong co-location provider could damage your business.

To put it simply, moving to the wrong co-location provider could damage your business. This is not just a technical issue. The total platform of the IT equipment, the facility and the way that it is managed is the bedrock of modern business operations. For all the reasons why it makes more business sense to outsource your data centre, it also makes sense to ensure the co-location provider is the right partner to support your business. The wrong co-location provider can make this bedrock more like sand; no matter how well you architect your IT equipment, no matter how good your systems management software, no matter how fast and intuitive your applications, the wrong choice can undermine your organisation's ability to carry out its business.

The importance of the whole package

It is far too common across many sales cycles that the quality of pre-sales is several orders of magnitude better than the post-sales support. All the effort seems to go into selling to you and savings are made once the seller has you in their clutches. Given the long term nature of the partnership it is far better to deal with a co-location provider willing to 'open up the kimono' to allow you to interact with its full team of sales people, service management teams and technical staff so that you can see the whole apparatus, not just the glossy sales front end. For example, areas such as promises of high availability through the use of 'N+1' or greater equipment redundancy must be checked – ask to see the actual equipment and the underlying design of the data centre.

© Quocirca 2014

Indeed, some co-location providers may be slightly economical with the truth. 'White labelling' is relatively common – an owner of a very large facility needs to gain greater occupancy levels, but cannot find enough small clients to achieve this. It hives off parts of its facility to a third party, who can then rent out smaller areas to its own clients, leading to a three tier system of facility owner, 3rd party sales engine and you, the potential client. The fact that the sales engine representative can take you into a building and show you around does not mean that they are the facility owners. You may find yourself signing a contract with an intermediary; someone who does not actually have any control over how the facility itself is being managed – or over the strategy for the facility's future. Imagine the issues that can arise if a problem occurs. There are additional links in the chain, and no-one in the data centre itself knows, or cares, who you are. More opportunities for finger-pointing as one group blames another while the root cause is not addressed effectively. The sales engine has little actual interest in you as a true client – they just want your monthly revenues so that they can pay some of it to the true facility owner and cream off their margin. Meanwhile, your organisation is going out of business.

Knowing who you will be dealing after the contract has been signed – and that they know who you are – will help to ensure you get the support you need, when you need it.

The role of Service Management

A direct relationship between your organisation and those responsible for identifying and rectifying problems within the facility is essential. This requires a strong service management team and a good ongoing working relationship. Trust is imperative; without it, there will always be the worry of what happens should something go wrong as only when things go wrong will the relationship will be truly tested. You have to know that the provider's teams and your teams will work together effectively to deal with any issues to support your organisation, both now and into the future.

For effective service management, ensure that prospective providers can meet the following seven criteria:

Named service manager	Ensure that will you be dealing with the same person or persons on an ongoing basis. Providers who attempt to minimise costs through employee utilisation may use a group telephone number, dealing with clients on a first come, first served basis. If there is a major issue, it could take a long time to deal with your call – and all the time, your business is being impacted. With poor service management, you will have little information on what is happening, and little capability to feed back into your business on when normal service will be resumed. Who will the business blame for this? Not the provider – you will be held responsible for the lack of information and your poor choice of partner.
Frequency of interaction	Ensure that you are not going to be making all the running and that there is a schedule of regular calls. Define 'regular' according to your needs – you may want this to be weekly, monthly or even quarterly. Define what will be covered, and who should be included to set expectations upfront. If the interactions reduce to a couple of minutes' call with no real depth, it is time to review the frequency and reset expectations of what needs discussing. Such empty interactions are not helping you or your business.
Information flows	If someone else has to be brought into any discussion, ensure that the service manager will fully brief that person to avoid duplicating conversations. This saves time and ensures that one person is the central point of control, able to see the complete picture and take action. Fragmented discussions lead to fragmented support – the nominal fixing of a single issue could have a knock-on effect to other areas. Only someone with full visibility of what is going on can ensure that a 'fix' is a real solution to get your organisation back up and working on a solid platform. The service manager should also keep a complete and traceable log of discussions so that trends and event occurrences can be easily spotted and fixed.

