



Your guide to hosted data centres: How to evaluate potential providers

Finding the right hosted data centre

More than ever, organizations require a secure, reliable and flexible data centre to meet growing business demands. Whether it's performing data analytics in order to stay competitive, or providing customers with streaming video and other rich Internet applications, the success of a business is often defined by how effectively it harnesses processing power.

But as your business needs change, so does the complexity and expense associated with running a data centre in-house. Competitive pressures dictate zero downtime and iron-clad security, and operating a secure and cost-effective on-premises data centre requires deep IT expertise, ongoing infrastructure investments and extensive emergency planning for power outages.

That's why many businesses are now exploring hosted solutions as an alternative. A hosted data centre eliminates the need to invest in infrastructure and can provide a more reliable and cost-effective method of providing the services your business relies on.

But choosing the right data centre requires careful analysis. Every service provider has a different approach to supplying cooling and power, ensuring compliance requirements and guaranteeing their service commitments.

This guide divides the process of assessing a data centre service provider into five key criteria:

- Power
- Scalability of infrastructure and services
- Certification
- Security
- Service level agreements

Each section includes a series of key questions we recommend you ask about the offerings of hosted data centre providers. Answering these questions will help you more fully evaluate potential service providers by gaining insights into their levels of service and support.

Note: this resource is intended to stimulate focused conversations about finding a hosted data centre. For a complete assessment of your needs, or to discuss implementation scenarios, please contact your Bell representative or [contact us to set up a call with a Bell data centre representative](#).



1.0 Is the data centre smart about power?

One of the biggest costs of operating a data centre involves power consumption and cooling requirements. The following sections will help you evaluate how the service provider supplies, allocates and monitors power going to its customers.

1.1 Power allocation

Your service provider's ability to accurately measure and monitor power usage within a data centre can have important consequences for reliability.

Q1. Does the service provider use:

- An over-subscription model
- A power reservation model

A service provider that relies on a single power reading for their entire data centre is probably using an over-subscription model that could put your data at risk. With an over-subscription model, customers are allocated a specific amount of power, but if their actual usage is lower, the data centre has the opportunity to resell this phantom surplus capacity to another customer. Customers do not have an accurate picture of how much power capacity is available to them. When a data centre manages capacity using this method, it raises the risk that spikes in power demand from one customer will rob another of capacity, potentially tripping breakers and taking equipment offline.

With a power reservation model, the service provider provides you with the total capacity for which you have contracted, regardless of actual usage. This ensures that power fluctuations caused by neighbouring servers being turned on and off will not affect the integrity of your data, and offers better uptime and reliability. The ability to accurately measure power usage for each customer cabinet also makes it easy for the service provider to quickly detect any increases in your demand so it can supply more capacity accordingly.


1.2 Tiering

Another method of assessing a service provider's investment in power infrastructure is through Tier ranking. Tiering is a method of certifying the power redundancy safeguards for a given data centre.

Q2. What Tier rating does the service provider offer?

- Tier 1
- Tier 2
- Tier 3
- Tier 4





A Tier 1 facility has almost no redundancy, making it inappropriate for most data centre applications. A Tier 2 data centre typically has a battery room that can only provide a few minutes of reserve power before it switches over to generators. This is sufficient only for a backup recovery site or a similar application.

A Tier 3 data centre is the minimum requirement for critical data needs or for testing and development applications. A Tier 3 data centre provides an N+1 configuration, which means there is one additional generator beyond the required backup capacity. Along with providing additional reserve power, the N+1 configuration of a Tier 3 centre allows for concurrent maintenance to take place on any crucial facility infrastructure with no risk to the overall system.

A Tier 4 data centre provides 2N redundancy, a level of reliability that very few data centre applications currently require.

One of the best ways to think about redundancy requirements is to ask yourself: How much would an outage cost your business on a per-hour or per-minute basis? In terms of availability, a Tier 2 data centre offers 99.741% uptime, compared to a Tier 3 data centre's 99.982%. Although that appears to be a small difference, there are 8760 hours in a year—so this translates into an average of 22.7 hours of annual downtime for a Tier 2 data centre, compared with 1.6 hours for a Tier 3 centre.

1.3 Energy diversification

Along with adequate redundancy and power allocation, it is important to know if your service provider is diversifying its sources of energy. New, greener approaches to power and cooling aren't just good for the earth—they can also be an important consideration for managing energy usage.

