



# Selecting the Right DRaaS Vendor



Choosing the right DRaaS service provider is almost akin to choosing the right health insurance plan from the plethora of options available to you. A good many CIOs will agree that cherry picking the right DRaaS vendor is the most fundamental part of a well-defined DR strategy.

**Rishikesh Kamat**

There's no dearth of DRaaS vendors in the market each muscling its way to get elbow room into an already crowded market. There's plenty to choose from. If only choices were that easy.

The DRaaS market is maturing steadily, however, challenges prevail in the form of associated complexities in choosing the right fit DR solution for your business. **According to the Gartner report, “Even though substantial market growth and increased provider service maturity have occurred, it is still difficult for many organizations to know whether they are making appropriate decisions or asking all the right questions of prospective DRaaS providers. These providers all offer a wide range of supported server platforms, service onboarding methodologies, recovery time service levels and different pricing policies.”**



**Hence, it is critical to understand how to choose the right DRaaS provider. Here are 6 factors to consider while conducting a smart vendor selection to bolster your DR strategy.**

## **1. BUSINESS AND SECTOR UNDERSTANDING**

---

First things first, you start with a vendor that helps you keep current with the latest steps in DRaaS and also knows the ropes of your business. If your DRaaS service provider has experience in your sector and knows your business processes, systems and applications in and out, he can have a crystal clear vision of your critical business requirements. In fact, it wouldn't be impractical by any stretch of the imagination to state that your external DRaaS provider should know as much about your existing IT infrastructure as the internal IT team.

You need to gauge how informed your provider is when it comes to your sector, business, and industry-specific application ecosystem. The best providers with broad expertise are able to not just spin up an application but also optimize in sync with the prevalent best practices within an industry.

The other reason for an in-depth business understanding on the part of a DRaaS provider is that in the eventuality of a disaster, the business and its DRaaS provider must be in close synchronization before, during and after an event. It ensures that your organization does not jeopardize its ability to return to full operating environment following a disaster.



## 2. GEOGRAPHICAL DIVERSITY

---

Before settling on a vendor you need to gauge if your provider offers the geographic range needed for an effective DRaaS solution. Naturally, most organizations would want their DR to be setup at a different location away from their primary business to avoid localized natural disasters and manmade disturbances. Ideally, you should determine the appropriate level of geographic diversity of your DRaaS provider.

## 3. MULTI-HOMED ARCHITECTURE AND REDUNDANCY

---

You also need to make sure that your vendor supports for multi-homed redundancy. Sometimes a single remote replica of core infrastructure may not be enough. In such cases, you can secure 100 percent business continuity by creating two or more entirely redundant technology deployments.

Any DRaaS solution primarily necessitates the unification of multiple systems, across multiple sites, into a single cloud-based DR platform, making it imperative for your DRaaS vendor to support multi-homed architecture.



## 4. ACCESS TO CARRIER-GRADE DATACENTER GRIDS TO REDUCE LATENCY

---

Latency can be a game killer. It is imperative to ensure that your DRaaS provider runs his own carrier-grade datacenters with seamless access to a superlative grid across geographies interconnected through diverse exchanges and multiple fiber connections. This is crucial in case you are maintaining business continuity for an environment where every millisecond counts. Always check whether your DRaaS vendor can deliver the required response times because experienced service providers with access to datacenter grids can ensure optimal backup and recovery environment with hands-on support to provide complete recovery efficiently as and when it's needed.



## 5. SLAS ARE SACROSANCT

---

Gartner cautions that service-level commitments of providers may vary by configuration size and required computing platforms. Problems may arise due to platform interoperability issues—which may occur when a company wants to move from one service provider to another—in the case of lack of open application programming interfaces or accepted standards in this domain.

If you don't want to face heartburn from wilting expectations from your DRaaS strategy then you must set metrics for the relationship with your DRaaS provider. Make sure the contract and SLA with the vendor specify time, transaction limits of the business continuity. Also, test your DR plan to check for performance and availability. In fact, get references from the existing customers of your DRaaS vendor or peer groups and seek their opinions about the service and support experience.



## 6. EXAMINE CLOSELY AND TEST

---

Finally, it is given that you should closely examine and compare the results of each vendor response, customer references, the robustness of their offerings, and how would they move ahead along with you in creating a dependable disaster recovery plan. Do opt to run a pilot program or get a taste of their full-scale program using select services for fewer systems. Once decided, work closely with your DRaaS provider to articulate and implement the DR strategy, with an apt focus on documentation, training, testing, and recovering to production environments. You should figure whether your provider seamlessly allows you to conduct tests to check the robustness of your plan. Lastly, it is obvious that pricing and payment terms are tactical parameters and shouldn't be the primary guiding star in your quest to select the right DRaaS provider.

Ovum Consulting, in its report *Ovum Decision Matrix: Selecting a Data Availability and Protection Solution for the Cloud Era, 2016-17*, points out, "Cloud computing and the move to an as-a-service delivery method is also beginning to create tensions and splits into organizations' data protection and availability strategies, with questions being raised about location, security, and latency (delay in movement of data through a network.). The issue for CIOs is that these technologies need to be administered and configured correctly to provide solutions to the many different requirements for resiliency that organizations demand." The first step to address such issues is, therefore, to select the right DRaaS partner.