© Quocirca 2014

Speed of response	There are two aspects to how fast you can expect a response to any issue. One is the large stick of the service level agreement (SLA): if the defined response time is not met, a formal complaint can be raised. However, this is shutting the stable door after the horse has bolted – your organisation will have been impacted with potential financial or reputational costs. The better approach is to ensure that the provider has a clear track record of employing people eager to fix problems. Ask what tools they have at their disposal to foresee issues in order to deal with them before any impact so that you are provided with high levels of service continuity, rather than rapid disaster recovery. Dealing with a provider who focuses on avoiding major issues is more valuable than one adept at dealing with major interruptions on a regular basis.
Disaster planning	When there is a more major failure, ensure that the provider has adequate plans in place to get everything working within timescales beyond any agreed terms in the SLA. The service manager must go through exactly how the facility is provisioned to deal with outages. They should also listen to you as you may see something additional or perhaps require something beyond what is currently there. A good service manager will work with you to put in place what you need or come to an agreed solution that works for all. Every minute that your IT platform is down is a minute closer to your organisation going out of business - disaster recovery and business continuity are two main considerations. Don't settle for weasel words and obfuscation: make sure that you and your organisation are happy with the responses given and that you fully understand what risk is being placed where.
Amount of advisory information provided	Both during and outside of regular planned interactions, the service manager should provide useful information such as proposed changes to the facility and what they mean to you and your business. It should also include advice on how best to architect and provision your IT equipment to ensure the most effective platform. For example, the use of specific racks with well-planned equipment levels can result in energy savings that not only help your organisation be greener but also ensure that you are a 'good citizen' within the overall data centre, helping everyone to maintain an efficient and effective platform. If changes take place without notice, there could be conflict between available resources and your plans or resource requirements - perhaps for a given workload or activity. With foreknowledge and discussion, the provider should be able to help through enabling other resources during the period of the change to avoid downtime and provide business continuity.
Reporting	You need to ensure you will receive meaningful reports with information to help you plan and manage physical and intellectual property risks. As an example, good reporting can ensure that service levels and resources will not be exceeded next quarter due to expected growth of your organisation's current workloads. With energy costs a significant area of concern, you should be able to work with the provider to identify better ways of deploying equipment to reduce energy consumption, or to simplify wiring or racking to reduce complexity and save costs. At the basic level, full reports of who has been into the facility and has had access to your equipment, tied into your own system logs, can help to identify problems ranging from simple human error through to malicious damage.

© Quocirca 2014

The relevance of physical location and security

A major area to look at is the physical location of the data centre. Ensuring that it is not prone to flooding or other natural disaster is one thing, but even those facilities which seem to pass basic location tests could have issues, particularly when it comes to the bête noir of outsourcing - security.

Although the facility itself may meet basic security requirements, ensure that its location enhances overall security. Some facilities are within larger environments such as controlled business parks under the ownership of a single entity where additional layers of security are available – for example, more CCTV, additional guards, extra checks on people entering and leaving and enhanced physical perimeter security. Such extra layers can provide additional peace of mind relating to the security of your intellectual property, and are hard to put in place for facilities built within existing industrial estates or similar environments. A trading estate has to accept that there will be traffic moving around at all times of the day. Even those with basic security will tend to leave the barrier open at night, relying on the one or two security guards to make their rounds around the estate at regular (often far too scheduled) intervals to pick up on any out-of-the-ordinary activities going on. Compare this to a dedicated environment with full 24x7 security – not just for the co-location facility, but for the rest of the environment around it.

Additionally, highly controlled areas will have better overall management. Industrial estates may have grown over a period of time and involve multiple different developers and owners. The position of key utilities may not be well laid out, and plans may have them showing in the wrong places as work has been carried out over the years. It is highly unlikely that any one group will have the complete plans showing exactly where everything is – and the public roads may be dug up by any one of multiple utility companies or contractors at any time risking the disturbance of key services to the data centre facility. An environment that is fully owned and managed by a single entity using proven project management skills and teams helps to ensure that such issues do not occur.

A data centre in a controlled environment delivers added peace of mind for the safe-keeping and security of your IT infrastructure.

There are very few facilities that are so located given the logistics of setting everything up complete with a landowner that has the skills and capabilities to operate a highly secure large area environment. One point to look out for is for land which is operated by defence contractors or other government suppliers – the requirements that are placed upon them means that they will have to continually prove their capabilities to maintain their positions as accredited suppliers.

The value-added ecosystem

Data centre ecosystems help businesses connect with other co-located organisations within the facility to grow business or facilitate the journey to hybrid cloud. More advanced co-location providers understand their role in enabling IT to support their clients' businesses. By investing in ecosystems that connect their clients, they provide mutually beneficial communities, often centered on key areas such as cloud, finance and media.