Q3. What green energy initiatives has the service provider incorporated?

- Virtualized environments
- Wind power
- Solar
- Free cooling solution
- Heat exchangers that re-circulate data centre heat to the surrounding community

Most of the significant ongoing costs associated with a data centre involve cooling and power. Data centres that take advantage of environmentally sustainable approaches to cooling can be more reliable and cost-effective over the long run.

1.4 Effective power management

Power management is an increasingly important factor in data infrastructure—it might be what convinced your company to consider moving from an in-house to a hosted model in the first place. The most common way to gauge the power efficiency of a potential data centre is through power usage effectiveness (PUE). This refers to the amount of power actually used to operate servers, as opposed to cooling and other energy requirements. PUE is a ratio of the total amount of power used by a computer data centre facility to the power delivered to computing equipment.

Q4. What is the PUE of your service provider?

- More than 2
- 1.5-2
- 1-1.5

A PUE of less than 1.5 means your service provider has taken significant steps to create a green footprint. Creating a lower PUE requires more initial up-front investment on the part of the data centre, but this will generate considerable savings over the long term.

By asking a data centre provider detailed questions about their approach to power allocation, efficiency and redundancy you can ensure that your data storage solution will remain reliable and cost-effective now and in the future.

2.0 Ensuring data centre infrastructure and services are scalable

Since it can be complex and costly to migrate infrastructure and data to another service provider, it's important that your hosted solution be able to adequately provide for both current and future needs.

2.1 Assessing immediate needs

One of the best ways to assess a potential hosted data service provider is to use a staged approach to implementation. By migrating a few servers or applications to start, a company can better ensure that a hosted model will provide the reliability, scalability and security it requires.

The first step in a staged approach is determining which of your applications would be best suited for a hosted environment.

Q5. Which of the following applications are you thinking about hosting in an external data centre?

- Development environment
- Virtualized environment
- Cloud initiatives such as IaaS, email or SaaS
- Networking capabilities and managed solutions

Virtualized environments, cloud initiatives and managed solutions are some of the most popular data centre applications and will demonstrate immediate benefits to your organization. They are also easy to implement—a virtualized environment can often be provided within a week or less.

2.2 Future technology needs

Another crucial factor when determining your hosting requirements is the data centre's ability to adapt to your future business needs and technology requirements.

Q6. Which of the following applications and options can the service provider provide if you decide to upgrade?

- Fully managed virtualized environments
- Cloud services
- Managed network capabilities (switching and firewalls)
- Environment monitoring (intrusion detection and other security services)
- Managed services running atop your servers

While your current needs may only involve connectivity and co-location, for example, you could require more advanced services in one or two years' time. A service provider with a large portfolio of easily configurable capabilities can provide you with the assurance that they will continue meet your organization's needs well into the future.


2.3 Expansion and capacity planning

Your organization's processing needs are likely to change and grow over time, so it's important to ensure you will have access to future space within the data centre.

Q7. What expansion plans does the service provider have in place to address the future space requirements of its customers?

- The service provider follows best practices and starts building a new data centre when current facilities reach 80% capacity
- Service provider has no official plan in place for expansion





Depending on the service provider, you might be able to expand into contiguous space within the same building. Some service providers also offer more than one data centre on the same site or nearby, linked by permanent connectivity, in order to provide backup and disaster recovery options.

In general, it's important to determine how prepared the service provider is to adapt to the future needs of your business. Consider for a moment the extent to which your company's technology plans have evolved over the past five years. In the next five to 10 years, most organizations will face similar or even more rapid technological changes, so you need to have confidence that your data centre service provider will adjust with ongoing developments and continue to meet your needs.

3.0 Safeguarding your data through comprehensive security

The move to a hosted data centre will change how your company addresses the security of critical business data. Hosted data centres are able to share the cost of security among multiple customers, typically this provides a more advanced environment with higher levels of security and reliability than an individual company would be able to cost effectively maintain on its own.

But every organization has its own requirements. In order to ensure compliance and manage your risk profile, you need to fully evaluate how your service provider physically protects their data centre as well as their network and server security.

3.1 Physical security

Preventing unauthorized visitors from entering your data centre is a central security concern that all service providers need to address convincingly.

Q8. What methods of physical security does the data centre provide?