If your choice of co-location provider provides such an ecosystem, you can directly connect as an enterprise to IT service providers within the ecosystem, increasing the performance and efficiency of your digital supply chain – and supporting hybrid infrastructure strategies through the ability to trial and flex into cloud services with unrivalled speed and security. As a service provider, you can expand your business by leveraging the community to directly connect with target markets to sell more products and services – and potentially partnering with other co-located providers to develop new solutions.

© Quocirca 2014

Differentiating your co-location partner

So, how do you assure yourself that you are choosing the right partner for your business and its future? All too often, those looking at co-location partners will concentrate purely on the technical aspects. Whilst these are important, it is also vital to understand how the whole facility measures up – and this has to include areas which are easy to overlook.

When selecting your co-location provider, keep in mind the impact of the whole package on your business, now and in the future.

At the basic level, elements that any provider should be able to offer are detailed in the Appendix and should be used for reference if this is your first foray into co-location. For those who already have a deeper understanding of co-location, the following checklist will help you to differentiate between the 'standard' providers, and those who have that extra capability; those areas that can make all the difference between a facility that enables your organisation to be successful now and in the future and one that ends up being a constraint on what the business can do.

The Differentiation Checklist

Quocirca recommends that when looking at the whole package and how it can support your business, you should also ensure that the following fourteen areas are covered in discussions with candidate co-location providers:

Goal Alignment	For long term success, it is important to ensure that the co-location provider supports your goals, particularly around pricing and service levels. Consider a data centre backed by a property company focused on maximising the value of the facility on a landlord-tenant base through the number and duration of leases. Contrast this with a facility owned by a service-based provider where the focus is to maintain service revenues by optimising client satisfaction. A completely different mentality in how clients are acquired and managed over the duration of the contract.
Flexible contracts	Many contracts try to put all the risk on the client. Ensure that the contract does not attempt to tie you in for extended periods of time. The key to a good co-location contract is one that allows for flexibility and ensures that both sides are involved in decision making and future planning. Make sure that you can sit down and write a contract with the provider that works for both sides.
Pricing and long term costs	Price should not be the main reason to enter into a co-location agreement. For many, selecting on price alone has resulted in longer term unexpected business costs when things have gone wrong, revealing that the price may have been low because the provider has cut corners. For others, where business needs have been placed above considerations of price, co-location has often been far more cost-effective than attempting to continue to run an in-house facility.
Enhanced and neutral connectivity	While multiple connections are a necessity, neutrality of connectivity around the choice of carrier and/or cloud provider gives users the most flexibility and competitive terms. As the availability of your IT systems is predicated on the availability of the facility, the ability to use multiple different connectivity providers of your own choosing can ensure that you can manage the contractual details with the connectivity provider under your own terms if necessary.

© Quocirca 2014

Multi-factor security	With any facility, security has to be a major concern. Ensuring that your organisation's intellectual property is adequately secured means that granularity of security at multiple levels has to be present, along with full auditing and reporting of activity. While use of identity checking provides a first line of defence, use of multi-level authentication and transit security helps to ensure that only those who should be doing something can do that something. Biometric tracking and active near field communication (NFC) or radio frequency identification (RFID) tags combined with CCTV can provide an auditable set of events showing who was where, when.
Accreditations	Independently awarded accreditations provide you with assurances that best-practice approaches have been adhered to. For example, ISO 27001 denotes processes to meet certain security requirements while Visa processing accreditation PCI DSS supports robust payment card data security. For the protection of confidential information, consider whether the site is additionally approved for UK government protectively marked information and whether the data centre is able to meet government information security standards such as Business Impact Level 3 (BIL3).
A workable ecosystem	More advanced co-location providers understand their role in enabling IT to support the business by investing in ecosystems around key areas such as cloud, finance and media. Promoting availability of co-located service providers not only accelerates their business with new partners and clients, but also enables enterprises to directly connect to a choice of service platforms. The popularity of a hybrid infrastructure strategy is now well established; data centre ecosystems provide greater agility to trial and flex into cloud services via direct connects with unrivalled speed and security.
Management systems	The facility needs to be managed just as much as your own equipment does. Not only should the provider be able to demonstrate adequate visibility of the key elements of its facility (for example monitoring for excess temperature, moisture, smoke, fire) but should also be able to supply information that you can integrate into existing systems management tools to help ensure that your platform is architected and running optimally. Data centre infrastructure management (DCIM) tools are a good way for a co-location provider to monitor and share what is going on within its facility.
Maintenance	A data centre's capability and performance is a snapshot in time. What is now a leading edge facility will be second-tier in just a short time. New approaches to energy supply and management means that the entire facility must be maintained on a regular basis, reviewing existing equipment for its continued fitness for purpose. Consider whether the operations team strive to always maintain 100% uptime as standard; and whether equipment maintenance and replacement schedules are adhered to in order to minimise the risk of any failure at key times.
Supported power densities	Recent US research[1] shows that average energy per rack within a data centre has increased from 7.9kW to 8.5kW. Increasing equipment densities means that many are already running at above 10kW per rack, with extreme density racks pushing 20-30kW. Many existing co-location facilities cannot meet these requirements, meaning that equipment has to be spread out across multiple racks across a larger area. Check to ensure that there will be sufficient headroom to meet higher equipment densities in the future, and that the facility owner has plans in place to stay ahead of equipment power densities through re-fitting new power distribution systems on a regular basis.