- 24/7 guard on site
- Data centre location is not publicly advertised
- Fencing around the site
- Entrance controlled by swipe card
- Entrance controlled by biometric capabilities and swipe card
- Caged server access by key and lock
- Caged server access by keypad code
- Servers housed in separate cages
- Secure geographic location (i.e., not near train tracks or refineries)

Biometric capabilities and caged servers with keypad codes are a clear indication that your data centre provider has invested heavily in security. Confirming these security measures first-hand through a data centre tour is the best method of verifying various safeguards and guarantees.



3.2 Network security

Along with physical security, your data centre network also needs to demonstrate an equal or greater commitment to network security.

Q9. Does your service provider provide all of the following critical network security features?

- Intrusion detection capability
- Virtualized firewalls and load balancers
- Ability to monitor lines for traffic
- Managed DDOS prevention
- Managed SIEM services

Advanced network security features are essential for maintaining the overall stability and accessibility of your data.

3.3 Cloud security

Depending on your business needs, your company might also benefit from a public or private cloud as part of a hosted data centre solution. You will need to work with your service providerservice provider to establish an approach to security that is appropriate for the type of cloud service you require.

Q10. What type of cloud model are you considering?

- **Public**—A hosted cloud service that provides IT resources for your customers that is accessed through the Internet
- **Private**—A hosted or in-house cloud service limited to particular users within an organization
- **Co-location**—A hosted cloud service that utilizes your company's hardware

With a public cloud, all security implementation is typically handled by the service provider. A hosted private cloud is also handled by the service provider, but with customer input. With a co-location solution, networking and security of the hosted cloud service is the sole responsibility of the customer.

The right service provider will be able to maintain or even improve upon the security of your current in-house data centre. It should also have rigorous physical precautions to keep your data safe.

4.0 Staying compliant when moving to a hosted model

When transferring data and applications to an offsite hosting location, you also transfer some of the compliance risks associated with managing sensitive company information. Since regulatory requirements have increased, it's critical that you have a very clear picture of the standards a data centre maintains.

4.1 Certifications

There are a number of key certifications that every service provider should be able to demonstrate.

Q11. Which certifications does the service provider currently hold?

- Section 5970 Type II (the Canadian equivalent of SAS 70)
- PCI ASV
- Uptime institute (this certifies the Tier rating of a data centre)
- LEED certification

Certifications such as Tier rating and PCI compliance provide a basic starting point for service provider evaluation. Other certifications, such as SAS 70, apply to any company that needs to comply with Sarbanes-Oxley legislation in the United States.

4.2 Recertification

It's also important to know when critical certifications were achieved in order to determine if they were upgraded at recommended intervals or when major regulatory standards were rewritten.

Q12. How often does the service provider recertify their critical standards?

- Annually
- Every five years
- As needed
- Other

A given certification might only mean that the service provider achieved the required standards at a particular moment in time. It's important to confirm that your service provider maintains or upgrades their certifications annually or as needed to keep pace with shifts in industry best practices or emerging government regulations.

A service provider's certifications and the audit reports it provides are the clearest indications you can have as to the security standards of a facility. A service provider that is missing a critical



certification should be viewed with caution. However, in some cases, a service provider that is lacking a particular certification may offer to achieve it if it is important to the customer.

4.3 Canadian compliance issues

Canadian organizations face legal restrictions in regards to where they store and transport their data. Because data can easily cross national borders, the legislation of other countries, like the United States, could also expose organizations to compliance risks.

For example, in Canada, particular types of data—including credit card and banking information—must by law reside within Canada, while the U.S. Patriot Act permits federal agencies to seize equipment and data and hold it for as long as they want in the interests of their national security.

Q13. To what degree does the data centre limit exposure to the U.S. Patriot Act?

- Operates only U.S.-based facilities
- Operates Canadian facilities under U.S. ownership control
- Operates in Canada exclusively, with Canadian employees

When evaluating data centre and hosting solutions, ensure that the service provider can meet your legal obligations and certification requirements so your company remains compliant.

5.0 The fine print: data centre contracts and SLAs

What the data centre promises and what it actually delivers can be two very different things. Before engaging with any service provider, you need to have a clear understanding of the service level agreement (SLA) guarantees that they will provide to you, as the SLA is the clearest indication of how they will deal with downtime and outages. It's important that the SLA you sign offers you sufficient recourse to protect your interests.


5.1 Addressing outages

An outage can cost your business thousands of dollars in lost revenue and damage your reputation with customers. A comprehensive SLA will generally offer you increased protection against downtime and outages.