[1] "N.American Campos Survey Results 2013", Digital Realty

Sustainability	The same research showed that a single-occupant data centre facility has a power utilisation effectiveness (PUE) rating of around 2.9, that is, for every kW of power used by the IT equipment, another 1.9 will be used by cooling, lighting etc. Many standard co-location facilities have PUEs of around 2.0 and above – yet through more efficiently designed infrastructure in purpose-built data centres, the energy demands of cooling in particular can be reduced below these figures.
Managing space to ensure an optimum environment	Whilst being able to add another rack or row somewhere in the facility is one thing, being able to grow your needs in an optimum way with all your IT equipment provisioned in close proximity for a more effective platform. A good provider should be able to ensure that growth can happen (within reason) in such a manner without the need to buy or lease unwanted space right from the beginning.
Location for performance and governance reasons	Where minimum latency is required, the distance between the facility and the users can introduce unacceptable delays in response times which should be monitored regularly. The physical location and ownership of the facility can also have implications for governance. Ensure that governing laws meet your organisation's governance, risk and compliance (GRC) policy and obligations, and that the facility owner is operating under legal reach that is acceptable to you. For example, if you have worries about the reach of US law enforcement and other agencies via The Patriot Act or FISMA, it makes sense to use a co-location provider that is not owned by a US company.
'Going the extra mile'	A service-based approach to the relationship is critical and sometimes the small details can make all the difference. In addition to the requirements laid out above, the provider should actively work to support you. Consider when third parties deliver new equipment to site. Is there a secure a covered delivery area or will the equipment be left outside? Will the provider dispose or recycle the packaging so that the client does not have to transport and dispose of it themselves? Such services enable a good 'tick mark' to be made against the CSR sustainability statement.

© Quocirca 2014

Conclusions

It should by now be apparent that not all co-location providers are the same. It cannot just come down to money, or to standard features that should be taken for granted. Your due diligence in choosing the right partner has to dig down under the skin of the provider and look for what makes them different; what it is that will help fully support your organisation in the way that it needs; what it is that will provide the flexibility with security needed to propel the business to the next level.

Choosing a co-location facility partner should not be undertaken lightly. Getting it wrong will lead to a raft of problems – poor availability of IT platform, poor performance and lack of flexibility in being able to grow and shrink your needs are just the basic technology issues that can arise.

More important are the direct business impacts – poor overall security can result in threats to your organisation's intellectual property. Not only through technical means of insecure connectivity, but also through insider data theft through unchecked personnel employed by the facility owner as well as other untracked staff from other clients or even from people completely outside the environment. Even where the co-location provider can demonstrate adequate security across the facility itself, the immediate vicinity must also be considered. The more physical security that is in place, the harder it will be for external entities to get anywhere near your systems and your data. A facility built within an existing secure environment will give these multiple layers of physical security – and will easily outstrip any levels of security that could be provided by providers working within an industrial estate, or even an organisation looking to build and run its own facility.

© Quocirca 2014

Appendix 1
The basics for data centre provision

When choosing a data centre – either self-owned or co-location – there are aspects that should be checked to ensure that the basics are covered. Any data centre that cannot meet these basic needs is likely to become a liability to your organisation. The chances of unplanned downtime increase and the capability to diagnose and fix the root cause of problems will be poor, leading to insufficient visibility of what is really happening and an inability to grow (or shrink) your space needs as required.

The impact on the business of using a data centre that does not meet these basics is immeasurable: lack of access to business-critical IT systems, slow user response, haphazard root cause analysis leading to the same problems occurring over and over again.

If the following elements are not covered by any candidate co-location provider, remove them immediately from your candidate list.

Basic location	Is the facility built in a flood plain or other area which could cause the facility to have to be shut down due to external forces? Is it in an area where a major incident outside of the facility could inhibit your staff or the facility owners getting to the facility if required? Many data centres built in major conurbations can even suffer from lack of accessibility during rush hours – try to ensure that accessibility will be easy for your own staff when required.
External security	Is CCTV used effectively? Are anti-crash devices (such as bollards or large flower planters) in place? Is there a secure internal wall between any windows and the main data centre facility itself? An insecure data centre lays your intellectual property open to threat. Your business is built on intellectual property, and physical security should be of high concern.
Entrance security	Is reception manned by professionally trained, fully background-checked security people? Are credentials checked through official photographic proof of identity? Is everyone on the premises photographed and logged in and out? Ensuring that access to your systems is limited to authorised personnel maintains the security of your intellectual property.
Internal security	Are only named people allowed into the data centre itself? Are they prevented from accessing anything but their own organisation's equipment? Is 'tailgating' (two people going through the same door at the same time) prevented or logged via CCTV? It is vital to ensure that only named personnel can enter the data centre and that people dealing with other clients' equipment have no access to your systems.
Energy distribution	Is there sufficient headroom in distribution systems to meet your envisaged power density needs? How would any needs over and above current provision capabilities be dealt with? Ensure that there is sufficient overall energy provision capability from the grid, uninterruptable power supplies (UPSs) and auxiliary generators to maintain the data centre at all times, even if 100% occupancy rates are achieved.
External data connectivity	Which providers are available for network connectivity? Are the main connections provisioned through one set of cables and fibre with a single point of failure, or are they distributed in a multi-directional arrangement? The choice of multiple connectivity providers provisioned through different access points ensures higher levels of availability to your IT platform.

© Quocirca 2014

Cooling	What type of cooling is available? Is it capable of meeting expected equipment densities and heat profiles for the foreseeable future? Is it low-carbon emissive? Full-volume data centre cooling is wasteful and requires large computer room air conditioning (CRAC) systems. Targeted low-energy cooling such as adiabatic or free air cooling can minimise cooling needs, making the data centre's energy costs and carbon emissions lower – benefits that can be passed on to you as the client.
Environmental monitoring	Are aspects such as moisture, temperature and particulates all monitored? What are the trigger points for any intervention actions? What types of intervention will be undertaken? It is far better for a co-location provider to monitor and intervene before equipment shutdown is required. Early-stage monitoring will enable action that will not impact the running of your IT equipment, enabling higher levels of systems availability.
Low impact fire suppression	Even with early-stage monitoring, fires can still occur should there be an electrical malfunction within any item of equipment. Therefore, systems need to be in place to swiftly and effectively deal with such an issue. Targeted zonal systems such as water mist are safe to use and can be immediately replenished.
Wiring	Is structured cabling mandated across the facility? Poor wiring can lead to many problems – for example, crosstalk between data and power cables, the blocking of cooling air flows from wiring in sub-floor spaces, hot spots caused by looped mains cables. The co-location provider should ensure that there is structured cabling within its own space and advise that it is also used within your space.
Auxiliary power	How are auxiliary generators provisioned? It will be difficult to find a data centre that does not have auxiliary generators in place, but the important question is whether they will actually provide the resilience your business demands. To minimise the risk of damaging your business through unplanned downtime, check that the facility's generators are tested regularly and appropriately, that the UPS is truly redundant and that all the auxiliary systems and supplies are properly checked and maintained.
Capability to extend space needed	The majority of co-location data centres are currently running below full capacity. However, this does not necessarily mean that more space will be easily available when needed and, the nearest available space might be at the other end of the facility, or in a different building. If your workloads are highly latency dependent, you may need any new space to be physically adjacent and whilst in some cases it might be possible to plan in the initial allocation, in others it will be down to the flexibility of the co-location provider.
Disaster and recovery planning	Co-location providers with multiple facilities can offer business continuity via mirroring. However, for those with a single facility and where clients choose not to use mirroring, any major impact to the facility may require a disaster recovery (DR) plan. It is important to understand what the co-location provider's DR plan is, and how long it will take to get things back to working order. For example, if extensive flooding or local disruption lead to an inability to directly restore services to the facility, does the provider have agreements with other providers such as infrastructure or platform as a service (I/PaaS) providers to restore systems rapidly?