Q14. How does the service provider's SLA address outages?

- Service level objectives (there is no penalty for the provider)
- Day-based percentage penalties (service provider pays a percentage of monthly bill for every day of outage)
- Hour-based percentage penalties (service provider pays a percentage of monthly bill for every hour of outage)





First, be cautious of a service provider that offers service level objectives without a penalty attached. They are under no legal obligation to reimburse you for an outage, and therefore accept a low amount of risk.

With regards to evaluating the proposed penalties in an SLA, a day-based percentage penalty—provided that it is substantial—generally indicates a service provider with more confidence in their offering, but an hour-based percentage penalty is the best SLA option and indicates a mature data centre service.

In other words, an SLA that will only refund 10 percent of your monthly bill for each *day* of outage demonstrates a lower degree of confidence in the stability of its data centre than a service provider that will reimburse you 70 percent of your monthly bill for each *hour* of outage.

You should also recognize that a service provider creates an SLA in large part to manage its own risk profile, and might not be indicative of its actual capabilities. In order to properly manage your business risk you need to assess a potential service provider's capabilities against their SLA.

5.2 Refunds for equipment failure

A minor equipment failure can have major consequences for your company. For example, a load balancer could fail due to a power surge and knock out access to your servers for hours. That's why it's important to evaluate SLAs in terms of penalties related to equipment failure.

Q15. How does your SLA deal with outages caused by equipment failure?

- Full refund on that month's services
- Refunds based on a percentage of the portion of whatever component fails

An SLA may only commit to refunding the cost or possibly a portion of replacing the component, rather than compensating you for the full value of the services that the malfunction disrupted.


5.3 Consolidating SLAs

If your company or individual departments are already using managed services from one or more service providers for other parts of your IT infrastructure—hosting a corporate intranet, for example, or running a dev/test environment—it might make sense when making the switch to a hosted data centre to also consider consolidating your service agreements.

Q16. Do you currently have contracts for any of the following services?

- Security
- Hosting
- Network
- Wireless
- Other





With multiple contracts, there can be a tendency for service providers to blame one another for a service outage. A single service provider working under a comprehensive SLA will work much faster to restore services knowing it is solely responsible for resolving the issue. Working with a single service provider also provides for one administrator and one sales person for negotiating annual contract renewals.

Get the best hosted data centre for your needs

For many companies, a reliable and high-performance data centre is becoming a central element of their business plans. Working with a hosted provider can help you manage complexity and reduce costs. But to gain the most benefit from a hosted model, you need to make sure your service provider can deliver what they promise for both your current and future needs—through scalability, security and reliable access to your data.

Talk to Bell

At Bell, we are able to help you optimize and consolidate your IT infrastructure to reduce costs, improve flexibility and enhance enterprise resiliency. Whether you have your own infrastructure or are looking to outsource your computing environment to a more scalable and dependable environment, Bell offers a number of solutions, including virtual data centres, managed or co-location hosting.

With new, highly secure, state-of-the-art data centres in the regions of Montréal, Calgary, Vancouver and Toronto, we continue to expand our footprint to offer best-in-class services to thousands of businesses nationwide.

[Learn more about our data centre solutions](#) or [request that a Bell representative contact you about your data centre needs](#)

Recommended Resources

Download these resources to further support your evaluation of data centre service providers and your organization's requirements.

[3 critical factors for successful data risk management – How to reduce risks in-house, in the cloud and anywhere in between](#)

This resource illustrates through real world scenarios how three critical factors determine the effectiveness of your data management strategy, and how moving to a cloud computing model can impact them.





[4 ways a virtualized data centre makes your business agile – The tremendous advantages of hardware, application and management layer virtualization](#)

Find out how virtualization can reduce latency and increase agility across your organization. Download this resource to discover all the possibilities that a fully virtualized environment can provide.

[Webinar: Explore how next generation data centres allow you to be more efficient](#)

Hear from our data centre experts on how you can define a data centre strategy that will achieve the agility, flexibility and business continuity your organization needs. Attend this virtual event to learn how to cope with the cost and complexity of managing data.

[Video series: See inside a state-of-the-art Bell data centre](#)

Get an inside look at the technology behind Bell's state-of-the-art data centre and discover how Bell provides efficient, secure and sustainable solutions for your data hosting needs.