© Quocirca 2014

About Datum Datacentres Ltd

Datum provides leading-edge carrier and cloud neutral co-location data centres to enterprises and service providers.

As a member of the Attenda IT Services group, delivering always-on availability, robust security and enterprise class service is hard wired into our operations. Our data centres are trusted as secure environments for content, data and business-critical IT to connect with a neutral choice of networks and cloud service providers.

Datum FRN1 has capacity for more than 1,000 co-location racks within a high security campus in Farnborough, which is fast developing as a strategic London-edge data centre hub. The facility incorporates a pressurised free cooling design that delivers enhanced environmental efficiencies and supports high density computing to 30kW per rack as standard. Always on availability is supported by resilience in both design and operations underwritten by a 100% uptime SLA with helpdesk and remote hands services which are available 24x365.

Datum Farnborough Key Features

- Strategic, London-edge, secure campus Location
- Pressurised free air cooling providing Leading-Edge Environmental Efficiency
- SLA backed 100% Power Availability
- Enhanced, Government-grade Security
- Dynamic & Flexible support for High-Density deployments (up to 30kW per rack as standard)
- Carrier & Cloud Neutral
- Comprehensive Accreditations
- Highly Resilient infrastructure design & operations to support business critical IT
- Enterprise Class Service Management including a dedicated Client Service Manager providing our clients with detailed environmental and usage reporting

More details of Datum's co-location offering can be found at www.datum.co.uk

Datum | BUSINESS CRITICAL DATA CENTRES

REPORT NOTE:
This report has been written independently by Quocirca Ltd to provide an overview of the issues facing organisations seeking to maximise the effectiveness of today's dynamic workforce.

The report draws on Quocirca's extensive knowledge of the technology and business arenas, and provides advice on the approach that organisations should take to create a more effective and efficient environment for future

About Quocirca

Quocirca is a primary research and analysis company specialising in the business impact of information technology and communications (ITC). With world-wide, native language reach, Quocirca provides in-depth insights into the views of buyers and influencers in large, mid-sized and small organisations. Its analyst team is made up of real-world practitioners with first-hand experience of ITC delivery who continuously research and track the industry and its real usage in the markets.

Through researching perceptions, Quocirca uncovers the real hurdles to technology adoption – the personal and political aspects of an organisation's environment and the pressures of the need for demonstrable business value in any implementation. This capability to uncover and report back on the end-user perceptions in the market enables Quocirca to provide advice on the realities of technology adoption, not the promises.

Quocirca research is always pragmatic, business orientated and conducted in the context of the bigger picture. ITC has the ability to transform businesses and the processes that drive them, but often fails to do so. Quocirca's mission is to help organisations improve their success rate in process enablement through better levels of understanding and the adoption of the correct technologies at the correct time.

Quocirca has a pro-active primary research programme, regularly surveying users, purchasers and resellers of ITC products and services on emerging, evolving and maturing technologies. Over time, Quocirca has built a picture of long term investment trends, providing invaluable information for the whole of the ITC community.

Quocirca works with global and local providers of ITC products and services to help them deliver on the promise that ITC holds for business. Quocirca's clients include Oracle, IBM, CA, O2, T-Mobile, HP, Xerox, Ricoh and Symantec, along with other large and medium sized vendors, service providers and more specialist firms.

Details of Quocirca's work and the services it offers can be found at http://www.quocirca.com

Disclaimer:
This report has been written independently by Quocirca Ltd. During the preparation of this report, Quocirca may have used a number of sources for the information and views provided. Although Quocirca has attempted wherever possible to validate the information received from each vendor, Quocirca cannot be held responsible for any errors in information received in this manner.

Although Quocirca has taken what steps it can to ensure that the information provided in this report is true and reflects real market conditions, Quocirca cannot take any responsibility for the ultimate reliability of the details presented. Therefore, Quocirca expressly disclaims all warranties and claims as to the validity of the data presented here, including any and all consequential losses incurred by any organisation or individual taking any action based on such data and advice.

All brand and product names are recognised and acknowledged as trademarks or service marks of their respective holders.

quocirca

quocirca

Data Centre Co-location: An easy decision; a difficult choice

For many organisations, co-location is the logical way forward for hosting, securing and connecting the IT infrastructure. However not all co-location providers are the same, and it is often the subtle differentiators that can make the difference between a successful or a stressful partnership.

To request a copy of this paper or for more information, contact Datum Datacentres on 0333 202 3195 ¦info@datum.co.uk
www.datum.co.uk